Cisco UCS Central GUI Configuration Guide, Release 1.0

First Published: November 16, 2012

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

Text Part Number: OL-28305-01

CONTENTS

Preface — Preface xiii

Audience xiii

Conventions xiii

Related Cisco UCS Documentation xv

Documentation Feedback xv

PART I — Introduction 1

CHAPTER 1 — Overview of Cisco UCS Central 3

About Cisco UCS Central 3

Service Registry 4

Identifier Manager 5

Resource Manager 5

Management Controller 5

Policy Manager 6

Policy Resolution 6

Domain Groups 6

Global Concurrency Control 7

Policies 7

Global Policies 8

Pools 9

CHAPTER 2 — Overview of the Cisco UCS Central GUI 11

Overview of Cisco UCS Central GUI 11

Logging into and out of the Cisco UCS Central GUI 12

Logging in to the Cisco UCS Central GUI through HTTP 12

Logging in to the Cisco UCS Central GUI through HTTPS 12

Logging out of the Cisco UCS Central GUI 13
Launching Cisco UCS Manager for a UCS Domain 13
Importing a Policy 14
Configuring Identifier Policies 14
Identifier Policies 14
Configuring an Identifier Policy 14
Determining Where a Pool Is Used 15

PART II System Configuration 17

CHAPTER 3 Configuring Domain Groups 19
Domain Groups 19
Creating a Domain Group 20
Deleting a Domain Group 20
Changing Group Assignment for a Cisco UCS Domain 20

CHAPTER 4 Configuring Communication Services 23
Remote Access Policies 23
Configuring HTTP 23
Configuring an HTTP Remote Access Policy 23
Deleting an HTTP Remote Access Policy 25
Configuring Telnet 25
Configuring a Telnet Remote Access Policy 25
Deleting a Telnet Remote Access Policy 27
Configuring Web Session Limits 27
Configuring a Web Session Limits Remote Access Policy 27
Deleting a Web Session Limits Remote Access Policy 29
Configuring CIM XML 29
Configuring a CIM XML Remote Access Policy 29
Deleting a CIM XML Remote Access Policy 30
Configuring Interfaces Monitoring 31
Configuring an Interfaces Monitoring Remote Access Policy 31
Deleting an Interfaces Monitoring Remote Access Policy 34
SNMP Policies 34
Configuring an SNMP Policy 34

Deleting an SNMP Policy 37
Creating an SNMP Trap 38
Deleting an SNMP Trap 39
Creating an SNMP User 39
Deleting an SNMP User 40

CHAPTER 5 Configuring Authentication 43
Authentication Services 43
Guidelines and Recommendations for Remote Authentication Providers 43
User Attributes in Remote Authentication Providers 44
LDAP Group Rule 45
Configuring LDAP Providers 45
Configuring Properties for LDAP Providers 45
Creating an LDAP Provider 46
Changing the LDAP Group Rule for an LDAP Provider 50
Deleting an LDAP Provider 53
LDAP Group Mapping 53
Creating an LDAP Group Map 54
Deleting an LDAP Group Map 55
Configuring RADIUS Providers 55
Configuring Properties for RADIUS Providers 55
Creating a RADIUS Provider 57
Deleting a RADIUS Provider 59
Configuring TACACS+ Providers 59
Configuring Properties for TACACS+ Providers 59
Creating a TACACS+ Provider 60
Deleting a TACACS+ Provider 62
Configuring Multiple Authentication Systems 63
Multiple Authentication Systems 63
Provider Groups 63
Creating an LDAP Provider Group 64
Deleting an LDAP Provider Group 65
Creating a RADIUS Provider Group 65
Deleting a RADIUS Provider Group 67
Creating a TACACS+ Provider Group 67

Deleting a TACACS+ Provider Group 69
Authentication Domains 69
Creating an Authentication Domain 70
Selecting a Primary Authentication Service 71
Selecting the Console Authentication Service 71
Selecting the Default Authentication Service 74
Role Policy for Remote Users 75
Configuring the Role Policy for Remote Users 76

CHAPTER 6 Configuring Role-Based Access Control 77
Role-Based Access Control 77
User Accounts for Cisco UCS 77
Guidelines for Cisco UCS Usernames 78
Reserved Words: Locally Authenticated User Accounts 79
Guidelines for Cisco UCS Passwords 80
Web Session Limits for User Accounts 80
Configuring User Roles 80
User Roles 80
Default User Roles 81
Reserved Words: User Roles 82
Privileges 82
Creating a User Role 84
Deleting a User Role 85
Adding Privileges to a User Role 85
Removing Privileges from a User Role 86
Configuring Locally Authenticated User Accounts 86
Creating a Locally Authenticated User Account 86
Deleting a Locally Authenticated User Account 90
Changing the Roles Assigned to a Locally Authenticated User Account 90
Enabling the Password Strength Check for Locally Authenticated Users 90
Clearing the Password History for a Locally Authenticated User 91
Enabling a Locally Authenticated User Account 91
Disabling a Locally Authenticated User Account 92
Configuring User Locales 92
User Locales 92

Creating a User Locale 93
Deleting a User Locale 94
Assigning an Organization to a User Locale 95
Deleting an Organization from a User Locale 95
Changing the Locales Assigned to a Locally Authenticated User Account 96
Configuring User Domain Groups 97
Creating a User Domain Group 97
Deleting a User Domain Group 97
Configuring User Organizations 98
User Organizations 98
Creating a User Organization 98
Deleting a User Organization 98
Creating a User Sub-Organization 99
Deleting a User Sub-Organization 99
Configuring Passwords 100
Password Profile for Locally Authenticated Users 100
Configuring the Maximum Number of Password Changes for a Change Interval 101
Configuring a No Change Interval for Passwords 101
Configuring the Password History Count 102
Monitoring User Sessions 102

CHAPTER 7 Configuring DNS Servers 105
DNS Policies 105
Configuring a DNS Policy 105
Deleting a DNS Policy 106
Configuring a DNS Server for a DNS Policy 107
Deleting a DNS Server from a DNS Policy 108

PART III Network Configuration 109

CHAPTER 8 Configuring MAC Pools 111
MAC Pools 111
Creating a MAC Pool 111
Deleting a MAC Pool 112

PART IV Storage Configuration 115

CHAPTER 9 Configuring WWN Pools 117

WWN Pools 117

Creating a WWN Pool 118

Deleting a WWN Pool 119

PART V Server Configuration 121

CHAPTER 10 Configuring Server-Related Pools 123

Configuring IP Pools 123

IP Pools 123

Creating an IP Pool 124

Deleting an IP Pool 125

Configuring IQN Pools 126

IQN Pools 126

Creating an IQN Pool 126

Deleting an IQN Pool 127

Configuring UUID Suffix Pools 128

UUID Suffix Pools 128

Creating a UUID Suffix Pool 128

Deleting a UUID Suffix Pool 129

CHAPTER 11 Managing Power in Cisco UCS 131

Power Policies 131

Configuring Global Power Allocation Equipment Policies 131

Configuring a Global Power Allocation Equipment Policy 131

Deleting a Global Power Allocation Equipment Policy 133

Configuring Power Equipment Policies 133

Configuring a Power Equipment Policy 133

Deleting a Power Equipment Policy 135

PART VI System Management 137

CHAPTER 12 **Managing Time Zones** 139

Date and Time Policies 139

Configuring a Date and Time Policy 139

Deleting a Date and Time Policy 140

Configuring an NTP Server for a Date and Time Policy 141

Configuring Properties for an NTP Server 142

Deleting an NTP Server for a Date and Time Policy 143

CHAPTER 13 **Starting the KVM Console** 145

KVM Console 145

Starting the KVM Console from the KVM Launch Manager 146

Starting the KVM Console from a Server 147

Starting the KVM Console from a Service Profile 147

CHAPTER 14 **Backing Up and Restoring the Configuration** 149

Backup and Restore in Cisco UCS Central 149

Backup Types 150

Considerations and Recommendations for Backup Operations 150

Import Configuration 151

Import Methods 152

System Restore 152

Required User Role for Backup and Import Operations 152

Backup Operations 152

Creating a Backup of Cisco UCS Central 152

Running a Backup Operation for Cisco UCS Central 155

Deleting a Cisco UCS Central Backup Operation 155

Creating a Full-State Backup Policy for Domain Groups 156

Import Operations 157

Creating a Domain Group Config-All Export Policy 157

Creating a Cisco UCS Central Import Operation 158

Creating a Cisco UCS Manager Import Operations 160

Running an Import Operation 161

Deleting Import Operations 162

PART VII System Monitoring 163

CHAPTER 15 Monitoring Inventory 165

Inventory Management 165

Physical Inventory 166

Service Profiles and Templates 166

Configuring Inventory Data Collection Schedule 166

Viewing Inventory Details 166

Viewing Details on an Individual Cisco UCS Domain 168

Viewing Service Profiles 170

Viewing Service Profile Details 171

Viewing Service Profile Templates 172

CHAPTER 16 Configuring Call Home 173

Call Home Policies 173

Configuring a Call Home Policy 173

Deleting a Call Home Policy 178

Configuring a Profile for a Call Home Policy 179

Adding Email Recipients to a Call Home Profile 181

Deleting a Profile for a Call Home Policy 182

Configuring a Policy for a Call Home Policy 182

Deleting a Policy for a Call Home Policy 183

CHAPTER 17 Managing the System Event Log 185

System Event Log Policy 185

System Event Log 185

Configuring a SEL Policy 186

Deleting a SEL Policy 188

CHAPTER 18 Configuring Settings for Faults, Events, and Logs 189

Configuring Global Fault Policies 189

Configuring a Global Fault Debug Policy 189

Deleting a Global Fault Debug Policy 191

Configuring TFTP Core Export Policies 192

Core File Exporter 192
Configuring a TFTP Core Export Debug Policy 192
Deleting a TFTP Core Export Debug Policy 193
Configuring Syslog Policies 194
Configuring a Syslog Console Debug Policy 194
Deleting a Syslog Console Debug Policy 195
Configuring a Syslog Monitor Debug Policy 196
Deleting a Syslog Monitor Debug Policy 198
Configuring a Syslog Remote Destination Debug Policy 198
Deleting a Syslog Remote Destination Debug Policy 200
Configuring a Syslog Source Debug Policy 200
Deleting a Syslog Source Debug Policy 201
Configuring a Syslog LogFile Debug Policy 202
Deleting a Syslog LogFile Debug Policy 203

Preface

This preface includes the following sections:

- Audience, page xiii
- Conventions, page xiii
- Related Cisco UCS Documentation, page xv
- Documentation Feedback, page xv

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

This document uses the following conventions:

Convention	Indication
bold font	Commands, keywords, GUI elements, and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
`courier` font	Terminal sessions and information that the system displays appear in `courier` font.

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

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

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

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

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

Warning IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS

Related Cisco UCS Documentation

Documentation Roadmaps

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

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

Other Documentation Resources

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

The ISO file is updated after every major documentation release.

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

Documentation Feedback

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

PART I

Introduction

- Overview of Cisco UCS Central, page 3
- Overview of the Cisco UCS Central GUI, page 11

CHAPTER 1

Overview of Cisco UCS Central

This chapter includes the following sections:

- About Cisco UCS Central, page 3
- Service Registry, page 4
- Identifier Manager, page 5
- Resource Manager, page 5
- Management Controller, page 5
- Policy Manager, page 6
- Policy Resolution, page 6
- Domain Groups, page 6
- Global Concurrency Control, page 7
- Policies, page 7
- Pools, page 9

About Cisco UCS Central

Cisco Unified Computing System (Cisco UCS) is a next generation platform and solution for data centers. Cisco UCS Manager is embedded device management software that provides a view of a Cisco UCS domain as a single logical, highly-available, and end-to-end management service. Large data centers that include hundreds of deployed Cisco UCS domains must consolidate the device management of those Cisco UCS domains.

Cisco UCS Central delivers a common management solution across all Cisco UCS domains. Cisco UCS Central provides a centralized resource inventory and a repository of policies. Cisco UCS Central simplifies configuration, maintains policy uniformity, resolves contention on global identities, and effectively and consistently manages Cisco UCS domains.

Cisco UCS Central provides a global view of the entire data center through multiple Cisco UCS Manager sessions. Cisco UCS Central can manage Cisco UCS operations for an individual data center or for multiple data centers. Cisco UCS Central facilitates operational management for firmware management, catalog management, configuration backup and restore operations, monitor log, core files, and faults.

Cisco UCS Central is designed for aggregated management functions beyond what Cisco UCS Manager supports today. Cisco UCS Central includes the following features:

- Provides simple and consistent Cisco UCS deployments such as the following:
  - Initial Cisco UCS configuration
  - Policy and service template definitions
- Ensures the uniqueness of namespace such as the following:
  - MAC, WWN, UUID
  - Multiple Cisco UCS search
- Provides inventory management such as the following:
  - Centralized view of physical and logical elements across Cisco UCS domains in a data center
  - Health of individual physical and logical elements
- Simplifies routine operational tasks such as the following:
  - Firmware updates
  - Backup and restore configurations
- Provides centralized diagnostics for the following:
  - Fault aggregation
  - Correlation and impact
  - Root cause analysis

Cisco UCS Central is deployed as a single virtual machine (VM) that resides on an external server. Cisco UCS Central contains the following services:

- Service Registry
- Policy Manager
- Operations Manager
- Resource Manager
- Identifier Manager
- Management Controller

Service Registry

The Service Registry provides a centralized registration repository that stores information from service providers such as Identifier Manager or Operation Manager, and the registered Cisco UCS domains. After a Cisco UCS domain is registered, the Service Registry distributes information about that domain to other service providers and registered Cisco UCS domains. Inter-service communications begin when this information is distributed.

The Service Registry is also responsible for distributing domain group structure changes.

Identifier Manager

Identifier Manager provides automatic and centralized management for UUIDs, MAC addresses, WWNs, IP addresses and IQN addresses across Cisco UCS domains. You can create pools of IDs in both Cisco UCS Manager and Cisco UCS Central, as follows:

- Local pools are defined in Cisco UCS Manager and can only be used in that Cisco UCS domain. These pools are sometimes referred to as domain pools.
- Global pools are defined in Cisco UCS Central and can be shared between Cisco UCS domains that are registered with Cisco UCS Central.

Identifier Manager tracks pool definitions and allows you to manage pools to avoid conflicts. When a domain pool ID is assigned from a Cisco UCS domain that is registered with Cisco UCS Central, Cisco UCS Manager reports the assignment to the Identifier Manager. When domain pools are absent or when domain pools are exhausted, Cisco UCS Manager requests IDs from the Cisco UCS Central global pools.

Conflicting pool assignments are reported as faults. Unallocated IDs that belong to overlapping pools are reported as warnings.

Resource Manager

The Resource Manager provides a centralized and consolidated view of the physical and logical resources across all of the Cisco UCS domains registered with Cisco UCS Central.

When you register a Cisco UCS domain with Cisco UCS Central, the Resource Manager summarizes and displays basic inventory information about the fabric interconnects, chassis, FEXs, blade servers, integrated rack servers, and the service profiles and templates in that domain. The Resource Manager provides a quick view of the available memory, CPU, availability status, and the health status of resources in a Cisco UCS domain. This inventory enables you to use to provision a Cisco UCS domain according to your data center's requirements.

With the Resource Manager, you can cross-launch the Cisco UCS Manager GUI for all Cisco UCS domains registered with Cisco UCS Central and the KVM console to access the servers in a Cisco UCS domain.

The Resource Manager also provides a summarized view of faults from registered Cisco UCS domains. You can view fault information by severity level or by fault types. You can also view additional data center fault information in a single place or cross-launch the Cisco UCS Manager GUI for a Cisco UCS domain to see a detailed contextual view of a particular fault.

Management Controller

The Management Controller is the Cisco UCS Central virtual machine (VM) controller. Configuration operations are performed by the Management Controller. Cisco UCS Central inherits behaviors from the policies that are resolved from the operation-mgr root group. These policies include AAA, HTTP, HTTPS, Telnet, SSH, session limits, Date,Time, DNS, and NTP configurations. The core is also used to carry the operations that are triggered by the Operation Manager, such as backup, export, and import.

The Management Controller also collects technical support information for Cisco UCS Central. This data can be collected from all installed components or only from selected components.

Policy Manager

The Policy Manager is an enhanced web server that you can use to configure all policies, pools, and templates. The organization structure that contains these objects is owned and managed by the policy server. ID pools, templates, and domain groups are also defined in the Policy Manager and then they are selectively distributed to the appropriate services. For example, ID pools are distributed to the Identifier Manager, while domain groups are distributed to the Resource Manager.

Policy Resolution

Policy resolution resolves policy configuration changes on the Policy Manager, which acts as a policy server. When a policy is changed, Cisco UCS Central notifies the registered Cisco UCS domains that use the changed policy immediately.

Domain Groups

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

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

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

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

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

After confirming the registration, if you want to manage all the member domains in a domain group with same operational policies, you can change the policy resolution to global on the Cisco UCS Manager GUI.

Policies configured at the domain group root will apply to all the domain groups under the root. Each domain group under the root group can have policies unique to the group. The domain group policies are resolved hierarchically in the member Cisco UCS domains.

Domain Group Management

Users with the following privileges can create and manage domain groups in Cisco UCS Central:

- **Admin privileges** — Create new domain groups and assign ungrouped Cisco UCS domains to domain groups.
- **Domain group management privileges** — Create and manage domain groups. But cannot assign ungrouped Cisco UCS domains to domain groups.

Global Concurrency Control

Global Concurrency Control allows you to control the number of concurrent operations in Cisco UCS Manager or Cisco UCS Central. You can associate a scheduler to trigger operations on objects that can control parallel tasks. If desired, you can set the scheduler to manually control the resumption of pending tasks. You can also choose to ignore or honor the concurrency limits for user-acknowledged schedules.

Policies

Cisco UCS Central acts as a global policy server for registered Cisco UCS domains. Configuring global Cisco UCS Central policies for remote Cisco UCS domains involves registering domains and assigning registered domains to domain groups. You can define the following global policies in Cisco UCS Central that are resolved by Cisco UCS Manager in a registered Cisco UCS domain:

- Firmware Image Management—Cisco UCS uses firmware obtained from and certified by Cisco to support the endpoints in Cisco UCS domains. Each endpoint is a component in Cisco UCS domains that requires firmware to function. The upgrade order for the endpoints in Cisco UCS domains depends upon the upgrade path, and includes Cisco UCS Manager, I/O modules, fabric interconnects, endpoints physically located on adapters, and endpoints physically located on servers. Cisco delivers all firmware updates to Cisco UCS components in bundles of images. Cisco UCS firmware updates are available for download to fabric interconnects in Cisco UCS domains.
- Host Firmware Package—This policy enables you to specify a set of firmware versions that make up the host firmware package (host firmware pack). The host firmware pack includes the firmware for server and adapter endpoints including adapters, BIOS, board controllers, Fibre Channel adapters, HBA option ROM, and storage controllers.
- Capability Catalog—This policy is a set of tunable parameters, strings, and rules. Cisco UCS Manager uses the catalog to update the display and component configurations such as newly qualified DIMMs and disk drives for servers.
- Fault Collection Policy—The fault collection policy controls the life cycle of a fault inCisco UCS domains, including when faults are cleared, the flapping interval (the length of time between the fault being raised and the condition being cleared), and the retention interval (the length of time a fault is retained in the system).
- Core Files Export Policy—Cisco UCS Manager 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.
- Syslog Policy—A syslog policy is a collection of four policy attributes including console, file, monitor, and remote destination attributes. The syslog policy includes creating, enabling, disabling, and setting attributes.
- Role-Based Access Control (RBAC) and Remote Authentication Policies—RBAC is a method of restricting or authorizing system access for users based on user roles and locales. A role defines the

privileges of a user in the system and the locale defines the organizations (domains) that a user is allowed access. Because users are not directly assigned privileges, management of individual user privileges is simply a matter of assigning the appropriate roles and locales.

- Call Home Policy—Call Home provides an email-based notification for critical system policies. A range of message formats are available for compatibility with pager services or XML-based automated parsing applications. You can use this feature to page a network support engineer, email a Network Operations Center, or use Cisco Smart Call Home services to generate a case with the Technical Assistance Center.
- Management Interface Monitoring Policy—This policy defines how the mgmt0 Ethernet interface on the fabric interconnect should be monitored. If Cisco UCS detects a management interface failure, a failure report is generated. If the configured number of failure reports is reached, the system assumes that the management interface is unavailable and generates a fault.
- Time Zone and NTP Policies—Cisco UCS requires a domain-specific time zone setting and an NTP server to ensure the correct time display in Cisco UCS Manager. If you do not configure both of these settings in Cisco UCS domains, the time does not display correctly.
- Simple Network Management Protocol (SNMP) Policy—SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network.
- Equipment—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), and SEL policy. 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.
- Full State Backup Policy—The full state backup policy allows you to schedule regular full-state backups of a snapshot of the entire system. You can choose whether to configure the full-state backup to occur on a daily, weekly, or bi-weekly basis.
- All Configuration Export Policy—The all configuration backup policy allows you to schedule a regular backup and export of all system and logical configuration settings. This backup does not include passwords for locally authenticated users. You can choose whether to configure the all configuration backup to occur on a daily, weekly, or bi-weekly basis.

Global Policies

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

Configuring global policies involves designating policies as global or local when registering the Cisco UCS domain, and assigning the registered domain to a Cisco UCS Central domain group. Upon assignment, global policies defined in that domain group are inherited by the registered domain assigned to that domain group.

Policies designated as Global in a registered Cisco UCS domain are inherited from Cisco UCS Central by that domain. Policies designated as Local in a Cisco UCS domain are based on local policy settings in that domain.

Pools

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

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

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

CHAPTER 2

Overview of the Cisco UCS Central GUI

This chapter includes the following sections:

- Overview of Cisco UCS Central GUI, page 11
- Logging into and out of the Cisco UCS Central GUI, page 12
- Launching Cisco UCS Manager for a UCS Domain, page 13
- Importing a Policy, page 14
- Configuring Identifier Policies, page 14
- Determining Where a Pool Is Used, page 15

Overview of Cisco UCS Central GUI

The Cisco UCS Central GUI provides a graphical interface to Cisco UCS Central. You can access the GUI from any computer that meets the requirements listed in the *System Requirements* section of the *Release Notes for Cisco UCS Central*.

The Cisco UCS Central GUI contains the following areas and panes:

- The **UCS Faults** area that shows the number of aggregated faults for all Cisco UCS domains registered with Cisco UCS Central.
- A menu bar across the top of the window that provides access to the main categories of information in Cisco UCS Central.
- A **Navigation** pane on the left that provides an expandable tree view of the information available under each menu category.
- A **Work** pane on the right that displays the tabs associated with the node selected in the **Navigation** pane.

The menu bar contains the following items:

- **Equipment**—Provides access to the Cisco UCS Central domain groups, domain group policies, registered Cisco UCS domains, and a fault summary for the Cisco UCS domains.

- **Servers**—Provides access to the service profiles and service profile templates configured in the registered Cisco UCS domains, as well as the global UUID suffix pools configured in Cisco UCS Central.
- **Network**—Provides access to the global IP pools and MAC pools configured in Cisco UCS Central.
- **Storage**—Provides access to the global IQN pools and WWN pools configured in Cisco UCS Central.
- **Operations Management**—Provides access to the following:
  - Firmware images
  - Backup and import files
  - Domain group level policies for backup and export, firmware management, maintenance, and operational features such as communication protocols, SNMP, Call Home, remote user authentication, power allocation, and error logging
- **Administration**—Provides access to the locales and users defined in Cisco UCS Central, a registry of all controllers, providers, and clients in Cisco UCS Central, and diagnostic information such as tech support files, audit logs, event logs, and faults.

Logging into and out of the Cisco UCS Central GUI

Logging in to the Cisco UCS Central GUI through HTTP

The default HTTP web link for the Cisco UCS Central GUI is `http://UCSCentral_IP`, where *`UCSCentral_IP`* represents the IP address assigned to Cisco UCS Central.

Procedure

Step 1 In your web browser, type the Cisco UCS Central GUI web link or select the bookmark in your browser.

Step 2 On the launch page, do the following:

a) Enter your username and password.

b) Click **Log In**.

Logging in to the Cisco UCS Central GUI through HTTPS

The default HTTPS web link for the Cisco UCS Central GUI is `https://UCSCentral_IP`, where *`UCSCentral_IP`* represents the IP address assigned to Cisco UCS Central.

Procedure

Step 1 In your web browser, type the Cisco UCS Central GUI web link or select the bookmark in your browser.

Step 2 On the launch page, do the following:

a) Enter your username and password.

b) Click **Log In**.

Logging out of the Cisco UCS Central GUI

Procedure

In the Cisco UCS Central GUI, click **Log Out** in the upper right.
The Cisco UCS Central GUI logs you out immediately and returns your browser to the launch page.

Launching Cisco UCS Manager for a UCS Domain

Before You Begin

To access Cisco UCS Manager from the Cisco UCS Central GUI, you need the following:

- Name of the Cisco UCS domain you want to access.
- Cisco UCS username and password.

Procedure

Step 1 On the menu bar, click **Equipment**.

Step 2 In the **Navigation** pane, expand **UCS Domains**.

Step 3 In the work pane, click on the **UCS Domains** tab.

Step 4 From the list of Cisco UCS domain names under the **UCS Name** column, choose the domain for which you want to launch Cisco UCS Manager.

Step 5 On the menu bar, click **Properties**.

Step 6 In the **General** tab, click **Launch UCS Manager**.

Step 7 If a **UCSM Certificate Error** dialog box appears, click the text to continue to the web browser.

Step 8 If a **Security Alert** dialog box appears, accept the security certificate and continue.

Step 9 In the Cisco UCS Manager launch page, click **Launch UCS Manager**.
Depending upon the web browser you use to log in, you may be prompted to download or save the .JNLP file.

Step 10 If Cisco UCS Manager displays a pre-login banner, review the message and click **OK** to close the dialog box.

Step 11 If a **Security** dialog box displays, do the following:

a) (Optional) Check the check box to accept all content from Cisco.
b) Click **Yes** to accept the certificate and continue.

Step 12 In the **Login** dialog box, do the following:

a) Enter your username and password.
b) If your Cisco UCS implementation includes multiple domains, select the appropriate domain from the **Domain** drop-down list.

c) Click **Login**.

Importing a Policy

Import a policy from one of the Cisco UCS domains registered with Cisco UCS Central.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the Work pane, click the policy to import.

Step 5 In the **Actions** area, click **Import** and do the following:

a) In the Import **Policy from UCSM** dialog, click the system name with the policy to import.

b) Click **Import and Close**.

Step 6 Click **Save**.

Configuring Identifier Policies

Identifier Policies

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

Configuring an Identifier Policy

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **Identifier**.

Step 6 In the **Actions** area, complete all applicable fields.

Name	Description
Soak Interval field	The number of seconds Cisco UCS Central waits before reassigning a pool entity that has been released by the Cisco UCS domain to which it was assigned. For example, if this option is set to 300 and a Cisco UCS domain releases a MAC address, Cisco UCS Central waits for 5 minutes before reassigning that MAC address to another Cisco UCS domain. This option only applies to the **root** domain group. Specify an integer between 0 and 86400.

Step 7 Click **Save**.

Determining Where a Pool Is Used

You can use this procedure to determine where pools are used, and if there are any duplicates.

Procedure

Step 1 In the **Navigation** pane, expand the node for the pool whose usage you want to view.

Step 2 Click **ID Usage**.
Cisco UCS Central GUI displays all of the pools of the type you selected.

PART II

System Configuration

- Configuring Domain Groups, page 19
- Configuring Communication Services, page 23
- Configuring Authentication, page 43
- Configuring Role-Based Access Control, page 77
- Configuring DNS Servers, page 105

CHAPTER 3

Configuring Domain Groups

This chapter includes the following sections:

- Domain Groups, page 19
- Creating a Domain Group, page 20
- Deleting a Domain Group, page 20
- Changing Group Assignment for a Cisco UCS Domain, page 20

Domain Groups

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

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

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

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

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

After confirming the registration, if you want to manage all the member domains in a domain group with same operational policies, you can change the policy resolution to global on the Cisco UCS Manager GUI.

Policies configured at the domain group root will apply to all the domain groups under the root. Each domain group under the root group can have policies unique to the group. The domain group policies are resolved hierarchically in the member Cisco UCS domains.

Domain Group Management

Users with the following privileges can create and manage domain groups in Cisco UCS Central:

- **Admin privileges** — Create new domain groups and assign ungrouped Cisco UCS domains to domain groups.
- **Domain group management privileges** — Create and manage domain groups. But cannot assign ungrouped Cisco UCS domains to domain groups.

Creating a Domain Group

You can create a domain group under the domain group root from the **Equipment** tab or from the **Operations Management** tab. You can create up to five hierarchical levels of domain groups under the root. This procedure describes the process to create a domain group from the equipment tab, under the domain group root.

Procedure

Step 1 On the menu bar, click **Equipment**.
Step 2 On the **Equipment** tab, expand **UCS Domains**.
Step 3 Right click on **Domain Group root**, and select **Create Domain Group**.
Step 4 In the **Create Domain Group** dialog box, enter **Name** and **Description**.
Step 5 Click **OK**.

Deleting a Domain Group

Procedure

Step 1 On the menu bar, click **Equipment**.
Step 2 On the **Equipment** tab, **UCS Domains** > **Domain Group root**.
Step 3 Right click on domain group name you want to delete, and select **Delete**.
Step 4 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Changing Group Assignment for a Cisco UCS Domain

You can assign a Cisco UCS domain to a domain group using any one of the following options:

- Changing the group assignment using the **Change Group Assignment** dialog box.
- Using the group assignment link under a specific domain group.
- Using domain group policy qualifiers.

This procedure describes the process to change the group assignment for a Cisco UCS domain.

Procedure

Step 1 On the menu bar, click **Equipment**.
Step 2 On the **Equipment** tab, expand **UCS Domains**.
Step 3 In the **Navigation** pane, expand **Ungrouped Domains**.
Step 4 Right click on the domain name and click **Change Group Assignment**.
Step 5 In the **Change Group Assignment** dialog box, choose the domain group and click **OK**.
Step 6 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

CHAPTER 4

Configuring Communication Services

This chapter includes the following sections:

- Remote Access Policies, page 23
- SNMP Policies, page 34

Remote Access Policies

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

Configuring HTTP

Configuring an HTTP Remote Access Policy

Before You Begin

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

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.

- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **Remote Access**.

Step 6 In the **Work** pane, click the **HTTP** tab.

Step 7 In the **Actions** area, click **Create** and complete all applicable fields.
For **Operational Policies** under the **Domain Group root** node, it is not necessary to click **Create** to complete all applicable fields.

Name	Description
Create button	Creates an instance of the policy that will be used by all Cisco UCS domains included in the selected domain group.
Import button	Allows you to import the policy from one of the Cisco UCS domains registered with Cisco UCS Central.
Delete button	Deletes the instance of the policy defined for the selected domain group. After you delete the policy, it remains greyed-out until you click **Save**. When you do so, Cisco UCS Central deletes the policy and any configuration data you may have specified. While you can create a new instance of the policy later, you cannot restore the configuration data from a deleted instance. To cancel the delete request, click **Reset**.
Admin State field	Whether Cisco UCS Central allows HTTP or HTTPS communication with the Cisco UCS domains included in the Cisco UCS Central domain group. This can be one fo the following: • **disabled**—Cisco UCS Central does not allow communication with any included Cisco UCS domain via HTTP or HTTPS. • **enabled**—Cisco UCS Central allows communication over HTTP if **Redirect HTTP to HTTPS** is set to **disabled**. All HTTP data is exchanged in clear text mode. If **Redirect HTTP to HTTPS** is set to **enabled**, Cisco UCS Central requires HTTPS communication for all included Cisco UCS domains.
Port field	The port to use for HTTP or HTTPS connections. Enter an integer between 1 and 65535. The default port is 80.
Redirect HTTP to HTTPS	If enabled, all attempts to communicate via HTTP are redirected to the equivalent HTTPS address. This option effectively disables HTTP access to all included Cisco UCS domains.

Step 8 Click **Save**.

What to Do Next

Optionally, configure the following remote access policies:

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

Deleting an HTTP Remote Access Policy

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

Procedure

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.
Step 3 Expand the node for a domain group containing the policy to delete.
Step 4 In the **Navigation** pane, click **Operational Policies**.
Step 5 In the **Work** pane, click **Remote Access**.
Step 6 In the **Work** pane, click the **HTTP** tab.
Step 7 In the **Actions** area, click **Delete**.
A policy that is deleted will inherit its settings from its domain group's parent until it is reconfigured.
Step 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.
Step 9 Click **Save**.

Configuring Telnet

Configuring a Telnet Remote Access Policy

Before You Begin

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

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **Remote Access**.

Step 6 In the **Work** pane, click the **Telnet** tab.

Step 7 In the **Actions** area, click **Create** and complete all applicable fields.
For **Operational Policies** under the **Domain Group root** node, it is not necessary to click **Create** to complete all applicable fields.

Name	Description
Create button	Creates an instance of the policy that will be used by all Cisco UCS domains included in the selected domain group.
Import button	Allows you to import the policy from one of the Cisco UCS domains registered with Cisco UCS Central.
Delete button	Deletes the instance of the policy defined for the selected domain group. After you delete the policy, it remains greyed-out until you click **Save**. When you do so, Cisco UCS Central deletes the policy and any configuration data you may have specified. While you can create a new instance of the policy later, you cannot restore the configuration data from a deleted instance. To cancel the delete request, click **Reset**.
Admin State field	If enabled, the Cisco UCS Manager CLI is available via Telnet in all Cisco UCS domains included in the Cisco UCS Central domain group.

Step 8 Click **Save**.

What to Do Next

Optionally, configure the following remote access policies:

- HTTP
- Web Session Limits

- CIM XML
- Interfaces Monitoring Policy
- SSH Configuration

Deleting a Telnet Remote Access Policy

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

Procedure

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.
Step 3 Expand the node for a domain group containing the policy to delete.
Step 4 In the **Navigation** pane, click **Operational Policies**.
Step 5 In the **Work** pane, click **Remote Access**.
Step 6 In the **Work** pane, click the **Telnet** tab.
Step 7 In the **Actions** area, click **Delete**.
A policy that is deleted will inherit its settings from its domain group's parent until it is reconfigured.
Step 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.
Step 9 Click **Save**.

Configuring Web Session Limits

Configuring a Web Session Limits Remote Access Policy

Before You Begin

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

Procedure

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.
Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.

- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **Remote Access**.

Step 6 In the **Work** pane, click the **Web Session Limits** tab.

Step 7 In the **Actions** area, click **Create** and complete all applicable fields.
For **Operational Policies** under the **Domain Group root** node, it is not necessary to click **Create** to complete all applicable fields.

Name	Description
Create button	Creates an instance of the policy that will be used by all Cisco UCS domains included in the selected domain group.
Import button	Allows you to import the policy from one of the Cisco UCS domains registered with Cisco UCS Central.
Delete button	Deletes the instance of the policy defined for the selected domain group. After you delete the policy, it remains greyed-out until you click **Save**. When you do so, Cisco UCS Central deletes the policy and any configuration data you may have specified. While you can create a new instance of the policy later, you cannot restore the configuration data from a deleted instance. To cancel the delete request, click **Reset**.
Maximum Sessions Per User field	The maximum number of concurrent HTTP and HTTPS sessions allowed for each user in the Cisco UCS domains included in the Cisco UCS Central domain group. Enter an integer between 1 and 256.
Maximum Sessions field	The maximum number of concurrent HTTP and HTTPS sessions allowed for all users within the in the Cisco UCS domains included in the Cisco UCS Central domain group. Enter an integer between 1 and 256.

Step 8 Click **Save**.

What to Do Next

Optionally, configure the following remote access policies:

- HTTP
- Telnet
- CIM XML

- Interfaces Monitoring Policy

Deleting a Web Session Limits Remote Access Policy

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

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Expand the node for a domain group containing the policy to delete.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **Remote Access**.

Step 6 In the **Work** pane, click the **Web Session Limits** tab.

Step 7 In the **Actions** area, click **Delete**.
A policy that is deleted will inherit its settings from its domain group's parent until it is reconfigured.

Step 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Step 9 Click **Save**.

Configuring CIM XML

Configuring a CIM XML Remote Access Policy

Before You Begin

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

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.

- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **Remote Access**.

Step 6 In the **Work** pane, click the **CIM XML** tab.

Step 7 In the **Actions** area, click **Create** and complete all applicable fields.
For **Operational Policies** under the **Domain Group root** node, it is not necessary to click **Create** to complete all applicable fields.

Name	Description
Create button	Creates an instance of the policy that will be used by all Cisco UCS domains included in the selected domain group.
Import button	Allows you to import the policy from one of the Cisco UCS domains registered with Cisco UCS Central.
Delete button	Deletes the instance of the policy defined for the selected domain group. After you delete the policy, it remains greyed-out until you click **Save**. When you do so, Cisco UCS Central deletes the policy and any configuration data you may have specified. While you can create a new instance of the policy later, you cannot restore the configuration data from a deleted instance. To cancel the delete request, click **Reset**.
Admin State field	If enabled, the Cisco UCS domains included in the Cisco UCS Central domain group can send XML messages over HTTP.

Step 8 Click **Save**.

What to Do Next

Optionally, configure the following remote access policies:

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

Deleting a CIM XML Remote Access Policy

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

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Expand the node for a domain group containing the policy to delete.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **Remote Access**.

Step 6 In the **Work** pane, click the **CIM XML** tab.

Step 7 In the **Actions** area, click **Delete**.
A policy that is deleted will inherit its settings from its domain group's parent until it is reconfigured.

Step 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Step 9 Click **Save**.

Configuring Interfaces Monitoring

Configuring an Interfaces Monitoring Remote Access Policy

Before You Begin

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

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **Remote Access**.

Step 6 In the **Work** pane, click the **Interfaces Monitoring** tab.

Step 7 In the **Actions** area, click **Create** and complete all applicable fields.
For **Operational Policies** under the **Domain Group root** node, it is not necessary to click **Create** to complete all applicable fields.

Name	Description
Create button	Creates an instance of the policy that will be used by all Cisco UCS domains included in the selected domain group.
Import button	Allows you to import the policy from one of the Cisco UCS domains registered with Cisco UCS Central.
Delete button	Deletes the instance of the policy defined for the selected domain group. After you delete the policy, it remains greyed-out until you click **Save**. When you do so, Cisco UCS Central deletes the policy and any configuration data you may have specified. While you can create a new instance of the policy later, you cannot restore the configuration data from a deleted instance. To cancel the delete request, click **Reset**.
Admin State field	Whether the monitoring policy is enabled or disabled for the management interfaces in the Cisco UCS domains included in the Cisco UCS Central domain group.
Poll Interval field	The number of seconds Cisco UCS waits between data recordings. Enter an integer between 90 and 300.
Max Fail Report Count field	The maximum number of monitoring attempts that can fail before Cisco UCS assumes that the management interface is unavailable and generates a fault message. Enter an integer between 2 and 5.
Monitoring Mechanism field	The type of monitoring you want Cisco UCS to use. This can be one of the following: • **Mii Status**—Cisco UCS monitors the availability of the Media Independent Interface (MII). If you select this option, Cisco UCS Central GUI displays the **Media Independent Interface Monitoring** area. • **Ping Arp Targets**—Cisco UCS pings designated targets using the Address Resolution Protocol (ARP). If you select this option, Cisco UCS Central GUI displays the **ARP Target Monitoring** area. • **Ping Gateway**—Cisco UCS pings the default gateway address configured for each Cisco UCS domain included in the Cisco UCS Central domain group. If you select this option, Cisco UCS Central GUI displays the **Gateway Ping Monitoring** area.

a) In the **Monitoring Mechanism** area, select **Mii Status** to select Media Independent Interface Monitoring.

Name	Description
Retry Interval field	The number of seconds Cisco UCS waits before requesting another response from the MII if a previous attempt fails. Enter an integer between 3 and 10.
Max Retry Count field	The number of times Cisco UCS polls the MII until the system assumes the interface is unavailable. Enter an integer between 1 and 3.

b) In the **Monitoring Mechanism** area, select **Ping ARP Targets** to select ARP Target Monitoring.

Name	Description
Target IP 1 field	The first IP address Cisco UCS pings.
Target IP 2 field	The second IP address Cisco UCS pings.
Target IP 3 field	The third IP address Cisco UCS pings.
Number of ARP Requests field	The number of ARP requests Cisco UCS sends to the target IP addresses. Enter an integer between 1 and 5.
Max Deadline Timeout field	The number of seconds Cisco UCS waits for responses from the ARP targets until the system assumes they are unavailable. Enter an integer between 5 and 15.

c) In the **Monitoring Mechanism** area, select **Ping Gateway** to select Gateway Ping Monitoring.

Name	Description
Number of Ping Requests field	The number of times Cisco UCS pings the gateway. Enter an integer between 1 and 5.
Max Deadline Timeout field	The number of seconds Cisco UCS waits for a response from the gateway until Cisco UCS assumes the address is unavailable. Enter an integer between 5 and 15.

Step 8 Click **Save**.

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

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

Procedure

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.
Step 3 Expand the node for a domain group containing the policy to delete.
Step 4 In the **Navigation** pane, click **Operational Policies**.
Step 5 In the **Work** pane, click **Remote Access**.
Step 6 In the **Work** pane, click the **Interfaces Monitoring** tab.
Step 7 In the **Actions** area, click **Delete**.
A policy that is deleted will inherit its settings from its domain group's parent until it is reconfigured.
Step 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.
Step 9 Click **Save**.

SNMP Policies

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

Configuring an SNMP Policy

Before You Begin

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

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **SNMP**.

Step 6 In the **Actions** area, click **Create** and complete all applicable fields.
For **Operational Policies** under the **Domain Group root** node, it is not necessary to click **Create** to complete all applicable fields.

a) In the Actions area, click the **Enabled** state and complete the following:
The default state is **Disabled** with no fields displayed. Leaving the default state disables the SNMP policy.

Name	Description
Create button	Creates an instance of the policy that will be used by all Cisco UCS domains included in the selected domain group.
Import button	Allows you to import the policy from one of the Cisco UCS domains registered with Cisco UCS Central.
Delete button	Deletes the instance of the policy defined for the selected domain group. After you delete the policy, it remains greyed-out until you click **Save**. When you do so, Cisco UCS Central deletes the policy and any configuration data you may have specified. While you can create a new instance of the policy later, you cannot restore the configuration data from a deleted instance. To cancel the delete request, click **Reset**.
Admin State field	If enabled, Cisco UCS uses SNMP in all Cisco UCS domains included in the Cisco UCS Central domain group and Cisco UCS Central GUI displays the rest of the fields in this area. You should only enable SNMP if all included Cisco UCS domains are integrated with an SNMP server.
Community/Username field	The default SNMP v1 or v2c community name or SNMP v3 username Cisco UCS includes on any trap messages it sends to the SNMP host. Enter an alphanumeric string between 1 and 32 characters. Do not use @ (at sign), \ (backslash), " (double quote), ? (question mark) or an empty space. The default is public.

Name	Description
System Contact field	The system contact person responsible for the SNMP implementation. Enter a string of up to 255 characters, such as an email address or a name and telephone number.
System Location field	The location of the host on which the SNMP agent (server) runs. Enter an alphanumeric string up to 510 characters.

b) In the **SNMP Traps** area, complete the following:

Name	Description
Filter button	Allows you to filter the data in the table. When you apply a filter, this button name changes to **Filter (on)**.
Create SNMP Trap button	Allows you to create an SNMP trap.
Properties button	Displays detailed properties for the object selected in the table.
Delete button	Deletes the object selected in the table.
Name column	The IP address of the SNMP host to which Cisco UCS should send the trap.
Community/Username column	The SNMP v1 or v2c community name or the SNMP v3 username Cisco UCS includes when it sends the trap to the SNMP host. This must be the same as the community or username that is configured for the SNMP service.
Port column	The port on which Cisco UCS communicates with the SNMP host for the trap.
Version column	The SNMP version and model used for the trap.
v3 Privilege column	The type of trap to send, if applicable.
Type column	The privilege associated with the trap, if applicable. This can be one of the following: • **auth**—Authentication but no encryption • **noauth**—No authentication or encryption • **priv**—Authentication and encryption

c) In the **SNMP Users** area, complete the following:

Name	Description
Filter button	Allows you to filter the data in the table. When you apply a filter, this button name changes to **Filter (on)**.
Create SNMP User button	Allows you to create an SNMP user.
Properties button	Displays detailed properties for the object selected in the table.
Delete button	Deletes the object selected in the table.
Name column	The SNMP user name.

Step 7 Click **Save**.

Deleting an SNMP Policy

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

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

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **SNMP**.

Step 6 In the **Actions** area, click **Delete**.
A policy that is deleted will inherit its settings from its domain group's parent until it is reconfigured.

Step 7 Click **Save**.

Creating an SNMP Trap

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 In the **Navigation** pane, click **Operational Policies**.

Step 4 In the **Work** pane, click **SNMP**.

Step 5 In the **SNMP Traps** area, click **Create SNMP Trap** and complete all applicable fields.

a) In the **Create SNMP Trap** dialog, complete the following:

Name	Description
IP Address field	The IP address of the SNMP host to which Cisco UCS should send the trap.
Community/Username field	The SNMP v1 or v2c community name or the SNMP v3 username Cisco UCS includes when it sends the trap to the SNMP host. This must be the same as the community or username that is configured for the SNMP service. Enter an alphanumeric string between 1 and 32 characters. Do not use @ (at sign), \ (backslash), " (double quote), ? (question mark) or an empty space.
Port field	The port on which Cisco UCS communicates with the SNMP host for the trap. Enter an integer between 1 and 65535. The default port is 162.
Version field	The SNMP version and model used for the trap. This can be one of the following: • **v1** • **v2c** • **v3**
Type field	If you select **v2c** or **v3** for the version, the type of trap to send. This can be one of the following: • **informs** • **traps**

Name	Description
v3 Privilege field	If you select **v3** for the version, the privilege associated with the trap. This can be one of the following: • **auth**—Authentication but no encryption • **noauth**—No authentication or encryption • **priv**—Authentication and encryption

b) Click **OK**.

Step 6 Click **Save**.

Deleting an SNMP Trap

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 In the **Navigation** pane, click **Operational Policies**.

Step 4 In the **Work** pane, click **SNMP**.

Step 5 In the **SNMP Traps** area, select the SNMP trap to delete and click **Delete**.
You can also right-click the SNMP trap to access that option.

Step 6 Click **Save**.

Creating an SNMP User

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 In the **Navigation** pane, click **Operational Policies**.

Step 4 In the **Work** pane, click **SNMP**.

Step 5 In the **SNMP Users** area, click **Create SNMP User** and complete all applicable fields.

a) In the **Create SNMP User** dialog, complete the following:

Name	Description
Name field	The username assigned to the SNMP user. Enter up to 32 letters or numbers. The name must begin with a letter and you can also specify _ (underscore), . (period), @ (at sign), and - (hyphen). **Note** You cannot create an SNMP username that is identical to a locally authenticated username.
Auth Type field	The authorization type. This can be one of the following: • **MD5** • **SHA**
Use AES-128 check box	If checked, this user uses AES-128 encryption.
Password field	The password for this user.
Set field	Whether the password has been set for this SNMP user.
Confirm Password field	The password again for confirmation purposes.
Privacy Password field	The privacy password for this user.
Set field	Whether the privacy password has been set for this SNMP user.
Confirm Privacy Password field	The privacy password again for confirmation purposes.

b) Click **OK**.

Step 6 Click **Save**.

Deleting an SNMP User

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 In the **Navigation** pane, click **Operational Policies**.

Step 4 In the **Work** pane, click **SNMP**.

Step 5 In the **SNMP Users** area, select the SNMP user to delete and click **Delete**.
You can also right-click the SNMP user to access that option.

Step 6 Click **Save**.

CHAPTER 5

Configuring Authentication

This chapter includes the following sections:

- Authentication Services, page 43
- Guidelines and Recommendations for Remote Authentication Providers, page 43
- User Attributes in Remote Authentication Providers, page 44
- LDAP Group Rule, page 45
- Configuring LDAP Providers, page 45
- Configuring RADIUS Providers, page 55
- Configuring TACACS+ Providers, page 59
- Configuring Multiple Authentication Systems, page 63
- Selecting a Primary Authentication Service, page 71

Authentication Services

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

Guidelines and Recommendations for Remote Authentication Providers

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

User Accounts in Remote Authentication Services

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

User Roles in Remote Authentication Services

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

Local and Remote User Authentication Support

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

User Attributes in Remote Authentication Providers

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

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

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

Table 1: Comparison of User Attributes by Remote Authentication Provider

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

Sample OID for LDAP User Attribute

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

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

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

LDAP Group Rule

The LDAP group rule is used to determine whether Cisco UCS should use LDAP groups when assigning user roles and locales to a remote user.

Configuring LDAP Providers

Configuring Properties 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.

Before You Begin

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

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **LDAP** and click **Providers**.

Step 6 In the **Actions** area, click **Properties** and complete all fields.
You can also right-click **LDAP** to access that option.

a) In the **Properties (LDAP)** dialog box, complete all fields on the **General** tab.

Name	Description
Timeout field	The length of time in seconds the system should spend trying to contact the LDAP database before it times out. Enter an integer from 1 to 60 seconds. The default value is 30 seconds. This property is required.
Attribute field	An LDAP attribute that stores the values for the user roles and locales. This property is always a name-value pair. The system queries the user record for the value that matches this attribute name. If you do not want to extend your LDAP schema, you can configure an existing, unused LDAP attribute with the Cisco UCS roles and locales. Alternatively, you can create an attribute named CiscoAVPair in the remote authentication service with the following attribute ID: 1.3.6.1.4.1.9.287247.1
Base DN field	The specific distinguished name in the LDAP hierarchy where the server should begin a search when a remote user logs in and the system attempts to get the user's DN based on their username. The maximum supported string length is 127 characters. This property is required. If you do not specify a base DN on this tab then you must specify one on the **General** tab for every LDAP provider defined in this Cisco UCS domain.
Filter field	The LDAP search is restricted to those usernames that match the defined filter. This property is required. If you do not specify a filter on this tab then you must specify one on the **General** tab for every LDAP provider defined in this Cisco UCS domain.

b) Click **OK**.

Step 7 Click **Save**.

Creating an LDAP Provider

Cisco UCS Central supports a maximum of 16 LDAP providers.

Before You Begin

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

- In the LDAP server, perform one of the following configurations:

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

  The Cisco LDAP implementation requires a unicode type attribute.

  If you choose to create the CiscoAVPair custom attribute, use the following attribute ID: 1.3.6.1.4.1.9.287247.1
- For a cluster configuration, add the management port IP addresses for both fabric interconnects. This configuration ensures that remote users can continue to log in if the first fabric interconnect fails and the system fails over to the second fabric interconnect. All login requests are sourced from these IP addresses, not the virtual IP address used by Cisco UCS Central.

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

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **LDAP** and click **Providers**.

Step 6 In the **Actions** area, click **Create LDAP Provider** and complete all fields.
You can also right-click **Providers** to access that option.

a) In the **Create LDAP Provider** dialog box, complete all **Properties** fields on the **General** tab.

Name	Description
Hostname field	The hostname or IP address on which the LDAP provider resides. **Note** If you use a hostname rather than an IP 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.
Order field	The order in which Cisco UCS uses this LDAP provider to authenticate users.

Name	Description
Timeout field	The length of time in seconds the system should spend trying to contact the LDAP database before it times out. Enter an integer from 1 to 60 seconds, or enter 0 (zero) to use the global timeout value specified on the LDAP **General** tab. The default is 30 seconds.
Bind DN field	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 127 ASCII characters.
Base DN field	The specific distinguished name in the LDAP hierarchy where the server should begin a search when a remote user logs in and the system attempts to get the user's DN based on their username. The maximum supported string length is 127 characters. This value is required unless a default base DN has been set on the LDAP **General** tab.
Port field	The port through which Cisco UCS communicates with the LDAP database. The standard port number is 389.
Enable SSL check box	If checked, encryption is required for communications with the LDAP database. If unchecked, authentication information will be sent as clear text. LDAP uses STARTTLS. This allows encrypted communication using port 389.
Filter field	The LDAP search is restricted to those usernames that match the defined filter. This value is required unless a default filter has been set on the LDAP **General** tab.
Attribute field	An LDAP attribute that stores the values for the user roles and locales. This property is always a name-value pair. The system queries the user record for the value that matches this attribute name. If you do not want to extend your LDAP schema, you can configure an existing, unused LDAP attribute with the Cisco UCS roles and locales. Alternatively, you can create an attribute named CiscoAVPair in the remote authentication service with the following attribute ID: 1.3.6.1.4.1.9.287247.1 This value is required unless a default attribute has been set on the LDAP **General** tab.
Password field	The password for the LDAP database account specified in the **Bind DN** field. You can enter any standard ASCII characters except for space, § (section sign), ? (question mark), or = (equal sign).

Name	Description
Confirm Password field	The LDAP database password repeated for confirmation purposes.

b) In the **Create LDAP Provider** dialog box, complete all **LDAP Group Rules** fields on the **General** tab.

Name	Description
Group Authorization field	Whether Cisco UCS also searches LDAP groups when authenticating and assigning user roles and locales to remote users. This can be one of the following: • **Disable**—Cisco UCS does not access any LDAP groups. • **Enable**—Cisco UCS searches all LDAP groups mapped in Cisco UCS Central. If the remote user is found, Cisco UCS assigns the user roles and locales defined for that LDAP group in the associated LDAP group map. **Note** Role and locale assignment is cumulative. If a user is included in multiple groups, or has a role or locale specified in the LDAP attribute, Cisco UCS assigns that user all the roles and locales mapped to any of those groups or attributes.
Group Recursion field	Whether Cisco UCS searches both the mapped groups and their parent groups. This can be one of the following: • **Non Recursive**—Cisco UCS searches only the groups mapped in Cisco UCS Central. If none of the groups containing the user explicitly set the user's authorization properties, Cisco UCS uses the default settings. • **Recursive**—Cisco UCS searches each mapped group and all its parent groups for the user's authorization properties. These properties are cumulative, so for each group Cisco UCS finds with explicit authorization property settings, it applies those settings to the current user. Otherwise it uses the default settings.
Target Attribute field	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.

c) Click **OK**.

Step 7 Click **Save**.

What to Do Next

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

For implementations involving multiple LDAP databases, configure an LDAP provider group.

Changing the LDAP Group Rule for an LDAP Provider

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **LDAP** > **Providers**.

Step 6 In the **Work** pane, click an **LDAP Provider**.

Step 7 In the **Actions** area, click **Properties**.
You can also right-click the **LDAP Provider** to access that option.

a) In the **Properties** dialog box, complete all **Properties** fields on the **General** tab.

Name	Description
Hostname field	The hostname or IP address on which the LDAP provider resides. **Note** If you use a hostname rather than an IP 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.
Order field	The order in which Cisco UCS uses this LDAP provider to authenticate users.
Timeout field	The length of time in seconds the system should spend trying to contact the LDAP database before it times out. Enter an integer from 1 to 60 seconds, or enter 0 (zero) to use the global timeout value specified on the LDAP **General** tab. The default is 30 seconds.
Bind DN field	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 127 ASCII characters.

Name	Description
Base DN field	The specific distinguished name in the LDAP hierarchy where the server should begin a search when a remote user logs in and the system attempts to get the user's DN based on their username. The maximum supported string length is 127 characters. This value is required unless a default base DN has been set on the LDAP **General** tab.
Port field	The port through which Cisco UCS communicates with the LDAP database. The standard port number is 389.
Enable SSL check box	If checked, encryption is required for communications with the LDAP database. If unchecked, authentication information will be sent as clear text. LDAP uses STARTTLS. This allows encrypted communication using port 389.
Filter field	The LDAP search is restricted to those usernames that match the defined filter. This value is required unless a default filter has been set on the LDAP **General** tab.
Attribute field	An LDAP attribute that stores the values for the user roles and locales. This property is always a name-value pair. The system queries the user record for the value that matches this attribute name. If you do not want to extend your LDAP schema, you can configure an existing, unused LDAP attribute with the Cisco UCS roles and locales. Alternatively, you can create an attribute named CiscoAVPair in the remote authentication service with the following attribute ID: 1.3.6.1.4.1.9.287247.1 This value is required unless a default attribute has been set on the LDAP **General** tab.
Password field	The password for the LDAP database account specified in the **Bind DN** field. You can enter any standard ASCII characters except for space, § (section sign), ? (question mark), or = (equal sign).
Confirm Password field	The LDAP database password repeated for confirmation purposes.

b) In the **Properties** dialog box, complete all **LDAP Group Rules** fields on the **General** tab.

Name	Description
Group Authorization field	Whether Cisco UCS also searches LDAP groups when authenticating and assigning user roles and locales to remote users. This can be one of the following: • **Disable**—Cisco UCS does not access any LDAP groups. • **Enable**—Cisco UCS searches all LDAP groups mapped in Cisco UCS Central. If the remote user is found, Cisco UCS assigns the user roles and locales defined for that LDAP group in the associated LDAP group map. **Note** Role and locale assignment is cumulative. If a user is included in multiple groups, or has a role or locale specified in the LDAP attribute, Cisco UCS assigns that user all the roles and locales mapped to any of those groups or attributes.
Group Recursion field	Whether Cisco UCS searches both the mapped groups and their parent groups. This can be one of the following: • **Non Recursive**—Cisco UCS searches only the groups mapped in Cisco UCS Central. If none of the groups containing the user explicitly set the user's authorization properties, Cisco UCS uses the default settings. • **Recursive**—Cisco UCS searches each mapped group and all its parent groups for the user's authorization properties. These properties are cumulative, so for each group Cisco UCS finds with explicit authorization property settings, it applies those settings to the current user. Otherwise it uses the default settings.
Target Attribute field	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.

c) Click **OK**.

Step 8 Click **Save**.

Deleting an LDAP Provider

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **LDAP** > **Providers**.

Step 6 In the **Work** pane, click the LDAP provider you want to delete.

Step 7 In the **Actions** area, click **Delete**.
You can also right-click the **LDAP Provider** you want to delete to access that option.

Step 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

LDAP Group Mapping

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

Note LDAP group mapping is not supported for Cisco UCS Central for this release. However, LDAP group maps are supported for locally managed Cisco UCS domains from the Cisco UCS Central Domain Group root.

When a user logs in to Cisco UCS Central, information about the user's role and locale are pulled from the LDAP group map. If the role and locale criteria match the information in the policy, access is granted.

Role and locale definitions are configured locally in Cisco UCS Central and do not update automatically based on changes to an LDAP directory. When deleting or renaming LDAP groups in an LDAP directory, it is important that you update Cisco UCS Central with the change.

An LDAP group map can be configured to include any of the following combinations of roles and locales:

- Roles only
- Locales only
- Both roles and locales

For example, consider an LDAP group representing a group of server administrators at a specific location. The LDAP group map might be configured to include user roles like server-profile and server-equipment. To restrict access to server administrators at a specific location, the locale could be set to a particular site name.

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

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

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **LDAP** and click **Group Maps**.

Step 6 In the **Actions** area, click **Create LDAP Group Map** and complete all fields.
You can also right-click **Group Maps** to access that option.

a) In the **Create LDAP Group Map** dialog box, complete all fields on the **General** tab.

Name	Description
LDAP Group DN field	The distinguished name of the group in the LDAP database. **Important** This name must match the name in the LDAP database exactly.
Roles table	A list of the user roles defined in the selected Cisco UCS Central domain group and all of its parent groups. If the associated check box is checked, users in this LDAP group will be assigned that user role.

Name	Description
Locales table	A list of the user locales defined in the selected Cisco UCS Central domain group and all of its parent groups. If the associated check box is checked, users in this LDAP group will be assigned that locale.

b) Click **OK**.

What to Do Next

Set the LDAP group rule.

Deleting an LDAP Group Map

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **LDAP** > **Group Maps**.

Step 6 In the **Work** pane, click the group map you want to delete.

Step 7 In the **Actions** area, click **Delete**.
You can also right-click the **Group Map** you want to delete to access that option.

Step 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

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 Central uses that setting and ignores the default setting.

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

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, click **RADIUS**.

Step 6 In the **Actions** area, click **Properties** and complete all fields.
You can also right-click **RADIUS** to access that option.

a) In the **Properties (RADIUS)** dialog box, complete all fields on the **General** tab.

Name	Description
Timeout field	The length of time in seconds the system should spend trying to contact the RADIUS database before it times out. Enter an integer from 1 to 60 seconds. The default value is 5 seconds. This property is required.
Retries field	The number of times to retry the connection before the request is considered to have failed. Enter an integer between 0 and 5. The default value is 1. This property is required.

b) Click **OK**.

Step 7 Click **Save**.

What to Do Next

Create a RADIUS provider.

Creating a RADIUS Provider

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

Before You Begin

Perform the following configuration in the RADIUS server:

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

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

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

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

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **RADIUS** and click **Providers**.

Step 6 In the **Actions** area, click **Create RADIUS Provider** and complete all fields.
You can also right-click **Providers** to access that option.

a) In the **Create RADIUS Provider** dialog box, complete all fields on the **General** tab.

Name	Description
Hostname field	The hostname or IP address on which the RADIUS provider resides. **Note** If you use a hostname rather than an IP 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.
Order field	The order in which Cisco UCS uses this RADIUS provider to authenticate users.
Key field	The SSL encryption key for the database.
Set field	Whether the SSL key is active.
Confirm Key field	The SSL encryption key repeated for confirmation purposes.
Authorization Port field	The port through which Cisco UCS communicates with the RADIUS database.
Timeout field	The length of time in seconds the system should spend trying to contact the RADIUS database before it times out. Enter an integer from 1 to 60 seconds, or enter 0 (zero) to use the global timeout value specified on the RADIUS **General** tab. The default is 5 seconds.
Retries field	The number of times to retry the connection before the request is considered to have failed. If desired, enter an integer between 0 and 5. If you do not specify a value, Cisco UCS uses the value specified on the RADIUS **General** tab.

b) Click **OK**.

Step 7 Click **Save**.

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

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **RADIUS** and click **Providers**.

Step 6 In the **Work** pane, click the **RADIUS Provider** you want to delete.

Step 7 In the **Actions** area, click **Delete**.
You can also right-click the **RADIUS Provider** you want to delete to access that option.

Step 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

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 Central uses that setting and ignores the default setting.

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

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.

- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, click **TACACS+**.

Step 6 In the **Actions** area, click **Properties**.
You can also right-click **TACACS+** to access that option.

a) In the **Properties (TACACS+)** dialog box, complete all fields on the **General** tab.

Name	Description
Timeout field	The length of time in seconds the system should spend trying to contact the TACACS+ database before it times out. Enter an integer from 1 to 60 seconds. The default value is 5 seconds. This property is required.

b) Click **OK**.

Step 7 Click **Save**.

What to Do Next

Create an TACACS+ provider.

Creating a TACACS+ Provider

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

Before You Begin

Perform the following configuration in the TACACS+ server:

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

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

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

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

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **TACACS+** and click **Providers**.

Step 6 In the **Actions** area, click **Create TACACS+ Provider** and complete all fields.
You can also right-click **Providers** to access that option.

a) In the **Create TACACS+ Provider** dialog box, complete all fields on the **General** tab.

Name	Description
Hostname field	The hostname or IP address on which the TACAS+ provider resides. **Note** If you use a hostname rather than an IP 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.
Order field	The order in which Cisco UCS uses this TACAS+ provider to authenticate users.
Key field	The SSL encryption key for the database.
Set field	Whether the SSL key is active.
Confirm Key field	The SSL encryption key repeated for confirmation purposes.
Port field	The port through which Cisco UCS should communicate with the TACACS+ database. Enter an integer between 1 and 65535. The default port is 49.
Timeout field	The length of time in seconds the system should spend trying to contact the TACACS+ database before it times out. Enter an integer from 1 to 60 seconds, or enter 0 (zero) to use the global timeout value specified on the TACACS+ **General** tab. The default is 5 seconds.

Name	Description
Retries field	The number of times to retry the connection before the request is considered to have failed. Enter an integer between 0 and 5. The default value is 1.

b) Click **OK**.

Step 7 Click **Save**.

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

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **TACACS+** > **Providers**.

Step 6 In the **Work** pane, click the TACACS+ provider you want to delete.

Step 7 In the **Actions** area, click **Delete**.
You can also right-click the **TACACS+ Provider** you want to delete to access that option.

Step 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Configuring Multiple Authentication Systems

Multiple Authentication Systems

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

- Provider groups
- Authentication domains

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

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

From a Linux terminal:

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

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

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

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

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

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

From a Putty client:

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

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

From a SSH client:

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

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

  ```
  Host Name: 192.0.20.11
  ```

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

Provider Groups

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

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

Creating an LDAP Provider Group

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

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

Before You Begin

Create one or more LDAP providers.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **LDAP** and click **Provider Groups**.

Step 6 In the **Actions** area, click **Create LDAP Provider Group** and complete all fields.
You can also right-click **Provider Groups** to access that option.

a) In the **Create LDAP Provider Group** dialog box, complete all fields on the **General** tab.

Name	Description
Name field	The name of the LDAP provider group.
Available Providers list box	The available LDAP providers that you can add to the LDAP group. You can use Shift+Click and Ctrl+Click to select multiple providers.
>> button	Adds all available providers to the group regardless of what providers are selected in the **Available Providers** list box.
> button	Adds the providers selected in the **Available Providers** list box to the group.
< button	Removes the providers selected in the **Assigned Providers** list box from the group.
<< button	Removes all providers from the group regardless of what providers are selected in the **Assigned Providers** list box.

Name	Description
Assigned Providers list box	The LDAP providers that are included in the LDAP group. Cisco UCS searches the providers in the order that they appear in the table. To change the provider priority, select a provider and use the arrow buttons above the list to move the provider to the desired position.

b) Click **OK**.

Step 7 Click **Save**.

What to Do Next

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

Deleting an LDAP Provider Group

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **LDAP** > **Provider Groups**.

Step 6 In the **Work** pane, click the LDAP provider group you want to delete.

Step 7 In the **Actions** area, click **Delete**.
You can also right-click the **LDAP Provider Group** you want to delete to access that option.

Step 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Creating a RADIUS Provider Group

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

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

Before You Begin

Create one or more RADIUS providers.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **RADIUS** and click **Providers**.

Step 6 In the **Actions** area, click **Create RADIUS Provider Group** and complete all fields.
You can also right-click **Provider Groups** to access that option.

a) In the **Create RADIUS Provider** dialog box, complete all fields on the **General** tab.

Name	Description
Name field	The name of the RADIUS provider group.
Available Providers list box	The available RADIUS providers that you can add to the RADIUS group. You can use Shift+Click and Ctrl+Click to select multiple providers.
>> button	Adds all available providers to the group regardless of what providers are selected in the **Available Providers** list box.
> button	Adds the providers selected in the **Available Providers** list box to the group.
< button	Removes the providers selected in the **Assigned Providers** list box from the group.
<< button	Removes all providers from the group regardless of what providers are selected in the **Assigned Providers** list box.
Assigned Providers list box	The RADIUS providers that are included in the RADIUS group. Cisco UCS searches the providers in the order that they appear in the table. To change the provider priority, select a provider and use the arrow buttons above the list to move the provider to the desired position.

b) Click **OK**.

Step 7 Click **Save**.

What to Do Next

Configure an authentication domain or select a default authentication service.

Deleting a RADIUS Provider Group

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **RADIUS** > **Provider Groups**.

Step 6 In the **Work** pane, click the RADIUS provider group you want to delete.

Step 7 In the **Actions** area, click **Delete**.
You can also right-click the **RADIUS Provider Group** you want to delete to access that option.

Step 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Creating a TACACS+ Provider Group

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

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

Before You Begin

Create one or more TACACS+ providers.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **TACACS+** and click **Provider Groups**.

Step 6 In the **Actions** area, click **Create TACACS+ Provider Group** and complete all fields.
You can also right-click **Provider Groups** to access that option.

a) In the **Create TACACS+ Provider Group** dialog box, complete all fields on the **General** tab.

Name	Description
Name field	The name of the TACACS+ provider group.
Available Providers list box	The available TACACS+ providers that you can add to the TACACS+ group. You can use Shift+Click and Ctrl+Click to select multiple providers.
>> button	Adds all available providers to the group regardless of what providers are selected in the **Available Providers** list box.
> button	Adds the providers selected in the **Available Providers** list box to the group.
< button	Removes the providers selected in the **Assigned Providers** list box from the group.
<< button	Removes all providers from the group regardless of what providers are selected in the **Assigned Providers** list box.
Assigned Providers list box	The TACACS+ providers that are included in the TACACS+ group. Cisco UCS searches the providers in the order that they appear in the table. To change the provider priority, select a provider and use the arrow buttons above the list to move the provider to the desired position.

b) Click **OK**.

Step 7 Click **Save**.

Deleting a TACACS+ Provider Group

You cannot delete a provider group if it is being used by an authentication configuration.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **TACACS+** > **Provider Groups**.

Step 6 In the **Work** pane, click the **TACACS+ Provider Group** you want to delete.

Step 7 In the **Actions** area, click **Delete**.
You can also right-click the **TACACS+ Provider Group** you want to delete to access that option.

Step 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Authentication Domains

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

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

Note Authentication domains for LDAP are not supported for Cisco UCS Central for this release. However, Authentication domains are supported for managed Cisco UCS domains from the Cisco UCS Central Domain Group root.

Creating an Authentication Domain

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **Authentication** and click **Authentication Domains**.

Step 6 In the **Actions** area, click **Create Authentication Domain** and complete all fields.
You can also right-click **Authentication Domains** to access that option.

a) In the **Create Authentication** dialog box, complete all fields on the **General** tab.

Name	Description
Name field	The name of the authentication domain. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved. **Note** For systems using RADIUS as their preferred authentication protocol, the authentication domain name is considered part of the user name and counts toward the 32 character limit for locally created user names. Because Cisco UCS inserts 5 characters for formatting, authentication will fail if the combined total of the domain name plus the user name is more than 27 characters.
Session Refresh Period field	When a web client connects to Cisco UCS Manager, the client needs to send refresh requests to Cisco UCS Manager to keep the web session active. This option specifies the maximum amount of time allowed between refresh requests for a user accessing a Cisco UCS domain included in the selected Cisco UCS Central domain group. If this time limit is exceeded, Cisco UCS Manager considers the web session to be inactive, but it does not terminate the session. Specify an integer between 60 and 172800. The default is 600 seconds.

Name	Description
Session Timeout field	The maximum amount of time that can elapse after the last refresh request before Cisco UCS Manager considers a web session to have ended. If this time limit is exceeded, Cisco UCS Manager automatically terminates the web session. Specify an integer between 60 and 172800. The default is 7200 seconds.
Realm field	The authentication protocol that will be applied to users in this domain. This can be one of the following: • **ldap**—The user must be defined on the LDAP server specified in Cisco UCS Central. • **local**—The user account must be defined locally in Cisco UCS Central or the Cisco UCS domain. • **radius**—The user must be defined on the RADIUS server specified in Cisco UCS Central. • **tacacs**—The user must be defined on the TACACS+ server specified in Cisco UCS Central.
Provider Group drop-down list	If the **Realm** is set to **ldap**, **radius**, or **tacacs**, this field allows you to select an associated provider group.

b) Click **OK**.

Step 7 Click **Save**.

Selecting a Primary Authentication Service

Selecting the Console Authentication Service

Before You Begin

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

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **Authentication** and click **Native Authentication**.

Step 6 In the **Actions** area, click **Properties** and complete all fields.
You can also right-click **Properties** to access that option.

a) In the **Properties (Native Authentication)** dialog box, complete all **Default Authentication** fields on the **General** tab.

Name	Description
Session Refresh Period field	When a web client connects to Cisco UCS Manager, the client needs to send refresh requests to Cisco UCS Manager to keep the web session active. This option specifies the maximum amount of time allowed between refresh requests for a user accessing a Cisco UCS domain included in the selected Cisco UCS Central domain group. If this time limit is exceeded, Cisco UCS Manager considers the web session to be inactive, but it does not terminate the session. Specify an integer between 60 and 172800. The default is 600 seconds.
Session Timeout field	The maximum amount of time that can elapse after the last refresh request before Cisco UCS Manager considers a web session to have ended. If this time limit is exceeded, Cisco UCS Manager automatically terminates the web session. Specify an integer between 60 and 172800. The default is 7200 seconds.
Realm drop-down list	The default method by which a user is authenticated when logging remotely into a Cisco UCS domain included in the selected Cisco UCS Central domain group. This can be one of the following: • **ldap**—The user must be defined on the LDAP server specified in Cisco UCS Central. • **local**—The user account must be defined locally in Cisco UCS Central or the Cisco UCS domain. • **none**—If the user account is local to Cisco UCS Central or the Cisco UCS domain, no password is required when the user logs in remotely. • **radius**—The user must be defined on the RADIUS server specified in Cisco UCS Central. • **tacacs**—The user must be defined on the TACACS+ server specified in Cisco UCS Central.

Name	Description
Provider Group drop-down list	If the **Realm** is set to **ldap**, **radius**, or **tacacs**, this field allows you to select an associated provider group.

b) In the **Properties (Native Authentication)** dialog box, complete all **Console Authentication** fields on the **General** tab.

Name	Description
Realm field	The method by which a user logging into the console is authenticated. This can be one of the following: • **ldap**—The user must be defined on the LDAP server specified in Cisco UCS Central. • **local**—The user account must be defined locally in Cisco UCS Central or the Cisco UCS domain. • **none**—If the user account is local to Cisco UCS Central or the Cisco UCS domain, no password is required when the user logs in remotely. • **radius**—The user must be defined on the RADIUS server specified in Cisco UCS Central. • **tacacs**—The user must be defined on the TACACS+ server specified in Cisco UCS Central.
Provider Group drop-down list	If the **Realm** is set to **ldap**, **radius**, or **tacacs**, this field allows you to select an associated provider group.

c) In the **Properties (Native Authentication)** dialog box, complete **Remote Users Policy** field on the **General** tab.

Name	Description
Role Policy for Remote Users field	The action to take when a user attempts to log in and the LDAP, RADIUS, or TACACS+ server does not supply a user role with the authentication information. This can be one of the following: • **assign-default-role**—The user is allowed to log in with a read-only user role. • **no-login**—The user is not allowed to log in to the system, even if the username and password are correct.

d) Click **OK**.

Step 7 Click **Save**.

Selecting the Default 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

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **Authentication** and click **Native Authentication**.

Step 6 In the **Actions** area, click **Properties** and complete all fields.
You can also right-click **Native Authentication** to access that option.

a) In the **Properties (Native Authentication)** dialog box, complete all **Default Authentication** fields on the **General** tab.

Name	Description
Session Refresh Period field	When a web client connects to Cisco UCS Manager, the client needs to send refresh requests to Cisco UCS Manager to keep the web session active. This option specifies the maximum amount of time allowed between refresh requests for a user accessing a Cisco UCS domain included in the selected Cisco UCS Central domain group. If this time limit is exceeded, Cisco UCS Manager considers the web session to be inactive, but it does not terminate the session. Specify an integer between 60 and 172800. The default is 600 seconds.
Session Timeout field	The maximum amount of time that can elapse after the last refresh request before Cisco UCS Manager considers a web session to have ended. If this time limit is exceeded, Cisco UCS Manager automatically terminates the web session. Specify an integer between 60 and 172800. The default is 7200 seconds.

Name	Description
Realm drop-down list	The default method by which a user is authenticated when logging remotely into a Cisco UCS domain included in the selected Cisco UCS Central domain group. This can be one of the following: • **ldap**—The user must be defined on the LDAP server specified in Cisco UCS Central. • **local**—The user account must be defined locally in Cisco UCS Central or the Cisco UCS domain. • **none**—If the user account is local to Cisco UCS Central or the Cisco UCS domain, no password is required when the user logs in remotely. • **radius**—The user must be defined on the RADIUS server specified in Cisco UCS Central. • **tacacs**—The user must be defined on the TACACS+ server specified in Cisco UCS Central.
Provider Group drop-down list	If the **Realm** is set to **ldap**, **radius**, or **tacacs**, this field allows you to select an associated provider group.

b) Click **OK**.

Step 7 Click **Save**.

Role Policy for Remote Users

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

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

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

- **assign-default-role**

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

  This is the default behavior.

- **no-login**

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

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

Configuring the Role Policy for Remote Users

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **Security**.

Step 5 In the **Work** pane, expand **Authentication** and click **Native Authentication**.

Step 6 In the **Actions** area, click **Properties** and complete all fields.
You can also right-click **Native Authentication** to access that option.

a) In the **Properties (Native Authentication)** dialog box, complete **Remote Users Policy** field on the **General** tab.

Name	Description
Role Policy for Remote Users field	The action to take when a user attempts to log in and the LDAP, RADIUS, or TACACS+ server does not supply a user role with the authentication information. This can be one of the following: • **assign-default-role**—The user is allowed to log in with a read-only user role. • **no-login**—The user is not allowed to log in to the system, even if the username and password are correct.

b) Click **OK**.

Step 7 Click **Save**.

CHAPTER 6

Configuring Role-Based Access Control

This chapter includes the following sections:

- Role-Based Access Control, page 77
- User Accounts for Cisco UCS , page 77
- Configuring User Roles, page 80
- Configuring Locally Authenticated User Accounts, page 86
- Configuring User Locales, page 92
- Configuring User Domain Groups, page 97
- Configuring User Organizations, page 98
- Configuring Passwords, page 100
- Monitoring User Sessions, page 102

Role-Based Access Control

Role-Based Access Control (RBAC) is a method of restricting or authorizing system access for users based on user roles and locales. A role defines the privileges of a user in the system and the locale defines the organizations (domains) that a user is allowed access. Because users are not directly assigned privileges, management of individual user privileges is simply a matter of assigning the appropriate roles and locales.

A user is granted write access to desired system resources only if the assigned role grants the access privileges and the assigned locale allows access. For example, a user with the Server Administrator role in the Engineering organization could update server configurations in the Engineering organization but could not update server configurations in the Finance organization unless the locales assigned to the user include the Finance organization.

User Accounts for Cisco UCS

User accounts are used to access the system. Up to 128 user accounts can be configured in each Cisco UCS Central domain. Each user account must have a unique username and password.

A user account can be set with a SSH public key. The public key can be set in either of the two formats: OpenSSH and SECSH.

Admin Account

Cisco UCS Central has an admin account. The admin account is a default user account and cannot be modified or deleted. This account is the system administrator or superuser account and has full privileges. There is no default password assigned to the admin account; you must choose the password during the initial system setup.

The admin account is always active and does not expire. You cannot configure the admin account as inactive.

The local admin user is able to login for fail over, even when authentication is set to remote.

Locally Authenticated User Accounts

A locally authenticated user account is authenticated through the Cisco UCS Central user database, and can be enabled or disabled by anyone with admin or aaa privileges. Once a local user account is disabled, the user cannot log in. Configuration details for disabled local user accounts are not deleted by the database. If you re-enable a disabled local user account, the account becomes active again with the existing configuration, including username and password.

Remotely Authenticated User Accounts

A remotely authenticated user account is any Cisco UCS Central user account that is authenticated through LDAP. Cisco UCS domainssupport LDAP, RADIUS and TACACS+.

If a user maintains a local user account and a remote user account simultaneously, the roles defined in the local user account override those maintained in the remote user account.

Expiration of User Accounts

User accounts can be configured to expire at a predefined time. When the expiration time is reached, the user account is disabled.

By default, user accounts do not expire.

Note After you configure a user account with an expiration date, you cannot reconfigure the account to not expire. You can, however, configure the account with the latest expiration date available.

Guidelines for Cisco UCS Usernames

The username is also used as the login ID for Cisco UCS Central. When you assign login IDs to Cisco UCS user accounts, consider the following guidelines and restrictions:

- The login ID can contain between 1 and 32 characters, including the following:
  - Any alphabetic character
  - Any digit
  - _ (underscore)
  - - (dash)
  - . (dot)

- The login ID must be unique within Cisco UCS Central.
- The login ID must start with an alphabetic character. It cannot start with a number or a special character, such as an underscore.
- The login ID is case-sensitive.
- You cannot create an all-numeric login ID.
- After you create a user account, you cannot change the login ID. You must delete the user account and create a new one.

Reserved Words: Locally Authenticated User Accounts

The following words cannot be used when creating a local user account in Cisco UCS and Cisco UCS Central.

- root
- bin
- daemon
- adm
- ip
- sync
- shutdown
- halt
- news
- uucp
- operator
- games
- gopher
- nobody
- nscd
- mailnull
- mail
- rpcuser
- rpc
- mtsuser
- ftpuser
- ftp
- man
- sys

- samdme
- debug

Guidelines for Cisco UCS Passwords

A password is required for each locally authenticated user account. A user with admin, aaa, or domain-group-management privileges can configure Cisco UCS Central to perform a password strength check on user passwords. If the password strength check is enabled, each user must have a strong password.

Cisco recommends that each user have a strong password. If you enable the password strength check for locally authenticated users, Cisco UCS Central rejects any password that does not meet the following requirements:

- Must contain a minimum of 8 characters and a maximum of 80 characters.
- Must contain at least three of the following:
  - Lower case letters
  - Upper case letters
  - Digits
  - Special characters
- Must not contain a character that is repeated more than 3 times consecutively, such as aaabbb.
- Must not be identical to the username or the reverse of the username.
- Must pass a password dictionary check. For example, the password must not be based on a standard dictionary word.
- Must not contain the following symbols: $ (dollar sign), ? (question mark), and = (equals sign).
- Should not be blank for local user and admin accounts.

Web Session Limits for User Accounts

Cisco UCS Central does not support managing a number of concurrent web sessions at this time. We do support 32 concurrent web sessions for Cisco UCS Central users and a total of 256 concurrent sessions for all users.

Configuring User Roles

User Roles

User roles contain one or more privileges that define the operations that are allowed for a user. One or more roles can be assigned to each user. Users with multiple roles have the combined privileges of all assigned roles. For example, if Role1 has storage-related privileges, and Role2 has server-related privileges, users with Role1 and Role2 have both storage-related and server-related privileges.

A Cisco UCS domain can contain up to 48 user roles, including the default user roles. Each domain group in Cisco UCS Central can contain 48 user roles, including the user roles that are inherited from the parent domain group. When user roles are pushed to Cisco UCS Manager from Cisco UCS Central, only the first 48 roles will be active. Any user roles after the first 48 will be inactive with faults raised.

All roles include read access to all configuration settings in the Cisco UCS domain. Users with read-only roles cannot modify the system state.

Roles can be created, modified to add new or remove existing privileges, or deleted. When a role is modified, the new privileges are applied to all users that have that role. Privilege assignment is not restricted to the privileges defined for the default roles. That is, you can use a custom set of privileges to create a unique role. For example, the default Server Administrator and Storage Administrator roles have a different set of privileges, but a new Server and Storage Administrator role can be created that combines the privileges of both roles.

If a role is deleted after it has been assigned to users, it is also deleted from those user accounts.

User profiles on AAA servers (RADIUS or TACACS+) should be modified to add the roles corresponding to the privileges granted to that user. The attribute is used to store the role information. The AAA servers return this attribute with the request and parse it to get the roles. LDAP servers return the roles in the user profile attributes.

Default User Roles

The system contains the following default user roles:

AAA Administrator

Read-and-write access to users, roles, and AAA configuration. Read access to the rest of the system.

Administrator

Complete read-and-write access to the entire system. The default admin account is assigned this role by default and it cannot be changed.

Facility Manager

Read-and-write access to power management operations through the power-mgmt privilege. Read access to the rest of the system.

Network Administrator

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

Operations

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

Read-Only

Read-only access to system configuration with no privileges to modify the system state.

Server Compute

Read and write access to most aspects of service profiles. However the user cannot create, modify or delete vNICs or vHBAs.

Server Equipment Administrator

Read-and-write access to physical server related operations. Read access to the rest of the system.

Server Profile Administrator

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

Server Security Administrator

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

Storage Administrator

Read-and-write access to storage operations. Read access to the rest of the system.

Reserved Words: User Roles

The following words cannot be used when creating custom roles in Cisco UCS.

- network-admin
- network-operator
- vdc-admin
- vdc-operator
- server-admin

Privileges

Privileges give users assigned to user roles access to specific system resources and permission to perform specific tasks. The following table lists each privilege and the user role given that privilege by default.

Table 2: User Privileges

Privilege	Description	Default Role Assignment
aaa	System security and AAA	AAA Administrator
admin	System administration	Administrator
domain-group-management	Domain Group Management	Domain Group Administrator
ext-lan-config	External LAN configuration	Network Administrator
ext-lan-policy	External LAN policy	Network Administrator
ext-lan-qos	External LAN QoS	Network Administrator
ext-lan-security	External LAN security	Network Administrator
ext-san-config	External SAN configuration	Storage Administrator

Privilege	Description	Default Role Assignment
ext-san-policy	External SAN policy	Storage Administrator
ext-san-qos	External SAN QoS	Storage Administrator
ext-san-security	External SAN security	Storage Administrator
fault	Alarms and alarm policies	Operations
operations	Logs and Smart Call Home	Operations
org-management	Organization management	Operations
pod-config	Pod configuration	Network Administrator
pod-policy	Pod policy	Network Administrator
pod-qos	Pod QoS	Network Administrator
pod-security	Pod security	Network Administrator
power-mgmt	Read-and-write access to power management operations	Facility Manager
read-only	Read-only access Read-only cannot be selected as a privilege; it is assigned to every user role.	Read-Only
server-equipment	Server hardware management	Server Equipment Administrator
server-maintenance	Server maintenance	Server Equipment Administrator
server-policy	Server policy	Server Equipment Administrator
server-security	Server security	Server Security Administrator
service-profile-compute	Service profile compute	Server Compute Administrator
service-profile-config	Service profile configuration	Server Profile Administrator
service-profile-config-policy	Service profile configuration policy	Server Profile Administrator
service-profile-ext-access	Service profile end point access	Server Profile Administrator
service-profile-network	Service profile network	Network Administrator
service-profile-network-policy	Service profile network policy	Network Administrator

Privilege	Description	Default Role Assignment
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

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane select a domain group for the user role.

a) Expand the **Domain Groups** node.

b) Expand the **Domain Groups root** node.

Step 3 Under the **Domain Groups** node, do one of the following choices:

- Click **Operational Policies**.
- Expand a **Domain Group** node and click **Operational Policies**.

Step 4 In the **Work** pane navigate to **Roles**.

a) Click **Security**.

b) Expand the **User Services** node.

c) Click **Roles**.

Step 5 Click **Create Role**.
You can also right-click **Roles** to access that option.

Step 6 In the **Create Role** dialog box, enter the **Name** to assign the role.

Step 7 Select all **Privileges** for the role.

Step 8 Click **OK**.

Deleting a User Role

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane select a domain group for the user role.

a) Expand the **Domain Groups** node.

b) Expand the **Domain Groups root** node.

Step 3 Under the **Domain Groups** node, do one of the following choices:

- Click **Operational Policies**.
- Expand a **Domain Group** node and click **Operational Policies**.

Step 4 In the **Work** pane display all roles.

a) Click **Security**.

b) Expand the **User Services** node.

c) Expand the **Roles** node.

Step 5 Click the role which you want to delete.

Step 6 Click **Delete**.

You can also right-click a **Role** to access that option.

Step 7 In the **Confirm** dialog box, click **Yes**.

Adding Privileges to a User Role

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane select a domain group for the user role.

a) Expand the **Domain Groups** node.

b) Expand the **Domain Groups root** node.

Step 3 Under the **Domain Groups** node, do one of the following choices:

- Click **Operational Policies**.
- Expand a **Domain Group** node and click **Operational Policies**.

Step 4 In the **Work** pane display all roles.

a) Click **Security**.

b) Expand the **User Services** node.

c) Expand the **Roles** node.

Step 5 Choose the role to which you want to add privileges.

Step 6 Click **Properties**.
You can also right-click a **Role** to access that option.

Step 7 In the **Properties** dialog box, check the boxes for the privileges you want to add to the role.

Step 8 Click **Save Changes**.

Removing Privileges from a User Role

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane select a domain group for the user role.
a) Expand the **Domain Groups** node.
b) Expand the **Domain Groups root** node.

Step 3 Under the **Domain Groups** node, do one of the following choices:

- Click **Operational Policies**.
- Expand a **Domain Group** node and click **Operational Policies**.

Step 4 In the **Work** pane display all roles.
a) Click **Security**.
b) Expand the **User Services** node.
c) Expand the **Roles** node.

Step 5 Choose the role from which you want to remove privileges.

Step 6 Click **Properties**.
You can also right-click a **Role** to access that option.

Step 7 In the **Properties** dialog box, uncheck the boxes for the privileges you want to remove from the role.

Step 8 Click **Save Changes**.

Configuring Locally Authenticated User Accounts

Creating a Locally Authenticated User Account

At a minimum, we recommend that you create the following users:

- Server administrator account

- Network administrator account
- Storage administrator

Before You Begin

Perform the following tasks, if the system includes any of the following:

- Remote authentication services, ensure the users exist in the remote authentication server with the appropriate roles and privileges.
- Multi-tenancy with organizations, create one or more locales. If you do not have any locales, all users are created in root and are assigned roles and privileges in all organizations.
- SSH authentication, obtain the SSH key.

Procedure

Step 1 On the menu bar, click **Administration**.

Step 2 In the **Navigation** pane, click the **Access Control** tab.

Step 3 On the **Access Control** tab, click **Locally Authenticated Users**.

Step 4 Click **Create Locally Authenticated User**.

Step 5 In the **Create Locally Authenticated User** dialog box, complete the following fields:

Name	Description
Login ID field	The username for the local Cisco UCS Central user. Login IDs must meet the following the following 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.

Name	Description
Description field	The description of the user account. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), and ' (single quote).
First Name field	The first name of the user. Enter up to 32 characters or spaces.
Last Name field	The last name of the user. Enter up to 32 characters or spaces.
Email field	The email address for the user.
Phone field	The telephone number for the user.
Password field	The password associated with this account. If password strength check is enabled, a user's password must be strong. Strong passwords must meet the following requirements: • Must contain a minimum of 8 characters and a maximum of 80 characters. • Must contain at least three of the following: ◦ Lower case letters ◦ Upper case letters ◦ Digits ◦ Special characters • Must not contain a character that is repeated more than 3 times consecutively, such as aaabbb. • Must not be identical to the username or the reverse of the username. • Must pass a password dictionary check. For example, the password must not be based on a standard dictionary word. • Must not contain the following symbols: $ (dollar sign), ? (question mark), and = (equals sign). • Should not be blank for local user and admin accounts.
Set field	Whether the password has been set for this user.
Confirm Password field	The password a second time for confirmation purposes.

Name	Description
Account Expiration check box	If checked, this account expires and cannot be used after the date specified in the **Expiration Date** field.
Account Status drop-down list	If the status is set to **Active**, a user can log into Cisco UCS Central with this login ID and password.
Expiration Date field	The date on which the account expires. The date should be in the format mm/dd/yyyy. Click the calendar icon at the end of this field to view a calendar that you can use to select the expiration date.

Step 6 In the **Create Locally Authenticated User** dialog box, click the **Roles/Locales** tab and complete the following fields:

Name	Description
Assigned Roles list box	A list of the user roles defined in Cisco UCS Central. If the associated check box is checked, the selected user has been assigned that user role.
Assigned Locales list box	A list of the locales defined in Cisco UCS Central. If the associated check box is checked, the selected user has been assigned that locale.

Step 7 (Optional) If the system includes organizations, check one or more check boxes in the **Assigned Role(s)** pane to assign the user to the appropriate locales.

Note Do not assign locales to users with an admin role.

Step 8 In the **Create Locally Authenticated User** dialog box, click the **SSH** tab and complete the following fields:

Name	Description
Type field	This can be one of the following: • **Key**—SSH encryption is used when this user logs in. • **Password**—The user must enter a password when they log in.
SSH Data field	If **Type** is set to **Key**, this field contains the associated SSH key.

Step 9 Click **OK**.

Deleting a Locally Authenticated User Account

Procedure

Step 1 On the menu bar, click **Administration**.

Step 2 In the **Navigation** pane, click the **Access Control** tab.

Step 3 On the **Access Control** tab, expand **Locally Authenticated Users**.

Step 4 Right-click the **User** you want to delete, and choose **Delete**.

Step 5 In the **Confirm** dialog box, click **Yes**.

Changing the Roles Assigned to a Locally Authenticated 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

Step 1 On the menu bar, click **Administration**.

Step 2 In the **Navigation** pane, click the **Access Control** tab.

Step 3 On the **Access Control** tab, expand **Locally Authenticated Users**.

Step 4 Click the user account that you want to modify.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the **Work** pane, click the **Roles/Locales** tab.

Step 7 In the **Assigned Role(s)** area, assign and remove roles.

- To assign a new role to the user account, check the appropriate check boxes.
- To remove a role from the user account, uncheck the appropriate check boxes.

Step 8 Click **Save**.

Enabling the Password Strength Check for Locally Authenticated Users

You must be a user with admin, aaa, or domain-group-management privileges to enable the password strength check. If the password strength check is enabled, Cisco UCS Central does not permit a user to choose a password that does not meet the guidelines for a strong password.

Procedure

Step 1 On the menu bar, click **Administration**.

Step 2 In the **Navigation** pane, click the **Access Control** tab.

Step 3 On the **Access Control** tab, click **Locally Authenticated Users**.

Step 4 In the **Work** pane, check the **Password Strength Check** check box in the **Properties** area.

Step 5 Click **Save**.

Clearing the Password History for a Locally Authenticated User

You must have admin, aaa, or domain-group-management privileges to change the password profile properties.

Procedure

Step 1 On the menu bar, click **Administration**.

Step 2 In the **Navigation** pane, click the **Access Control** tab.

Step 3 On the **Access Control** tab, click **Locally Authenticated Users**.

Step 4 In the **Password Profile** area, enter 0 for the number of unique passwords that a locally authenticated user must create before that user can reuse a previously used password in the **History Count** field.
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 5 Click **Save**.

Enabling a Locally Authenticated User Account

You must be a user with admin, aaa, or domain-group-management privileges to enable or disable a local user account.

Before You Begin

Create a local user account.

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click the **Access Control** tab.
Step 3 On the **Access Control** tab, expand **Locally Authenticated Users**.
Step 4 Click the user account that you want to modify.
Step 5 In the **Work** pane, click the **General** tab.
Step 6 In the **Account Status** field, click the **active** radio button.
Step 7 Click **Save**.

Disabling a Locally Authenticated User Account

You must be a user with admin, aaa, or domain-group-management privileges to enable or disable a local user account.

Note If you change the password on a disabled account through the Cisco UCS Central GUI, the user cannot use this changed password after you enable the account and make it active. The user must enter the required password again after the account is enabled and made active.

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click the **Access Control** tab.
Step 3 On the **Access Control** tab, expand **Locally Authenticated Users**.
Step 4 Click the user account that you want to modify.
Step 5 In the **Work** pane, click the **General** tab.
Step 6 In the **Account Status** field, click the **inactive** radio button.
The admin user account is always set to active. It cannot be modified.
Step 7 Click **Save**.

Configuring User Locales

User Locales

A user can be assigned one or more locales. Each locale defines one or more organizations (domains) the user is allowed access, and access would be limited to the organizations specified in the locale. One exception to

this rule is a locale without any organizations, which gives unrestricted access to system resources in all organizations.

A Cisco UCS domain can contain up to 48 user locales. Each domain group in Cisco UCS Central can contain 48 user locales, including the user locales that are inherited from the parent domain group. When user locales are pushed to Cisco UCS Manager from Cisco UCS Central, only the first 48 locales will be active. Any user locales after the first 48 will be inactive with faults raised.

Users with admin, aaa, or domain-group-management privileges can assign organizations to the locale of other users.

Note You cannot assign a locale to users with the admin privilege.

You can hierarchically manage organizations. A user that is assigned at a top level organization has automatic access to all organizations under it. For example, an Engineering organization can contain a Software Engineering organization and a Hardware Engineering organization. A locale containing only the Software Engineering organization has access to system resources only within that organization; however, a locale that contains the Engineering organization has access to the resources for both the Software Engineering and Hardware Engineering organizations.

Creating a User Locale

Before You Begin

One or more organizations must exist before you create a locale.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane select a domain group for the locale.

a) Expand the **Domain Groups** node.
b) Expand the **Domain Groups root** node.

Step 3 Under the **Domain Groups** node, do one of the following:

- Click **Operational Policies**.
- Expand a **Domain Group** node and click **Operational Policies**.

Step 4 In the **Work** pane navigate to **Locales**.

a) Click **Security**.
b) Expand the **User Services** node.
c) Click **Locales**.

Step 5 Click **Create Locales**.
You can also right-click **Locales** to access that option.

Step 6 In the **Create Locale** dialog box enter requested information.

a) In the **Name** field, enter a unique name for the locale.

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.

b) In the **Description** field, enter a description for the locale.

Step 7 Click **Filter**.

Step 8 In the **Table Filter** dialog box enter requested information.

a) Choose the **Assigned Organization** filter.

b) Enter the **Assigned Organization** filter value.

Step 9 Click **OK**.

Step 10 Click **Assign Organization**.

Step 11 In the **Assign Organizations** dialog box assign the organization to the locale.

a) Expand the **Organizations** area to view the organizations in the Cisco UCS domain.

b) Expand the **root** node to see the sub-organizations.

c) Click an organization that you want to assign to the locale.

d) Drag the organization from the **Organizations** area and drop it into the design area on the right.

e) Repeat Steps b and c until you have assigned all desired organizations to the locale.

Step 12 Click **OK** to assign organization.

Step 13 Click **OK** to create locale.

Deleting a User Locale

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane select a domain group for the locale.

a) Expand the **Domain Groups** node.

b) Expand the **Domain Groups root** node.

Step 3 Under the **Domain Groups** node, do one of the following:

- Click **Operational Policies**.
- Expand a **Domain Group** node and click **Operational Policies**.

Step 4 In the **Work** pane display all locales.

a) Click **Security**.

b) Expand the **User Services** node.

c) Expand the **Locales** node.

Step 5 Click the locale which you want to delete.

Step 6 Click **Delete**.

You can also right-click a **Locale** you want to delete to access that option.

Step 7 In the **Confirm** dialog box, click **Yes**.

Assigning an Organization to a User Locale

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane select a domain group for the locale.

a) Expand the **Domain Groups** node.
b) Expand the **Domain Groups root** node.

Step 3 Under the **Domain Groups** node, do one of the following:

- Click **Operational Policies**.
- Expand a **Domain Group** node and click **Operational Policies**.

Step 4 In the **Work** pane select a locale.

a) Click **Security**.
b) Expand the **User Services** node.
c) Expand the **Locales** node.

Step 5 Click the locale to which you want to add an organization.

Step 6 Click **Assign Organization**.
You can also right-click the **Locale** to access that option.

Step 7 In the **Assign Organizations** dialog box enter the **Organization**.

Step 8 Click **OK**.

Deleting an Organization from a User Locale

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane select a domain group for the locale.

a) Expand the **Domain Groups** node.
b) Expand the **Domain Groups root** node.

Step 3 Under the **Domain Groups** node, do one of the following:

- Click **Operational Policies**.

- Expand a **Domain Group** node and click **Operational Policies**.

Step 4 In the **Work** pane display all locales.
a) Click **Security**.
b) Expand the **User Services** node.
c) Expand the **Locales** node.

Step 5 Click the locale with an assigned organization you want to delete.

Step 6 Click **Properties**.

Step 7 In the **Work** pane, click the **Organization** you want to delete.

Step 8 Click **Delete**.
You can also right-click an **Organization** you want to delete to access that option.

Step 9 In the **Confirm** dialog box, click **Yes**.

Changing the Locales Assigned to a Locally Authenticated User Account

Note Do not assign locales to users with an admin role.

Procedure

Step 1 On the menu bar, click **Administration**.

Step 2 In the **Navigation** pane, click the **Access Control** tab.

Step 3 On the **Access Control** tab, expand **Locally Authenticated Users**.

Step 4 Click the user account that you want to modify.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the **Work** pane, click the **Roles/Locales** tab.

Step 7 In the **Assigned Locale(s)** area, assign and remove locales.

- To assign a new locale to the user account, check the appropriate check boxes.
- To remove a locale from the user account, uncheck the appropriate check boxes.

Step 8 Click **Save**.

Configuring User Domain Groups

Creating a User Domain Group

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, click **Domain Groups** and do one of the following choices:

- In the **Domain Groups** pane under the **Name** column, click a **Domain Group** and click **Create Domain Group**.
- In the **Navigation** pane, click **Domain Groups root** and click **Create Domain Group**.
- In the **Navigation** pane, expand the **Domain Groups root** node, click a **Domain Group** and click **Create Domain Group**.

Step 3 In the **Create Domain Group** dialog box enter requested information.

a) In the **Name** field, enter a unique name for the domain group.
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.

b) In the **Description** field, enter a description for the domain group.

Step 4 Click **OK** to create domain group.

Deleting a User Domain Group

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, click **Domain Groups**.

Step 3 In the **Domain Groups** pane under the **Name** column, click the **Domain Group** you want to delete.

Step 4 Click **Delete**.
You can also right-click the **Domain Group** you want to delete to access that option.

Note You cannot delete the domain group root.

Step 5 In the **Confirm** dialog box, click **Yes**.

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

Step 1 On the menu bar, click **Servers**.

Step 2 In the **Navigation** pane create an organization.

a) Expand the **Pools** node.

b) Click **root**.

c) In the **Work** pane, click **Create Organization**.

Step 3 In the **Create Organization** dialog box enter requested information.

a) In the **Name** field, enter a unique name for the organization.
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.

b) In the **Description** field, enter a description for the organization.

Step 4 Click **OK** to create an organization.

Deleting a User Organization

Procedure

Step 1 On the menu bar, click **Servers**.

Step 2 In the **Navigation** pane select an organization.

a) Expand the **Pools** node.

b) Expand the **root** node.

c) Click **Sub-Organizations**.

d) In the **Sub-Organizations** pane, click the **Organization** you want to delete.

Step 3 Click **Delete**.
You can also right-click the **Organization** you want to delete to access that option.

Step 4 In the **Confirm** dialog box, click **Yes**.

Creating a User Sub-Organization

Procedure

Step 1 On the menu bar, click **Servers**.

Step 2 In the **Navigation** pane create a sub-organization.

a) Expand the **Pools** node.
b) Expand the **root** node.
c) Click **Sub-Organizations**.

Step 3 In the **Sub-Organizations** pane, click applicable assigned organization name.

Step 4 In the **Work** pane, click **Create Organization**.

Step 5 In the **Create Organization** dialog box enter requested information.

a) In the **Name** field, enter a unique name for the organization.
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.

b) In the **Description** field, enter a description for the organization.

Step 6 Click **OK** to create a sub-organization.

Deleting a User Sub-Organization

Procedure

Step 1 On the menu bar, click **Servers**.

Step 2 In the **Navigation** pane select an organization.

a) Expand the **Pools** node.
b) Expand the **root** node.
c) Click **Sub-Organizations**.
d) In the **Sub-Organizations** pane, expand applicable assigned organization node.
e) In the **Sub-Organizations** pane, click the **Organization** you want to delete.
Expand applicable assigned organization nodes until reaching the applicable organization name.

Step 3 Click **Delete**.
You can also expand the **Organizations** until reaching the target you want to delete, and right-click an **Organization** to access that option.

Step 4 In the **Confirm** dialog box, click **Yes**.

Configuring Passwords

Password Profile for Locally Authenticated Users

The password profile contains the password history and password change interval properties for all locally authenticated users of Cisco UCS Central. You cannot specify a different password profile for each locally authenticated user.

Note You must have admin, aaa, or domain-group-management privileges to change the password profile properties. Except for password history, these properties do not apply to users with these administrative privileges.

Password History Count

The password history count allows you to prevent locally authenticated users from reusing the same password over and over again. When this property is configured, Cisco UCS Central stores passwords that were previously used by locally authenticated users up to a maximum of 15 passwords. The passwords are stored in reverse chronological order with the most recent password first to ensure that the only the oldest password can be reused when the history count threshold is reached.

A user must create and use the number of passwords configured in the password history count before being able to reuse one. For example, if you set the password history count to 8, a locally authenticated user cannot reuse the first password until after the ninth password has expired.

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

If necessary, you can clear the password history count for a locally authenticated user and enable reuse of previous passwords.

Password Change Interval

The password change interval enables you to restrict the number of password changes a locally authenticated user can make within a given number of hours. The following table describes the two configuration options for the password change interval.

Interval Configuration	Description	Example
No password change allowed	This option does not allow passwords for locally authenticated users to be changed within a specified number of hours after a password change. You can specify a no change interval between 1 and 745 hours. By default, the no change interval is 24 hours.	For example, to prevent passwords from being changed within 48 hours after a locally authenticated user changes his or her password, set the following: • Change during interval to disable • No change interval to 48

Interval Configuration	Description	Example
Password changes allowed within change interval	This option specifies the maximum number of times that passwords for locally authenticated users can be changed within a pre-defined interval. You can specify a change interval between 1 and 745 hours and a maximum number of password changes between 0 and 10. By default, a locally authenticated user is permitted a maximum of 2 password changes within a 48 hour interval.	For example, to allow to be changed a maximum of once within 24 hours after a locally authenticated user changes his or her password, set the following: • Change during interval to enable • Change count to 1 • Change interval to 24

Configuring the Maximum Number of Password Changes for a Change Interval

You must have admin or aaa privileges to change the password profile properties. Except for password history, these properties do not apply to users with admin or aaa privileges.

Procedure

Step 1 On the menu bar, click **Administration**.

Step 2 In the **Navigation** pane, click the **Access Control** tab.

Step 3 On the **Access Control** tab, click **Locally Authenticated Users**.

Step 4 In the **Password Profile** area complete all fields.

a) In the **Change During Interval** field, click **Enable**.

b) In the **Change Interval** field, enter 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.

c) In the **Change Count** field, enter 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 5 Click **Save**.

Configuring a No Change Interval for Passwords

You must have admin or aaa privileges to change the password profile properties. Except for password history, these properties do not apply to users with admin or aaa privileges.

Procedure

Step 1 On the menu bar, click **Administration**.

Step 2 In the **Navigation** pane, click the **Access Control** tab.

Step 3 On the **Access Control** tab, click **Locally Authenticated Users**.

Step 4 In the **Password Profile** area complete all fields.

a) In the **Change During Interval** field, click **Disable**.

b) In the **No Change Interval** field, enter the minimum number of hours that a locally authenticated user must wait before changing a newly created password.
This value can be anywhere from 1 to 745 hours.

This interval is ignored if the **Change During Interval** property is not set to **Disable**.

Step 5 Click **Save**.

Configuring the Password History Count

You must have admin or aaa privileges to change the password profile properties.

Procedure

Step 1 On the menu bar, click **Administration**.

Step 2 In the **Navigation** pane, click the **Access Control** tab.

Step 3 On the **Access Control** tab, click **Locally Authenticated Users**.

Step 4 In the **Password Profile** area, enter the number of unique passwords that a locally authenticated user must create before that user can reuse a previously used password in the **History Count** field.
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 5 Click **Save**.

Monitoring User Sessions

You can monitor Cisco UCS Central sessions for both locally authenticated users and remotely authenticated users, whether they logged in through the CLI or the GUI.

Procedure

Step 1 On the menu bar, click **Administration**.

Step 2 On the **Access Control** tab, click **Locally Authenticated Users** or **Remotely Authenticated Users**.

Step 3 In the **Navigation** pane, user sessions are monitored under **Locally Authenticated Users** for all users or each user.

- In the **Navigation** pane, click **Locally Authenticated Users** to monitor all user sessions.
- In the **Navigation** pane, expand the **Locally Authenticated Users** node and click a user name to monitor that individual user.

Step 4 In the **Work** pane, click the **Sessions** tab.
The tab displays the following details of user sessions:

Name	Description
Filter button	Allows you to filter the data in the table. When you apply a filter, this button name changes to **Filter (on)**.
Terminate Session button	Ends the selected user session.
Host column	The IP address from which the user logged in.
Login Time column	The date and time at which the user logged in.
Terminal Type column	The type of terminal from which the user logged in.
Current Session column	Whether the session is currently active.

CHAPTER 7

Configuring DNS Servers

This chapter includes the following sections:

- DNS Policies, page 105
- Configuring a DNS Policy, page 105
- Deleting a DNS Policy, page 106
- Configuring a DNS Server for a DNS Policy, page 107
- Deleting a DNS Server from a DNS Policy, page 108

DNS Policies

Cisco UCS Central supports global DNS policies defining the DNS server. 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

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.

- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **DNS**.

Step 6 In the **Actions** area, click **Create** and complete all applicable fields.
For **Operational Policies** under the **Domain Group root** node, it is not necessary to click **Create** to complete all applicable fields.

Name	Description
Create button	Creates an instance of the policy that will be used by all Cisco UCS domains included in the selected domain group.
Import button	Allows you to import the policy from one of the Cisco UCS domains registered with Cisco UCS Central.
Delete button	Deletes the instance of the policy defined for the selected domain group. After you delete the policy, it remains greyed-out until you click **Save**. When you do so, Cisco UCS Central deletes the policy and any configuration data you may have specified. While you can create a new instance of the policy later, you cannot restore the configuration data from a deleted instance. To cancel the delete request, click **Reset**.
Domain field	The domain name associated with the Domain Name Server (DNS) server.
Filter button	Allows you to filter the data in the table. When you apply a filter, this button name changes to **Filter (on)**.
Add DNS Server button	Allows you to add a DNS to the selected domain group.
Properties button	Displays detailed properties for the object selected in the table.
Delete button	Deletes the object selected in the table.
DNS IP column	The IP address of the DNS server.

Step 7 Click **Save**.

Deleting a DNS Policy

Deleting a DNS policy will remove all DNS server settings within that policy.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **DNS**.

Step 6 In the **Actions** area, click **Delete**.
A policy that is deleted will inherit its settings from its domain group's parent until it is reconfigured.

Step 7 Click **Save**.

Configuring a DNS Server for a DNS Policy

Before You Begin

Configure a DNS policy.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **DNS**.

Step 5 In the **Actions** area, click **Add DNS Server** and complete all fields.

a) In the **Add DNS Server** dialog box, complete all fields.

Name	Description
DNS Server field	The IP address of the DNS server you want to use.

b) Click **OK**.

Step 6 Click **Save**.

Deleting a DNS Server from a DNS Policy

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **DNS**.

Step 5 In the **Actions** area, select the DNS server to delete and click **Delete**.
You can also right-click the DNS server to access that option.

Step 6 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Step 7 Click **Save**.

PART III

Network Configuration

- Configuring MAC Pools, page 111

CHAPTER 8

Configuring MAC Pools

This chapter includes the following sections:

- MAC Pools, page 111
- Creating a MAC Pool, page 111
- Deleting a MAC Pool, page 112

MAC Pools

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

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

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

You can specify your own MAC addresses or use a group of MAC addresses provided by Cisco.

Creating a MAC Pool

Procedure

Step 1 On the menu bar, click **Network**.

Step 2 In the **Network** tab, expand **Network** > **Pools** > **Root**.
If you want to create or access a pool in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***

Step 3 Right-click **MAC Pools** and select **Create MAC Pool**.

Step 4 In the **General** tab of the **Create MAC Pool** dialog box, fill in the following fields:

Name	Description
Name field	The name of the MAC address pool. 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.
Description field	The user-defined description of the pool. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), and ' (single quote).

Step 5 In the **MAC Blocks** tab of the **Create MAC Pool** dialog box, click **Create a Block of MAC Addresses**.

Step 6 In the **Create a Block of MAC Addresses** dialog box, fill in the following fields:

Name	Description
From field	The first MAC address in the block.
Size field	The number of MAC addresses in the block.

Step 7 Click **OK**.

Step 8 Click **OK**.

Note If you plan to create another pool, wait at least 5 seconds.

What to Do Next

Include the MAC pool in a vNIC template.

Deleting a MAC Pool

If you delete a pool, Cisco UCS Central does not reallocate any addresses from that pool that have been assigned to vNICs or vHBAs in Cisco UCS Manager. All assigned addresses from a deleted pool remain with the vNIC or vHBA to which they are assigned until one of the following occurs:

- The associated service profiles are deleted.
- The vNIC or vHBA to which the address is assigned is deleted.
- The vNIC or vHBA is assigned to a different pool.

Procedure

Step 1 On the menu bar, click **Network**.

Step 2 In the **Network** tab, expand **Network** > **Pools** > **Root**.
If you want to create or access a pool in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***

Step 3 Expand the **MAC Pools** node.

Step 4 Right-click the pool you want to delete and select **Delete**.

Note If you plan to delete another pool, wait at least 5 seconds.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

PART IV

Storage Configuration

- Configuring WWN Pools, page 117

CHAPTER 9

Configuring WWN Pools

This chapter includes the following sections:

- WWN Pools, page 117
- Creating a WWN Pool, page 118
- Deleting a WWN Pool, page 119

WWN Pools

A WWN pool is a collection of WWNs for use by the Fibre Channel vHBAs in a Cisco UCS domain. WWN pools created in Cisco UCS Central can be shared between Cisco UCS domains. You create separate pools for the following:

- WW node names assigned to the server
- WW port names assigned to the vHBA
- Both WW node names and WW port names

Important A WWN pool can include only WWNNs or WWPNs in the ranges from 20:00:00:00:00:00:00:00 to 20:FF:FF:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00:00 to 5F:FF:FF:FF:FF:FF:FF:FF. All other WWN ranges are reserved. To ensure the uniqueness of the Cisco UCS WWNNs and WWPNs in the SAN fabric, we recommend that you use the following WWN prefix for all blocks in a pool: 20:00:00:25:B5:XX:XX:XX

If you use WWN pools in service profiles, you do not have to manually configure the WWNs that will be used by the server associated with the service profile. In a system that implements multi-tenancy, you can use a WWN pool to control the WWNs used by each organization.

You assign WWNs to pools in blocks.

WWNN Pools

A WWNN pool is a WWN pool that contains only WW node names. If you include a pool of WWNNs in a service profile, the associated server is assigned a WWNN from that pool.

WWPN Pools

A WWPN pool is a WWN pool that contains only WW port names. If you include a pool of WWPNs in a service profile, the port on each vHBA of the associated server is assigned a WWPN from that pool.

WWxN Pools

A WWxN pool is a WWN pool that contains both WW node names and WW port names. You can specify how many ports per node are created with WWxN pools. The pool size for WWxN pools must be a multiple of *ports-per-node* + 1. For example, if there are 7 ports per node, the pool size must be a multiple of 8. If there are 63 ports per node, the pool size must be a multiple of 64.

Creating a WWN Pool

Procedure

Step 1 On the menu bar, click **Storage**.

Step 2 In the **Storage** tab, expand **Storage** > **Pools** > **Root**.
If you want to create or access a pool in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***

Step 3 Right-click **WWN Pools** and select **Create WWN Pool**.

Step 4 In the **General** tab of the **Create WWN Pool** dialog box, fill in the following fields:

Name	Description
Name field	The name of the WWN pool. 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.
Description field	The user-defined description of the pool. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), and ' (single quote).
Purpose drop-down list	This can be one of the following: • **Node and Port Wwn Assignment**—The pool is used for both World Wide Node Names (WWNNs) and World Wide Port Names (WWPNs). • **Node Wwn Assignment**—The pool is used for WWNNs. • **Port Wwn Assignment**—The pool is used for WWPNs. This option cannot be changed after the pool has been saved.

Name	Description
Max Ports per Node field	The maximum number of ports that can be assigned to each node name in this pool. **Note** This field is only available if **Purpose** is set to **Node and Port Wwn Assignment**. This option cannot be changed after the pool has been saved.

Step 5 In the **WWN Initiator Blocks** tab of the **Create WWN Pool** dialog box, click **Create Block**.

Step 6 In the **Create Block** dialog box, fill in the following fields:

Name	Description
From field	The first WWN in the block.
Size field	The number of WWNs in the block. For WWxN pools, the pool size 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.

Step 7 Click **OK**.

Step 8 Click **OK**.

Note If you plan to create another pool, wait at least 5 seconds.

What to Do Next

- Include the WWPN pool in a vHBA template.
- Include the WWNN pool in a service profile and/or template.
- Include the WWxN pool in a service profile and/or template.

Deleting a WWN Pool

If you delete a pool, Cisco UCS Central does not reallocate any addresses from that pool that have been assigned to vNICs or vHBAs in Cisco UCS Manager. All assigned addresses from a deleted pool remain with the vNIC or vHBA to which they are assigned until one of the following occurs:

- The associated service profiles are deleted.
- The vNIC or vHBA to which the address is assigned is deleted.
- The vNIC or vHBA is assigned to a different pool.

Procedure

Step 1 On the menu bar, click **Storage**.

Step 2 In the **Storage** tab, expand **Storage** > **Pools** > **Root**.
If you want to create or access a pool in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***

Step 3 Expand the **WWN Pools** node.

Step 4 Right-click the pool you want to delete and select **Delete**.

Note If you plan to delete another pool, wait at least 5 seconds.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

PART V

Server Configuration

- Configuring Server-Related Pools, page 123
- Managing Power in Cisco UCS, page 131

CHAPTER 10

Configuring Server-Related Pools

This chapter includes the following sections:

- Configuring IP Pools, page 123
- Configuring IQN Pools, page 126
- Configuring UUID Suffix Pools, page 128

Configuring IP Pools

IP Pools

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

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

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

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

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

Cisco UCS Central creates public IP pools by default.

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

Creating an IP Pool

Procedure

Step 1 On the menu bar, click **Network**.

Step 2 In the **Network** tab, expand **Network** > **Pools** > **Root**.
If you want to create or access a pool in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***

Step 3 Right-click **IP Pools** and select **Create IP Pool**.

Step 4 In the **General** tab of the **Create IP Pool** dialog box, fill in the following fields:

Name	Description
Name field	The name of the IP pool. 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.
Description field	The user-defined description of the pool. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), and ' (single quote).

Step 5 In the **IP Blocks** tab of the **Create IP Pool** dialog box, click **Create a Block of IP Addresses**.

Step 6 In the **Create a Block of IP** dialog box, fill in the following fields:

Name	Description
From field	The first IP address in the block.
Size field	The number of IP addresses in the block.
Subnet field	The subnet mask associated with the IP addresses in the block.
Default Gateway field	The default gateway associated with the IP addresses in the block.
Primary DNS field	The primary DNS server that this block of IP addresses should access.
Secondary DNS field	The secondary DNS server that this block of IP addresses should access.

Name	Description
Scope drop-down list	Whether the IP addresses in the block can be assigned to one or more Cisco UCS domains registered with Cisco UCS Central. This can be one of the following: • **public**—The IP addresses in the block can be assigned to one and only one registered Cisco UCS domain. • **private**—The IP addresses in the block can be assigned to multiple registered Cisco UCS domains. **Note** If any of the IP addresses in the block are already defined in one or more existing IP pools, Cisco UCS Central ignores the value in this field and sets the scope of all addresses in the block to the scope originally assigned to the existing IP addresses.

Step 7 Click **OK**.

Step 8 Click **OK**.

Note If you plan to create another pool, wait at least 5 seconds.

What to Do Next

Include the IP pool in a service profile and/or template.

Deleting an IP Pool

If you delete a pool, Cisco UCS Central does not reallocate any addresses from that pool that have been assigned to vNICs or vHBAs in Cisco UCS Manager. All assigned addresses from a deleted pool remain with the vNIC or vHBA to which they are assigned until one of the following occurs:

- The associated service profiles are deleted.
- The vNIC or vHBA to which the address is assigned is deleted.
- The vNIC or vHBA is assigned to a different pool.

Procedure

Step 1 On the menu bar, click **Network**.

Step 2 In the **Network** tab, expand **Network** > **Pools** > **Root**.
If you want to create or access a pool in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***

Step 3 Expand the **IP Pools** node.

Step 4 Right-click the pool you want to delete and select **Delete**.

Note If you plan to delete another pool, wait at least 5 seconds.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Configuring IQN Pools

IQN Pools

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

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

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

Creating an IQN Pool

Note In most cases, the maximum IQN size (prefix + suffix + additional characters) is 223 characters. When using the Cisco UCS NIC M51KR-B adapter, you must limit the IQN size to 128 characters.

Procedure

Step 1 On the menu bar, click **Storage**.

Step 2 In the **Storage** tab, expand **Storage** > **Pools** > **Root**.
If you want to create or access a pool in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***

Step 3 Right-click **IQN Pools** and select **Create IQN Pool**.

Step 4 In the **General** tab of the **Create IQN Pool** dialog box, fill in the following fields:

Name	Description
Name field	The name of the iSCSI Qualified Name (IQN) pool. 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.
Description field	The user-defined description of the pool. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), and ' (single quote).

Name	Description
Prefix field	The prefix for any IQN blocks created for this pool. Unless limited by the adapter card, the prefix can contain from 1 to 150 characters. You can use any letter or number, as well as the special characters . (period), : (colon), and - (hyphen). For example, you could use iqn1.alpha.com.

Step 5 In the **IQN Blocks** tab of the **Create IQN Pool** dialog box, click **Create a Block of IQN Suffixes**.

Step 6 In the **Create a Block of IQN** dialog box, fill in the following fields:

Name	Description
From field	The first iSCSI Qualified Name (IQN) suffix in the block.
Size field	The number of suffixes in the block.
Suffix field	The suffix for this block of IQNs. Enter from 1 to 64 characters. You can use any letter or number, as well as the special characters . (period), : (colon), and - (hyphen). For example, you could use alphadc-1.

Step 7 Click **OK**.

Step 8 Click **OK**.

Note If you plan to create another pool, wait at least 5 seconds.

What to Do Next

Include the IQN suffix pool in a service profile and/or template.

Deleting an IQN Pool

If you delete a pool, Cisco UCS Central does not reallocate any addresses from that pool that have been assigned to vNICs or vHBAs in Cisco UCS Manager. All assigned addresses from a deleted pool remain with the vNIC or vHBA to which they are assigned until one of the following occurs:

- The associated service profiles are deleted.
- The vNIC or vHBA to which the address is assigned is deleted.
- The vNIC or vHBA is assigned to a different pool.

Procedure

Step 1 On the menu bar, click **Storage**.

Step 2 In the **Storage** tab, expand **Storage** > **Pools** > **Root**.
If you want to create or access a pool in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***

Step 3 Expand the **IQN Pools** node.

Step 4 Right-click the pool you want to delete and select **Delete**.
Note If you plan to delete another pool, wait at least 5 seconds.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Configuring UUID Suffix Pools

UUID Suffix Pools

A UUID suffix pool is a collection of SMBIOS UUIDs that are available to be assigned to servers. The first number of digits that constitute the prefix of the UUID are fixed. The remaining digits, the UUID suffix, are variable. A UUID suffix pool ensures that these variable values are unique for each server associated with a service profile which uses that particular pool to avoid conflicts.

If you use UUID suffix pools in service profiles, you do not have to manually configure the UUID of the server associated with the service profile. Assigning global UUID suffix pools from Cisco UCS Central to service profiles in Cisco UCS Central or Cisco UCS Manager allows them to be shared across Cisco UCS domains.

Creating a UUID Suffix Pool

Procedure

Step 1 On the menu bar, click **Servers**.

Step 2 In the **Servers** tab, expand **Servers** > **Pools** > **Root**.
If you want to create or access a pool in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***

Step 3 Right-click **UUID Suffix Pools** and select **Create UUID Suffix Pool**.

Step 4 In the **General** tab of the **Create UUID Suffix Pool** dialog box, fill in the following fields:

Name	Description
Name field	The name of the UUID pool. 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.

Name	Description
Description field	The user-defined description of the pool. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), and ' (single quote).
Prefix field	This can be one of the following: • **Derived**—Cisco UCS Central creates the suffix. • **other**—You specify the suffix. If you select this option, Cisco UCS Central GUI displays a text field where you can enter the UUID suffix, in the format XXXXXXXX-XXXX-XXXX.

Step 5 In the **UUID Blocks** tab of the **Create UUID Suffix Pool** dialog box, click **Create a Block of UUID Suffixes**.

Step 6 In the **Create a Block of UUID** dialog box, fill in the following fields:

Name	Description
From field	The first UUID suffix in the block.
Size field	The number of UUID suffixes in the block.

Step 7 Click **OK**.

Step 8 Click **OK**.

Note If you plan to create another pool, wait at least 5 seconds.

What to Do Next

Include the UUID suffix pool in a service profile and/or template.

Deleting a UUID Suffix Pool

If you delete a pool, Cisco UCS Central does not reallocate any addresses from that pool that have been assigned to vNICs or vHBAs in Cisco UCS Manager. All assigned addresses from a deleted pool remain with the vNIC or vHBA to which they are assigned until one of the following occurs:

- The associated service profiles are deleted.
- The vNIC or vHBA to which the address is assigned is deleted.
- The vNIC or vHBA is assigned to a different pool.

Procedure

Step 1 On the menu bar, click **Servers**.

Step 2 In the **Servers** tab, expand **Servers** > **Pools** > **Root**.
If you want to create or access a pool in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***

Step 3 Expand the **UUID Suffix Pools** node.

Step 4 Right-click the pool you want to delete and select **Delete**.

Note If you plan to delete another pool, wait at least 5 seconds.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

CHAPTER 11

Managing Power in Cisco UCS

This chapter includes the following sections:

- Power Policies, page 131
- Configuring Global Power Allocation Equipment Policies, page 131
- Configuring Power Equipment Policies, page 133

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.

Configuring Global Power Allocation Equipment Policies

Configuring a Global Power Allocation Equipment Policy

Before You Begin

Before configuring a global power allocation 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

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.

- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **Equipment**.

Step 6 In the **Work** pane, click the **Global Power Allocation Policy** tab.

Step 7 In the **Actions** area, click **Create** and complete all applicable fields.
For **Operational Policies** under the **Domain Group root** node, it is not necessary to click **Create** to complete all applicable fields.

Name	Description
Create button	Creates an instance of the policy that will be used by all Cisco UCS domains included in the selected domain group.
Import button	Allows you to import the policy from one of the Cisco UCS domains registered with Cisco UCS Central.
Delete button	Deletes the instance of the policy defined for the selected domain group. After you delete the policy, it remains greyed-out until you click **Save**. When you do so, Cisco UCS Central deletes the policy and any configuration data you may have specified. While you can create a new instance of the policy later, you cannot restore the configuration data from a deleted instance. To cancel the delete request, click **Reset**.
Allocation Method field	The power allocation management mode used in the Cisco UCS domains included in the Cisco UCS Central domain group. This can be one of the following: • **Policy Driven Chassis Group Cap**—Power allocation is configured at the chassis level through power control policies included in the associated service profiles. If you select this option, you can also create power groups that contain one or more chassis in the Cisco UCS domain. • **Manual Blade Level Cap**—Power allocation is configured on each individual blade server in all chassis. If you select this option, you cannot create power groups.

Step 8 Click **Save**.

Deleting a Global Power Allocation Equipment Policy

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **Equipment**.

Step 6 In the **Work** pane, click the **Global Power Allocation Policy** tab.

Step 7 In the **Actions** area, click **Delete**.
A policy that is deleted will inherit its settings from its domain group's parent until it is reconfigured.

Step 8 Click **Save**.

Configuring Power Equipment Policies

Configuring a Power Equipment 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

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.

- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **Equipment**.

Step 6 In the **Work** pane, click the **Power Policy** tab.

Step 7 In the **Actions** area, click **Create** and complete all applicable fields.
For **Operational Policies** under the **Domain Group root** node, it is not necessary to click **Create** to complete all applicable fields.

Name	Description
Create button	Creates an instance of the policy that will be used by all Cisco UCS domains included in the selected domain group.
Import button	Allows you to import the policy from one of the Cisco UCS domains registered with Cisco UCS Central.
Delete button	Deletes the instance of the policy defined for the selected domain group. After you delete the policy, it remains greyed-out until you click **Save**. When you do so, Cisco UCS Central deletes the policy and any configuration data you may have specified. While you can create a new instance of the policy later, you cannot restore the configuration data from a deleted instance. To cancel the delete request, click **Reset**.
Redundancy field	This can be one of the following: • **Non Redundant**—All installed power supplies are turned on and the load is evenly balanced. Only smaller configurations (requiring less than 2500W) can be powered by a single power supply. • **n+1**—The total number of power supplies to satisfy non-redundancy, plus one additional power supply for redundancy, are turned on and equally share the power load for the chassis. If any additional power supplies are installed, Cisco UCS Manager sets them to a "turned-off" state. • **Grid**—Two power sources are turned on, or the chassis requires greater than N+1 redundancy. If one source fails (which causes a loss of power to one or two power supplies), the surviving power supplies on the other power circuit continue to provide power to the chassis.

Step 8 Click **Save**.

Deleting a Power Equipment Policy

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **Equipment**.

Step 6 In the **Work** pane, click the **Power Policy** tab.

Step 7 In the **Actions** area, click **Delete**.
A policy that is deleted will inherit its settings from its domain group's parent until it is reconfigured.

Step 8 Click **Save**.

PART VI

System Management

- Managing Time Zones, page 139
- Starting the KVM Console, page 145
- Backing Up and Restoring the Configuration, page 149

CHAPTER 12

Managing Time Zones

This chapter includes the following sections:

- Date and Time Policies, page 139
- Configuring a Date and Time Policy, page 139
- Deleting a Date and Time Policy, page 140
- Configuring an NTP Server for a Date and Time Policy, page 141
- Configuring Properties for an NTP Server, page 142
- Deleting an NTP Server for a Date and Time Policy, page 143

Date and Time Policies

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

Before You Begin

Before configuring a date and time 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

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.

- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **DateTime**.

Step 6 In the **Actions** area, click **Create** and complete all applicable fields.
For **Operational Policies** under the **Domain Group root** node, it is not necessary to click **Create** to complete all applicable fields.

Name	Description
Create button	Creates an instance of the policy that will be used by all Cisco UCS domains included in the selected domain group.
Import button	Allows you to import the policy from one of the Cisco UCS domains registered with Cisco UCS Central.
Delete button	Deletes the instance of the policy defined for the selected domain group. After you delete the policy, it remains greyed-out until you click **Save**. When you do so, Cisco UCS Central deletes the policy and any configuration data you may have specified. While you can create a new instance of the policy later, you cannot restore the configuration data from a deleted instance. To cancel the delete request, click **Reset**.
Time Zone drop-down list	Select the appropriate time zone from the list.
Filter button	Allows you to filter the data in the table. When you apply a filter, this button name changes to **Filter (on)**.
Add NTP Server button	Allows you to add an NTP server to the selected domain group.
Properties button	Displays detailed properties for the object selected in the table.
Delete button	Deletes the object selected in the table.
Name column	The hostname or IP address of the NTP server.

Step 7 Click **Save**.

Deleting a Date and Time Policy

A date and time policy is deleted from a domain group under the domain group root. Date and time policies under the domain groups root cannot be deleted.

Deleting a date and time policy will remove all NTP server settings within that policy.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Expand the node for a domain group containing the policy to delete.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **DateTime**.

Step 6 In the **Actions** area, click **Delete**.
A policy that is deleted will inherit its settings from its domain group's parent until it is reconfigured.

Step 7 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Step 8 Click **Save**.

Configuring an NTP Server for a Date and Time Policy

Before You Begin

To configure an NTP server for a domain group under the domain group root, a date and time policy must first have been created.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **DateTime**.

Step 5 In the **Actions** area, click **Add NTP Server** and complete all fields.

a) In the **Add NTP Server** dialog box, complete all fields.

Name	Description
NTP Server field	The IP address or hostname of the NTP server you want to use. **Note** If you use a hostname rather than an IP 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.

b) Click **OK**.

Step 6 Click **Save**.

Configuring Properties for an NTP Server

An existing NTP server's properties may be updated before saving an NTP server instance. To change the name of an NTP server that is saved, it must be deleted and recreated.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **DateTime**.

Step 6 In the **Actions** area, select the NTP server to configure, click **Properties** and complete all fields.
You can also right-click the NTP server to access that option. The **Properties (NTP Provider)** dialog accessed by clicking **Properties** in the in the **Actions** area cannot be edited if the NTP server has been saved. To change the server name of an NTP server that was saved, delete and recreate the NTP server.

a) In the **Properties (NTP Provider)** dialog box, complete all fields.

Name	Description
NTP Server field	The IP address or hostname of the NTP server you want to use. **Note** If you use a hostname rather than an IP 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.

b) Click **OK**.

Step 7 Click **Save**.

Deleting an NTP Server for a Date and Time Policy

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **DateTime**.

Step 5 In the **Actions** area, select the NTP server to delete and click **Delete**.
You can also right-click the NTP server to access that option. An NTP server that is deleted will inherit its settings from its domain group's parent until it is reconfigured.

Step 6 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

CHAPTER 13

Starting the KVM Console

This chapter includes the following sections:

- KVM Console, page 145
- Starting the KVM Console from the KVM Launch Manager, page 146
- Starting the KVM Console from a Server, page 147
- Starting the KVM Console from a Service Profile, page 147

KVM Console

You can use the Cisco UCS Central GUI to access the KVM console for any Cisco UCS domain that has been properly registered and configured.

The KVM console is an interface accessible from the Cisco UCS Manager GUI or the KVM Launch Manager that emulates a direct KVM connection. Unlike the KVM dongle, which requires you to be physically connected to the server, the KVM console allows you to connect to the server from a remote location across the network.

You must ensure that either the server or the service profile associated with the server is configured with a CIMC IP address if you want to use the KVM console to access the server. The KVM console uses the CIMC IP address assigned to a server or a service profile to identify and connect with the correct server in a Cisco UCS domain.

Instead of using CD/DVD or floppy drives directly connected to the server, the KVM console uses virtual media, which are actual disk drives or disk image files that are mapped to virtual CD/DVD or floppy drives. You can map any of the following to virtual drives:

- CD/DVD or floppy drives on your computer
- Disk image files on your computer
- CD/DVD or floppy drives on the network
- Disk image files on the network

Starting the KVM Console from the KVM Launch Manager

The KVM Launch Manager enables you to access a server through the **KVM Console** without logging in to Cisco UCS Manager.

Before You Begin

To access the **KVM Console** for a server through the KVM Launch Manager, you need the following:

- Name of the Cisco UCS domain the server belongs to.
- Cisco UCS username and password.
- Name of the service profile associated with the server for which you want KVM access.

Procedure

Step 1 On the menu bar, click **Equipment**.

Step 2 In the **Navigation** pane, expand **UCS Domains**.

Step 3 In the work pane, click on the **UCS Domains** tab.

Step 4 From the list of Cisco UCS domain names under the **UCS Name** column, choose the domain for which you want to launch Cisco UCS Manager.

Step 5 On the menu bar, click **Properties**.

Step 6 In the **General** tab, click **Launch UCS Manager**.

Step 7 If a **UCSM Certificate Error** dialog box appears, click the text to continue to the web browser.

Step 8 If a **Security Alert** dialog box appears, accept the security certificate and continue.

Step 9 On the Cisco UCS Manager launch page, click **Launch KVM Manager**.

Step 10 If a **Security Alert** dialog box appears, click **Yes** to accept the security certificate and continue.

Step 11 On the **UCS - KVM Launch Manager Login** page, do the following:

a) Enter your Cisco UCS username and password.

b) (Optional) If your Cisco UCS implementation includes multiple domains, select the appropriate domain from the **Domain** drop-down list.

c) Click **OK**.

Step 12 In the **Service Profiles** table of the KVM Launch Manager, do the following:

a) Locate the row containing the service profile and associated server for which you need KVM access.

b) In the **Launch KVM** column for that server, click **Launch**.
The **KVM Console** opens in a separate window.

Tip If the Caps Lock key on your keyboard is on when you open a KVM session, and you subsequently turn off your Caps Lock key, the **KVM Console** may continue to act as if Caps Lock is turned on. To synchronize the **KVM Console** and your keyboard, press Caps Lock once without the **KVM Console** in focus and then press Caps Lock again with the **KVM Console** in focus.

Starting the KVM Console from a Server

You can start the **KVM Console** from a server only if there is a service profile associated with the server.

Before You Begin

To access the **KVM Console** from a service profile in the Cisco UCS Central GUI, you need the following:

- Cisco UCS username and password.

Procedure

Step 1 On the menu bar, click **Equipment**.

Step 2 In the **Navigation** pane, expand **UCS Domains**.

Step 3 In the work pane, click on the **Servers** tab.

Step 4 Choose the server from the list under the **Servers** column for which you want to launch the KVM Console.

Step 5 On the menu bar, click **Properties**.

Step 6 In the **Actions** area, click **KVM Console**.

Step 7 In the **Launch KVM for Server** dialog box, click the IP address you want to use to connect to the server. The **KVM Console Pooled IP** address is the IP address assigned to the server by Cisco UCS Manager from the **mgmt-ip** IP address pool. The **KVM Console Derived IP** address is the IP address assigned to the server through the associated service profile. One or both of these IP addresses may be available, depending on how the server is configured in the Cisco UCS domain.

Step 8 If a **Security Alert** dialog box appears, accept the security certificate and continue.

Step 9 When the **KVM Login** dialog box appears, enter your Cisco UCS Manager username and password. The **KVM Console** opens in a separate window.

Tip If the Caps Lock key on your keyboard is on when you open a KVM session, and you subsequently turn off your Caps Lock key, the **KVM Console** may continue to act as if Caps Lock is turned on. To synchronize the **KVM Console** and your keyboard, press Caps Lock once without the **KVM Console** in focus and then press Caps Lock again with the **KVM Console** in focus.

Starting the KVM Console from a Service Profile

You can start the **KVM Console** from a service profile only if there is a service profile associated with the server.

Before You Begin

To access the **KVM Console** from a service profile in the Cisco UCS Central GUI, you need the following:

- Name of the service profile associated with the server for which you want KVM access.
- Cisco UCS username and password.

Procedure

Step 1 On the menu bar, click **Servers**.

Step 2 In the **Servers** tab, expand **Servers** > **Service Profiles** > **Root**.
If you want to access a service profile in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand the service profile for which you need KVM access to the associated server.

Step 4 Select the appropriate service profile instance in the **Navigation** pane.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the **Actions** area, click **KVM Console**.

Step 7 In the **Launch KVM for Server** dialog box, click the IP address you want to use to connect to the server. The **KVM Console Pooled IP** address is the IP address assigned to the server by Cisco UCS Manager from the **mgmt-ip** IP address pool. The **KVM Console Derived IP** address is the IP address assigned to the server through the associated service profile. One or both of these IP addresses may be available, depending on how the server is configured in the Cisco UCS domain.

Step 8 If a **Security Alert** dialog box appears, accept the security certificate and continue.

Step 9 When the **KVM Login** dialog box appears, enter your Cisco UCS Manager username and password.
The **KVM Console** opens in a separate window.

Tip If the Caps Lock key on your keyboard is on when you open a KVM session, and you subsequently turn off your Caps Lock key, the **KVM Console** may continue to act as if Caps Lock is turned on. To synchronize the **KVM Console** and your keyboard, press Caps Lock once without the **KVM Console** in focus and then press Caps Lock again with the **KVM Console** in focus.

CHAPTER 14

Backing Up and Restoring the Configuration

This chapter includes the following sections:

- Backup and Restore in Cisco UCS Central, page 149
- Backup Types, page 150
- Considerations and Recommendations for Backup Operations, page 150
- Import Configuration, page 151
- Import Methods, page 152
- System Restore, page 152
- Required User Role for Backup and Import Operations, page 152
- Backup Operations, page 152
- Import Operations, page 157

Backup and Restore in Cisco UCS Central

The fundamental step to managing the backup and restore functionality with Cisco UCS Manager domains registered with Cisco UCS Central, is creating domain groups. A domain group is a user-defined group or classification of domains that are added to Cisco UCS Central. You can manually add domains to an existing domain group using the Cisco UCS Central GUI or automatically by configuring a rule.

When you perform a backup using Cisco UCS Central, you can backup and restore Cisco UCS Central itself or backup and restore Cisco UCS Manager. and you can export the file to a location on your network. Database backup and full configuration export policies can be created under domain groups similar to other policies and from a Cisco UCS Manager perspective, they can be configured remotely or locally based on the backup control setting. For global backup policies, Cisco UCS Manager domains that are part of a domain group inherit the policy creation, 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.

Remotely configured policies are restricted to use the Cisco UCS Central repository for backups which is internally mounted by Cisco UCS Manager. Local configurations allow you to specify any external backup server. You can use SCP, SFTP, FTP, and TFTP protocols.

Saved configurations can be used to restore and configure any managed Cisco UCS domain. In recovery situations, full-state backups can be used. TFTP can be used to access the backup configurations and you can use the Cisco UCS Central GUI or the CLI to copy the URL of the back up file and use it to configure a new domain.

You can perform a backup while the domain is up and running. The backup operation saves information from the management plane. It does not have any impact on the server or network traffic.

To manage the backup archives, you can specify the maximum number of backup versions that are saved. The policy specifications can be used to indicate the number of backups to maintain for each Cisco UCS Manager domain. You can also view the list of backups for each Cisco UCS Manager domain from the Cisco UCS Central GUI and you can delete saved or unused backup directories and configurations.

Note You can delete backups only after a Cisco UCS Manager domain (from which the backup has been taken) has been unregistered.

Backup Types

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

- **Full state**—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. This file can restore or rebuild the configuration on the original fabric interconnect, or recreate the configuration on a different fabric interconnect. You cannot use this file for an import.
- **All configuration**—An XML file that includes all system and logical configuration settings. You can use the file generated from this backup to import these configuration settings to the original fabric interconnect or to a different fabric interconnect. You cannot use this file for a system restore. This file does not include passwords for locally authenticated users.
- **System configuration**—An XML file that includes all system configuration settings such as usernames, roles, and locales. You can use the file generated from this backup to import these configuration settings to the original fabric interconnect or to a different fabric interconnect. You cannot use this file for a system restore.
- **Logical configuration**—An XML file that includes all logical configuration settings such as service profiles, VLANs, VSANs, pools, and policies. You can use the file generated from this backup to import these configuration settings to the original fabric interconnect or to a different fabric interconnect. You cannot use this file for a system restore.

Considerations and Recommendations for Backup Operations

Before you create a backup operation, consider the following:

Backup Locations

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

Potential to Overwrite Backup Files

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

Multiple Types of Backups

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

Scheduled Backups

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

You can use Cisco UCS Central to backup and restore Cisco UCS Central itself or Cisco UCS Manager. The backup and restore policy can be scheduled or, you can perform an immediate backup operation. There are two types of scheduled and immediate backup operations:

- Cisco UCS Central backup and restore functions Policy(scheduled) and Immediate operations.
- Cisco UCS Manager backup and restore functions Policy(scheduled) and Immediate operations when the policy is resolved from Cisco UCS Central

There are two types of policies: the scheduled all-config backup policy, and the scheduled db backup policy. These policies can either be defined locally or defined in Cisco UCS Central

Incremental Backups

You cannot perform incremental backups of Cisco UCS.

Encryption of Full State Backups

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

Import Configuration

You can import any configuration file that was exported from Cisco UCS. The file does not need to have been exported from the same Cisco UCS.

The import function is available for all configuration, system configuration, and logical configuration files. You can perform an import while the system is up and running. An import operation modifies information on the management plane only. Some modifications caused by an import operation, such as a change to a vNIC assigned to a server, can cause a server reboot or other operations that disrupt traffic.

You cannot schedule an import operation. You can, however, create an import operation in advance and leave the admin state disabled until you are ready to run the import.Cisco UCS will not run the import operation on the configuration file until you set the admin state to enabled.

You can maintain only one import operation for each location where you saved a configuration backup file.

Import Methods

You can use one of the following methods to import and update a system configuration through Cisco UCS:

- **Merge**—The information in the imported configuration file is compared with the existing configuration information. If there are conflicts, the import operation overwrites the information on the Cisco UCS domain with the information in the import configuration file.
- **Replace**—The current configuration information is replaced with the information in the imported configuration file one object at a time.

System Restore

You can use the restore function for disaster recovery.

You can restore a system configuration from any full state backup file that was exported from Cisco UCS. The file does not need to have been exported from Cisco UCS on the system that you are restoring. When restoring using a backup file that was exported from a different system, we strongly recommend that you use a system with the same or similar system configuration and hardware, including fabric interconnects, servers, adapters, and I/O module or FEX connectivity. Mismatched hardware and/or system configuration can lead to the restored system not fully functioning. If there is a mismatch between the I/O module links or servers on the two systems, acknowledge the chassis and/or servers after the restore operation.

The restore function is only available for a full state backup file. You cannot import a full state backup file. You perform a restore through the initial system setup.

Required User Role for Backup and Import Operations

You must have a user account that includes the admin role to create and run backup and import operations.

Backup Operations

Creating a Backup of Cisco UCS Central

Use this task to perform an immediate backup operation for Cisco UCS Central itself.

Before You Begin

Obtain the backup server IP address and authentication credentials.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the Navigation pane, expand **Backup and Import.**

Step 3 Click the **UCS Central System** node.

Step 4 In the work pane, click **Create System Backup.**

Step 5 In the **Create System Backup** dialog box, complete the following fields:

Name	Description
Backup State field	This can be one of the following: • **enabled**—Cisco UCS Central GUI unlocks the properties fields for the selected backup operation so that you can make changes if desired. If you click **OK**, Cisco UCS Central reruns the backup operation. • **disabled**—Cisco UCS Central GUI displays the properties of the backup operation but does not allow you to make changes.
Type field	The information saved in the backup configuration file. This can be one of the following: • **full-state**—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. • **config-all**—An XML file that includes all system and logical configuration settings. You cannot use this file for a system restore. This file does not include passwords for locally authenticated users. • **config-logical**—An XML file that includes all logical configuration settings such as service profiles, VLANs, VSANs, pools, and policies. You can use the file generated from this backup to import these configuration settings to the original fabric interconnect or to a different fabric interconnect. You cannot use this file for a system restore. • **config-system**—An XML file that includes all system configuration settings such as usernames, roles, and locales. You can use the file generated from this backup to import these configuration settings to the original fabric interconnect or to a different fabric interconnect. You cannot use this file for a system restore.

Name	Description
Location of the Image File field	Where the backup file that you want to import is located. This can be one of the following: • **Local File System**—The backup XML file is stored locally. You can download the file after the backup task has completed. • **Remote File System**—The backup XML file is stored on a remote server. Cisco UCS Central GUI displays the fields described below that allow you to specify the protocol, host, filename, username, and password for the remote system.
Protocol field	The remote server communication protocol. This can be one of the following: • **FTP** • **TFTP** • **SCP** • **SFTP**
Hostname field	The hostname or IP address of the remote server. This can be a server, storage array, local drive, or any read/write media that Cisco UCS Central can access through the network. **Note** If you use a hostname rather than an IP 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.
User field	The username Cisco UCS Central should use to log in to the remote server. This field does not apply if the protocol is TFTP.
Password field	The password for the remote server username. This field does not apply if the protocol is TFTP.
Absolute Path Remote File field	The fully-qualified name of the file on the remote server, including the path and file extension.

Step 6 Click **OK**.

Step 7 If Cisco UCS Central displays a confirmation dialog box, click **OK**.

If you set the Backup State to enabled, Cisco UCS Central takes a snapshot of the configuration type that you selected and exports the file to the network location. The backup operation displays in the **Backup Operations** table in the **Backup Configuration** dialog box.

Step 8 (Optional) To view the progress of the backup operation or the individual module export operation, in the work pane, click **Properties** and then click the **Status** tab.

Step 9 Click **OK** to close the **Backup Configuration** dialog box.
The backup operation continues to run until it is completed. To view the progress, re-open the **Backup Configuration** dialog box.

Running a Backup Operation for Cisco UCS Central

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the Navigation pane, expand **Backup and Import.**

Step 3 Click the **UCS Central System** node.

Step 4 In the **Backup** table, click the backup operation that you want to run.

Step 5 Click**Properties**.

a) Click the **General** tab and click the **Enabled** radio button.

Step 6 Click **Ok**.
Cisco UCS Central takes a snapshot of the configuration type that you selected and exports the file to the network location. To view the progress of the backup operation, click the **Task** tab in the **Properties** dialog box.

Deleting a Cisco UCS Central Backup Operation

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the Navigation pane, expand **Backup and Import.**

Step 3 Click the **UCS Central System** node.

Step 4 In the **Backup** table, click the backup operation that you want to delete. You cannot click a backup operation in the table if the admin state of the operation is set to **Enabled**.

Step 5 In the **Backup Operations** table of the **Backup Configuration** dialog box, click the backup operations that you want to delete.

Tip You cannot click a backup operation in the table if the admin state of the operation is set to **Enabled.**

Step 6 Click the **Delete** icon in the icon bar of the **Backup Operations** table.

Step 7 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Step 8 In the **Backup Configuration** dialog box, click **Yes** to delete the backup operation.

Creating a Full-State Backup Policy for Domain Groups

You can specify the full-state backup policy that you want to associate with the Cisco UCS domains included in the Cisco UCS Central domain group.

Note All policies created under the root domain group apply to Cisco UCS Central itself. The scheduled backup policies created under the root group will cause Cisco UCS Central to perform self backups into it's internal backup repository as well.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the Navigation pane, expand **Domain Groups** > **Domain Group root.**

Step 3 Click the **Backup/Export Policy** node.

Step 4 In the work pane, click **Full-State Backup Policy**.

Step 5 Click **+Create**.

Step 6 In the **Create** dialog box, complete the following fields:

Name	Description
Create button	Allows you to specify the full state backup policy you want to associate with the Cisco UCS domains included in the Cisco UCS Central domain group. The backup policy defined here overrides the policy inherited from any parent groups, if an inherited policy exists.
Delete button	Deletes the instance of the policy defined for the selected domain group. After you delete the policy, it remains greyed-out until you click **Save**. When you do so, Cisco UCS Central deletes the policy and any configuration data you may have specified. While you can create a new instance of the policy later, you cannot restore the configuration data from a deleted instance. To cancel the delete request, click **Reset**.

Name	Description
Backup State field	Whether Cisco UCS automatically creates full state backups for the Cisco UCS domains included in the Cisco UCS Central domain group. This can be one of the following: • **disable**—Cisco UCS does not create automatic backups. • **enable**—Cisco UCS creates automatic full state backups using the specified schedule. A 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.
Schedule drop-down list	The length of time Cisco UCS waits between creating full state backups.
Max Files field	The maximum number of backup files that Cisco UCS maintains. When that number is exceeded, Cisco UCS overwrites the oldest backup file.

The backup files are saved in a storage location shared by Cisco UCS Central. The list of backup files that are viewable using the Cisco UCS Central GUI, shows the names used.

Step 7 Click **Save**.

Import Operations

Creating a Domain Group Config-All Export Policy

You can specify the configuration backup policy that you want to associate with the Cisco UCS domains included in the Cisco UCS Central domain group.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the Navigation pane, expand **Domain Groups** > **Domain Group root.**

Step 3 Click the **Backup/Export Policy** node.

Step 4 In the work pane, click **Config-All Export Policy**.

Step 5 Click **+Create**.

Step 6 In the **Create** dialog box, complete the following fields:

Name	Description
Create button	Allows you to specify the configuration backup policy you want to associate with the Cisco UCS domains included in the Cisco UCS Central domain group. The configuration backup policy defined here overrides the policy inherited from any parent groups, if an inherited policy exists.
Delete button	Deletes the instance of the policy defined for the selected domain group. After you delete the policy, it remains greyed-out until you click **Save**. When you do so, Cisco UCS Central deletes the policy and any configuration data you may have specified. While you can create a new instance of the policy later, you cannot restore the configuration data from a deleted instance. To cancel the delete request, click **Reset**.
Export State field	Whether Cisco UCS automatically creates full configuration backups for the Cisco UCS domains included in the Cisco UCS Central domain group. This can be one of the following: • **disable**—Cisco UCS does not create automatic configuration backups. • **enable**—Cisco UCS creates automatic full configuration backups using the specified schedule. A full configuration backup is an XML file that includes all system and logical configuration settings. You cannot use this file for a system restore. This file does not include passwords for locally authenticated users.
Schedule drop-down list	The length of time Cisco UCS waits between creating full configuration backups.
Max Files field	The maximum number of backup files that Cisco UCS maintains. When that number is exceeded, Cisco UCS overwrites the oldest backup file.

Step 7 Click **Save**.

Creating a Cisco UCS Central Import Operation

You cannot import a Full State configuration file. You can import any of the following configuration files:

- All configuration
- System configuration
- Logical configuration

Before You Begin

Collect the following information that you will need to import a configuration file:

- Backup server IP address and authentication credentials
- Fully qualified name of a backup file

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the Navigation pane, expand **Backup and Import.**

Step 3 Click the **UCS Central System** node.

Step 4 In the work pane, click the **Import** tab.

Step 5 Click **Create Import Operation.**

Step 6 In the **Create Import Operation** dialog box, complete the following fields:

Name	Description
Configuration File drop-down list	The configuration file you want to apply to a registered Cisco UCS domain.
UCS Name drop-down list	The Cisco UCS domain to which you want to apply the imported configuration information. **Note** You cannot change the domain after you save the import operation.
Import State field	This can be one of the following: • **enabled**—Cisco UCS runs the import operation as soon as you click **OK**. • **disabled**—Cisco UCS does not run the import operation when you click **OK**. You can manually run the import at a later date by selecting it on the **Import** tab and clicking **Properties**.
Action drop-down list	This can be one of the following: • **merge**—Cisco UCS merges the configuration information in the import file with the existing configuration information. If there are conflicts, Cisco UCS replaces the current configuration with the information in the import configuration file. • **replace**—Cisco UCS takes each object in the import configuration file and overwrites the corresponding object in the current configuration.
Hostname field	The IP address of the server on which the configuration file is stored. This must be the IP address of the Cisco UCS Central server.

Name	Description
Remote File field	The fully qualified name of the configuration file on the remote server.
Protocol field	The protocol to use when communicating with the remote server. You cannot change this protocol.

Step 7 (Optional) If you select Local File System, you will need to download the file after the task is finished. Click **Download into backup file library**.

Step 8 (Optional) Click **Choose file** to browse to the file that you want to upload and import in the backup file library.

Step 9 Click **OK**.

Step 10 In the confirmation dialog box, click **OK**.
If you set the **Import State** to enabled, Cisco UCS Central imports the configuration file from the network location. Depending upon which action you selected, the information in the file is either merged with the existing configuration or replaces the existing configuration. The import operation displays in the **Import Operations** table of the **Import Configuration** dialog box.

Step 11 (Optional) To view the progress of the import operation and the individual module status, do the following:

a) If the operation does not automatically display in the **Properties** area, click the operation in the **Import Operations** table.

b) In the **Properties** area, click the down arrows on the **FSM Details** bar.

The **FSM Details** area expands and displays the operation status.

Step 12 Click **OK** to close the **Import Configuration** dialog box.
The import operation continues to run until it is completed. To view the progress, re-open the **Import Configuration** dialog box.

Creating a Cisco UCS Manager Import Operations

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the Navigation pane, expand **Backup and Import**.

Step 3 Click the **UCS System** node.

Step 4 In the work pane, click the **Import** tab.

Step 5 Click **+Create Import Operation**.

Step 6 In the **Create Import Operation** dialog box, complete the following fields:

Name	Description
Configuration File drop-down list	The configuration file you want to apply to a registered Cisco UCS domain.

Name	Description
UCS Name drop-down list	The Cisco UCS domain to which you want to apply the imported configuration information. **Note** You cannot change the domain after you save the import operation.
Import State field	This can be one of the following: • **enabled**—Cisco UCS runs the import operation as soon as you click **OK**. • **disabled**—Cisco UCS does not run the import operation when you click **OK**. You can manually run the import at a later date by selecting it on the **Import** tab and clicking **Properties**.
Action drop-down list	This can be one of the following: • **merge**—Cisco UCS merges the configuration information in the import file with the existing configuration information. If there are conflicts, Cisco UCS replaces the current configuration with the information in the import configuration file. • **replace**—Cisco UCS takes each object in the import configuration file and overwrites the corresponding object in the current configuration.
Hostname field	The IP address of the server on which the configuration file is stored. This must be the IP address of the Cisco UCS Central server.
Remote File field	The fully qualified name of the configuration file on the remote server.
Protocol field	The protocol to use when communicating with the remote server. You cannot change this protocol.

Step 7 Click **Ok**.

Running an Import Operation

Choose the **UCS Central System** option to run an import operation for Cisco UCS Central. Use the **UCS Central** option to run an import operation for Cisco UCS Manager.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the Navigation pane, expand **Backup and Import.**

Step 3 Click the **UCS Central System** node to run an import operation for Cisco UCS Central.

Step 4 (Optional) Click the **UCS Central** node to run the import operation for Cisco UCS Manager .

Step 5 In the **Import** table, click the hostname and remote file name that you want to import.

Step 6 Click**Properties**.

a) Click the **General** tab and click the **Enabled** radio button.

b) Click the **merge** or **replace** radio button.

Step 7 Click **Ok**.

Cisco UCS Central imports the backup configuration file that you selected. To view the progress of the backup operation, click the **Task** tab in the **Properties** dialog box.

Deleting Import Operations

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the Navigation pane, expand **Backup and Import.**

Step 3 Click the **UCS Central System** node.

Step 4 In the work pane, click the **Import** tab.

Step 5 In the **Import** table, click the import operation that you want to delete. You cannot click a backup operation in the table if the admin state of the operation is set to **Enabled**.

Step 6 In the **Import** table , click the import operation that you want to delete.

Tip You cannot click an import operation in the table if the admin state of the operation is set to **Enabled.**

Step 7 Click the **Delete** icon in the icon bar of the **Import** table.

Step 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

PART VII

System Monitoring

- Monitoring Inventory, page 165
- Configuring Call Home, page 173
- Managing the System Event Log, page 185
- Configuring Settings for Faults, Events, and Logs, page 189

CHAPTER 15

Monitoring Inventory

This chapter includes the following sections:

- Inventory Management, page 165
- Configuring Inventory Data Collection Schedule, page 166
- Viewing Inventory Details, page 166
- Viewing Details on an Individual Cisco UCS Domain, page 168
- Viewing Service Profiles, page 170
- Viewing Service Profile Details, page 171
- Viewing Service Profile Templates, page 172

Inventory Management

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

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

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

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

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

Physical Inventory

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

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

Service Profiles and Templates

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

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

Configuring Inventory Data Collection Schedule

Procedure

Step 1 On the menu bar, click **Equipment**.

Step 2 In the **Navigation** Pane, click **Domain Management**.

Step 3 In the **Work** pane, **General** tab, **Summary** > **Polling Interval** click the drop down option. Select the interval from the options.

Step 4 Click **Save**.

Viewing Inventory Details

The **UCS Domains** pane displays a comprehensive list of all registered Cisco UCS domains.

Tip To view details of an individual domain, in the **UCS Name** column, click and choose the name of a Cisco UCS domain and click **Properties**.

Procedure

Step 1 On the menu bar, click **Equipment**.

Step 2 In the **Navigation** pane, expand **UCS Domains**.

Step 3 The work pane displays the following:

Option	Description
General	Provides an overview of the servers in the registered Cisco UCS domains: • **Summary**—Displays the percentage level of **In Use** and **Available** servers in the registered UCS domains. • **Servers**—Points to the overview of In use and available servers. • **Polling Interval**—Displays the specified interval in which Cisco UCS Central system collects data from all registered Cisco UCS domains.
UCS Domains	Displays the following details on the registered Cisco UCS domains: • **Systems**—Displays the registered systems with name and other related details. • **Firmware**—Displays Cisco UCS domain name, site and the firmware version used in the domain. • **Usage**—Displays the number of servers managed by the Cisco UCS domain, the number of available servers and the number of servers in use.
Fabric Interconnect	Displays the following details on the FIs connected to the registered Cisco UCS domains: • **Status**—Displays the FI ID, connected Cisco UCS domain name, status, operability and other related details for all FIs in the registered UCS domains. • **Hardware**—Displays all hardware related to the FI. • **Firmware**—Displays the firmware version used in the FI.
Servers	Displays the following details of all servers in the connected Cisco UCS domains: • **Status**—Displays the server number, connected Cisco UCS domain name, status, power, availability and other related details of the servers. • **Hardware**—Displays all hardware details including the adapters and adapter model numbers in the servers. • **Firmware**—Displays the firmware version used in the servers.

Option	Description
Chassis	Displays the following details of all chassis in the connected Cisco UCS domains: • **Status**—Displays the chassis ID, connected Cisco UCS domain name, configuration details and other related details of the servers. • **Hardware**—Displays all hardware details including the connection details.
FSM Stage Status	Displays the FSM stages, such as configurations, discovery of servers and service profiles.

Viewing Details on an Individual Cisco UCS Domain

Procedure

Step 1 On the menu bar, click **Equipment**.

Step 2 In the **Navigation** pane, expand **UCS Domains**.

Step 3 In the work pane, click on the **UCS Domains** tab.

Step 4 From the list of Cisco UCS domain names under **UCS Name** column, choose the domain you want to view the details for.
When you select the Cisco UCS domain, two menu items appears on the menu bar next to **Filter**.

Step 5 On the menu bar, click **Properties**.
The **Properties** dialog box displays the following details of the selected Cisco UCS domain:

Option	Description
Fault Summary	Displays the number of faults under each severity level in the selected Cisco UCS domain. Cisco UCS Central refreshes fault information from the connected Cisco UCS domains at every one minute interval.

Option	Description
Properties	Provides the following details for the selected Cisco UCS domain: • **Servers** —A graphical representation of the number of servers in use versus available. • **Management IP**—The management IP address of this Cisco UCS domain. Cisco UCS Manager uses this IP address to launch the Cisco UCS Manager GUI. • **FW Version**—The Cisco UCS Manager firmware version running on the Cisco UCS domain. • **Description**— The description of the Cisco UCS domain, if any. • **FW Status**—The status of the firmware on the Cisco UCS domain. • **Site**—The site associated with the Cisco UCS domain, if any. • **Domain Group**—The domain group in which the Cisco UCS domain is included, if any. • **Owner**— • **Last Refresh**— The last date and time that Cisco UCS Central refreshed the information for the Cisco UCS domain.
Fabric Interconnect	Displays the following details on the FIs connected to this Cisco UCS domain : • **Status**—Displays the FI ID, status, operability and other related details for the connected FIs. • **Hardware**—Displays all hardware related to the FI. • **Firmware**—Displays the firmware version used in the FI.
Servers	Displays the following details of all servers in the Cisco UCS domain: • **Status**—Displays the server number, status, power, availability and other related details of the servers. • **Hardware**—Displays all hardware details including the adapters and adapter model numbers in the servers. • **Firmware**—Displays the firmware version used in the servers.
Chassis	Displays the following details of all chassis in the Cisco UCS domain: • **Status**—Displays the chassis ID, configuration details and other related details of the servers. • **Hardware**—Displays all hardware details including the connection details.

Option	Description
IO Modules	Displays the following details of the IO modules in the Cisco UCS domain: • **Status**—Displays the chassis ID, IO module, and other related details of the servers. • **Hardware**—Displays all hardware details including the FI to which this IO module is connected and other related details. • **Firmware**—Displays the firmware version used in the IO module.

Viewing Service Profiles

Procedure

Step 1 On the menu bar, click **Servers**.

Step 2 In the **Navigation** pane, click the **Service Profiles**.

Step 3 The **Work** pane displays the following:

Name	Description
Filter button	Allows you to filter the data in the table. When you apply a filter, this button name changes to **Filter (on)**.
Properties button	Displays detailed properties for the object selected in the table.
Name column	The service profile name.
Org column	The organization associated with the service profile.
Status column	A brief description of the service profile status.
Instances column	The number of times a service profile with this name is used in all registered Cisco UCS domains.
UCS Name field	The system name of the Cisco UCS domain.

a) (Optional) Click the number in the **Instances** column to view the number of times this service profile is used in the registered Cisco UCS domains.

Viewing Service Profile Details

You can also view the service profile details by clicking on the number in instances column. This procedure describes how to access detailed information on each service profile from the navigation pane.

Procedure

Step 1 On the menu bar, click **Servers**.

Step 2 In the Navigation pane, expand **Servers** > **Service Profile** > **Root** , and click the service profile name.

Step 3 The **Work** pane displays the following:

Name	Description
Filter button	Allows you to filter the data in the table. When you apply a filter, this button name changes to **Filter (on)**.
Properties button	Displays detailed properties for the object selected in the table.
UCS Name field	The system name of the Cisco UCS domain.
Status column	A brief description of the overall status of the service profile.
Association State column	The relationship between the server and a service profile. This can be one of the following: • **Associated**—A service profile is assigned to the server, which means the server can be used as required by the Cisco UCS domain. • **Associating**—A service profile has been assigned to this server, but the association process has not yet completed. The server is ready for use when the state changes to **Associated**. • **Disassociating**—The previously assigned service profile is being removed from this server. When the process has finished, the state changes to **Unassociated**. • **Unassociated**—A service profile has not been assigned to this server, which means it cannot be used by Cisco UCS.
Associated Server column	The name of the server to which this profile is assigned, if any.
Template column	The name of the associated service profile template, if any.

Viewing Service Profile Templates

Procedure

Step 1 On the menu bar, click **Servers**.

Step 2 In the **Navigation** pane, click the **Service Profile Templates**.

Step 3 The **Work** pane displays the following:

Name	Description
Filter button	Allows you to filter the data in the table. When you apply a filter, this button name changes to **Filter (on)**.
Properties button	Displays detailed properties for the object selected in the table.
Name column	The service profile template name.
Org column	The organization associated with the service profile template.
Placement Count column	The number of times a service profile with this name is used in all registered Cisco UCS domains.

CHAPTER 16

Configuring Call Home

This chapter includes the following sections:

- Call Home Policies, page 173
- Configuring a Call Home Policy, page 173
- Deleting a Call Home Policy, page 178
- Configuring a Profile for a Call Home Policy, page 179
- Adding Email Recipients to a Call Home Profile, page 181
- Deleting a Profile for a Call Home Policy, page 182
- Configuring a Policy for a Call Home Policy, page 182
- Deleting a Policy for a Call Home Policy, page 183

Call Home Policies

Cisco UCS Central supports global call home policies for notifying all email recipients defined in call home profiles to specific Cisco UCS Central 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.

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 were already created by the system and ready to configure.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 In the **Navigation** pane, click **Operational Policies**.

Step 4 In the **Work** pane, click **CallHome**.

Step 5 (Optional) In the **Actions** area, click **Create**.
Call home policies under the domain groups root were created by the system and ready to configure by default

Step 6 In the **Work** pane, click the **General** tab.

Step 7 In the **Actions** area, complete all applicable fields.

Name	Description
Create button	Creates an instance of the policy that will be used by all Cisco UCS domains included in the selected domain group.
Import button	Allows you to import the policy from one of the Cisco UCS domains registered with Cisco UCS Central.
Delete button	Deletes the instance of the policy defined for the selected domain group. After you delete the policy, it remains greyed-out until you click **Save**. When you do so, Cisco UCS Central deletes the policy and any configuration data you may have specified. While you can create a new instance of the policy later, you cannot restore the configuration data from a deleted instance. To cancel the delete request, click **Reset**.
State field	Whether Call Home is used for the Cisco UCS domains included in the Cisco UCS Central domain group. This can be one of the following: • **Off**—Call Home is not used for the Cisco UCS domains. • **On**—Cisco UCS generates Call Home alerts based on the Call Home policies and profiles defined in the domain group. **Note** If this field is set to **On**, Cisco UCS Central GUI displays the rest of the fields on this tab.
Throttling field	Whether the system limits the number of duplicate messages received for the same event. This can be one of the following: • **On**—If the number of duplicate messages sent exceeds 30 messages within a 2-hour time frame, then the system discards further messages for that alert type. • **Off**—The system sends all duplicate messages, regardless of how many are encountered.

Name	Description
Phone field	The telephone number for the main contact. Enter the number in international format, starting with a + (plus sign) and a country code. You can use hyphens but not parentheses.
Email field	The email address for the main contact. Cisco Smart Call Home sends the registration email to this email address. **Note** If an email address includes special characters, such as # (hash), spaces, or & (ampersand), the email server may not be able to deliver email messages to that address. Cisco recommends that you use email addresses which comply with RFC2821 and RFC2822 and include only 7bit ASCII characters.
Address field	The mailing address for the main contact. Enter up to 255 ASCII characters.
From field	The email address that should appear in the From field on Call Home alert messages sent by the system.
Reply To field	The return email address that should appear in the From field on Call Home alert messages sent by the system.
Switch Priority drop-down list	This can be one of the following: • **Alerts** • **Critical** • **Debugging** • **Emergencies** • **Errors** • **Information** • **Notifications** • **Warnings**
Hostname field	The IP address or hostname of the SMTP server. **Note** If you use a hostname rather than an IP 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.
Port field	The port number the system should use to talk to the SMTP server. Enter an integer between 1 and 65535. The default is 25.

Name	Description
Customer ID field	The CCO ID that includes the contract numbers for the support contract in its entitlements. Enter up to 510 ASCII characters.
Contract ID field	The Call Home contract number for the customer. Enter up to 510 ASCII characters.
Site field	The unique Call Home identification number for the customer site. Enter up to 510 ASCII characters.

Step 8 In the **Work** pane, click the **Profiles** tab.

Step 9 In the **Actions** area, complete all applicable fields.

Name	Description
Create button	Creates an instance of the policy that will be used by all Cisco UCS domains included in the selected domain group.
Import button	Allows you to import the policy from one of the Cisco UCS domains registered with Cisco UCS Central.
Delete button	Deletes the instance of the policy defined for the selected domain group. After you delete the policy, it remains greyed-out until you click **Save**. When you do so, Cisco UCS Central deletes the policy and any configuration data you may have specified. While you can create a new instance of the policy later, you cannot restore the configuration data from a deleted instance. To cancel the delete request, click **Reset**.
Filter button	Allows you to filter the data in the table. When you apply a filter, this button name changes to **Filter (on)**.
Create Profile button	Allows you to create a Call Home profile.
Add Email Recipient button	Allows you to add an email recipient to an existing Call Home profile.
Properties button	Displays detailed properties for the object selected in the table.
Delete button	Deletes the object selected in the table.
Name column	The name of the Call Home profile.
Level column	The lowest fault level that triggers the profile. Cisco UCS generates a Call Home alert for every fault that is at or above this level.

Name	Description
Alert Groups column	The group or groups that are alerted based on this Call Home profile.

Step 10 In the **Work** pane, click the **Policies** tab.

Step 11 In the **Actions** area, complete all applicable fields.

Name	Description
Create button	Creates an instance of the policy that will be used by all Cisco UCS domains included in the selected domain group.
Import button	Allows you to import the policy from one of the Cisco UCS domains registered with Cisco UCS Central.
Delete button	Deletes the instance of the policy defined for the selected domain group. After you delete the policy, it remains greyed-out until you click **Save**. When you do so, Cisco UCS Central deletes the policy and any configuration data you may have specified. While you can create a new instance of the policy later, you cannot restore the configuration data from a deleted instance. To cancel the delete request, click **Reset**.
Filter button	Allows you to filter the data in the table. When you apply a filter, this button name changes to **Filter (on)**.
Create Policy button	Allows you to create a new Call Home policy.
Properties button	Displays detailed properties for the object selected in the table.
Delete button	Deletes the object selected in the table.
Cause column	The event that triggers the alert. Each policy defines whether an alert is sent for one type of event.
Call Home Policy State column	If this is **enabled**, Cisco UCS uses this policy when an error matching the associated cause is encountered. Otherwise, Cisco UCS ignores this policy even if a matching error occurs. By default, all policies are enabled.

Step 12 In the **Work** pane, click the **System Inventory** tab.

Step 13 In the **Actions** area, complete all applicable fields.

Name	Description
Create button	Creates an instance of the policy that will be used by all Cisco UCS domains included in the selected domain group.

Name	Description
Import button	Allows you to import the policy from one of the Cisco UCS domains registered with Cisco UCS Central.
Delete button	Deletes the instance of the policy defined for the selected domain group. After you delete the policy, it remains greyed-out until you click **Save**. When you do so, Cisco UCS Central deletes the policy and any configuration data you may have specified. While you can create a new instance of the policy later, you cannot restore the configuration data from a deleted instance. To cancel the delete request, click **Reset**.
Send Periodically field	If this field is set to **on**, Cisco UCS sends the system inventory to the Call Home database. When the information is sent depends on the other fields in this area.
Send Interval field	The number of days that should pass between automatic system inventory data collection. Enter an integer between 1 and 30.
Hour of Day to Send field	The hour that the data should be sent using the 24-hour clock format.
Minute of Hour to Send field	The number of minutes after the hour that the data should be sent.

Step 14 Click **Save**.

Deleting a Call Home Policy

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

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

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 In the **Navigation** pane, click **Operational Policies**.

Step 4 In the **Work** pane, click **CallHome**.

Step 5 In the **Actions** area, click **Delete**.
A policy that is deleted will inherit its settings from its domain group's parent until it is reconfigured.

Step 6 Click **Save**.

Configuring a Profile for a Call Home Policy

Before You Begin

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

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **CallHome**.

Step 5 In the **Work** pane, click the **Profiles** tab.

Step 6 In the **Actions** area, click **Create Profile** and complete all applicable fields.

a) In the **Create Profile** dialog, click and complete the following fields:

Name	Description
Name field	The user-defined name for this profile.
Level field	The lowest fault level that triggers the profile. Cisco UCS generates a Call Home alert for each fault that is at or above this level. This can be one of the following: • **critical** • **debug** • **disaster** • **fatal** • **major** • **minor** • **normal** • **notification** • **warning**

b) In the **Alert Groups** area, complete the following fields:

Name	Description
Alert Groups field	The group or groups that are alerted based on this Call Home profile. This can be one or more of the following: • **ciscoTac** • **diagnostic** • **environmental** • **inventory** • **license** • **lifeCycle** • **linecard** • **supervisor** • **syslogPort** • **system** • **test**

c) In the **Email Configuration** area, complete the following fields:

Name	Description
Format field	This can be one of the following: • **xml**—A machine readable format that uses Extensible Markup Language (XML) and Adaptive Messaging Language (AML) XML schema definition (XSD). This format enables communication with the Cisco Systems Technical Assistance Center. • **fullTxt**—A fully formatted message with detailed information that is suitable for human reading. • **shortTxt**—A one or two line description of the fault that is suitable for pagers or printed reports.

Name	Description
Max Message Size field	The maximum message size that is sent to the designated Call Home recipients. Enter an integer between 1 and 5000000. The default is 5000000. For full text and XML messages, the maximum recommended size is 5000000. For short text messages, the maximum recommended size is 100000. For the Cisco TAC alert group, the maximum message size must be 5000000.

d) In the **Email Recipients** area, complete the following fields:

Name	Description
Filter button	Allows you to filter the data in the table. When you apply a filter, this button name changes to **Filter (on)**.
Add Email Recipients button	Allows you to add an email recipient.
Properties button	Displays detailed properties for the object selected in the table.
Delete button	Deletes the object selected in the table.
Email column	The email address of the recipient.

e) Click **OK**.

Step 7 Click **Save**.

Adding Email Recipients to a Call Home Profile

Before You Begin

Before adding email recipients to a profile for a call home policy, this profile must first be created.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.

- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **CallHome**.

Step 5 In the **Work** pane, click the **Profiles** tab.

Step 6 In the **Work** pane, click an existing profile for adding the email recipient.

Step 7 In the **Action** are, click **Add Email Recipients**.

Step 8 In the **Add Email Recipients** dialog box, enter an email address for the recipient.

Step 9 Click **OK**.

Step 10 Click **Save**.

Deleting a Profile for a Call Home Policy

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **CallHome**.

Step 5 In the **Actions** area, click the profile in call home you want to delete.
You can also right-click the profile in call home you want to delete to access that option. A profile that is deleted will inherit its settings from its domain group's parent until it is reconfigured.

Step 6 In the **Actions** area, click **Delete**.
Deleting a profile for a call home policy will delete all email recipients and other settings defined for that profile.

Step 7 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Configuring a Policy for a Call Home Policy

Before You Begin

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 were already created by the system and ready to configure.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Work** pane, click **CallHome**.

Step 5 In the **Work** pane, click the **Policies** tab.

Step 6 In the **Actions** area, click **Create Policy** and complete all applicable fields.

a) In the **Create Policy** dialog, click and complete the following fields:

Name	Description
State field	If this is **enabled**, Cisco UCS uses this policy when an error matching the associated cause is encountered. Otherwise, Cisco UCS ignores this policy even if a matching error occurs. By default, all policies are enabled.
Cause field	The event that triggers the alert. Each policy defines whether an alert is sent for one type of event. You cannot change the cause after the policy has been saved.

b) Click **OK**.

Step 7 Click **Save**.

Deleting a Policy for a Call Home Policy

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.

- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **CallHome**.

Step 6 In the **Actions** area, click the policy in call home you want to delete.
You can also right-click the policy in call home you want to delete to access that option. A policy that is deleted will inherit its settings from its domain group's parent until it is reconfigured.

Step 7 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

CHAPTER 17

Managing the System Event Log

This chapter includes the following sections:

- System Event Log Policy, page 185
- System Event Log, page 185
- Configuring a SEL Policy, page 186
- Deleting a SEL Policy, page 188

System Event Log Policy

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

System Event Log

The system event log (SEL) resides on the CIMC in NVRAM. It records most server-related events, such as over and under voltage, temperature events, fan events, and events from BIOS. The SEL is mainly used for troubleshooting purposes.

The SEL file is approximately 40KB in size, and no further events can be recorded when it is full. It must be cleared before additional events can be recorded.

You can use the SEL policy to backup the SEL to a remote server, and optionally clear the SEL after a backup operation occurs. Backup operations can be triggered based on specific actions, or they can occur at regular intervals. You can also manually backup or clear the SEL.

The backup file is automatically generated. The filename format is sel-*SystemName-ChassisID-ServerID-ServerSerialNumber-Timestamp*; for example, sel-UCS-A-ch01-serv01-QCI12522939-20091121160736.

Tip For more information about the SEL, including how to view the SEL for each server and configure the SEL policy, see the Cisco UCS Manager configuration guides, which are accessible through the Cisco UCS B-Series Servers Documentation Roadmap.

Configuring a SEL Policy

Before You Begin

Before configuring a SEL 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

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **Equipment**.

Step 6 In the **Work** pane, click the **SEL Policy** tab.

Step 7 In the **Actions** area, click **Create** and complete all applicable fields.
For **Operational Policies** under the **Domain Group root** node, it is not necessary to click **Create** to complete all applicable fields.

a) In the **General** area, complete the following:

Name	Description
Name field	The name of the Server Event Log (SEL) policy must be "sel".
Type field	The type of this policy must be "SEL".
Description field	The user-defined description of the policy. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), and ' (single quote).

b) In the **Backup Configuration** area, complete the following:

Name	Description
Protocol field	The remote server communication protocol. This can be one of the following: • **FTP** • **TFTP** • **SCP** • **SFTP**
Hostname field	The hostname or IP address of the remote server. This can be a server, storage array, local drive, or any read/write media that Cisco UCS Central can access through the network. The name of the backup file is generated by Cisco UCS. The name is in the following format: `sel-system-name-chchassis-id-servblade-id-blade-serial-timestamp` **Note** If you use a hostname rather than an IP 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.
Remote Path field	The absolute path to the file on the remote server. If you use SCP, the absolute path is always required. If you use any other protocol, you may not need to specify a remote path if the file resides in the default download folder. For details about how your file server is configured, contact your system administrator.
Backup Interval drop-down list	The time to wait between automatic backups. If you select **Never**, Cisco UCS does not perform any automatic SEL data backups. **Note** If you want the system to create automatic backups, make sure you check the **Timer** check box in the **Action** option box.
Format field	The format to use for the backup file. This can be one of the following: • **ASCII** • **Binary**
Clear on Backup check box	If checked, Cisco UCS clears all system event logs after the backup.
User field	The username Cisco UCS Central should use to log in to the remote server. This field does not apply if the protocol is TFTP.

Name	Description
Password field	The password for the remote server username. This field does not apply if the protocol is TFTP.
Action option box	For each box that is checked, Cisco UCS creates a SEL backup when that event is encountered: • **Log Full**—The log reaches the maximum size allowed. • **On Change of Association**—The association between a server and its service profile changes. • **On Clear**—The user manually clears a system event log. • **Timer**—The time interval specified in the **Backup Interval** drop-down list is reached.

Step 8 Click **Save**.

Deleting a SEL Policy

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **Equipment**.

Step 6 In the **Work** pane, click the **SEL Policy** tab.

Step 7 In the **Actions** area, click **Delete**.
A policy that is deleted will inherit its settings from its domain group's parent until it is reconfigured.

Step 8 Click **Save**.

CHAPTER 18

Configuring Settings for Faults, Events, and Logs

This chapter includes the following sections:

- Configuring Global Fault Policies, page 189
- Configuring TFTP Core Export Policies, page 192
- Configuring Syslog Policies, page 194

Configuring Global Fault Policies

Configuring a Global Fault Debug Policy

Before You Begin

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

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **Debug**.

Step 6 In the **Work** pane, click the **Global Fault Policy** tab.

Step 7 In the **Actions** area, click **Create** and complete all applicable fields.

For **Operational Policies** under the **Domain Group root** node, it is not necessary to click **Create** to complete all applicable fields.

Name	Description
Create button	Creates an instance of the policy that will be used by all Cisco UCS domains included in the selected domain group.
Import button	Allows you to import the policy from one of the Cisco UCS domains registered with Cisco UCS Central.
Delete button	Deletes the instance of the policy defined for the selected domain group. After you delete the policy, it remains greyed-out until you click **Save**. When you do so, Cisco UCS Central deletes the policy and any configuration data you may have specified. While you can create a new instance of the policy later, you cannot restore the configuration data from a deleted instance. To cancel the delete request, click **Reset**.
Flapping Interval field	Flapping occurs when a fault is raised and cleared several times in rapid succession. To prevent this, Cisco UCS does not allow a fault to change its state until this amount of time has elapsed since the last state change. If the condition reoccurs during the flapping interval, the fault returns to the active state. If the condition does not reoccur during the flapping interval, the fault is cleared. What happens at that point depends on the setting in the **Clear Action** field. Enter an integer between 5 and 3,600. The default is 10.
Initial Severity field	This can be one of the following: • **info** • **condition** • **warning**
Action on Acknowledgment field	This can be one of the following: • **delete-on-clear** • **initial-severity**
Clear Action field	The action the system takes when a fault is cleared. This can be one of the following: • **retain**—Cleared faults are retained for the length of time specified in the **Retention Interval** field. • **delete**—Cleared faults are deleted immediately.

Name	Description
Clear Interval field	Whether Cisco UCS automatically marks faults as cleared based on their age. This can be one of the following: • **Never**—Faults are not automatically cleared. • **Other**—Cisco UCS automatically clears fault messages after the length of time you specify in the associated interval field. Specify the interval using the format dd:hh:mm:ss
Retention Interval field	If the **Clear Action** field is set to **Retain**, this is the length of time Cisco UCS retains a fault once it is marked as cleared. This can be one of the following: • **Forever**—Cisco UCS retains all cleared fault messages regardless of how old they are. • **Other**—Cisco UCS retains cleared fault messages for the length of time you specify in the associated interval field. Specify the interval using the format dd:hh:mm:ss.

Step 8 Click **Save**.

Deleting a Global Fault Debug Policy

A global fault debug policy is deleted from a domain group under the domain group root. Global fault debug policies under the domain groups root cannot be deleted.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Expand the node for a domain group containing the policy to delete.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **Debug**.

Step 6 In the **Work** pane, click the **Global Fault Policy** tab.

Step 7 In the **Actions** area, click **Delete**.
A policy that is deleted will inherit its settings from its domain group's parent until it is reconfigured.

Step 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Step 9 Click **Save**.

Configuring TFTP Core Export Policies

Core File Exporter

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

Configuring a TFTP Core Export Debug Policy

Before You Begin

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

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **Debug**.

Step 6 In the **Work** pane, click the **TFTP Core Export Policy** tab.

Step 7 In the **Actions** area, click **Create** and complete all applicable fields.
For **Operational Policies** under the **Domain Group root** node, it is not necessary to click **Create** to complete all applicable fields.

Name	Description
Create button	Creates an instance of the policy that will be used by all Cisco UCS domains included in the selected domain group.
Import button	Allows you to import the policy from one of the Cisco UCS domains registered with Cisco UCS Central.

Name	Description
Delete button	Deletes the instance of the policy defined for the selected domain group. After you delete the policy, it remains greyed-out until you click **Save**. When you do so, Cisco UCS Central deletes the policy and any configuration data you may have specified. While you can create a new instance of the policy later, you cannot restore the configuration data from a deleted instance. To cancel the delete request, click **Reset**.
Admin State field	This can be one of the following: • **enabled**—If an error causes the server to perform a core dump, the system sends the core dump file via TFTP to a given location. When this option is selected, Cisco UCS Central GUI displays the other fields in this area that enable you to specify the TFTP export options. • **disabled**—Core dump files are not automatically exported.
Description field	The user-defined description of the policy. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), and ' (single quote).
Port field	The port number to use when exporting the core dump file via TFTP.
Hostname field	The hostname or IP address to connect with via TFTP. **Note** If you use a hostname rather than an IP 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.
Path field	The path to use when storing the core dump file on the remote system.

Step 8 Click **Save**.

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

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.
Step 3 Expand the node for a domain group containing the policy to delete.
Step 4 In the **Navigation** pane, click **Operational Policies**.
Step 5 In the **Work** pane, click **Debug**.
Step 6 In the **Work** pane, click the **TFTP Core Export Policy** tab.
Step 7 In the **Actions** area, click **Delete**.
A policy that is deleted will inherit its settings from its domain group's parent until it is reconfigured.
Step 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.
Step 9 Click **Save**.

Configuring Syslog Policies

Configuring a Syslog Console Debug Policy

Before You Begin

Before configuring a syslog console 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

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.
Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Navigation** pane, click **Operational Policies**.
Step 5 In the **Work** pane, click **Debug**.
Step 6 In the **Work** pane, click the **Syslog Policy** tab.
Step 7 In the **Work** pane, click the **Console** tab.
Step 8 In the **Actions** area, click **Create** and complete all applicable fields.
For **Operational Policies** under the **Domain Group root** node, it is not necessary to click **Create** to complete all applicable fields.

Name	Description
Create button	Creates an instance of the policy that will be used by all Cisco UCS domains included in the selected domain group.
Import button	Allows you to import the policy from one of the Cisco UCS domains registered with Cisco UCS Central.
Delete button	Deletes the instance of the policy defined for the selected domain group. After you delete the policy, it remains greyed-out until you click **Save**. When you do so, Cisco UCS Central deletes the policy and any configuration data you may have specified. While you can create a new instance of the policy later, you cannot restore the configuration data from a deleted instance. To cancel the delete request, click **Reset**.
Console Access field	Whether Cisco UCS displays Syslog messages on the console. This can be one of the following: • **Enabled**—Syslog messages are displayed on the console as well as added to the log. • **Disabled**—Syslog messages are added to the log but not displayed on the console.
Severity field	If this option is **enabled**, select the lowest message level that you want displayed. Cisco UCS displays that level and above on the console. This can be one of the following: • **Emergencies** • **Alerts** • **Critical**

Step 9 Click **Save**.

Deleting a Syslog Console Debug Policy

A syslog console debug policy is deleted from a domain group under the domain group root. Syslog console debug policies under the domain groups root cannot be deleted.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Expand the node for a domain group containing the policy to delete.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **Debug**.

Step 6 In the **Work** pane, click the **Syslog Policy** tab.

Step 7 In the **Work** pane, click the **Console** tab.

Step 8 In the **Actions** area, click **Delete**.
A policy that is deleted will inherit its settings from its domain group's parent until it is reconfigured.

Step 9 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Step 10 Click **Save**.

Configuring a Syslog Monitor Debug Policy

Before You Begin

Before configuring a syslog monitor 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

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **Debug**.

Step 6 In the **Work** pane, click the **Syslog Policy** tab.

Step 7 In the **Work** pane, click the **Monitor** tab.

Step 8 In the **Actions** area, click **Create** and complete all applicable fields.
For **Operational Policies** under the **Domain Group root** node, it is not necessary to click **Create** to complete all applicable fields.

Name	Description
Create button	Creates an instance of the policy that will be used by all Cisco UCS domains included in the selected domain group.
Import button	Allows you to import the policy from one of the Cisco UCS domains registered with Cisco UCS Central.
Delete button	Deletes the instance of the policy defined for the selected domain group. After you delete the policy, it remains greyed-out until you click **Save**. When you do so, Cisco UCS Central deletes the policy and any configuration data you may have specified. While you can create a new instance of the policy later, you cannot restore the configuration data from a deleted instance. To cancel the delete request, click **Reset**.
Monitor Access field	Whether Cisco UCS displays Syslog messages on the monitor. This can be one of the following: • **Enabled**—Syslog messages are displayed on the monitor as well as added to the log. • **Disabled**—Syslog messages are added to the log but not displayed on the monitor.
Severity field	If this option is **enabled**, select the lowest message level that you want displayed. The system displays that level and above on the monitor. This can be one of the following: • **Emergencies** • **Alerts** • **Critical** • **Errors** • **Warnings** • **Notifications** • **Information** • **Debugging**

Step 9 Click **Save**.

Deleting a Syslog Monitor Debug Policy

A syslog monitor debug policy is deleted from a domain group under the domain group root. Syslog monitor debug policies under the domain groups root cannot be deleted.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Expand the node for a domain group containing the policy to delete.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **Debug**.

Step 6 In the **Work** pane, click the **Syslog Policy** tab.

Step 7 In the **Work** pane, click the **Monitor** tab.

Step 8 In the **Actions** area, click **Delete**.
A policy that is deleted will inherit its settings from its domain group's parent until it is reconfigured.

Step 9 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Step 10 Click **Save**.

Configuring a Syslog Remote Destination Debug Policy

Before You Begin

Before configuring a syslog remote destination 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

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **Debug**.

Step 6 In the **Work** pane, click the **Syslog Policy** tab.

Step 7 In the **Work** pane, click the **Remote Destination** tab.

Step 8 In the **Actions** area, click **Create** and complete all applicable fields.

For **Operational Policies** under the **Domain Group root** node, it is not necessary to click **Create** to complete all applicable fields.

Name	Description
State field	Whether Cisco UCS stores component messages in the external log. This can be one of the following: • **enabled**—Component messages are logged in the external file. • **disabled**—Component messages are not logged in the external file.
Forwarding Facility drop-down list	The facility associated with the remote destination.
Level drop-down list	Select the lowest message level that you want the system to store. The system stores that level and above in the remote file. This can be one of the following: • **alerts** • **critical** • **debugging** • **emergencies** • **errors** • **information** • **notifications** • **warnings**
Hostname field	The hostname or IP address on which the remote log file resides. **Note** If you use a hostname rather than an IP 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 9 Click **Save**.

Deleting a Syslog Remote Destination Debug Policy

A syslog remote destination debug policy is deleted from a domain group under the domain group root. Syslog remote destination debug policies under the domain groups root cannot be deleted.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Expand the node for a domain group containing the policy to delete.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **Debug**.

Step 6 In the **Work** pane, click the **Syslog Policy** tab.

Step 7 In the **Work** pane, click the **Remote Destination** tab.

Step 8 In the **Actions** area, click **Delete**.
A policy that is deleted will inherit its settings from its domain group's parent until it is reconfigured.

Step 9 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Step 10 Click **Save**.

Configuring a Syslog Source Debug Policy

Before You Begin

Before configuring a syslog source 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

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **Debug**.

Step 6 In the **Work** pane, click the **Syslog Policy** tab.

Step 7 In the **Work** pane, click the **Source** tab.

Step 8 In the **Actions** area, click **Create** and complete all applicable fields.

For **Operational Policies** under the **Domain Group root** node, it is not necessary to click **Create** to complete all applicable fields.

Name	Description
Create button	Creates an instance of the policy that will be used by all Cisco UCS domains included in the selected domain group.
Import button	Allows you to import the policy from one of the Cisco UCS domains registered with Cisco UCS Central.
Delete button	Deletes the instance of the policy defined for the selected domain group. After you delete the policy, it remains greyed-out until you click **Save**. When you do so, Cisco UCS Central deletes the policy and any configuration data you may have specified. While you can create a new instance of the policy later, you cannot restore the configuration data from a deleted instance. To cancel the delete request, click **Reset**.
Audits drop-down list	If this field is **enabled**, Cisco UCS logs all system faults.
Events drop-down list	If this field is **enabled**, Cisco UCS logs all audit log events.
Faults drop-down list	If this field is **enabled**, Cisco UCS logs all system events.

Step 9 Click **Save**.

Deleting a Syslog Source Debug Policy

A syslog source debug policy is deleted from a domain group under the domain group root. Syslog source debug policies under the domain groups root cannot be deleted.

Procedure

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.
Step 3 Expand the node for a domain group containing the policy to delete.
Step 4 In the **Navigation** pane, click **Operational Policies**.
Step 5 In the **Work** pane, click **Debug**.
Step 6 In the **Work** pane, click the **Syslog Policy** tab.
Step 7 In the **Work** pane, click the **Source** tab.
Step 8 In the **Actions** area, click **Delete**.
A policy that is deleted will inherit its settings from its domain group's parent until it is reconfigured.

Step 9 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Step 10 Click **Save**.

Configuring a Syslog LogFile Debug Policy

Before You Begin

Before configuring a syslog logfile 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

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **Debug**.

Step 6 In the **Work** pane, click the **Syslog Policy** tab.

Step 7 In the **Work** pane, click the **LogFile** tab.

Step 8 In the **Actions** area, click **Create** and complete all applicable fields.
For **Operational Policies** under the **Domain Group root** node, it is not necessary to click **Create** to complete all applicable fields.

Name	Description
Create button	Creates an instance of the policy that will be used by all Cisco UCS domains included in the selected domain group.
Import button	Allows you to import the policy from one of the Cisco UCS domains registered with Cisco UCS Central.
Delete button	Deletes the instance of the policy defined for the selected domain group. After you delete the policy, it remains greyed-out until you click **Save**. When you do so, Cisco UCS Central deletes the policy and any configuration data you may have specified. While you can create a new instance of the policy later, you cannot restore the configuration data from a deleted instance. To cancel the delete request, click **Reset**.

Name	Description
System Log File field	Whether Cisco UCS stores messages in a system log file on the fabric interconnect. This can be one of the following: • **Enabled**—Messages are saved in the log file. • **Disabled**—Messages are not saved.
Level drop-down list	Select the lowest message level that you want the system to store. Cisco UCS stores that level and above in a file on the fabric interconnect. This can be one of the following: • **Emergencies** • **Alerts** • **Critical** • **Errors** • **Warnings** • **Notifications** • **Information** • **Debugging**
Name field	The name of the file in which the messages are logged. 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.
Size field	The maximum size, in bytes, the file can be before Cisco UCS begins to write over the oldest messages with the newest ones. Enter an integer between 4096 and 4194304.

Step 9 Click **Save**.

Deleting a Syslog LogFile Debug Policy

A syslog logfile debug policy is deleted from a domain group under the domain group root. Syslog logfile debug policies under the domain groups root cannot be deleted.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Expand the node for a domain group containing the policy to delete.

Step 4 In the **Navigation** pane, click **Operational Policies**.

Step 5 In the **Work** pane, click **Debug**.

Step 6 In the **Work** pane, click the **Syslog Policy** tab.

Step 7 In the **Work** pane, click the **LogFile** tab.

Step 8 In the **Actions** area, click **Delete**.
A policy that is deleted will inherit its settings from its domain group's parent until it is reconfigured.

Step 9 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Step 10 Click **Save**.