Cisco UCS Central Software User Manual, Release 1.1

First Published: October 31, 2013

Last Modified: March 06, 2014

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-30698-01

CONTENTS

Preface

Preface xxi

Audience xxi

Conventions xxi

Related Cisco UCS Documentation xxiii

Documentation Feedback xxiii

CHAPTER 1

Cisco UCS Central Overview 1

Introducing Cisco UCS Central 1

Cisco UCS Central Features 2

Multi-version Management Support 4

Feature Support Matrix 5

Cisco UCS Central GUI Overview 6

Logging in to the Cisco UCS Central GUI through HTTP 7

Logging in to the Cisco UCS Central GUI through HTTPS 7

Logging out of the Cisco UCS Central GUI 8

CHAPTER 2

License Management 9

Managing Licenses in Cisco UCS Central 9

Obtaining a License 10

Downloading a License from a Local File System 11

Downloading a License from a Remote File System 12

Installing a License 13

Deleting a License 13

CHAPTER 3

Managing Administrative Settings 15

Administrative Settings for Cisco UCS Central 15

Policies and Authentication 15

Users and Authentication 15
Creating Locally Authenticated Users 16
Creating Remote Users 16
Creating User Roles 17
Creating User Locales 17
Creating an Authentication Domain 17
Creating an LDAP Provider 18
Creating an LDAP Provider Group 18
Creating an LDAP Group Map 19
Deleting an LDAP Provider 19
Deleting an LDAP Provider Group 19
Deleting an LDAP Group Map 20
General Settings 20
Creating an SNMP Trap 21
Creating an SNMP User 21
Configuring an HTTPS Certificate 21
Configuring an NTP Server 22
Configuring a DNS Server 22
Configuring Fault Policy 23
Configuring Export Policy 23
IPv6 Configuration 23
Configuring IPv6 in Standalone Mode 23
Configuring IPv6 in HA mode 24
Key Rings 24
Creating a Key Ring 25
Creating a Trusted Point 25
Deleting a Key Ring 25
Deleting a Trusted Point 26
Administrative Settings for Cisco UCS Domains 26
Remote Access Policies 26
Configuring HTTP 26
Configuring an HTTP Remote Access Policy 26
Deleting an HTTP Remote Access Policy 27
Configuring Telnet 28
Configuring a Telnet Remote Access Policy 28

Deleting a Telnet Remote Access Policy 28
Configuring Web Session Limits 29
Configuring a Web Session Limits 29
Deleting a Web Session Limits 30
Configuring CIM XML 30
Configuring a CIM XML Remote Access Policy 30
Deleting a CIM XML Remote Access Policy 31
Configuring Interfaces Monitoring 31
Configuring an Interfaces Monitoring Remote Access Policy 31
Deleting an Interfaces Monitoring Remote Access Policy 32
Authentication Services 33
Guidelines and Recommendations for Remote Authentication Providers 33
User Attributes in Remote Authentication Providers 33
LDAP Providers 34
Creating an LDAP Provider 35
Configuring Default Settings for LDAP Providers 36
Deleting an LDAP Provider 36
Changing the LDAP Group Rule for an LDAP Provider 37
LDAP Group Maps 37
Nested LDAP Groups 38
Creating an LDAP Group Map 38
Deleting an LDAP Group Map 39
Configuring RADIUS Providers 39
Configuring Properties for RADIUS Providers 39
Creating a RADIUS Provider 40
Deleting a RADIUS Provider 41
Configuring TACACS+ Providers 41
Configuring Properties for TACACS+ Providers 41
Creating a TACACS+ Provider 42
Deleting a TACACS+ Provider 43
Configuring Multiple Authentication Systems 44
Multiple Authentication Systems 44
Provider Groups 44
Creating an LDAP Provider Group 45
Deleting an LDAP Provider Group 45

Creating a RADIUS Provider Group 46
Deleting a RADIUS Provider Group 46
Creating a TACACS+ Provider Group 47
Deleting a TACACS+ Provider Group 48
Authentication Domains 48
Creating an Authentication Domain 49
Selecting a Primary Authentication Service 49
Selecting the Console Authentication Service 49
Selecting the Default Authentication Service 50
Role Policy for Remote Users 50
Configuring the Role Policy for Remote Users 51
Configuring DNS Servers 51
Managing DNS Policies 51
Configuring a DNS Policy 51
Deleting a DNS Policy 52
Configuring a DNS Server for a DNS Policy 52
Deleting a DNS Server from a DNS Policy 53
Managing Power Policies 53
Configuring a Global Power Allocation Equipment Policy 53
Deleting a Global Power Allocation Equipment Policy 54
Configuring a Power Equipment Policy 54
Deleting a Power Equipment Policy 55
Managing Time Zones 55
Managing Time Zones 55
Configuring a Date and Time Policy 56
Deleting a Date and Time Policy 56
Configuring an NTP Server for a Date and Time Policy 57
Configuring Properties for an NTP Server 57
Deleting an NTP Server from a Date and Time Policy 58
SNMP Policies 58
SNMP Functional Overview 58
SNMP Notifications 59
SNMP Security Features 59
SNMP Security Levels and Privileges 60
SNMP Security Models and Levels 60

SNMP Support in Cisco UCS Central 61
Configuring an SNMP Policy 62
Creating an SNMP Trap 64
Creating an SNMP User 64
Deleting an SNMP Policy 65
Deleting an SNMP Trap 65
Deleting an SNMP User 66

CHAPTER 4 Domain Management 67
Domain Groups 67
Creating a Domain Group 68
Deleting a Domain Group 68
Changing Group Assignment for a Cisco UCS Domain 68
Domain Group and Registration Policies 69
Creating a Domain Group Policy 69
Deleting a Domain Group Policy 69
Creating a Registration Policy 70
Creating a Site Qualifier 70
Deleting a Site Qualifier 70
Creating an Address Qualifier 71
Deleting an Address Qualifier 71
Creating an Owner Qualifier 71
Deleting an Owner Qualifier 72
Deleting a Registration Policy 72
ID Range Qualification Policies 72
Creating an ID Range Qualification Policy 73
Deleting an ID Range Qualification Policy 73
Call Home Policies 73
Configuring a Call Home Policy 74
Deleting a Call Home Policy 79
Configuring a Profile for a Call Home Policy 79
Adding Email Recipients to a Call Home Profile 82
Deleting a Profile for a Call Home Policy 82
Configuring a Policy for a Call Home Policy 83
Deleting a Policy for a Call Home Policy 84

CHAPTER 5 **Remote Management** 85

Remote Management 85

Recommission a Server 86

Decommissioning a Server 86

Removing a Server 87

Resetting a Server CIMC 88

Resetting Server CMOS 88

Resetting a Server IPMI 89

Resetting a Server KVM 90

Turning on/off Server Locator LED 90

Acknowledging a Chassis 91

Decommissioning a Chassis 92

Recommissioning a Chassis 92

Turning on or off the Chassis Locator LED 93

Acknowledging a Fabric Extender 94

Decommissioning a Fabric Extender 94

Recommissioning a Fabric Extender 95

Removing a Fabric Extender 95

Turning on of off Fabric Extender Locator LED 96

Remote Tech Support for UCS Domains 96

Creating a Tech Support File for a UCS Domain 97

CHAPTER 6 **Firmware Management** 99

Downloading Firmware 99

Firmware Download from Cisco 99

Firmware Library of Images 99

Configuring Firmware Download from Cisco 100

Downloading a Firmware Image from Cisco 100

Downloading Firmware from a Remote Location 101

Downloading Firmware from a Local File System 101

Viewing Image Download Faults 102

Viewing Firmware Images in the Library 102

Deleting Image Metadata from the Library of Images 103

Upgrading Firmware in Cisco UCS Domains 103

Firmware Upgrades for Cisco UCS Domains 103
Configuring an Infrastructure Firmware Upgrade for a Cisco UCS Domain 104
Acknowledging a Pending Activity 105
Deleting an Infrastructure Firmware Package 105
Creating a Host Firmware Package 106
Deploying a Host Firmware Upgrade 106
Deleting a Host Firmware Package 107
Scheduling Firmware Upgrades 107
Firmware Upgrade Schedules 107
Creating a Maintenance Policy 107
Creating a One Time Occurrence Schedule 108
Creating a Recurring Occurrence Schedule 109
Deleting a Firmware Upgrade Schedule 109
Managing Capability Catalog 109
Capability Catalog 109
Contents of the Capability Catalog 110
Updates to the Capability Catalog 110
Configuring a Capability Catalog Update for a Cisco UCS Domain 111

CHAPTER 7 Monitoring Inventory 113
Inventory Management 113
Physical Inventory 114
Service Profiles and Templates 114
Overview to Global Logical Resources 114
Configuring Inventory Data Collection Schedule 115
Viewing Inventory Details 115
Viewing Inventory Details of a Server 115
Viewing Details on an Individual Cisco UCS Domain 116
Viewing Service Profiles 116
Viewing Service Profile Details 116
Viewing Service Profile Templates 117
Viewing Local service profiles 117
Creating an Organization Under Sub-Organizations 118

CHAPTER 8 Managing Backup and Restore 119

Backup and Import in Cisco UCS Central 119
Considerations and Recommendations for Backup Operations 120
Backup Types 121
System Restore 122
Enabling Backup in Cisco UCS Central 122
Backing up and Restoring Cisco UCS Central 122
Creating a Full-State Backup Policy for Cisco UCS Central 123
Creating a Config-all Backup Policy for Cisco UCS Central 123
Creating an On Demand Backup for Cisco UCS Central 124
Creating a Backup Schedule for Cisco UCS Central 125
Deleting a Cisco UCS Central Backup Operation 125
Backing up and Restoring Cisco UCS Domains 126
Creating a Full-State Backup Policy for Cisco UCS Domains 126
Creating a Config-All Export Policy for Cisco UCS Domains 127
Import Configuration 127
Import Methods 128
Importing Cisco UCS Central Configuration 128
Importing Cisco UCS Manager Configuration 129
Running an Import Operation 130
Deleting Import Operations 130

CHAPTER 9 **Working with Policies** 131
Global Policies 131
Creating a Global Policy 131
Including a Global Policy in a Local Service Profile 132
Policy Conversion Between Global and Local 133
Converting a Global Policy to a Local Policy 133
Converting a Local Policy to a Global Policy 134
Policy Resolution between Cisco UCS Manager and Cisco UCS Central 134
Consequences of Policy Resolution Changes 135
Consequences of Service Profile Changes on Policy Resolution 139
Modifying Policy Resolutions between Cisco UCS Manager and Cisco UCS Central using the Cisco UCS Manager GUI 140
Policy and Policy Component Import in Cisco UCS Central 140
Cautions and Guidelines for Policy or Component Import 141

Policies and Policy Dependents 142
Importing a Policy or a Policy Component from a UCS Domain 144
Local Policies 145
Statistics Threshold Policy 145
Creating a Threshold Policy 146
Adding a Threshold Class to an Existing Threshold Policy 147
Adding a Threshold Definition to an Existing Threshold Class 147
Deleting a Threshold Policy 148
Deleting a Threshold Class from a Threshold Policy 148
Deleting a Threshold Definition from a Threshold Class 149

CHAPTER 10 **Service Profiles and Templates 151**
Global Service Profiles 151
Guidelines and Cautions for Global Service Profile 152
Creating a Global Service Profile 153
Creating Global Service Profiles from a Service Profile Template 154
Deleting a Global Service Profile 154
Global Service Profile Deployment 154
Changing the Service Profile Association 155
Unassigning a Server from a Global Service Profile 156
Renaming a Global Service Profile 156
Changing the UUID in a Service Profile 157
Resetting the UUID for a Global Service Profile 157
Resetting the Management IP for a Global Service Profile 158
Global Service Profile Template 158
Creating a Global Service Profile Template 158
Cloning a Global Service Profile Template 160
Deleting a Global Service Profile Template 160
Binding a Global Service Profile to a Service Profile Template 160
Unbinding a Global Service Profile from a Service Profile Template 161
Scheduling Service Profile Updates 161
Deferred Deployment of Service Profiles 161
Guidelines and Limitations for Deferred Deployment 162
Deferred Deployment Schedules 163
Maintenance Policy 163

Creating a Maintenance Policy 164
Creating a Schedule 164
Creating a One Time Occurrence Schedule 165
Creating a Recurring Occurrence for a Schedule 165
Pending Activities 166
Viewing Pending Activities 166

CHAPTER 11 Server Policies 167
Ethernet and Fibre Channel Adapter Policies 167
Creating an Ethernet Adapter Policy 168
Deleting an Ethernet Adapter Policy 169
Server BIOS Settings 169
Main BIOS Settings 170
Processor BIOS Settings 171
Intel Directed I/O BIOS Settings 176
RAS Memory BIOS Settings 177
Serial Port BIOS Settings 179
USB BIOS Settings 180
PCI Configuration BIOS Settings 181
Boot Options BIOS Settings 182
Server Management BIOS Settings 183
BIOS Policy 187
Default BIOS Settings 187
Creating a BIOS Policy 187
Modifying a BIOS Policy 188
Deleting a BIOS Policy 189
IPMI Access Profile 189
Creating an IPMI Access Profile 189
Adding an IPMI User to an IPMI Access Profile 190
Deleting an IPMI Access Profile 190
Deleting an IPMI User from an IPMI Access Profile 191
Local Disk Configuration Policy 191
Boot Policy 192
Creating a Boot Policy 192
Modifying a Boot Policy 193

Deleting a Boot Policy 194
LAN Boot 194
Configuring a LAN Boot for a Boot Policy 194
SAN Boot 195
Configuring a SAN Boot for a Boot Policy 195
Adding a SAN Boot Target 196
iSCSI Boot 196
iSCSI Boot Process 197
iSCSI Boot Guidelines and Prerequisites 197
Configuring an iSCSI Boot for a Boot Policy 199
Creating an iSCSI Adapter Policy 199
Deleting an iSCSI Adapter Policy 200
Creating an iSCSI Authentication Profile 200
Deleting an iSCSI Authentication Profile 200
Guidelines for all Local Disk Configuration Policies 201
Guidelines for Local Disk Configuration Policies Configured for RAID 201
Creating a Local Disk Configuration Policy 203
Deleting a Local Disk Configuration Policy 203
Power Control Policy 204
Creating a Power Control Policy 204
Deleting a Power Control Policy 204
Scrub Policy 205
Creating a Scrub Policy 206
Deleting a Scrub Policy 206
Serial over LAN Policy 207
Creating a Serial over LAN Policy 207
Deleting a Serial over LAN Policy 207
Server Pool Policy 208
Creating a Server Pool Policy 208
Deleting a Server Pool Policy 208
Server Pool Policy Qualifications 209
Creating Server Pool Policy Qualifications 209
Creating a Domain Qualification 210
Creating an Adapter Qualification 211
Creating a Memory Qualification 211

Creating a Processor Qualification 212
Creating a Storage Qualification 212
Creating a Server PID Qualification 213
Creating a Chassis/Server Qualification 213
Creating a Server Qualification 214
Creating an Address Qualification 214
Creating an Owner Qualification 215
Creating a Rack Qualification 215
Creating a Site Qualification 216
Deleting Server Pool Policy Qualifications 216
Deleting a Domain Qualification from a Policy Qualification 216
Deleting a Chassis/Server Qualification from a Domain Qualification 217
Deleting a Server Qualification from a Chassis/Server Qualification 217
Deleting an Address Qualification from a Domain Qualification 218
Deleting an Owner Qualification from a Domain Qualification 218
Deleting a Rack Qualification from a Domain Qualification 219
Deleting a Site Qualification from a Domain Qualification 219
Deleting an Adapter Qualification from a Policy Qualification 220
Deleting a Memory Qualification from a Policy Qualification 220
Deleting a Processor Qualification from a Policy Qualification 221
Deleting a Storage Qualification from a Policy Qualification 221
Deleting a Server Qualification from a Policy Qualification 222
vNIC/vHBA Placement Policies 222
Creating a vNIC/vHBA Placement Policy 223
Deleting a vNIC/vHBA Placement Policy 223
vCon to Adapter Placement 223
vCon to Adapter Placement for N20-B6620-2 and N20-B6625-2 Blade Servers 224
vCon to Adapter Placement for All Other Supported Servers 224
vNIC/vHBA to vCon Assignment 225

CHAPTER 12 **Network Policies 229**
vNIC Template 229
Creating a vNIC Template 230
Deleting a vNIC Template 230
Default vNIC Behavior Policy 230

Configuring Default vNIC Behavior 231
LAN and SAN Connectivity Policies 231
Privileges Required for LAN and SAN Connectivity Policies 232
Creating a LAN Connectivity Policy 232
Creating a vNIC for a LAN Connectivity Policy 233
Creating an iSCSI vNIC for a LAN Connectivity Policy 233
Deleting a LAN Connectivity Policy 234
Deleting a vNIC from a LAN Connectivity Policy 234
Deleting an iSCSI vNIC from a LAN Connectivity Policy 235
Network Control Policy 235
Creating a Network Control Policy 236
Deleting a Network Control Policy 237
Dynamic vNIC Connection Policy 237
Creating a Dynamic vNIC Connections Policy 237
Deleting a Dynamic vNIC Connections Policy 238
Quality of Service Policy 238
Creating a QoS Policy 238
Deleting a QoS Policy 239

CHAPTER 13 Storage Policies 241
vHBA Template 241
Creating a vHBA Template 241
Deleting a vHBA Template 242
Default vHBA Behavior Policy 242
Configuring Default vHBA Behavior 242
Ethernet and Fibre Channel Adapter Policies 243
Creating a Fibre Channel Adapter Policy 244
Deleting a Fibre Channel Adapter Policy 244
LAN and SAN Connectivity Policies 245
Privileges Required for LAN and SAN Connectivity Policies 245
Creating a SAN Connectivity Policy 246
Deleting a SAN Connectivity Policy 246

CHAPTER 14 Statistics Management 247
Statistics Management 247

Statistics Data Collection in Cisco UCS Central 248
External Database for Statistics 248
Standard Reports 250
Generating a Network Report 252
Generating a Peak Fan Speed Report 253
Generating a Peak Temperature Report 253
Generating an Average Power Report 254
Custom Reports 254
Creating a Custom Report Group 255
Deleting a Report Group 255
Creating a Custom Report 256
Running a Custom Report 256
Deleting a Custom Report 257

CHAPTER 15 System Management 259
Managing DNS Policies 259
Configuring a DNS Policy 259
Deleting a DNS Policy 260
Configuring a DNS Server for a DNS Policy 260
Deleting a DNS Server from a DNS Policy 261
Managing Power Policies 261
Configuring a Global Power Allocation Equipment Policy 262
Deleting a Global Power Allocation Equipment Policy 262
Configuring a Power Equipment Policy 262
Deleting a Power Equipment Policy 263
Managing Time Zones 263
Configuring a Date and Time Policy 264
Deleting a Date and Time Policy 264
Configuring an NTP Server for a Date and Time Policy 265
Configuring Properties for an NTP Server 265
Deleting an NTP Server from a Date and Time Policy 266
SNMP Policies 266
SNMP Functional Overview 267
SNMP Support in Cisco UCS Central 267
SNMP Notifications 268

SNMP Security Features 269
SNMP Security Levels and Privileges 269
SNMP Security Models and Levels 269
Configuring an SNMP Policy 270
Creating an SNMP Trap 272
Creating an SNMP User 272
Deleting an SNMP Policy 273
Deleting an SNMP Trap 273
Deleting an SNMP User 274
About High Availability in Cisco UCS Central 274
Cautions and Guidelines for Using High Availability 275

CHAPTER 16 Monitoring Logs 277
System Event Log 277
System Event Log 277
Configuring a SEL Policy 278
Deleting a SEL Policy 278
Configuring Settings for Faults, Events and Logs 279
Configuring Global Fault Policies 279
Configuring a Global Fault Debug Policy 279
Deleting a Global Fault Debug Policy 279
Configuring TFTP Core Export Policies 280
Core File Exporter 280
Configuring a TFTP Core Export Debug Policy 280
Deleting a TFTP Core Export Debug Policy 280
Configuring Syslog Policies 281
Configuring a Syslog Console Debug Policy 281
Deleting a Syslog Console Debug Policy 282
Configuring a Syslog Monitor Debug Policy 282
Deleting a Syslog Monitor Debug Policy 283
Configuring a Syslog Remote Destination Debug Policy 283
Deleting a Syslog Remote Destination Debug Policy 284
Configuring a Syslog Source Debug Policy 284
Deleting a Syslog Source Debug Policy 285
Configuring a Syslog LogFile Debug Policy 285

Deleting a Syslog LogFile Debug Policy 286
Viewing Logs and Faults 286
Active Sessions 286

CHAPTER 17 User Management 289
Cisco UCS Central User Accounts 289
Guidelines for Creating Usernames 290
Guidelines for Creating Passwords 290
Password Profile for Locally Authenticated Users 291
Configuring the Maximum Number of Password Changes for a Change Interval 292
Configuring a No Change Interval for Passwords 293
Configuring the Password History Count 293
Creating a Locally Authenticated User Account 294
Reserved Words: Locally Authenticated User Accounts 297
Deleting a Locally Authenticated User Account 298
Enabling a Locally Authenticated User Account 298
Disabling a Locally Authenticated User Account 299
Changing the Roles Assigned to a Locally Authenticated User Account 299
Enabling the Password Strength Check for Locally Authenticated Users 300
Clearing the Password History for a Locally Authenticated User 300
Web Session Limits for User Accounts 301
Monitoring User Sessions 301
Role-Based Access Control 302
User Roles 302
Default User Roles 303
Privileges 304
Creating a User Role 306
Reserved Words: User Roles 306
Deleting a User Role 307
Adding Privileges to a User Role 307
Removing Privileges from a User Role 308
User Locales 308
Creating a User Locale 309
Deleting a User Locale 310
Assigning an Organization to a User Locale 311

Deleting an Organization from a User Locale 311
Changing the Locales Assigned to a Locally Authenticated User Account 312
User Organizations 312
Creating a User Organization 313
Deleting a User Organization 313
Creating a User Sub-Organization 314
Deleting a User Sub-Organization 314

Preface

This preface includes the following sections:

- Audience, page xxi
- Conventions, page xxi
- Related Cisco UCS Documentation, page xxiii
- Documentation Feedback, page xxiii

Audience

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

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

Conventions

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

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

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

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

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

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

Warning IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS

Related Cisco UCS Documentation

Documentation Roadmaps

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

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

Other Documentation Resources

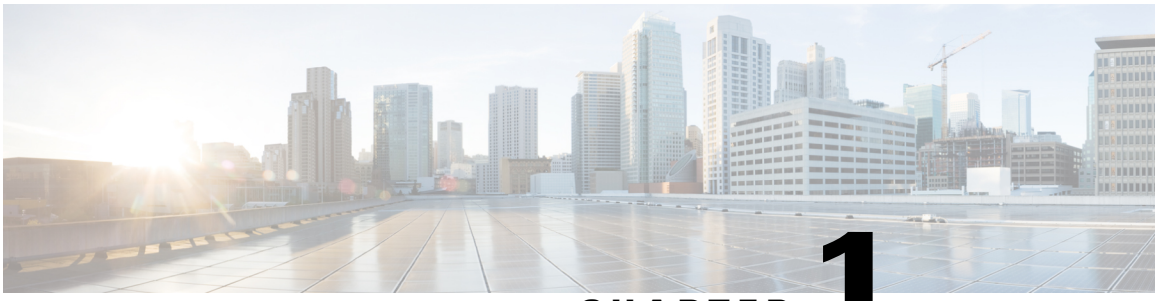
An ISO file containing all B and C-Series documents is available at the following URL: http://www.cisco.com/cisco/software/type.html?mdfid=283853163&flowid=25821. From this page, click **Unified Computing System (UCS) Documentation Roadmap Bundle**.

The ISO file is updated after every major documentation release.

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

Documentation Feedback

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



CHAPTER 1

Cisco UCS Central Overview

This chapter includes the following sections:

- Introducing Cisco UCS Central, page 1
- Cisco UCS Central Features, page 2
- Multi-version Management Support, page 4
- Feature Support Matrix , page 5
- Cisco UCS Central GUI Overview, page 6

Introducing Cisco UCS Central

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

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

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

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

Cisco UCS Central Features

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

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

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

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

Multi-version Management Support

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

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

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

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

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

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

Supported Features in Cisco UCS Manager

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

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

Management Exclusion

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

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

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

Feature Support Matrix

The following table provides a list of features in Cisco UCS Central, release 1.1(2a) and Cisco UCS Manager release versions in which these features are supported:

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

Cisco UCS Central Features	Supported Cisco UCS Manager Versions		
	2.1(2a)*	2.2(1b)	Upcoming 2.2 Maintenance Release
Multi-version management support and viewing supported Cisco UCS Manager features	No	Yes	Yes
Importing policy/policy component and resources	No	Yes	Yes
Specifying remote location for backup image files	No	No	Yes
3rd party certificate	No	No	Yes

Cisco UCS Central Features	Supported Cisco UCS Manager Versions		
	2.1(2a)*	2.2(1b)	Upcoming 2.2 Maintenance Release
IPv6 inband management support	No	No	Yes

Note

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

Cisco UCS Central GUI Overview

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:

- **Domains—**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 the option to create global service profiles and policies and 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 network policies, common VLANs, IP pools and MAC pools configured in Cisco UCS Central.
- **Storage—**Provides access to the global storage policies, fabric specific VSANs, global IQN pools and WWN pools configured in Cisco UCS Central.

- **Operations Management—**Provides access to manage registered Cisco UCS Domain settings and global configurations:
  - 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
- **Statistics—**Provides option to generate reports on network, cooling, temperature, and power. You can create Standard and Custom reports.
- **Logs and Faults—**Provides view audit logs, event logs, and faults.
- **Administration—**Provides access to manage Cisco UCS Central management settings. , 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.
- **Import—**Provides ability to import policies/policy components and resources from registered Cisco UCS domains into Cisco UCS Central.

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:

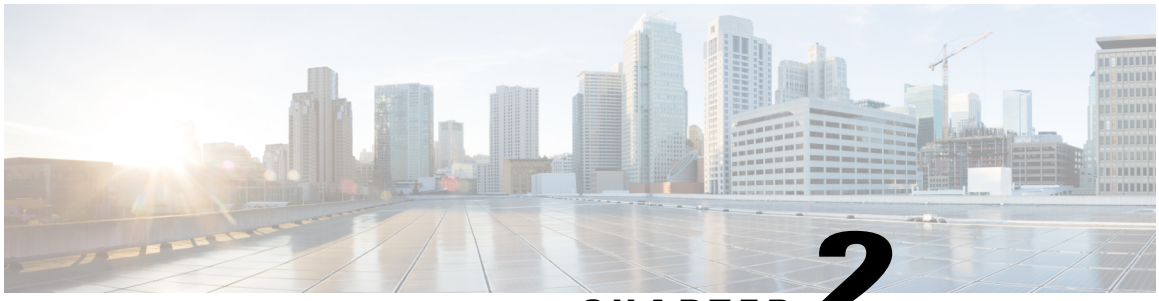
a) Enter your username and password.

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.



CHAPTER 2

License Management

This chapter includes the following sections:

- Managing Licenses in Cisco UCS Central, page 9
- Obtaining a License, page 10
- Downloading a License from a Local File System, page 11
- Downloading a License from a Remote File System, page 12
- Installing a License, page 13
- Deleting a License, page 13

Managing Licenses in Cisco UCS Central

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

Grace Period

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

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

License Types

The following are the two available license types:

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

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

Obtaining a License

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

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

Before You Begin

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

Procedure

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

Step 2 In the **Navigation** pane, click **License Management**.

Step 3 In the Work pane, select the **License** tab.

Step 4 In the **UCS Central Details** area, click **GUID** to copy the GUID to Clipboard.

GUID is unique to each Cisco UCS Central instance for obtaining licenses.

Step 5 Click **Cisco SWIFT** to open the License Administration Portal.

Step 6 Login to the License Administration Portal, and click **Continue to Product License Registration**.

Step 7 On the **Quickstart** page, enter the PAK in the **Enter a Single PAK or Token to fulfill** field and click **Fulfill Single PAK/Token**.

Step 8 On the **Assign SKUs to Devices** page, check the **Quantity Available** checkbox next to the PAK that you entered.

Step 9 Enter the GUID in the **GUID** field, and click **Assign**.

Step 10 Click **Next**.

Step 11 On the **Review** page, enter your email address, select the user ID, and check the **License Agreement** checkbox.

Step 12 Click **Get License**.
Cisco sends you the license zip file by email. The license file is digitally signed to authorize use on only the specified Cisco UCS domain.

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

What to Do Next

Unzip the license file, and using Cisco UCS Central GUI, download the license into the system.

Downloading a License from a Local File System

Before You Begin

To download a license from the local file system to Cisco UCS Central, make sure you have the following:

- Obtained the license from Cisco and saved it to your local system.
- Administrative permission for Cisco UCS Central to perform this task.

Procedure

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

Step 2 In the **Navigation** pane, click **License Management**.

Step 3 In the **Work** pane, click on the **Licenses** tab.

Step 4 Under the **Licenses** tab, click **Download**.

Step 5 In the **Filename** dialog box, type the full path and the name of the license.
If you do not know the exact path to the folder where the license is located, click **Choose File** to navigate and select the file.

Step 6 Click **OK**.
Cisco UCS Central begins downloading the license. You can monitor the status of the download on the **Download Tasks** tab.

Downloading a License from a Remote File System

Before You Begin

To download a license from a remote location to Cisco UCS Central, make sure you have the following:

- Obtained the license from Cisco and saved it to the remote location from where you want to download. If that is a FTP, SCP or SFTP server, then the username and Password for access authentication.
- Administrative permission for Cisco UCS Central to perform this task.

Procedure

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

Step 2 In the **Navigation** pane, click **License Management**.

Step 3 In the **Work** pane, click on the **Licenses** tab.

Step 4 Under the **Licenses** tab, click **Download**.

Step 5 In the **Download License** dialog box, click the **Remote File System** radio button.

Step 6 Select a protocol to be used while communicating with the remote server.
It can be one of the following protocols:

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

Step 7 In the **Server** field, enter the IP address or host name of the server on which the license file resides.

Step 8 In the **License File Name** field, enter the name of the license file you want to download.

Step 9 In the **Path** field, enter the absolute path to the license file on the remote server, if required.
If you use SCP, the absolute path is always required. If you use any other protocol, you may not need to specify a remote path if the file resides in the default download folder. For details about how your file server is configured, contact your system administrator.

Step 10 In the **User Name** field, enter the user name to log into the remote server.
If you selected TFTP, this field does not apply.

Step 11 In the **Password** field, enter the password for the remote server user name.
If you selected TFTP, this field does not apply.

Step 12 Click **OK**.
Cisco UCS Central begins downloading the license. You can monitor the status of the download on the **Download Tasks** tab.

Installing a License

Make sure the license is downloaded in Cisco UCS Central.

Procedure

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

Step 2 In the **Navigation** pane, click **License Management**.

Step 3 In the **Work** pane, click the **Licenses** tab.
You can view lists of all downloaded licenses here. Check for licenses with **Validated** status in **Overall License Status** column. These are available for installation.

Step 4 Choose the license you want to install and click **Install**.
The **Overall License Status** column displays the status of the installation. When you initiate the installation, the status in this column displays **Install-pending**. After the license is installed, the status changes to **Installed**.

Deleting a License

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

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

Procedure

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

Step 2 In the **Navigation** pane, click **License Management**.

Step 3 In the **Work** pane, click the **Licenses** tab.

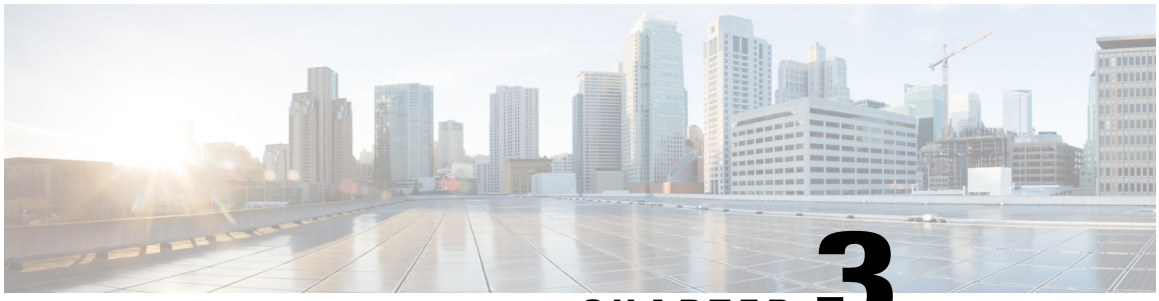
Step 4 Select the license you want to uninstall.

Step 5 Click **Delete**.

Step 6 Click **Yes** in the confirmation dialog box.
The license file is deleted from Cisco UCS Central.

What to Do Next

Delete the associated license download task from **Operations Management** > **License Management** > **Download Tasks** tab for this license. This removes any related instances of this license from the system.



CHAPTER 3

Managing Administrative Settings

This chapter includes the following sections:

- Administrative Settings for Cisco UCS Central, page 15
- Policies and Authentication, page 15
- Administrative Settings for Cisco UCS Domains, page 26

Administrative Settings for Cisco UCS Central

Policies and Authentication

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

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

- General Settings
- Users and Authentication

Users and Authentication

Cisco UCS Central supports creating local and remote users to access the system. You can configure up to 128 user accounts in each Cisco UCS Central domain. Each of these users must have a unique username and password. For more information, see User Management, on page 289.

Cisco UCS Central uses LDAP for native authentication, but excludes RADIUS and TACACS+ authentication in this release. However, RADIUS, TACACS+ and LDAP authentication are supported in locally managed Cisco UCS domains. For more information, see Managing Administrative Settings, on page 15.

Creating Locally Authenticated Users

Procedure

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

Step 2 In the **Navigation** pane, click **Users and Authentication**.

Step 3 In the **Work** pane, click **Local Users**.

Step 4 In the **Actions** area, click **Create Locally Authenticated Users** and complete all the fields.

Step 5 Click the **Roles/Locales** tab so assign the type of role or locale, and click the **SSH** tab to assign the type of security key.

Step 6 Click **OK**.

Step 7 Click **Save**.

Creating Remote Users

Procedure

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

Step 2 In the **Navigation** pane, click **Users and Authentication**.

Step 3 In the **Work** pane, click **Remote Users**.

Step 4 In the **Actions** area, click **Create Remote Users** and complete all the fields.

Step 5 Click the **Roles/Locales** tab so assign the type of role or locale, and click the **SSH** tab to assign the type of security key.

Step 6 Click **OK**.

Step 7 Click **Save**.

Creating User Roles

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **Users and Authentication**.
Step 3 In the **Work** pane, click **Roles**.
Step 4 In the **Actions** area, click **Create Role** and complete all the fields.
Step 5 Click **OK**.
Step 6 Click **Save**.

Creating User Locales

Before You Begin

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **Users and Authentication**.
Step 3 In the **Work** pane, click **Locales**.
Step 4 In the **Actions** area, click **Create Locales** and complete all the fields.
Step 5 Click **Assign/Unassign Organization**, and/or **Assign/Unassign Domain Group**, to assign or unassign organizations and/or domain groups to the locale selected from Cisco UCS Central.
Step 6 Click **OK**.
Step 7 Click **Save**.

Creating an Authentication Domain

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

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **Users and Authentication**.
Step 3 In the **Work** pane, click **Authentication Domains**.
Step 4 In the **Actions** area, click **Create Authentication Domain** and complete all the fields.
Step 5 Click **OK**.
Step 6 Click **Save**.

Creating an LDAP Provider

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **Users and Authentication**.
Step 3 In the **Work** pane, click **LDAP**.
Step 4 Click **Providers**.
Step 5 In the **Actions** area, click **Create LDAP Provider** and complete all the fields.
Step 6 Click **OK**.
Step 7 Click **Save**.

Creating an LDAP Provider Group

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **Users and Authentication**.
Step 3 In the **Work** pane, click **LDAP**.
Step 4 Click **Provider Groups**.
Step 5 In the **Actions** area, click **Create LDAP Provider Group** and complete all the fields.
Step 6 Click **OK**.
Step 7 Click **Save**.

Creating an LDAP Group Map

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **Users and Authentication**.
Step 3 In the **Work** pane, click **LDAP**.
Step 4 Click **Group Maps**.
Step 5 In the **Actions** area, click **Create LDAP Group Map** and complete all the fields.
Step 6 Click **OK**.
Step 7 Click **Save**.

Deleting an LDAP Provider

Before You Begin

You need to create an LDAP provider.

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **Users and Authentication**.
Step 3 In the **Work** pane, click **LDAP**.
Step 4 Click **LDAP Providers**.
Step 5 In the **Actions** area, right-click the LDAP provider you wish to remove and click **Delete LDAP Provider**.
Step 6 Click **Save**.

Deleting an LDAP Provider Group

Before You Begin

You need to create an LDAP provider group.

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **Users and Authentication**.
Step 3 In the **Work** pane, click **LDAP**.
Step 4 Click **Provider Groups**.
Step 5 In the **Actions** area, right-click the provider group you wish to remove and click **Delete LDAP Provider Group**.
Step 6 Click **Save**.

Deleting an LDAP Group Map

Before You Begin

You need to create an LDAP group map.

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **Users and Authentication**.
Step 3 In the **Work** pane, click **LDAP**.
Step 4 Click **Group Maps**.
Step 5 In the **Actions** area, right-click the LDAP map you wish to remove and click **Delete LDAP Group Map**.
Step 6 Click **Save**.

General Settings

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

Creating an SNMP Trap

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **General**.
Step 3 In the **Work** pane, click **SNMP**.
Step 4 In the **Properties** area, select the **enabled** radio button.
By default the Admin State is disabled. You need to manually change it to enabled.
Step 5 In the **Actions** area, click **Create SNMP Trap** and complete all the fields.
Step 6 Click **OK**.
Step 7 Click **Save**.

What to Do Next

Create an SNMP user.

Creating an SNMP User

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **General**.
Step 3 In the **Work** pane, click **SNMP**.
Step 4 In the **Actions** area, click **Create SNMP User** and complete all the fields.
Step 5 Click **OK**.
Step 6 Click **Save**.

Configuring an HTTPS Certificate

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **General**.
Step 3 In the **Work** pane, click **HTTPS**.
Step 4 In the **Actions** area, select a third party key ring from the **Key Ring** drop down list.
Step 5 Click **Save**.

Configuring an NTP Server

Cisco UCS Central supports global date and time policies based on international time zones and a defined NTP server.

Before You Begin

To configure an NTP server for Cisco UCS Central, you must first create a date and time policy.

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **General**.
Step 3 In the **Work** pane, click **Date/Time** and select a time zone from the **Time Zone** drop down list.
Step 4 In the **Actions** area, click **Add NTP Server**.
Step 5 Click **OK**.
Step 6 Click **Save**.

Configuring a DNS Server

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **General**.
Step 3 In the **Work** pane, click **DNS**.
Step 4 In the **Actions** area, click **Add DNS Server** and complete all the fields.
Step 5 Click **OK**.
Step 6 Click **Save**.

Configuring Fault Policy

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **General**.
Step 3 In the **Work** pane, click **Fault Policy**.
Step 4 In the **Actions** area, complete all the fields.
Step 5 Click **Save**.

What to Do Next

Configuring Export Policy

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **General**.
Step 3 In the **Work** pane, click **TFTP Core Export Policy**.
Step 4 In the **Actions** area, complete all the fields.
Step 5 Click **Save**.

IPv6 Configuration

You can enable IPv6 on Cisco UCS Central in the standalone and High Availability (HA) modes. Cisco UCS Central configured on a single virtual machine is a standalone setup. A standalone setup is not part of any cluster. A UCS Central HA setup comprises two virtual machines, also known as primary node and secondary node respectively.

These virtual machines form an HA cluster, which is accessed through a common IP address. This IP address is known as a cluster IP address or a virtual IP address. You can assign an IPv6 address to the virtual IP Address (VIP) in addition to the IPv4 address.

Configuring IPv6 in Standalone Mode

Procedure

Step 1 On the menu bar, click **Administration**
Step 2 In the Navigation pane, select General.

By default the **General** tab would display tabs in the work pane

Step 3 Under the **Management Interface** tab, in the Node A area, click the **IPv6** tab, and complete all the required fields.

Step 4 Click **Save**.

Configuring IPv6 in HA mode

Procedure

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

Step 2 In the Navigation pane, select General.
By default the **General** tab would display tabs in the work pane.

Step 3 Under the **Management Interface** tab, in the Node A and Node B area, click the **IPv6** tab, and complete all the required fields.

Step 4 Click **Save**.

Step 5 In the main area above the Nodes, add the Virtual IPv6 address information.

Step 6 Click **Save**.

Key Rings

Cisco UCS Central allows creation of key rings as a third party certificate for stronger authentication. HTTPS uses components of the Public Key Infrastructure (PKI) to establish secure communications between two devices.

Each PKI device holds a pair of asymmetric Rivest-Shamir-Adleman (RSA) encryption keys, one kept private and one made public, stored in an internal key ring. A message encrypted with either key can be decrypted with the other key. To send an encrypted message, the sender encrypts the message with the receiver's public key, and the receiver decrypts the message using its own private key. A sender can also prove its ownership of a public key by encrypting (also called 'signing') a known message with its own private key. If a receiver can successfully decrypt the message using the public key in question, the sender's possession of the corresponding private key is proven. Encryption keys can vary in length, with typical lengths from 2048 bits to 4096 bits. In general, a longer key is more secure than a shorter key. Cisco UCS Central provides a default key ring with an initial 2048-bit key pair, and allows you to create additional key rings.

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

Creating a Key Ring

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **Users and Authentication**.
Step 3 In the **Work** pane, click **Certificates**.
Step 4 In the **Actions** area, click **Create Key Ring** and complete all the fields.
Step 5 In the **Certificate Request Actions** area, click **Create** and complete all the fields.
Step 6 Click **OK**.
Step 7 Click **Save**.

Creating a Trusted Point

Cisco UCS Central allows you to create a trusted point containing the certificate of the root certificate authority (CA) and a subordinate CA in a bundled format. The root CA must contain a primary and self-signed certificate.

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **Users and Authentication**.
Step 3 In the **Work** pane, click **Certificates**.
Step 4 In the **Actions** area, click **Create Trusted Point** and complete all the fields.
Step 5 Click **OK**.
Step 6 Click **Save**.

Deleting a Key Ring

Before You Begin

Ensure that the HTTPS is not using the key ring.

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **Users and Authentication**.
Step 3 In the **Work** pane, click **Certificates**.
Step 4 In the **KeyRings Actions** area, right-click the key ring you want to delete and choose**Delete**.
Step 5 Click **Yes** in the confirmation dialog box.

The key ring is deleted from Cisco UCS Central.

Deleting a Trusted Point

Before You Begin

Ensure that the trusted point is not in use.

Procedure

Step 1 On the menu bar, click **Administration**.
Step 2 In the **Navigation** pane, click **Users and Authentication**.
Step 3 In the **Work** pane, click **Certificates**.
Step 4 In the **KeyRings Actions** area, right-click the trusted point you want to delete and choose**Delete**.
Step 5 Click **Yes** in the confirmation dialog box.
The trusted point is deleted from Cisco UCS Central.

Administrative Settings for Cisco UCS Domains

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, 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.

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, 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.

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

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, 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.
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

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, 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.

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, 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.
a) In the **Monitoring Mechanism** area, select **Mii Status** to select Media Independent Interface Monitoring.
b) In the **Monitoring Mechanism** area, select **Ping ARP Targets** to select ARP Target Monitoring.
c) In the **Monitoring Mechanism** area, select **Ping Gateway** to select Gateway Ping Monitoring.
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**.

Authentication Services

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

Guidelines and Recommendations for Remote Authentication Providers

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

User Accounts in Remote Authentication Services

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

User Roles in Remote Authentication Services

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

Local and Remote User Authentication Support

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

User Attributes in Remote Authentication Providers

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

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

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

Table 1: Comparison of User Attributes by Remote Authentication Provider

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

Sample OID for LDAP User Attribute

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

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

LDAP Providers

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

LDAP Provider Groups

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

Creating an LDAP Provider

Cisco UCS Central supports a maximum of 16 LDAP providers.

Before You Begin

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

- In the Cisco UCS Central, configure one of the following:
  - LDAP groups: LDAP groups contain user role and locale information.
  - 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 Central 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, click **Operational Policies**.
Step 4 In the **Work** pane, click **Security**.
Step 5 In the **Work** pane, expand **LDAP** and click **Providers**.
Step 6 Click **Create LDAP Provider** and fill in required information in all fields.
Step 7 Click **OK**.

What to Do Next

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

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

Configuring Default Settings for LDAP Providers

You can configure the default settings for all providers defined in Cisco UCS Central from this **Properties (LDAP)** dialog box. If an individual provider includes a setting for any of these properties, Cisco UCS uses that setting and ignores the default setting.

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, 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.
Step 7 In the **Properties (LDAP)** dialog box, complete all fields on the **General** tab and click **OK**.

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, 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**.

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, click **Operational Policies**.

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

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

Step 6 Right click on the LDAP Provider name to which you want to change the group rules for.

Step 7 In the **Properties (LDAP Provider name)** dialog box, in the **LDAP Group Rules** section, change the group rules.

Step 8 Click **OK**.

LDAP Group Maps

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

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

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

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

- Roles only
- Locales only
- Both roles and locales

Example: If you want to configure authentication for an LDAP group representing a group of server administrators at a specific location, you can include user roles such as server-profile and server-equipment to the LDAP group. If you want to restrict access to server administrators at a specific location, you can specify locales with specific site names.

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

Nested LDAP Groups

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

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

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

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

Creating an LDAP Group Map

Before You Begin

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

Procedure

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, 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 and 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, 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, 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.

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, 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.
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, 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, 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.
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, 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.
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, 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, 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.
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, 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, 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.
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, 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, 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.

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

Creating an Authentication Domain

Procedure

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

b) Click **OK**.

Step 7 Click **Save**.

Configuring DNS Servers

Managing DNS Policies

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

Configuring a DNS Policy

Before You Begin

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

Procedure

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, 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.
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, 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, 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.
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, 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**.

Managing Power Policies

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

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, 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.
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, 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 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, 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.
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, 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**.

Managing Time Zones

Managing Time Zones

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

Configuring a Date and Time Policy

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, 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.
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, 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 and 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, 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 IPv4 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 from 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, 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**.

SNMP Policies

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

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

SNMP Functional Overview

The SNMP framework consists of three parts:

- An SNMP manager—The system used to control and monitor the activities of network devices using SNMP.
- An SNMP agent—The software component within Cisco UCS Central, the managed device, that maintains the data for Cisco UCS Central and reports the data, as needed, to the SNMP manager. Cisco UCS

Central includes the agent and a collection of MIBs. To enable the SNMP agent and create the relationship between the manager and agent, enable and configure SNMP in Cisco UCS Central.

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

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

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

SNMP Notifications

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

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

SNMP Security Features

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

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

SNMP Security Levels and Privileges

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

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

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

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

SNMP Security Models and Levels

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

Table 2: SNMP Security Models and Levels

Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for authentication.

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

SNMP Support in Cisco UCS Central

Support for MIBs

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

- SNMP MIB-2 System
- HOST-RESOURCES-MIB
  - hrSystem
  - hrStorage
  - hrDevice
  - hrSWRun
  - hrSWRunPerf
- UCD-SNMP-MIB
  - Memory

    - dskTable
    - systemStats
    - fileTable
- SNMP MIB-2 Interfaces
    - ifTable
- IP-MIB
- SNMP-FRAMEWORK-MIB
    - snmpEngine
- IF-MIB
- DISMAN-EVENT-MIB
- SNMP MIB-2 snmp

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

Authentication Protocols for SNMPv3 Users

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

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

AES Privacy Protocol for SNMPv3 Users

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

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

Configuring an SNMP Policy

Before You Begin

Before configuring a SNMP policy under a domain group, ensure that a SNMP policy is first created. Policies under the Domain Groups root which were already created by the system and are 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**, or the **Domain Group** name where you want to create the policy.

Step 3 Under the **Domain Groups root** node, 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 **Enabled** to choose the **Admin State**.
If **Enabled**, Cisco UCS Central uses SNMP to monitor the Cisco UCS Central system. Cisco UCS uses SNMP in all Cisco UCS domains included in the domain group if the groups themselves are not configured with SNMP.

The default state is **Disabled** with no fields displayed. Leaving the default state disables the SNMP policy

b) Enter the community or the username in the **Community/Username** field.
You can use 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.

c) Enter the system contact person information in the **System Contact** field.
The **System Contact** person is responsible for the SNMP implementation. Enter a string of up to 255 characters, such as an email address or a name and telephone number.

d) Enter the system location in the **System Location** field.
The **System Location** defines the location of the host on which the SNMP agent (server) runs. Enter an alphanumeric string up to 510 characters.

Step 7 Click **Save**.

What to Do Next

Create SNMP traps and SNMP users.

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 in the **Create SNMP Trap** dialog box.

a) Enter the SNMP host IP in the **IP Address** field.
Cisco UCS sends the trap to the defined IP address.

b) Enter the community or the username in the **Community/Username** field.
You can use 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.

c) Enter the port number in the **Port** field.
Cisco UCS uses the defined port to communicate with the SNMP host for the trap. Enter an integer between 1 and 65535. The default port is 162.

d) Click **v1**, **v2c**, or **v3** to choose the SNMP **Version**.

e) Click **trap** to choose the SNMP trap**Type**.

f) Click **auth**, **no auth**, or **priv** to define the **v3Privilege**.

g) Click **OK**.

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 in the **Create SNMP User** dialog.

a) Enter the SNMP username in the **Name** field.
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 locally authenticated username.

b) Click **md5** or **sha** to chose the authorization type.
c) Check the **AES-128** checkbox.
If checked, this user uses AES-128 encryption.
d) Enter the user password in the **Password** field.
e) Re-enter the user password in the **Confirm Password** field.
f) Enter the privacy password for this user in the **Privacy Password** field.
g) Re-enter the privacy password for this user in the **Confirm Privacy Password** field.
h) Click **OK**.

Step 6 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, 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**.

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**.

Deleting an SNMP User

Procedure

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

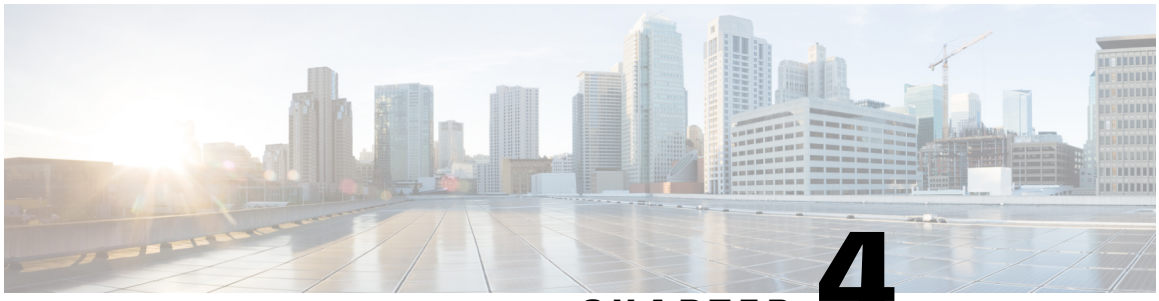
Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

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 4

Domain Management

This chapter includes the following sections:

- Domain Groups, page 67
- Domain Group and Registration Policies, page 69
- Call Home Policies, page 73

Domain Groups

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

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

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

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

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

Creating a Domain Group

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**.

Domain Group and Registration Policies

Creating a Domain Group Policy

Procedure

Step 1 On the menu bar, click **Equipment**.
Step 2 In the **Navigation** Pane, on the **Equipment** tab, expand **UCS Domains** > **Policies**.
Step 3 Right-click **Domain Group Policies** and choose **Create Domain Group Policy**.
Step 4 In the **Create Domain Group Policy** dialog box, enter the **Name** and optional description.
Step 5 Choose a **Domain Group** and **Domain Group Policy Qualification** from the drop-down lists.
Step 6 Click **OK**.

Deleting a Domain Group Policy

Procedure

Step 1 On the menu bar, click **Equipment**.
Step 2 In the **Navigation** Pane, on the **Equipment** tab, expand **UCS Domains** > **Policies**.
Step 3 Expand **Domain Group Policies**.
Step 4 Right-click the policy that you want to delete and choose **Delete**.
Step 5 If the Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Creating a Registration Policy

Procedure

Step 1 On the menu bar, click **Equipment**.
Step 2 In the **Navigation** Pane, on the **Equipment** tab, expand **UCS Domains** > **Policies**.
Step 3 Right-click **Registration Policies** and choose **Create Registration Policy**.
Step 4 In the **Create Registration Policy** dialog box, enter the **Name** and optional description.
Step 5 Click **OK**.

What to Do Next

Add an address qualifier, owner qualifier, and site qualifier to the policy qualification.

Creating a Site Qualifier

Procedure

Step 1 On the menu bar, click **Equipment**.
Step 2 In the **Navigation** Pane, on the **Equipment** tab, expand **UCS Domains** > **Policies**.
Step 3 Expand **Registration Policies**.
Step 4 Right-click the registration policy that you want to update, and choose **Create Site Qualifier**.
Step 5 In the **Create Site Qualifier** dialog box, enter the **Name** and **Regex**.
Step 6 Click **OK**.

Deleting a Site Qualifier

Procedure

Step 1 On the menu bar, click **Equipment**.
Step 2 In the **Navigation** Pane, on the **Equipment** tab, expand **UCS Domains** > **Policies**.
Step 3 Expand **Registration Policies**.
Step 4 In the **Work** pane, expand **Sites**.
Step 5 Right-click the site that you want to delete, and choose **Delete**.
Step 6 If the Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Creating an Address Qualifier

Procedure

Step 1 On the menu bar, click **Equipment**.
Step 2 In the **Navigation** Pane, on the **Equipment** tab, expand **UCS Domains** > **Policies**.
Step 3 Expand **Registration Policies**.
Step 4 Right-click the registration policy that you want to update, and choose **Create Address Qualifier**.
Step 5 In the **Create Address Qualifier** dialog box, enter the minimum and maximum IP addresses.
Step 6 Click **OK**.

Deleting an Address Qualifier

Procedure

Step 1 On the menu bar, click **Equipment**.
Step 2 In the **Navigation** Pane, on the **Equipment** tab, expand **UCS Domains** > **Policies**.
Step 3 Expand **Registration Policies**.
Step 4 In the **Work** pane, expand **Addresses**.
Step 5 Right-click the address range that you want to delete, and choose **Delete**.
Step 6 If the Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Creating an Owner Qualifier

Procedure

Step 1 On the menu bar, click **Equipment**.
Step 2 In the **Navigation** Pane, on the **Equipment** tab, expand **UCS Domains** > **Policies**.
Step 3 Expand **Registration Policies**.
Step 4 Right-click the registration policy that you want to update, and choose **Create Owner Qualifier**.
Step 5 In the **Create Owner Qualifier** dialog box, enter the **Name** and **Regex**.
Step 6 Click **OK**.

Deleting an Owner Qualifier

Procedure

Step 1 On the menu bar, click **Equipment**.
Step 2 In the **Navigation** Pane, on the **Equipment** tab, expand **UCS Domains** > **Policies**.
Step 3 Expand **Registration Policies**.
Step 4 In the **Work** pane, expand **Owners**.
Step 5 Right-click the owner that you want to delete, and choose **Delete**.
Step 6 If the Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Deleting a Registration Policy

Procedure

Step 1 On the menu bar, click **Equipment**.
Step 2 In the **Navigation** Pane, on the **Equipment** tab, expand **UCS Domains** > **Policies**.
Step 3 Expand **Registration Policies**.
Step 4 Right-click the policy that you want to delete and choose **Delete**.
Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

ID Range Qualification Policies

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

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

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

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

Creating an ID Range Qualification Policy

Procedure

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

Step 2 In the **Navigation** Pane, on the **Equipment** tab, expand **UCS Domains** > **Policies**.

Step 3 Right-click **ID Range Qualification Policies** and choose **Create ID Range Qualification Policy**.

Step 4 In the **Create ID Range Qualification Policy** dialog box, enter the **Name** and optional description.

Step 5 In the **Qualified Domain Groups** area, choose a **Context**.
The contexts you choose appear next to the **Selected** field.

Step 6 In the **Qualified Domain IP Addresses** area, enter an **IP Address**, and click the plus sign.
The IP addresses you enter appear next to the **Selected** field.

Step 7 Click **OK**.

What to Do Next

Assign the ID range qualification policy to a block.

Deleting an ID Range Qualification Policy

Procedure

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

Step 2 In the **Navigation** Pane, on the **Equipment** tab, expand **UCS Domains** > **Policies**.

Step 3 Expand **ID Range Qualification Policies**.

Step 4 Right-click the policy that you want to delete and choose **Delete**.

Step 5 If the Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Call Home Policies

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

Alert notifications are sent with predefined content based on alert levels (including major, minor, normal, notification and warning) and selected alert groups identifying events that trigger notification (such as diagnostic, environmental, inventory, license and other predefined events). Individual email recipients may be individually added to existing profiles. Registered Cisco UCS domains choosing to define security policies

globally within that client's policy resolution control will defer all call home policies to its registration with Cisco UCS Central.

Configuring a Call Home Policy

A call home policy is created from a domain group under the domain group root. Call home policies under the Domain Groups root 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.

Name	Description
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.
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**

Name	Description
Hostname field	The IP address or hostname of the SMTP server. **Note** If you use a hostname rather than an IPv4 or IPv6 address, you must configure a DNS server. If the Cisco UCS domain is not registered with Cisco UCS Central or DNS management is set to **local**, configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to **global**, configure a DNS server in Cisco UCS Central.
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.
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.

Name	Description
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.
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.

Name	Description
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.
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, 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.

Name	Description
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.
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, 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, 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, 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**.

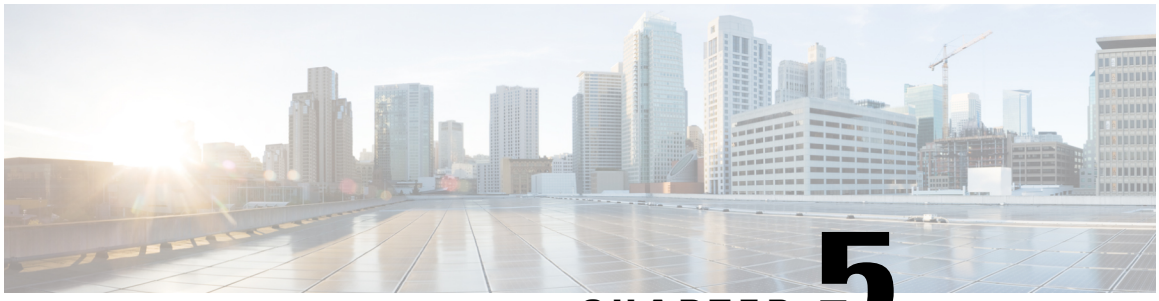
Step 3 Under the **Domain Groups root** node, click **Operational Policies**.

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 5

Remote Management

This chapter includes the following sections:

- Remote Management, page 85
- Remote Tech Support for UCS Domains, page 96

Remote Management

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

Important

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

Using remote management capability you can do the following:

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

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

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

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

Recommission a Server

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

Procedure

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

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

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

Decommissioning a Server

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

Procedure

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

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

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

Removing a Server

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

Procedure

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

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

Resetting a Server CIMC

Procedure

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

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

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

Resetting Server CMOS

Procedure

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

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

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

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

Resetting a Server IPMI

Procedure

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

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

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

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

Resetting a Server KVM

Procedure

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

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

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

Turning on/off Server Locator LED

Procedure

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

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

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

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

Acknowledging a Chassis

Procedure

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

The following example acknowledges chassis 7 and commits transaction:

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

Decommissioning a Chassis

Procedure

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

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

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

Recommissioning a Chassis

Procedure

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

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

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

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

Turning on or off the Chassis Locator LED

Procedure

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

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

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

Acknowledging a Fabric Extender

Procedure

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

The following example acknowledges fabric extender 7 and commits transaction:

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

Decommissioning a Fabric Extender

Procedure

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

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

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

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

Recommissioning a Fabric Extender

Procedure

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

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

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

Removing a Fabric Extender

You can remove a fabric extender from the UCS domain.

Procedure

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

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

Turning on of off Fabric Extender Locator LED

Procedure

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

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

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

Remote Tech Support for UCS Domains

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

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

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

Creating a Tech Support File for a UCS Domain

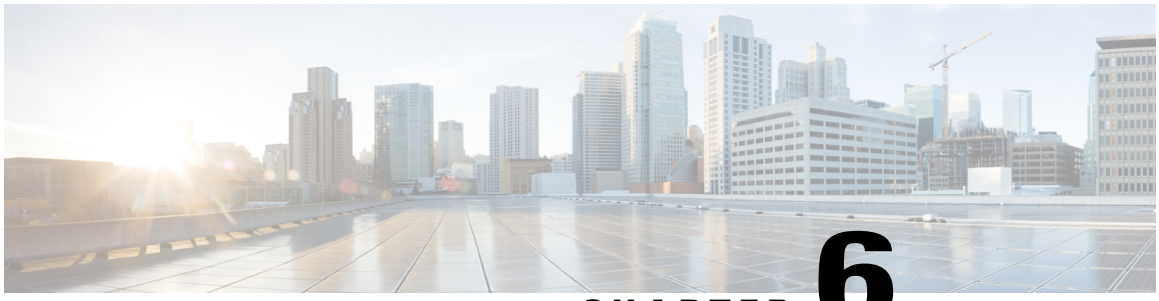
From the registered Cisco UCS domains, you can collect a full set of tech support files for options corresponding to "ucsm" in Cisco UCS Manager.

Procedure

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

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

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



CHAPTER 6

Firmware Management

This chapter includes the following sections:

- Downloading Firmware, page 99
- Upgrading Firmware in Cisco UCS Domains, page 103
- Scheduling Firmware Upgrades, page 107
- Managing Capability Catalog, page 109

Downloading Firmware

Firmware Download from Cisco

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

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

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

Firmware Library of Images

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

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

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

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

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

Configuring Firmware Download from Cisco

When you configure firmware download from Cisco, Cisco UCS Central downloads the firmware metadata from Cisco.com and keeps the information available for you to download and save anytime from Cisco UCS Central.

Procedure

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

Step 2 In the **Navigation** pane, expand **Images**.

Step 3 Click **Configure Downloads From Cisco**.

Step 4 In the **Work** pane, **General** tab, fill in the fields with the required information.
Make sure to have the username and password for the Cisco.com account that Cisco UCS Central uses to log in.

Step 5 In the **Proxy** tab, fill in the required information for the proxy account.

Step 6 Click **Save**.

Downloading a Firmware Image from Cisco

When you configure firmware image download from Cisco.com and refresh the library of images, Cisco UCS Central is able to access to all available firmware image metadata. You can download the firmware image in the following ways:

- **Creating a firmware policy —** When you create a firmware policy and select the specific image, Cisco UCS Central automatically downloads the image specified in the firmware policy.

- **Storing the image locally —** When you select the store locally option, the selected firmware image is downloaded from Cisco.com and stored in the image library.

This procedure describes the process to download the image using store locally option.

Procedure

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Images**.
Step 3 Click **Library**.
Step 4 In the **Work** pane, click **Packages** tab.
The image metadata downloaded from Cisco will have the **Source** as **Cisco** and **State** as **not-downloaded**.
Step 5 Right click on the bundle and from the options, choose **Store Locally**.

Downloading Firmware from a Remote Location

Before You Begin

You must have the remote server configured to support the file transfer protocol that you choose and they must be accessible to Cisco UCS Central.

Procedure

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Images**.
Step 3 Click **Library**.
Step 4 In the **Work** pane, click **Downloads** tab.
Step 5 In the **Downloads** tab, click **Download Firmware**.
Step 6 In the **Download Firmware** dialog box, **Location of the Image File**, choose **Remote File System** and fill in the required fields.
Step 7 Click **OK**.

Downloading Firmware from a Local File System

Before You Begin

You must have obtained and saved the firmware image from Cisco in your local file system to configure downloading the firmware from local system into Cisco UCS Central.

Procedure

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Images**.
Step 3 Click **Library**.
Step 4 In the **Work** pane, click **Downloads** tab.
Step 5 In the **Downloads** tab, click **Download Firmware**.
Step 6 In the **Download Firmware** dialog box, **Location of the Image File**, choose **Local File System**.
Step 7 Click **Download Image into Image Library**.
A dialog box opens with an option to select the file.
Step 8 Click **Browse** to browse to the firmware file location in your local system and select the file.
Step 9 Click **Submit**.
If the image download is successful, **Firmware Image Download** dialog box opens with a confirmation message.
Step 10 In the **Firmware Image Download** dialog box, click **OK**.

Viewing Image Download Faults

You can view the faults in firmware image download process from the same **Library of Images** panel.

Procedure

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Images**.
Step 3 Click **Library**.
Step 4 In the **Work** pane, click **Faults** tab.
The faults table displays all download faults with details.

Viewing Firmware Images in the Library

You can view the downloaded firmware images and image metadata in the **Library of Images** panel.

Procedure

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

Step 2 In the **Navigation** pane, expand **Images**.

Step 3 Click **Library**.

Step 4 The **Work** pane click the **Packages** tab.
The available packages are displayed. You can select a package and click **Properties** to view details on specific packages.

Deleting Image Metadata from the Library of Images

You can delete the firmware image metadata from the **Library of Images** using the purge option. The purge option clears only the metadata of already downloaded images.

Note If you want to delete any of the firmware packages such as the capability catalog, infrastructure and host firmware packages, you can do so from the firmware management section under each domain groups or from the domain group root.

Procedure

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

Step 2 In the **Navigation** pane, expand **Images**.

Step 3 Click **Library**.

Step 4 In the **Work** pane, choose the firmware image metadata you want to delete from **Library of Images**and click **Purge**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Upgrading Firmware in Cisco UCS Domains

Firmware Upgrades for Cisco UCS Domains

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

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

Configuring an Infrastructure Firmware Upgrade for a Cisco UCS Domain

You can create only one infrastructure firmware package for one Cisco UCS Domain group in Cisco UCS Central . The member Cisco UCS domains in a domain group will run the same infrastructure firmware version.

Note You can configure infrastructure firmware update from domain group root or at the domain group level. When you update the firmware at the domain group root level, all the domain groups under the root will get the same infrastructure firmware version.

Procedure

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

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Groups Root** > **Firmware Management**.

Step 3 Click **Infrastructure Firmware**.

Step 4 In the **Work** pane, **Policies** tab, click **Create**.

Step 5 In the **Scheduler** area, specify a schedule to apply the infrastructure firmware on the Cisco UCS domains in the domain group.

Step 6 In the **Version** area, select the infrastructure firmware version.
Impacted Endpoints area displays the endpoints that will get impacted by the infrastructure firmware policy. During a firmware upgrade, these endpoints will be rebooted and will therefore be unavailable during part of the upgrade process.

Step 7 Click **Save**.

What to Do Next

Cisco UCS Central automatically creates two schedules for infrastructure firmware update and fabric interconnect reboot. These schedules are also updated in Cisco UCS Manager. Based on the schedule, the infrastructure firmware upgrade process begins in the registered Cisco UCS domains and generates the first acknowledge pending activities message in Cisco UCS Central. When you acknowledge the first pending activity, the components are updated with the specified infrastructure firmware package.

After the infrastructure firmware is updated, you will receive another pending activity notification. This acknowledgment prevents any accidental reboot of fabric interconnects. You have to acknowledge this pending activity to reboot the fabric interconnect and complete the infrastructure firmware upgrade.

Note If you have multiple domains in a domain group, you will have acknowledge each pending activity for each Cisco UCS domains to complete the infrastructure firmware upgrade process.

Acknowledging a Pending Activity

if the service profiles in Cisco UCS domains use a global maintenance policy and global host firmware package, Cisco UCS Central provides you an option to enable user acknowledgment before deploying the firmware upgrade.

If you have created a maintenance policy with **User Ack** reboot policy, you must acknowledge the actual firmware upgrade in Cisco UCS Manager. If you have created a maintenance policy with a global schedule and enabled **User Ack**, you must acknowledge the actual upgrade for all Cisco UCS domains in Cisco UCS Central.

Note You can view and acknowledge pending activities from **Infrastructure Firmware** and **Host Firmware** sections. This procedure describes the process to acknowledge a pending activity from the host firmware section.

Procedure

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

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Groups Root** > **Firmware Management**.

Step 3 In the **Work** pane, click **Pending Activities** tab.

Step 4 Choose the pending activity from the displayed list, right click and click **Acknowledge**.

Deleting an Infrastructure Firmware Package

Procedure

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

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Groups Root** > **Firmware Management**.

Step 3 The **Work** pane displays a list of all created infrastructure firmware packages.

Step 4 Click **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Creating a Host Firmware Package

Procedure

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

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Groups Root** > **Firmware Management**.

Step 3 Click **Host Firmware**.

Step 4 In the **Work** pane, **Policies** tab, click **Create a Pack**.

Step 5 In **Create a Pack** dialog box, fill in the following fields:

a) Fill in **Name** and **Description**.

b) In the **Blade Version** area, choose the blade server version.

c) In the **Rack Version** area, choose the rack server version.

Step 6 The **Impacted Endpoints** dialog box displays the list of end points that will be affected by this host firmware policy.
During a firmware upgrade, these endpoints will be rebooted and will therefore be unavailable during part of the upgrade process

Step 7 Click **OK**.

What to Do Next

The host firmware policy you create in Cisco UCS Central will be available for association to a service profile in a Cisco UCS Domain registered to a domain group.

Deploying a Host Firmware Upgrade

You can update all host firmware policies defined in Cisco UCS Central to specific B and C bundles using the **Install Servers**.

Before You Begin

You must have created a host firmware package.

Procedure

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

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Groups Root** > **Firmware Management**.

Step 3 Click **Host Firmware**.

Step 4 In the **Work** pane, from the displayed list of host firmware packages, choose the firmware version you want to deploy.

Step 5 Click **Install Servers** on the table header.

Step 6 In the **Install Servers** dialog box, select **Blade Version**, **Rack version** and **Impacted Endpoints**.

Step 7 In **Upgrade host Firmware Warning** message dialog box, click **Yes**.

If the servers in the selected endpoints use the global host firmware upgrade policy, they will be upgraded with the host firmware package.

Deleting a Host Firmware Package

Procedure

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

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Groups Root** > **Firmware Management**.

Step 3 The **Work** pane displays a list of all created host firmware packages.

Step 4 Click and choose the host firmware package name you want to delete.
The table header area shows action icons.

Step 5 Click **Delete**.

Step 6 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Scheduling Firmware Upgrades

Firmware Upgrade Schedules

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

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

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

Creating a Maintenance Policy

You can create the following types of maintenance policies for host firmware update in Cisco UCS Central:

- **Immediate —** The immediate option reboots the servers immediately without any user acknowledgment.
- **Timer-automatic —** In timer-automatic option, the server reboot will happen based on the schedule you select for this maintenance policy.

Important If you use the timer automatic option, you must create a schedule in Cisco UCS Central to specify in the maintenance policy. When you create a schedule in Cisco UCS Central, you can acknowledge this scheduled maintenance policy only in Cisco UCS Central.Servers using this maintenance policy will reboot only during the maintenance window defined in the schedule. If user-ack is enabled in the schedule, then you must acknowledge the server reboot.

- **User-acknowledgment —** The user-ack option sends a pending activity notification in each Cisco UCS Domain before rebooting servers.

Important The user-ack option provides Cisco UCS domains administrators the option to decide on rebooting servers in individual Cisco UCS domains at different times.

Procedure

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** Pane, expand **Domain Groups** > **Domain Group Root** > **Maintenance**.
Step 3 In the **Work** pane, click **Create Maintenance Policy**.
Step 4 In the **Create Maintenance Policy** dialog box, do fill in the required fields.
Step 5 Click **OK**.

What to Do Next

Associate the maintenance policy to a service profile in Cisco UCS Manager.

Creating a One Time Occurrence Schedule

Procedure

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Groups Root** > **Schedules**.
Step 3 In the **Work** pane, click **Create Schedule**.
Step 4 In the **Create Schedule** dialog box, enter the details in the **Properties** area.
Step 5 Choose **One Time Occurrences** tab and click **Create One Time Occurrence**.
Step 6 In the **Create One Time Occurrence** dialog box, fill in the details.
Step 7 Click **OK**.
Step 8 Click OK in the **Create Schedule** dialog box.
The one time schedule you created is added to the **Schedules** table.

Creating a Recurring Occurrence Schedule

Procedure

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Groups Root** > **Schedules**.
Step 3 In the **Work** pane, click **Create Schedule**.
Step 4 In the **Create Schedule** dialog box, enter the details in the **Properties** area.
Step 5 Choose **Recurring Occurrences** tab and click **Create Recurring Occurrence**.
Step 6 In the **Create Recurring Occurrence** dialog box, fill in the details.
Step 7 Click **OK**.
Step 8 Click OK in the **Create Schedule** dialog box.
The recurring schedule you created is added to the table.

Deleting a Firmware Upgrade Schedule

Procedure

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Groups Root** > **Schedules**.
Step 3 The **Work** pane displays a list of all scheduled firmware events.
Step 4 Click and choose the schedule name you want to delete.
The table header area shows action icons.
Step 5 Click **Delete**.
Step 6 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Managing Capability Catalog

Capability Catalog

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

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

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

Contents of the Capability Catalog

The contents of the Capability Catalog include the following:

Implementation-Specific Tunable Parameters

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

Hardware-Specific Rules

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

User Display Strings

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

Updates to the Capability Catalog

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

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

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

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

Configuring a Capability Catalog Update for a Cisco UCS Domain

You can create only one capability catalog per each Cisco UCS Domain group in Cisco UCS Central. All the member Cisco UCS domains of a group will run the same firmware version.

Note You can configure capability catalog update from domain group root or at the domain group level. When you update the capability catalog at the domain group root level, if the domain groups under the root do not have a capability catalog defined, will get the same capability catalog version.

Procedure

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

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Groups Root** > **Firmware Management**.

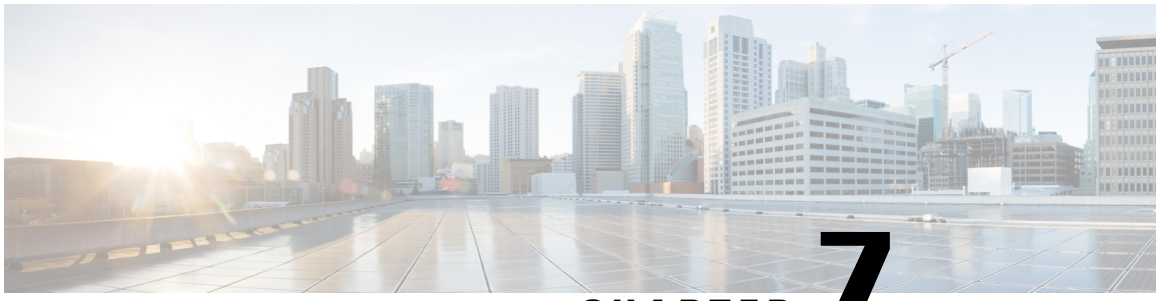
Step 3 Click **Capability Catalog**.

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

Step 5 In the **Version** table, select the version of the capability catalog you want to associate with the Cisco UCS domains included in the selected Cisco UCS Central domain group.
The capability catalog version selected here overrides the version inherited from any parent groups, if an inherited version exists.

Step 6 Click **Save**.

Cisco UCS Central triggers the capability catalog update in the specified Cisco UCS domains.



CHAPTER 7

Monitoring Inventory

This chapter includes the following sections:

- Inventory Management, page 113
- Overview to Global Logical Resources, page 114
- Configuring Inventory Data Collection Schedule, page 115
- Viewing Inventory Details, page 115
- Viewing Inventory Details of a Server, page 115
- Viewing Details on an Individual Cisco UCS Domain, page 116
- Viewing Service Profiles, page 116
- Viewing Service Profile Details, page 116
- Viewing Service Profile Templates, page 117
- Viewing Local service profiles, page 117
- Creating an Organization Under Sub-Organizations, page 118

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.

Overview to Global Logical Resources

In Cisco UCS Central Web UI, Global Service Profiles are created under Global Service Profile section, once they are associated to any server or server pool, they are deployed on Cisco UCS domains, and are pulled back to Cisco UCS Central. These Global service profiles are reported as part of logical resources/inventory as an instance under local service profile section. You can view the list of local service profiles and local service profile templates available in the registered Cisco UCS domain from the **Servers** tab. The local service panel displays an aggregated list of local service profiles. Local service profiles with the same name are grouped under the organization they are assigned to. Instance count next to the local service profile name will provide the number of service profiles with this name across all Cisco UCS domain registered with Cisco UCS Central.

From the Local Service Profile Template panel, you can view the available local service profile templates, organizations and the number of times a service profile is used with this name in all registered Cisco UCS domains.

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 details for all registered Cisco UCS domains.

Viewing Inventory Details of a Server

Before You Begin

- Cisco UCS domains should be registered with Cisco UCS Central.
- Inventory status should be marked OK.

Procedure

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

Step 2 In the **Navigation** pane, expand **UCS Domains** > **Domain Groups** > **Domain Group root** > **UCS Domain** > **Chassis** > **Chassis number** > **Server**.

If you want to view inventory details of a rack servers, expand **UCS Domains** > **Domain Groups** > **Domain Group root** > **UCS Domain** > **Rack-Mounts** > **Server**.

Step 3 Select the server that you want to view the inventory details.

Step 4 In the **Work** pane, click **Inventory** tab.

Step 5 Select the component that you want to see the inventory details.

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 details of selected Cisco UCS domain.

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 service profiles.

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 details of selected service profile.

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 details for selected service profile template.

Viewing Local service profiles

Procedure

Step 1 On the menu bar, click **Servers**.
Step 2 In the **Navigation** pane, expand **Local Service Profiles** > **Root** > **Local Service Profile_Name**.
Step 3 Click **Instance**, of the local service profile that you want to view the information.
Step 4 Similarly, to view properties of other listed local service profiles, expand the local service profile you want to view, and click Instance.

Creating an Organization Under Sub-Organizations

Procedure

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

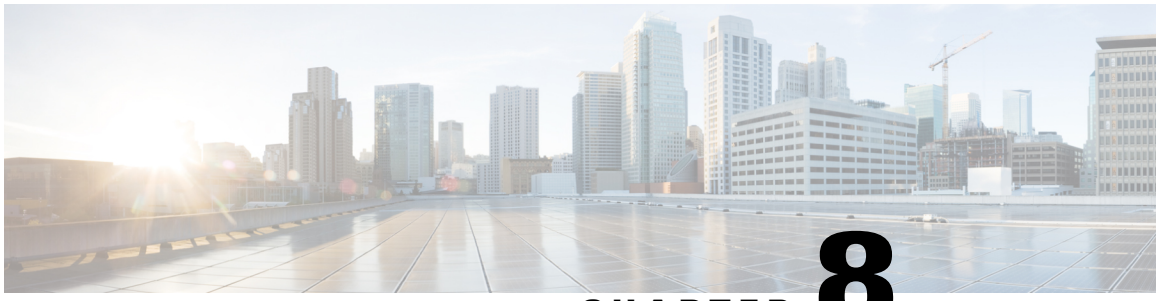
Step 2 In the **Navigation** pane, expand **Server** > **Local Service Profiles** > **Root**.

Step 3 Click **Sub-Organization** tab. in the **Work** pane, click **Create Organization** tab.

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

Step 5 In the **Create Organization** dialog box, fill in the required fields.

Step 6 Click **Ok**.



CHAPTER 8

Managing Backup and Restore

This chapter includes the following sections:

- Backup and Import in Cisco UCS Central, page 119
- Backing up and Restoring Cisco UCS Central, page 122
- Backing up and Restoring Cisco UCS Domains, page 126
- Import Configuration, page 127

Backup and Import in Cisco UCS Central

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

You can schedule the following backup policies separately for both Cisco UCS Central and Cisco UCS domains:

- **Full state backup policy**: Backs up database.
- **Config all export policy**: Backs up the configuration in XML format.

For a UCS domains, these policies can either be defined locally or defined in Cisco UCS Central

Scheduled backup policies are disabled by default. If you want to backup Cisco UCS Central or the registered UCS domains, you must enable the backup state for both. Backup process does not interrupt or impact any server or network traffic. You can perform a backup while the domain is up and running. The backup operation saves information from the management plane.

Remotely configured policies are restricted to use the Cisco UCS Central repository for backups which is internally mounted by Cisco UCS Manager.

When you schedule regular backup, the backup repository can start accumulating data. To manage the backup archives, you can specify the maximum number of backup versions that are saved. Use policy specifications to indicate the number of backups to maintain for each Cisco UCS domain.

Note The maximum number does not impact the number of backup image files you can store on a remote location.

You can view the list of backups for each Cisco UCS domain from the Cisco UCS Central GUI and you can also delete saved or unused backup directories and configurations.

Important

- You must have a user account that includes the admin role to create and run backup and import operations.
- You can delete backups only after a Cisco UCS domain (from which the backup has been taken) has been unregistered.
- Config-all, config-logical and config-system type backups are only supported in Cisco UCS Central on demand back up.

Backup Image Files

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

- **Local File System**: In a local file system.
- **Remote Location**: Remote locations using any one of the protocol such as, TFTP, FTP, SCP, or SFTP.

Important You must have Cisco UCS Manager, release 2.2(2x) in registered Cisco UCS domains to specify a global backup policy with the option to store the image file in a remote location. If you do not have Cisco UCS Manager, release 2.2(2x) in the Cisco UCS domain, the global backup policy with remote backup will not work.

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

Restoring Configuration

You can use the saved configuration from backup repository to restore and configure any of the managed Cisco UCS domain. Make sure to use full-state backup for recovery situations. Use TFTP protocol to access the backup configurations. You can use both Cisco UCS Central GUI or CLI to copy the backup file URL and use it to configure a new domain.

Considerations and Recommendations for Backup Operations

Before you create a backup operation, consider the following:

Backup Locations

The backup location is the destination or folder on the network where you want Cisco UCS Central to export the backup file. You can maintain only one backup operation for each location where you plan to save a backup file.

Potential to Overwrite Backup Files

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

Multiple Types of Backups

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

Scheduled Backups

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

Incremental Backups

You cannot perform incremental backups of Cisco UCS Manager or Cisco UCS Central.

Encryption of Full State Backups

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

Backup Types

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

- **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.

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.

Enabling Backup in Cisco UCS Central

By default the backup operation is disabled. You much enable the backup policy for Cisco UCS Central back up and Cisco UCS Domains backup to automatically backup the database or system configuration.

Note This procedure describes the process to enable Cisco UCS Central backup. You will do the same for Cisco UCS Domains from **Operations Management** > **Domain Groups root** or the specific **Domain Group**.

Procedure

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

Step 2 In the Navigation pane, click **General** tab.

Step 3 In the work pane, click **Full-State Backup Policy** or **Config-All Backup Policy**.

Step 4 In **Backup State**, click **Enable**.

Step 5 Click **Save**.
Cisco UCS Central takes a snapshot of the configuration type that you selected and exports the file to the specified location. To view the progress of the backup operation, click the **Task** tab in the **Properties** dialog box.

Backing up and Restoring Cisco UCS Central

You can back up Cisco UCS Central database or configuration using scheduled backup policies and on creating on demand backup of the system. The following are two types of scheduled backup policies for Cisco UCS Central from the **Administration** tab:

- **Full-State Backup Policy**: This policy backs up complete Cisco UCS Central database based on the specified schedule. You can store the backup image file either in a local system or on a remote location using protocols such as SCP, SFTP, FTP, and TFTP. The full state backup retains the management interfaces in the complete state.
- **Config-All Export Policy**: The config-all export policy backs up only the system configuration in XML format.

You can also create an on demand backup for Cisco UCS Central at anytime from the **Operations Management** > **Backup and Import** > **UCS Central** > **Create System Backup**.

Creating a Full-State Backup Policy for Cisco UCS Central

Make sure to enable Backup state to trigger backup on specified schedule.

Note If you specify a remote location, make sure that location exists. You must have an absolute remote path ready when you select the remote location.

Procedure

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

Step 2 In the Navigation pane, click **General**.

Step 3 In the work pane, click **Full-State Backup Policy** tab.

a) Provide a description for this backup.
b) In **Location of the Image File**, select the appropriate radio button to save the image file .
c) In **Schedule** drop-down, select the frequency you want to schedule the backup for.
d) In **Max Files**, specify the maximum number of files you want to save in this location for ths system.

Step 4 Click **Save**.

Based on the schedule, Cisco UCS Central takes a snapshot of the database and exports the file to the specified location. To view the progress of the backup operation, click the **Task** tab in the **Properties** dialog box.

Creating a Config-all Backup Policy for Cisco UCS Central

Make sure to enable Backup state to trigger backup on specified schedule.

Note If you specify a remote location, make sure that location exists. You must have an absolute remote path ready when you select the remote location.

Procedure

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

Step 2 In the Navigation pane, click **General**.

Step 3 In the work pane, click **Config-all Export Policy** tab.

a) Provide a description for this backup.
b) In **Location of the Image File**, select the appropriate radio button to save the image file .
c) In **Schedule** drop-down, select the frequency you want to schedule the backup for.
d) In **Max Files**, specify the maximum number of files you want to save in this location for ths system.

Step 4 Click **Save**.

Based on the schedule, Cisco UCS Central takes a snapshot of the database and exports the file to the specified location. To view the progress of the backup operation, click the **Task** tab in the **Properties** dialog box.

Creating an On Demand Backup for Cisco UCS Central

Before You Begin

Obtain the backup server IPv4 or IPv6 address and authentication credentials.

Procedure

Step 1 In the Navigation pane, expand **Backup and Import.**

Step 2 Click the **UCS Central** node.

Step 3 In the work pane, click **Create System Backup.**

Step 4 In the **Create System Backup** dialog box, fill in the required fields.

Step 5 Click **OK**.

Step 6 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 7 (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 8 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.

Creating a Backup Schedule for Cisco UCS Central

You can create a backup schedule for both full state backup policy and config-all back up policy and save the image file either in a network location or in a remote file system. The **Backup State** must be in **Enable** for Cisco UCS Central to trigger backup at the scheduled time.

Procedure

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

Step 2 In the Navigation pane, click **General** tab.

Step 3 In the work pane, click **Full-State Backup Policy** or **Config-All Backup Policy** and do the following:.

a) Provide a description for this backup.

b) In **Location of the Image File**, select the appropriate radio button to save the image file .

c) In **Schedule** drop-down, select the frequency you want to schedule the backup for.

d) In **Max Files**, specify the maximum number of files you want to save in this location for ths system.

Step 4 Click **Save**.

Based on the specified schedule, Cisco UCS Central takes a snapshot of the configuration type that you selected and exports the file to the specified 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.

Backing up and Restoring Cisco UCS Domains

You can create global backup policies for registered UCS domains in Cisco UCS Central at the domain group root or at the domain group levels.

When you create a global backup policy, Cisco UCS domains that are part of the domain group inherit the policy creating, update and deletion events. Deleting these policies remotely resets the admin state to disabled in Cisco UCS Manager since these are global policies that cannot be completely deleted. You can schedule a backup and restore operation or you can perform an immediate backup and restore operation.

Important Backing up UCS domains to a remote locations is supported only from Cisco UCS Manager, release 2.2(2x) and above. Trying to backup a UCS domain that is running on any earlier Cisco UCS Manager release versions will not work.

Recommendations

- Make sure to enable **Backup & Export Polices** to **Global** in Cisco UCS Manager.
- You must register a Cisco UCS Domain under a domain group to enable the global backup policy.
- When you have multiple Cisco UCS Manager release versions in your setup, make sure to same release versions of UCS Manager are registered under one domain group.
- You cannot specify multiple backup policies under different domain groups. All of the backup policies must be named default.

Creating a Full-State Backup Policy for Cisco UCS Domains

You can specify global full-state backup policy for the Cisco UCS domains at the domain group root and at the domain groups level. This policy will apply to all domain groups under the root.

Note If you specify a remote location, make sure that location exists. You must have an absolute remote path ready when you select the remote location.

Procedure

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

Step 2 In the Navigation pane, expand **Domain Groups** > **Domain Group root** or click **Domain Group root** and expand to navigate to a specific domain group.

Step 3 Click the **Backup/Export Policy** node.

Step 4 In the work pane, click **Full-State Backup Policy**.

a) Provide a description for this backup.

b) In **Location of the Image File**, select the appropriate radio button to save the image file .

Note You must have Cisco UCS Manager, release 2.2(2x) to use a remote location to save the backup image file.

c) In **Schedule** drop-down, select the frequency you want to schedule the backup for.

d) In **Max Files**, specify the maximum number of files you want to save in this location for ths system.

Step 5 Click **Save**.

Based on the schedule, Cisco UCS Central takes a snapshot of the Cisco UCS domain database and exports the file to the specified location. To view the progress of the backup operation, click the **Task** tab in the **Properties** dialog box.

Creating a Config-All Export Policy for Cisco UCS Domains

You can specify global config-all backup policy for Cisco UCS domains at the domain group root or at the domain group level. This policy will apply to all domain groups under the root.

Note If you specify a remote location, make sure that location exists. You must have an absolute remote path ready when you select the remote location.

Procedure

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

Step 2 In the Navigation pane, expand **Domain Groups** > **Domain Group root** or click **Domain Group root** and expand to navigate to a specific domain group.

Step 3 Click the **Backup/Export Policy** node.

Step 4 In the work pane, click **Config-All Export Policy**.

a) Provide a description for this backup.

b) In **Location of the Image File**, select the appropriate radio button to save the image file .

Important You must have Cisco UCS Manager, release 2.2(2x) to use a remote location to save the backup image file.

c) In **Schedule** drop-down, select the frequency you want to schedule the backup for.

d) In **Max Files**, specify the maximum number of files you want to save in this location for ths system.

Step 5 Click **Save**.

Based on the schedule, Cisco UCS Central takes a snapshot of the Cisco UCS domain configuration and exports the file to the specified location. To view the progress of the backup operation, click the **Task** tab in the **Properties** dialog box.

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.

Importing Cisco UCS Central Configuration

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:

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.

Importing Cisco UCS Manager Configuration

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:

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.

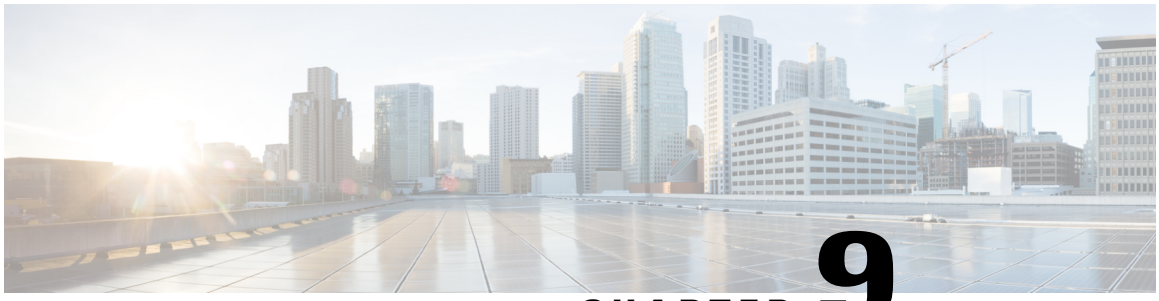
Step 5 In the **Import** table, click the import operation that you want to delete. You cannot click a backup operation in the table if the admin state of the operation is set to **Enabled**.

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**.



CHAPTER 9

Working with Policies

This chapter includes the following sections:

- Global Policies, page 131
- Policy and Policy Component Import in Cisco UCS Central, page 140
- Local Policies, page 145
- Statistics Threshold Policy, page 145

Global Policies

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

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

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

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

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

Creating a Global Policy

You can create global policies under the **Servers**, **Network** and **Storage** tabs.

Before You Begin

You must be logged in as an admin or as a user with admin privileges to perform this task.

Procedure

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

Step 2 Expand **Policies** and then **root.**
If you want to create a global policy in a sub-organization, expand **Sub-Organizations** > **Organization_Name**

Step 3 Select the item in the tree under which you want to create a global policy.

Step 4 Click **Create** on the right pane of the screen.

Step 5 Enter the **Name**, **Description** and other information in the create window.

Step 6 Click **Ok.**
Global policy is created and appears in the tree.

Note To create global policies under the **Network** and **Storage** tabs, click on the respective tab and perform Steps 2 through 6 in the preceding procedure.

Including a Global Policy in a Local Service Profile

Procedure

Step 1 Launch Cisco UCS Manager.
You can launch Cisco UCS Manager through the Cisco UCS Central GUI, as described in Launching Cisco UCS Manager for a Cisco UCS Domain.

Step 2 In the **Navigation** pane of Cisco UCS Manager, click the **Servers** tab.

Step 3 On the **Servers** tab, expand **Servers** > **Service Profiles**.

Step 4 Expand the node for the organization that contains the service profile for which you want to include a global policy.
If the system does not include multitenancy, expand the **root** node.

If the service profile is in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 5 Choose the service profile in which you want to include a global policy.

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

Step 7 Click the policy for which you want to include a global policy.

Step 8 From the **Policy** drop-down list, choose the global policy.

Step 9 Click **Save Changes**.

Policy Conversion Between Global and Local

Under certain circumstances you can convert a global policy to a local policy or a local policy to a global policy in Cisco UCS Manager.

Global service profiles and templates can only refer to global policies. Upon deployment, you cannot convert global policies that are included in global service profiles and templates to local policies. You must first convert the service profile or any policies that use the global policy, such as a LAN or SAN connectivity policy or a vNIC or vHBA template, to local.

When a service profile refers to a global template in Cisco UCS Central and the template includes a global policy, the ownership of the template is with the service profile. The ownership of the global policy remains with Cisco UCS Central, and you cannot make any changes to the policy ownership using Cisco UCS Manager. You can make changes to the policy ownership locally only if the policy is included in a local service profile or template.

Converting a Global Policy to a Local Policy

You can convert a policy from global to local only if the policy is included in a local service profile or service profile template.

Before You Begin

You must be logged in as an admin or as a user with admin privileges to perform this task.

Procedure

Step 1 Launch Cisco UCS Manager.
You can launch Cisco UCS Manager through the Cisco UCS Central GUI, as described in Launching Cisco UCS Manager for a Cisco UCS Domain.

Step 2 In the **Navigation** pane of Cisco UCS Manager, click the tab where the policy is located.
For example, click the **Servers** tab to convert a server-related policy, the **LAN** tab to convert a network-related policy, or the **SAN** tab to convert a storage-related policy.

Step 3 In the **Navigation** pane, expand **Policies**.

Step 4 Expand the node for the organization that contains the policy you want to convert.
If the system does not include multitenancy, expand the **root** node.

If the policy is in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 5 Choose the global policy that you want to convert to local.

Step 6 In the **Actions** section, click **Use Local.**

Step 7 If the Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

The policy is now a local policy that can be managed by Cisco UCS Manager.

Converting a Local Policy to a Global Policy

You can change the ownership of the local policies to global only if they are associated with a service profile.

Before You Begin

You must be logged in as an admin or as a user with admin privileges to perform this task.

Procedure

Step 1 Launch Cisco UCS Manager.
You can launch Cisco UCS Manager through the Cisco UCS Central GUI, as described in Launching Cisco UCS Manager for a Cisco UCS Domain.

Step 2 In the **Navigation** pane of Cisco UCS Manager, click the tab where the policy is located.
For example, click the **Servers** tab to convert a server-related policy, the **LAN** tab to convert a network-related policy, or the **SAN** tab to convert a storage-related policy.

Step 3 In the **Navigation** pane, expand **Policies**.

Step 4 Expand the node for the organization that contains the policy you want to convert.
If the system does not include multitenancy, expand the **root** node.

If the policy is in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 5 Choose the local policy that you want to convert to global.

Step 6 In the **Actions** area, click **Use Global**.

Step 7 If the Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

The policy is now a global policy that can only be managed by Cisco UCS Central and displays as read-only policy in the Cisco UCS Manager.

Policy Resolution between Cisco UCS Manager and Cisco UCS Central

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

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

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

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

Name	Description
Infrastructure & Catalog Firmware	Determines whether the Capability Catalog and infrastructure firmware policy are defined locally or come from Cisco UCS Central.

Name	Description
Date & Time	Determines whether the date and time is defined locally or comes from Cisco UCS Central.
Communication	Determines whether HTTP, CIM XML, Telnet, SNMP, web session limits, and Management Interfaces Monitoring Policy settings are defined locally or in Cisco UCS Central.
Faults	Determines whether the Global Fault Policy is defined locally or in Cisco UCS Central.
Security	Determines whether authentication and native domains, LDAP, RADIUS, TACACS+, trusted points, locales, and user roles are defined locally or in Cisco UCS Central.
DNS Management	Determines whether DNS servers are defined locally or in Cisco UCS Central.
Config Backup	Determines whether the Full State Backup Policy and All Configuration Export Policy are defined locally or in Cisco UCS Central.
Monitoring	Determines whether Call Home, Syslog, and TFTP Core Exporter settings are defined locally or in Cisco UCS Central.
Managed Endpoint	Determines whether managed endpoints are defined locally or in Cisco UCS Central.
Power Management	Determines whether the power management is defined locally or in Cisco UCS Central.
Power Supply Unit	Determines whether power supply units are defined locally or in Cisco UCS Central.

Consequences of Policy Resolution Changes

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

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

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

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

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

Policies and Configuration	Policy Source		Behavior in Cisco UCS Manager on Registration with Cisco UCS Central		Behavior in Cisco UCS Manager when Registration Changed	
	Cisco UCS Central	Cisco UCS Manager	Domain Group Unassigned	Domain Group Assigned	Unassigned from Domain Group	Deregistered from Cisco UCS Central
Maintenance Policy Schedule Host Firmware Packs	N/A	Assigned domain group	See Consequences of Service Profile Changes on Policy Resolution, on page 139	See Consequences of Service Profile Changes on Policy Resolution, on page 139	Deletes remote policies	Converted to a local policy
Maintenance Policy Schedule Host Firmware Packs	N/A	Assigned domain group	See Consequences of Service Profile Changes on Policy Resolution, on page 139	See Consequences of Service Profile Changes on Policy Resolution, on page 139	Deletes remote policies	Converted to a local policy
Maintenance Policy Schedule Host Firmware Packs	N/A	Assigned domain group	See Consequences of Service Profile Changes on Policy Resolution, on page 139	See Consequences of Service Profile Changes on Policy Resolution, on page 139	Deletes remote policies	Converted to a local policy

Consequences of Service Profile Changes on Policy Resolution

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

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

Policy	Behavior in Cisco UCS Manager on Registration with Cisco UCS Central		Domain Group Assigned after Registration with Cisco UCS Central
	Domain Group Unassigned / Domain Group Assigned		
	Service Profile not Modified	Service Profile Modified	
Maintenance Policy	Local	Local, but any "default" policies are updated on domain group assignment	Local/Remote (if resolved to "default" post registration)

Policy	Behavior in Cisco UCS Manager on Registration with Cisco UCS Central		Domain Group Assigned after Registration with Cisco UCS Central
	Domain Group Unassigned / Domain Group Assigned		
	Service Profile not Modified	Service Profile Modified	
Schedule	Local	Local, but any "default" policies are updated on domain group assignment	Local/Remote (if resolved to "default" post registration)
Host Firmware Packages	Local	Local, but any "default" policies are updated on domain group assignment	Local/Remote (if resolved to "default" post registration)

Modifying Policy Resolutions between Cisco UCS Manager and Cisco UCS Central using the Cisco UCS Manager GUI

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All** > **Communication Management**.

Step 3 Click the **UCS Central** node.

Step 4 In the **Actions** area, click **UCS Central**.

Step 5 In the **Policy Resolution Control** area, click one of the following radio buttons for each of the fields:

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

Step 6 Click **Save Changes**.

Policy and Policy Component Import in Cisco UCS Central

Cisco UCS Central enables you to import policies, pools, vLANs, vSANs directly from one registered Cisco UCS domain into Cisco UCS Central. When you have a perfect policy or a policy component in one of your UCS domains, you can import the policy and apply it to multiple domains. This import option enables you to import and apply a policy from one registered UCS domain to multiple UCS domains with a single click.

Using the Cisco UCS Central GUI, you can search for a policy or a component in the registered UCS domains. You can also refine your search using the available filters. From the search results, select the policy or component and import that into Cisco UCS Central.

Note If the search results are more than 1000, the results truncates. Make sure to refine the search using filters.

Depending on the policy or component you are importing, you can import them into either of the following destinations:

- Domain group root or to a specific domain
- Org root or a specific org

Estimate Impact During Import

Cisco UCS Central provides you the option to estimate the impact of most of the management actions you perform using the GUI. Make sure to run estimate impact during an import. Make sure to review the estimate impact results. The results will help you to identify any potential issues such as unintentional server reboot or policy overwrite and take proper precautionary measures before importing the selected policy or component.

Cautions and Guidelines for Policy or Component Import

Make sure to review the following information before importing a policy or a policy component:

- In the registered Cisco UCS Domains, if you have Cisco UCS Manager releases 2.1(2x) and 2.1(3x), you can only search for policies or components in the domains. You must have Cisco UCS Manager, release 2.2 and above to be able to import policies.
- When you import a policy to the root or any domain, if a policy with the same name already exist in the domain, Cisco UCS Central displays a confirmation dialog box that warns you about the policy overwrite. If you select import, the imported policy overwrites the existing policy. You can not retrieve the existing policy after the import.
- Cisco UCS Central does not maintain back up copies of any policy in the registered UCS domains. For example, if you have a specific BIOS policy in a domain, and you import another BIOS policy without estimating impact, the existing BIOS policy will get overwritten and you will not be able to recover that. When you click **Estimate Impact** and review the impacts, you can identify the potential risk and take precautionary measures.
- To avoid losing any customized policies from the domains by import, before importing, make sure to run **Estimate Impact**. Estimate impact provides you a detailed list of potential issues. You can review the results and make import decision based on the information.
- If the policy you are importing causes server reboot, when you run the estimate impact you can review that and take proper precautionary measures before performing the import. Sometimes, even if the estimate impact warns about a reboot, the reboot may not happen immediately. The reboot option in the global default maintenance policy would trigger the reboot action based on the selected option.
- When you import a policy from a Cisco UCS Domain, if Cisco UCS Central does not support some component of that policy, the unsupported components are dropped from the policy during import.
- If you are importing a policy that causes a server reboot, sometimes the server reboot may not happen immediately after the import. It will happen based on the schedule associated with the maintenance policy.

Policies and Policy Dependents

The following tables lists the policies or dependents that you can import from Cisco UCS Manager:

Polices or Dependents	Description
Policies	You can import the following policies: • BIOS Policy • Boot Policy • CIM XML Policy • Call Home Policy • DNS Policy • Dynamic vNIC Connection Policy • Ethernet Adapter Policy • Fibre Channel Adapter Policy • Global Fault Policy • Global Power Allocation Policy • HTTP Policy • Interface Monitoring Policy • LAN Connectivity Policy • Local Disk Configuration Policy • Maintenance Policy • SEL Policy • SNMP Policy • Scrub Policy • Serial over LAN Policy • Server Pool Policy • Server Pool Policy Qualification • Shell Session Limits Policy • Syslog Policy • TFTP Core Export Policy • Telnet Policy • Threshold Policy • Time Zone Policy • Web Session Limits Policy • iSCSI Channel Adapter Policy • vNIC. vHBA Placement Policy

Polices or Dependents	Description
Pools	• IP Pools • IQN Pool • MAC Pool • UUID Suffix Pool • WWN Pool
Policy dependents	• Host Firmware Package • IPMI Access Profile • Schedule • Service Profile Template • iSCSI Authentication Profile • vHBA Template • vNIC Template • vLAN • vSAN

Policies that Cause Server Reboot During Import

The following policies cause server reboot in the destination after import:

- Boot Policy

Importing a Policy or a Policy Component from a UCS Domain

Make sure the policy you are importing does not cause a server reboot in the destination. For information on policies or policy component you can import and policies that cause server reboot, see Policies and Policy Dependents, on page 142

Important

- When you import a policy to the root or any domain, if a policy with the same name already exist in the domain, Cisco UCS Central displays a confirmation dialog box that warns you about the policy overwrite. If you select import, the imported policy overwrites the existing policy. You can not retrieve the existing policy after the import.
- To avoid losing any customized policies from the domains by import, before importing, make sure to run **Estimate Impact**. Estimate impact provides you a detailed list of potential issues. You can review the results and make import decision based on the information.

Procedure

Step 1 Click **Import** tab.

Step 2 **Search** for the policy you want to import.
You can search for the policy in one of the following two ways:

- Click **Select Type** drop down option to find the policy you want to import, and click **Search**.
- If you know the policy name, type the name in **Search policies, pools, vLANs, vSANs in UCS Domains by name** field and click **Search**.

Note Click the arrow next to Search to expand search filter options to refine your search for a policy. You can narrow your search by specifying options in fields such as, **Select Ownership**, **Domain Group**, **UCS Domain**, and **Org**.

Step 3 From the displayed list of search results, click and select the policy you want to import.
Selecting the policy displays **Import** and **Properties (UCS View)**.

Step 4 Click **Import** to launch the **Import** dialog box.
Options in the **Import** dialog box depends on the policy you have selected for import. Certain policies will display **Import As** option. You can import the selected policy with a different name in the selected destination.

Step 5 Specify the Destination for import.
Depending on the policy or component you are importing, you can import them into either of the following destinations:

- Domain group root or to a specific domain
- Policy name or org level

Step 6 Click **Estimate Impact**.
Progress bar displays the estimate impact status. When that reaches **100%**, click **Review Impact** to review the impact of the import in the specified destination.

Step 7 Click **Import**.
If the import is successful system displays **Import Successful** message.

Local Policies

The policies you create and manage in Cisco UCS Manager are local to the registered Cisco UCS domain. In Cisco UCS Central you can view the policies available in the registered Cisco UCS Domains as local policies. These policies can only be included in local service profiles or service profile templates that are created and managed within that Cisco UCS domain.

Statistics Threshold Policy

A statistics threshold policy monitors statistics about certain aspects of the system and generates an event if the threshold is crossed. You can set both minimum and maximum thresholds. For example, you can configure

the policy to raise an alarm if the CPU temperature exceeds a certain value, or if a server is overutilized or underutilized.

These threshold policies do not control the hardware or device-level thresholds enforced by endpoints, such as the CIMC. Those thresholds are burned in to the hardware components at manufacture.

Cisco UCS enables you to configure statistics threshold policies for the following components:

- Servers and server components
- Uplink Ethernet ports
- Ethernet server ports, chassis, and fabric interconnects
- Fibre Channel port

Note You cannot create or delete a statistics threshold policy for Ethernet server ports, uplink Ethernet ports, or uplink Fibre Channel ports. You can only configure the existing default policy.

Creating a Threshold Policy

You can create and configure threshold policies within the appropriate organization in the Policies node on the **Network** tab, the **Servers** tab, and the **Equipment** tab.

Procedure

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

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Right-click **Threshold Policies** and choose **Create Threshold Policy**.

Step 4 In the **Create Threshold Policy** dialog box, enter the **Name** and optional description.

Note You can create a threshold class and threshold definition at this time, or close the dialog box and add them later later. Click **Create Threshold Class** to create a threshold class, and then click **Create Threshold Definition** on the **Create Threshold Class** dialog box.

Step 5 Click **OK**.

What to Do Next

- Add a threshold class to the threshold policy
- Add a threshold definition to the threshold class

Adding a Threshold Class to an Existing Threshold Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Threshold Policies**.

Step 4 Select the policy for which you want to create a threshold class.

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

Step 6 In the **Threshold Classes** table, click **Create Threshold Class**.

Step 7 In the **Create Threshold Class** dialog box, choose the statistics class that you want to configure.

Step 8 Click **OK**.
The new class appears in the **Threshold Classes** table.

Step 9 In the **Work** pane, click **Save**.

What to Do Next

- Add additional threshold classes to the threshold policy.
- Add a threshold definition.

Adding a Threshold Definition to an Existing Threshold Class

Procedure

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

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Threshold Policies**.

Step 4 Select the policy for which you want to create a threshold definition.

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

Step 6 In the **Threshold Classes** table, right-click the threshold class that you want to modify and choose **Create Threshold Definition**.

Step 7 In the **Create Threshold Definition** dialog box, choose the **Property Type**, enter the **Normal Value (packets)**, and choose the alarm triggers above and below normal value.

Step 8 Click **OK**.

Step 9 In the **Work** pane, click **Save**.

Deleting a Threshold Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Threshold Policies**.

Step 4 Right-click the policy that you want to delete and choose **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Deleting a Threshold Class from a Threshold Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Threshold Policies**.

Step 4 Select the policy for which you want to delete a threshold class.

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

Step 6 In the **Threshold Classes** table, right-click the threshold definition you want to delete and choose **Delete**

Step 7 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Deleting a Threshold Definition from a Threshold Class

Procedure

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

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Threshold Policies**.

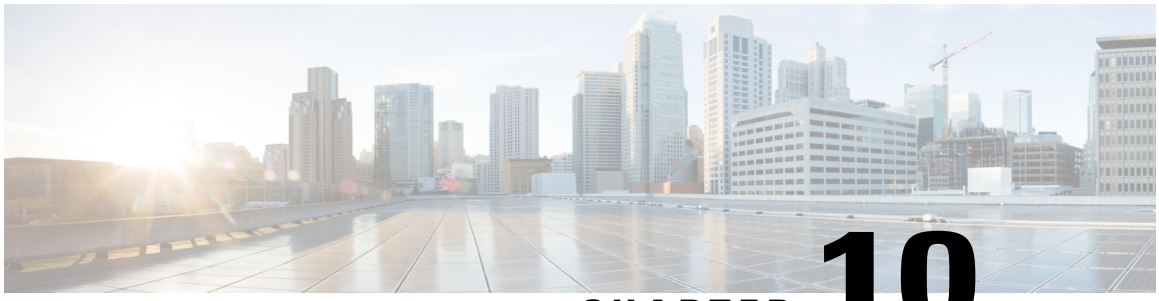
Step 4 Select the policy for which you want to delete a threshold definition.

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

Step 6 In the **Threshold Classes** table, expand the threshold class for which you want to delete a threshold definition.

Step 7 Right-click the threshold definition you want to delete and choose **Delete**.

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



CHAPTER 10

Service Profiles and Templates

This chapter includes the following sections:

- Global Service Profiles, page 151
- Global Service Profile Template, page 158
- Scheduling Service Profile Updates, page 161

Global Service Profiles

Global service profile centralizes the logical configuration deployed in across the data center. This centralization enables the maintenance of all service profiles in the Cisco UCS domains from one central location in Cisco UCS Central. When you use a global service profile, you can do the following across the data center:

- Pick a compute element for the service profile from any of the Cisco UCS domains.
- Migrate the service profile from one element to another.
- Select servers from the available global server pools from any of the Cisco UCS domains.
- Associate global resources such as ID pools and policies.
- Reference to any of the global policies in the Cisco UCS domain.

Creating Global Service Profiles

You can create a global service profile from Cisco UCS Central GUI or Cisco UCS Central CLI or as regular service profiles from Cisco UCS Manager and reference the global polices. When you create the global service profile from Cisco UCS Central, you can create ID pools, vNICs and vHBAs in Cisco UCS Central and reference to the ID.

Configuring Management IP Addresses for Global Service Profiles

Each server in a Cisco UCS domain must have one or more management IP addresses assigned to its Cisco Integrated Management Controller (CIMC) or to the service profile associated with the server. In Cisco UCS Central, the following management IP addresses can be configured to create a service profile:

- Zero or one outband IPv4 address, through which traffic traverses the fabric interconnect through the management port.
- Zero or one inband (IPv4 or IPv6) address, through which traffic traverses the fabric interconnect through the fabric uplink port.

You can configure either a pooled or a static management IP address through the Cisco UCS Central GUI or CLI. However, while creating a global service profile using the global service profile template, you can only configure a pooled management IP address. Static IP address is not supported for this release.

Guidelines and Cautions for Global Service Profile

Make sure to remember the following when you are creating global service profiles:

- When you create a global service profile in Cisco UCS Central, the system validates the following information:
  - Use od ID along with vNICs, vHBAs, iSCSI vNICs etc
  - vLAN and vSAN assignment
  - Association to the compute element based on the availability index
  - Server qualification criteria

    Any incompatibility in these information will be flagged. You can successfully create the global service profile only after resolving these issues.
- After any of the policy reference is resolved in the global service profile, if any of the remote policy is changed, that will result in reconfiguration of the global service profile.
- The VLANs and VSANs in Cisco UCS Central belong to domain groups. Make sure to create the VLANS or VSANs under a domain group. In case of VLAN also assign them to Orgs before a vNIC or vHBA from the global service profile can access the VLAN or VSAN.
- You can modify, disassociate or delete any of the global service profile only from Cisco UCS Central.
- You can rename a global service profile only from Cisco UCS Central. When you rename a service profile, Cisco UCS Central deletes the global service profile with old name and creates a new service profile with the new name in the inventory.
- If a server that is associated to the global service profile is removed from the Cisco UCS domain, when you re-acknowledge the server, it will be unassociated from the service profile.
- You cannot define or access domain specific policies, such as multi-cast policy and flow-control policy from Cisco UCS Central. But, you can reference to these policies from Cisco UCS Central by global service profile resources. When you define the global service profile, you can view the available domain specific policies and refer to them in the service profile by name. When the service profile is deployed, the Cisco UCS domain resolves to the policy and includes it in the service profile for that domain.
- You can localize a global service profile from the deployed Cisco UCS Manager. When you localize, the global service profile is deleted from Cisco UCS Central. But all the global policies still remain global. If you want to localize the global policies, you have to localize each policy separately.

Creating a Global Service Profile

When you create a global service profile in Cisco UCS Central, you can specify a name for the new service profile and then use the default values from the system for all other information.

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Global Service Profiles** > **root**.
If you want to create or access a global service profile in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Right-click on the organization where you want to create the global service profile and choose **Create Service Profile**.

Step 4 In the **General** information panel, specify the **Service Profile Name**, UUID assignment and click **Next**.
You can provide an optional description for this service profile. If the UUID is not available, you can also create a UUID Suffix Pool from this panel.

Note To create a global service profile quickly, you can click **Finish** after specifying the name. Cisco UCS Central creates a new global service profile with the specified name and all system default values.

Step 5 (Optional) In the **Networking** panel, specify the required information for **Dynamic vNIC Connections** and **LAN Connectivity** sections, then click **Next**.
You can create dynamic vNIC connection policy and LAN connectivity policy from this panel.

Step 6 (Optional) In the **Storage** panel, specify the SAN configuration information such as, **Local Storage Policy**, **SAN Connectivity** and **WWNN**, then click **Next**.
You can create a local disk configuration policy and SAN connectivity policy from this panel.

Step 7 (Optional) In the **vNIC/vHBA Placement** panel, specify the **Placement Method** and **PCI Order**, then click**Next**.
If you cannot find the policy you would like to use for **Assignment Method**, you can create the VNIC/VHBA placement policy from this panel.

Step 8 (Optional) In the **Boot Order** panel, specify the **Configuration Type** from the drop-down list, then click **Next**.
If you want to specify a new boot policy, you can create a boot policy from this panel.

Step 9 (Optional) In the **Maintenance Policy** panel, specify the maintenance policy, then click **Next**.
You can create a new maintenance policy and specify a maintenance schedule from this panel.

Step 10 (Optional) In the **Server Assignment** panel, specify the **Server Assignment Method** from the drop down list, the **Power State to Apply on Assignment**, then click **Next**.
Based on your selection in the **Server Assignment Method** drop down, you can select server from the list or identify server location in the Cisco UCS Domain.

Step 11 (Optional) In the **Operational Policies** panel, specify the system operational information such as, **Host Firmware Management**, **BIOS Configuration**, **External IPMI Management**, **Management IP Address Policy**, **Monitoring Threshold Configuration**, **Power Control Configuration**, and **Server Scrub Configuration**, then click **Finish**.

Note To set up an Outband IPv4 address or an Inband IPv4 or IPv6 address, click the respective tabs and complete the required fields.

If you do not find the policies you need for each of these configurations, you can create them from this panel.

What to Do Next

Deploy the Global Service profile in UCS Domains.

Creating Global Service Profiles from a Service Profile Template

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Global Service Profile Templates** > **root**.
If you want to create or access a global service profile template in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Click the global service profile template from which you want to create service profiles.

Step 4 In the **Work** pane, from the **Actions** drop-down list, choose **Create Service Profiles From Template**.

Step 5 In the **Create Service Profiles From Template** dialog box, enter the **Name Prefix** and choose the **Number** of service profiles to create.

Step 6 Click **OK**.

Deleting a Global Service Profile

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Global Service Profiles** > **root**.
If you want to create or access a global service profile in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Right-click the global service profile that you want to delete and choose **Delete**.

Step 4 If the Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Global Service Profile Deployment

When you deploy a global service profile from Cisco UCS Central, the service profile definition is sent to the Cisco UCS domain. Then the Cisco UCS domain identifies the server and deploys the service profile to the server. The service profile definition that is sent to the Cisco UCS domain includes the following information :

- Service profile with reference policy names

- vNICs and vHBAs along with their vLAN bindings
- VCON assignment information for placement of VIFs in to appropriate VCON
- The global VLAN and VSAN definition referred to by a vNIC or vHVA in this service profile

You can deploy the global service profile to any of the compute element in either one of the following two ways:

- Direct assignment: Assign the global service profile to one of the available server in any of the registered Cisco UCS domain. You can also pre-provision a non-existent server.
- Server pool assignment: Assign the global service profile to a server pool. The global service profile will pick one of the available server from the pool for association.
- When the Cisco UCS domain receives the global service profile, the Cisco UCS Domain does the following:
  - Configures the global service profile at the local level
  - Resolves the VLAN and VSAN conditions
  - Reports the configuration and operational states to Cisco UCS Central

Changing the Service Profile Association

Follow this procedure if you did not associate the service profile with a server pool when you created it, or to change the server pool with which a service profile is associated.

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Global Service Profiles** > **root**.
If you want to create or access a global service profile in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Click the global service profile that you want to modify.

Step 4 In the **Work** pane, from the **Actions** drop-down list, choose **Change Service Profile Association**.

Step 5 In the **Change Service Profile Association** dialog box, choose the **Server Assignment Method** and select the **Power state to apply on assignment**.

Step 6 In the **Server Pool** area, choose the **Server Pool** and select whether to **Restrict migration of server.**.
You can also create a new server pool.

Step 7 Click **OK**.

Step 8 Click **Save**.

Unassigning a Server from a Global Service Profile

When you disassociate a server from a service profile, Cisco UCS Central attempts to shutdown the operating system on the server. If the operating system does not shutdown within a reasonable length of time, Cisco UCS Central forces the server to shutdown.

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Global Service Profiles** > **root**.
If you want to create or access a global service profile in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Click the global service profile that you want to modify.

Step 4 In the **Work** pane, from the **Actions** drop-down list, choose **Unassign SP**.

Step 5 Click **Yes**.

Step 6 Click **Save**.

Renaming a Global Service Profile

When you rename a global service profile, the following occurs:

- Event logs and audit logs that reference the previous name for the service profile are retained under that name.
- A new audit record is created to log the rename operation.
- All records of faults against the service profile under its previous name are transferred to the new service profile name.

Note You cannot rename a global service profile that has pending changes.

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Global Service Profiles** > **root**.
If you want to create or access a global service profile in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Click the global service profile that you want to modify.
Step 4 In the **Work** pane, from the **Actions** drop-down list, choose **Rename Service Profile**.
Step 5 In the **Rename Service Profile** dialog box, enter the **New Name**.
Step 6 Click **OK**.

Changing the UUID in a Service Profile

Procedure

Step 1 On the menu bar, click **Servers**.
Step 2 In the **Navigation** Pane, expand **Servers** > **Global Service Profiles** > **root**.
If you want to create or access a global service profile in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.
Step 3 Click the global service profile that you want to modify.
Step 4 In the **Work** pane, from the **Actions** drop-down list, choose **Change UUID**.
Step 5 In the **Change UUID** dialog box, choose the **UUID Assignment** that you want to use.
You can also create a UUID suffix pool.
Step 6 Click **OK**.
Step 7 Click **Save**.

Resetting the UUID for a Global Service Profile

If the UUID assignment for your service profile is UUID pool, resetting the UUID automatically assigns a new UUID from the selected UUID pool.

Procedure

Step 1 On the menu bar, click **Servers**.
Step 2 In the **Navigation** Pane, expand **Servers** > **Global Service Profiles** > **root**.
If you want to create or access a global service profile in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.
Step 3 Click the global service profile that you want to modify.
Step 4 In the **Work** pane, from the **Actions** drop-down list, choose **Reset UUID**.
Step 5 Click **Yes**.

Resetting the Management IP for a Global Service Profile

Resetting the management IP automatically assigns a new management IP from the selected IP pool.

Before You Begin

Consider the following points before resetting the management IP address:

- You must not have modified the pool's IP address block, for instance, when the acquired IP address got deleted from the pool.
- You deleted the pool from Cisco UCS Central, or the pool got deleted.
- You created a global service profile using an updated template and assigned a new name to the pool.

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Global Service Profiles** > **root**.
If you want to create or access a global service profile in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Click the global service profile that you want to modify.

Step 4 In the **General** information panel's Management IP Address **Work** pane, click **Reset Management IP**.

Step 5 Click **Yes**.

Step 6 Click **Save**.

Global Service Profile Template

Global service profile templates enable to quickly create several service profiles with the same basic parameters, such as the number of vNICs and vHBAs, and with identity information drawn from the same pools. The service profile template in Cisco UCS Central is similar to the service profile templates in Cisco UCS Manager.

Creating a Global Service Profile Template

When you create a global service profile template in Cisco UCS Central, you can specify a name for the new service profile template and then use the default values from the system for all other information.

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Global Service Profile Templates** > **root**.
If you want to create or access a global service profile template in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Right-click on the organization where you want to create the global service profile template and choose **Create Service Profile Template**.

Step 4 In the **General** information panel, specify the **Service Profile Name**, Type, and UUID assignment, then click **Next**.
You can provide an optional description for this service profile. If the UUID is not available, you can also create a UUID Suffix Pool from this panel.

Note To create a global service profile template quickly, you can click **Finish** after specifying the name. Cisco UCS Central creates a new global service profile template with the specified name and all system default values.

Step 5 (Optional) In the **Networking** panel, specify the required information for the **Dynamic vNIC Connections** and **LAN Connectivity** sections, then click **Next**.
You can create dynamic a vNIC connection policy and LAN connectivity policy from this panel.

Step 6 (Optional) In the **Storage** panel, specify the SAN configuration information such as, **Local Storage Policy**, **SAN Connectivity**, **WWNN**, and **vHBAs**, then click **Next**.
You can create a local disk configuration policy and SAN connectivity policy from this panel.

Step 7 (Optional) In the **vNIC/vHBA Placement** panel, specify the **Placement Method** and **PCI Order**, then click**Next**.
If you cannot find the policy you would like to use for **Assignment Method**, you can create the VNIC/VHBA placement policy from this panel.

Step 8 (Optional) In the **Boot Order** panel, specify the **Configuration Type** from the drop-down list, then click **Next**.
You can create a boot policy from this panel.

Step 9 (Optional) In the **Maintenance Policy** panel, specify the maintenance policy, then click **Next**.
You can create a new maintenance policy and specify a maintenance schedule from this panel.

Step 10 (Optional) In the **Server Assignment** panel, specify the **Server Assignment Method** from the drop-down list and the **Power State to Apply on Assignment**, then click **Next**.
Based on your selection in the **Server Assignment Method** drop down, you can select a server from the list or identify a server location in the Cisco UCS Domain.

Step 11 (Optional) In the **Operational Policies** panel, specify the system operational information such as, **Host Firmware Management**, **BIOS Configuration**, **External IPMI Management**, **Management IP Address Policy**, **Monitoring Threshold Configuration**, **Power Control Configuration**, and **Server Scrub Configuration**, then click **Finish**.

Note To set up an Outband IPv4 address or an Inband IPv4 or IPv6 address, click the respective tabs and complete the required fields.

If you do not find the policies you need for each of these configurations, you can create them from this panel.

Cloning a Global Service Profile Template

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Global Service Profile Templates** > **root**.
If you want to create or access a global service profile template in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Click the global service profile template that you want to clone.

Step 4 In the **Work** pane, from the **Actions** drop-down list, choose **Clone Service Profile Template**.

Step 5 In the **Clone Service Profile Template** dialog box, enter the **New Name** and choose an **Org**.

Step 6 Click **OK**.

Step 7 Navigate to the service profile template that you just created and make sure that all options are correct.

Deleting a Global Service Profile Template

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Global Service Profile Templates** > **root**.
If you want to create or access a global service profile template in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Right-click the global service profile template that you want to delete and choose **Delete**.

Step 4 If the Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Binding a Global Service Profile to a Service Profile Template

You can bind a global service profile to a global service profile template. When you bind the service profile to a template, Cisco UCS Central configures the service profile with the values defined in the service profile template. If the existing service profile configuration does not match the template, Cisco UCS Central reconfigures the service profile. You can only change the configuration of a bound service profile through the associated template.

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Global Service Profiles** > **root**.
If you want to create or access a global service profile in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Click the global service profile that you want to modify.

Step 4 In the **Work** pane, from the **Actions** drop-down list, choose **Bind to Template**.

Step 5 In the **Bind to Template** dialog box, choose the **Service Profile Template**.
You can also create a new service profile template.

Step 6 Click **OK**.

Step 7 Click **Save**.

Unbinding a Global Service Profile from a Service Profile Template

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Global Service Profiles** > **root**.
If you want to create or access a global service profile in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Click the global service profile that you want to modify.

Step 4 In the **Work** pane, from the **Actions** drop-down list, choose **Unbind from Template**.

Step 5 Click **Save**.

Scheduling Service Profile Updates

Deferred Deployment of Service Profiles

Some modifications to a service profile or to an updating service profile template can be disruptive and require a reboot of the server. You can, however, configure deferred deployment to control when those disruptive configuration changes are implemented. For example, you can choose to deploy the service profile changes immediately or have them deployed during a specified maintenance window. You can also choose whether or not a service profile deployment requires explicit user acknowledgement.

Deferred deployment is available for all configuration changes that occur through the association of a service profile with a server. These configuration changes can be prompted by a change to a service profile, to a policy

that is included in a service profile, or to an updating service profile template. For example, you can defer the upgrade and activation of firmware through host firmware packages and management firmware packages, such as server BIOS, RAID controller, host HBA, and network adapters. However, you cannot defer the direct deployment of firmware images for components that do not use either of the firmware packages, such as Cisco UCS Central, fabric interconnects, and I/O modules.

Deferred deployment is not available for the following actions which require the reboot of a server:

- Initial association of a service profile with a server
- Final disassociation of a service profile from a server, without associating the service profile with a different server
- Decommissioning a server
- Reacknowledging a server
- Resetting a server

If you want to defer the deployment of service profile changes, you must configure one or more maintenance policies and configure each service profile with a maintenance policy. If you want to define the time period when the deployment should occur, you also need to create at least one schedule with one or more recurring occurrences or one time occurrences, and include that schedule in a maintenance policy.

Guidelines and Limitations for Deferred Deployment

Cannot Undo All Changes to Service Profiles or Service Profile Templates

If you cancel a pending change, Cisco UCS Central attempts to roll back the change without rebooting the server. However, for complex changes, Cisco UCS Central may have to reboot the server a second time to roll back the change. For example, if you delete a vNIC, Cisco UCS Central reboots the server according to the maintenance policy included in the service profile. You cannot cancel this reboot and change, even if you restore the original vNIC in the service profile. Instead, Cisco UCS Central schedules a second deployment and reboot of the server.

Association of Service Profile Can Exceed Boundaries of Maintenance Window

After Cisco UCS Central begins the association of the service profile, the scheduler and maintenance policy do not have any control over the procedure. If the service profile association does not complete within the allotted maintenance window, the process continues until it is completed. For example, this can occur if the association does not complete in time because of retried stages or other issues.

Cannot Specify Order of Pending Activities

Scheduled deployments run in parallel and independently. You cannot specify the order in which the deployments occur. You also cannot make the deployment of one service profile change dependent upon the completion of another.

Cannot Perform Partial Deployment of Pending Activity

Cisco UCS Central applies all changes made to a service profile in the scheduled maintenance window. You cannot make several changes to a service profile at the same time and then have those changes be spread across several maintenance windows. When Cisco UCS Central deploys the service profile changes, it updates the service profile to match the most recent configuration in the database.

Deferred Deployment Schedules

A schedule contains a set of occurrences. These occurrences can be one time only or can recur at a specified time and day each week. The options defined in the occurrence, such as the duration of the occurrence or the maximum number of tasks to be run, determine whether a service profile change is deployed. For example, if a change cannot be deployed during a given maintenance window because the maximum duration or number of tasks has been reached, that deployment is carried over to the next maintenance window.

Each schedule checks periodically to see whether the Cisco UCS domain has entered one or more maintenance windows. If it has, the schedule executes the deployments that are eligible according to the constraints specified in the maintenance policy

A schedule contains one or more occurrences, which determine the maintenance windows associated with that schedule. An occurrence can be one of the following:

One Time Occurrence

One time occurrences define a single maintenance window. These windows continue until the maximum duration of the window or the maximum number of tasks that can be run in the window has been reached.

Recurring Occurrence

Recurring occurrences define a series of maintenance windows. These windows continue until the maximum number of tasks or the end of the day specified in the occurrence has been reached.

Maintenance Policy

A maintenance policy determines how Cisco UCS Central reacts when a change that requires a server reboot is made to a service profile associated with a server or to an updating service profile bound to one or more service profiles.

The maintenance policy specifies how Cisco UCS Central deploys the service profile changes. The deployment can occur in one of the following ways:

- Immediately
- When acknowledged by a user with admin privileges
- Automatically at the time specified in a schedule

If the maintenance policy is configured to deploy the change during a scheduled maintenance window, the policy must include a valid schedule. The schedule deploys the changes in the first available maintenance window.

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

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

Creating a Maintenance Policy

Procedure

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Domain Groups**.
Step 3 In the **Navigation** pane, expand **Domain Groups**.
Step 4 Expand the node for the domain group where you want to create a policy
Step 5 Right-click **Maintenance** and choose **Create Maintenance Policy**.
Step 6 In the **Create Maintenance Policy** dialog box, enter the **Name** and optional description, and choose the **Reboot Policy**.
Step 7 Click **OK**.

What to Do Next

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

Creating a Schedule

Procedure

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Domain Groups**.
Step 3 Expand the node for the domain group where you want to create a schedule.
Step 4 Right-click **Schedules** and choose **Create Schedule**.
Step 5 In the **Create Schedule** dialog box, enter the **Name** and optional description, and check the **User Ack** check box to require explicit user acknowledgement.
You can also create a one time or recurring occurrence from this dialog box.

Step 6 Click **OK**.

What to Do Next

Add a one time or recurring occurrence to the schedule.

Creating a One Time Occurrence Schedule

Procedure

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Domain Groups**.
Step 3 Expand the node for the domain group where you want to modify a schedule.
Step 4 Expand **Schedules**.
Step 5 Click the schedule you want to modify.
Step 6 In the **Work** pane, click the **One Time Occurrence** tab.
Step 7 Click **Create One Time Occurrence**.
Step 8 In the **Create One Time Occurrence** dialog box, enter the **Name** and choose the **Start Time**.
Step 9 Choose the **Maximum Number of Tasks**, **Maximum Number of Concurrent Tasks**, **Maximum Duration**, and **Minimum Interval Between Tasks**.
Step 10 Click **OK**.

Creating a Recurring Occurrence for a Schedule

Procedure

Step 1 On the menu bar, click **Operations Management**.
Step 2 In the **Navigation** pane, expand **Domain Groups**.
Step 3 Expand the node for the domain group where you want to modify a schedule.
Step 4 Expand **Schedules**.
Step 5 Click the schedule you want to modify.
Step 6 In the **Work** pane, click the **Recurring Occurrence** tab.
Step 7 Click **Create Recurring Occurrence**.
Step 8 In the **Create Recurring Occurrence** dialog box, enter the **Name** and choose the start time.
Step 9 Choose the **Maximum Number of Tasks**, **Maximum Number of Concurrent Tasks**, **Maximum Duration**, and **Minimum Interval Between Tasks**.
Step 10 Click **OK**.

Pending Activities

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

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

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

- Name of the service profile to be deployed and associated with a server
- Server affected by the deployment
- Disruption caused by the deployment
- Change performed by the deployment

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

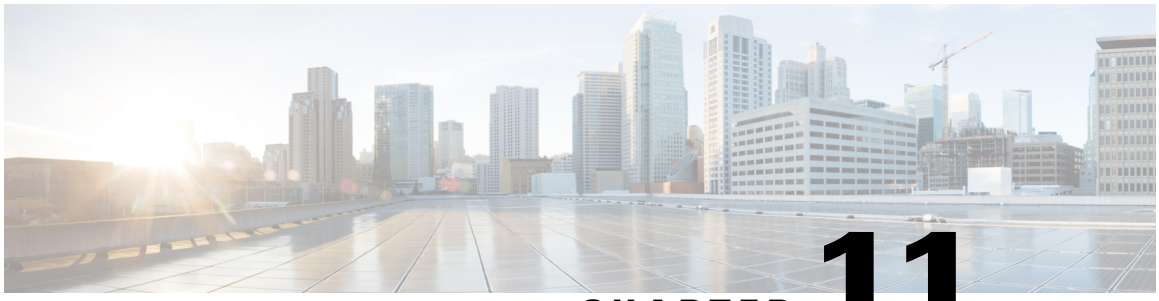
Viewing Pending Activities

Procedure

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

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

Step 3 In the **Work** pane, click the **Pending Activities** tab.



CHAPTER 11

Server Policies

This chapter includes the following sections:

- Ethernet and Fibre Channel Adapter Policies, page 167
- Server BIOS Settings, page 169
- BIOS Policy, page 187
- IPMI Access Profile, page 189
- Local Disk Configuration Policy, page 191
- Power Control Policy, page 204
- Scrub Policy, page 205
- Serial over LAN Policy, page 207
- Server Pool Policy, page 208
- Server Pool Policy Qualifications, page 209
- vNIC/vHBA Placement Policies, page 222

Ethernet and Fibre Channel Adapter Policies

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

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

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

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

Operating System Specific Adapter Policies

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

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

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

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

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

Completion Queues = 1 + 8 = 9
Interrupt Count = (9 + 2) rounded up to the nearest power of 2 = 16

Creating an Ethernet Adapter Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Right-click **Adapter Policies** and choose **Create Ethernet Adapter Policy**.

Step 4 In the **Create Ethernet Adapter Policy** dialog box, enter the **Name** and optional description.

Step 5 In the **Resources** area, enter the **Transmit Queues**, **Receive Queues**, and **Completion Queues**, and the **Ring Size** for each queue.

Step 6 In the **Options** area, choose the **Transmit Checksum Offload**, **Receive Checksum Offload**, **TCP Segmentation Offload**, **TCP Large Receive Offload** and **Receive Side Scaling (RSS)**.

Step 7 Enter the **Failback Timeout (Seconds)**, choose the **Interrupt Mode** and **Interrupt Coalescing Type**, and enter the **Interrupt Time (us)**

Step 8 Click **OK**.

Deleting an Ethernet Adapter Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Adapter Policies**.

Step 4 Right-click the policy that you want to delete and choose **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Server BIOS Settings

Cisco UCS provides two methods for making global modifications to the BIOS settings on servers in an Cisco UCS domain. You can create one or more BIOS policies that include a specific grouping of BIOS settings that match the needs of a server or set of servers, or you can use the default BIOS settings for a specific server platform.

Both the BIOS policy and the default BIOS settings for a server platform enable you to fine tune the BIOS settings for a server managed by Cisco UCS Central.

Depending upon the needs of the data center, you can configure BIOS policies for some service profiles and use the BIOS defaults in other service profiles in the same Cisco UCS domain, or you can use only one of them. You can also use Cisco UCS Central to view the actual BIOS settings on a server and determine whether they are meeting current needs.

Note Cisco UCS Central pushes BIOS configuration changes through a BIOS policy or default BIOS settings to the Cisco Integrated Management Controller (CIMC) buffer. These changes remain in the buffer and do not take effect until the server is rebooted.

We recommend that you verify the support for BIOS settings in the server that you want to configure. Some settings, such as Mirroring Mode for RAS Memory, are not supported by all Cisco UCS servers.

Main BIOS Settings

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

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

Name	Description
Post Error Pause	What happens when the server encounters a critical error during POST. This can be one of the following: • **disabled**—The BIOS continues to attempt to boot the server. • **enabled**—The BIOS pauses the attempt to boot the server and opens the Error Manager when a critical error occurs during POST. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Resume Ac On Power Loss	How the server behaves when power is restored after an unexpected power loss. This can be one of the following: • **stay-off**—The server remains off until manually powered on. • **last-state**—The server is powered on and the system attempts to restore its last state. • **reset**—The server is powered on and automatically reset. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Front Panel Lockout	Whether the power and reset buttons on the front panel are ignored by the server. This can be one of the following: • **disabled**—The power and reset buttons on the front panel are active and can be used to affect the server. • **enabled**—The power and reset buttons are locked out. The server can only be reset or powered on or off from the CIMC GUI. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Processor BIOS Settings

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

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

Name	Description
Core Multi Processing	Sets the state of logical processor cores in a package. If you disable this setting, Hyper Threading is also disabled. This can be one of the following: • **all—**Enables multi processing on all logical processor cores. • **1** through **10—**Specifies the number of logical processor cores that can run on the server. To disable multi processing and have only one logical processor core running on the server, select 1. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Execute Disabled Bit	Classifies memory areas on the server to specify where where application code can execute. As a result of this classification, the processor disables code execution if a malicious worm attempts to insert code in the buffer. This setting helps to prevent damage, worm propagation, and certain classes of malicious buffer overflow attacks. This can be one of the following: • **disabled—**The processor does not classify memory areas. • **enabled—**The processor classifies memory areas. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.
Virtualization Technology (VT)	Whether the processor uses Intel Virtualization Technology, which allows a platform to run multiple operating systems and applications in independent partitions. This can be one of the following: • **disabled—**The processor does not permit virtualization. • **enabled—**The processor allows multiple operating systems in independent partitions. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. **Note** If you change this option, you must power cycle the server before the setting takes effect.

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

Name	Description
Processor C3 Report	Whether the processor sends the C3 report to the operating system. This can be one of the following: • **disabled—**The processor does not send the C3 report. • **acpi-c2—**The processor sends the C3 report using the ACPI C2 format. • **acpi-c3—**The processor sends the C3 report using the ACPI C3 format. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. On the B440 server, the BIOS Setup menu uses enabled and disabled for these options. If you specify acpi-c2 or acpi-c2, the server sets the BIOS value for that option to enabled.
Processor C6 Report	Whether the processor sends the C6 report to the operating system. This can be one of the following: • **disabled—**The processor does not send the C6 report. • **enabled—**The processor sends the C6 report. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Processor C7 Report	Whether the processor sends the C7 report to the operating system. This can be one of the following: • **disabled—**The processor does not send the C7 report. • **enabled—**The processor sends the C7 report. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
CPU Performance	Sets the CPU performance profile for the server. This can be one of the following: • **enterprise—**For M3 servers, all prefetchers and data reuse are enabled. For M1 and M2 servers, data reuse and the DCU IP prefetcher are enabled, and all other prefetchers are disabled. • **high-throughput—**Data reuse and the DCU IP prefetcher are enabled, and all other prefetchers are disabled. • **hpc—**All prefetchers are enabled and data reuse is disabled. This setting is also known as high performance computing.

Name	Description
Max Variable MTRR Setting	Allows you to select the number of MTRR variables. This can be one of the following: • **auto-max—**The BIOS uses the default value for the processor. • **8—**The BIOS uses the number specified for the variable MTRR. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Local X2 APIC	Allows you to set the type of APIC architecture. This can be one of the following: • **xapic—**Uses the standard xAPIC architecture. • **x2apic—**Uses the enhanced x2APIC architecture to support 32 bit addressability of processors. • **auto—**Automatically uses the xAPIC architecture that is detected. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Intel Directed I/O BIOS Settings

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

Name	Description
VT for Directed IO	Whether the processor uses Intel Virtualization Technology for Directed I/O (VT-d). This can be one of the following: • **disabled—**The processor does not use virtualization technology. • **enabled—**The processor uses virtualization technology. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. **Note** This option must be enabled if you want to change any of the other Intel Directed I/O BIOS settings.

Name	Description
Interrupt Remap	Whether the processor supports Intel VT-d Interrupt Remapping. This can be one of the following: • **disabled—**The processor does not support remapping. • **enabled—**The processor uses VT-d Interrupt Remapping as required. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Coherency Support	Whether the processor supports Intel VT-d Coherency. This can be one of the following: • **disabled—**The processor does not support coherency. • **enabled—**The processor uses VT-d Coherency as required. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
ATS Support	Whether the processor supports Intel VT-d Address Translation Services (ATS). This can be one of the following: • **disabled—**The processor does not support ATS. • **enabled—**The processor uses VT-d ATS as required. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Pass Through DMA Support	Whether the processor supports Intel VT-d Pass-through DMA. This can be one of the following: • **disabled—**The processor does not support pass-through DMA. • **enabled—**The processor uses VT-d Pass-through DMA as required. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

RAS Memory BIOS Settings

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

Name	Description
Memory RAS Config	How the memory reliability, availability, and serviceability (RAS) is configured for the server. This can be one of the following: • **maximum performance—**System performance is optimized. • **mirroring—**System reliability is optimized by using half the system memory as backup. • **lockstep—**If the DIMM pairs in the server have an identical type, size, and organization and are populated across the SMI channels, you can enable lockstep mode to minimize memory access latency and provide better performance. Lockstep is enabled by default for B440 servers. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
NUMA	Whether the BIOS supports NUMA. This can be one of the following: • **disabled—**The BIOS does not support NUMA. • **enabled—**The BIOS includes the ACPI tables that are required for NUMA-aware operating systems. If you enable this option, the system must disable Inter-Socket Memory interleaving on some platforms. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Mirroring Mode	Memory mirroring enhances system reliability by keeping two identical data images in memory. This option is only available if you choose the **mirroring** option for **Memory RAS Config**. It can be one of the following: • **inter-socket—**Memory is mirrored between two Integrated Memory Controllers (IMCs) across CPU sockets. • **intra-socket—**One IMC is mirrored with another IMC in the same socket. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
Sparing Mode	Sparing optimizes reliability by holding memory in reserve so that it can be used in case other DIMMs fail. This option provides some memory redundancy, but does not provide as much redundancy as mirroring. The available sparing modes depend on the current memory population. This option is only available if you choose **sparing** option for **Memory RAS Config**. It can be one of the following: • **dimm-sparing**—One DIMM is held in reserve. If a DIMM fails, the contents of a failing DIMM are transferred to the spare DIMM. • **rank-sparing**—A spare rank of DIMMs is held in reserve. If a rank of DIMMs fails, the contents of the failing rank are transferred to the spare rank. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
LV DDR Mode	Whether the system prioritizes low voltage or high frequency memory operations. This can be one of the following: • **power-saving-mode**—The system prioritizes low voltage memory operations over high frequency memory operations. This mode may lower memory frequency in order to keep the voltage low. • **performance-mode**—The system prioritizes high frequency operations over low voltage operations. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
DRAM Refresh Rate	This option controls the refresh interval rate for internal memory.

Serial Port BIOS Settings

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

Name	Description
Serial Port A	Whether serial port A is enabled or disabled. This can be one of the following: • **disabled—**The serial port is disabled. • **enabled—**The serial port is enabled. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

USB BIOS Settings

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

Name	Description
Make Device Non Bootable	Whether the server can boot from a USB device. This can be one of the following: • **disabled—**The server can boot from a USB device. • **enabled—**The server cannot boot from a USB device. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
USB System Idle Power Optimizing Setting	Whether the USB System Idle Power Optimizing setting is used to reduce USB EHCI idle power consumption. Depending upon the value you choose, this setting can have an impact on performance. This can be one of the following: • **high-performance—**The USB System Idle Power Optimizing setting is disabled, because optimal performance is preferred over power savings. Selecting this option can significantly improve performance. We recommend you select this option unless your site has server power restrictions. • **lower-idle-power—**The USB System Idle Power Optimizing setting is enabled, because power savings are preferred over optimal performance. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
USB Front Panel Access Lock	USB front panel lock is configured to enable or disable the front panel access to USB ports. This can be one of the following: • **disabled** • **enabled** • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

PCI Configuration BIOS Settings

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

Name	Description
Max Memory Below 4G	Whether the BIOS maximizes memory usage below 4GB for an operating system without PAE support, depending on the system configuration. This can be one of the following: • **disabled—**Does not maximize memory usage. Choose this option for all operating systems with PAE support. • **enabled—**Maximizes memory usage below 4GB for an operating system without PAE support. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Memory Mapped IO Above 4Gb Config	Whether to enable or disable memory mapped I/O of 64-bit PCI devices to 4GB or greater address space. Legacy option ROMs are not able to access addresses above 4GB. PCI devices that are 64-bit compliant but use a legacy option ROM may not function correctly with this setting enabled. This can be one of the following: • **disabled—**Does not map I/O of 64-bit PCI devices to 4GB or greater address space. • **enabled—**Maps I/O of 64-bit PCI devices to 4GB or greater address space. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Boot Options BIOS Settings

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

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

Server Management BIOS Settings

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

General Settings

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

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

Console Redirection Settings

Name	Description
Console Redirection	Allows a serial port to be used for console redirection during POST and BIOS booting. After the BIOS has booted and the operating system is responsible for the server, console redirection is irrelevant and has no effect. This can be one of the following: • **disabled—**No console redirection occurs during POST. • **serial-port-a—**Enables serial port A for console redirection during POST. This option is valid for blade servers and rack-mount servers. • **serial-port-b—**Enables serial port B for console redirection and allows it to perform server management tasks. This option is only valid for rack-mount servers. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. **Note** If you enable this option, you also disable the display of the Quiet Boot logo screen during POST.
Flow Control	Whether a handshake protocol is used for flow control. Request to Send / Clear to Send (RTS/CTS) helps to reduce frame collisions that can be introduced by a hidden terminal problem. This can be one of the following: • **none—**No flow control is used. • **rts-cts—**RTS/CTS is used for flow control. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. **Note** This setting must match the setting on the remote terminal application.

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

BIOS Policy

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

To use a BIOS policy, do the following:

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

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

Default BIOS Settings

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

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

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

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

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

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

Creating a BIOS Policy

Cisco UCS Central pushes BIOS configuration changes through a BIOS policy or default BIOS settings to the Cisco Integrated Management Controller (CIMC) buffer. These changes remain in the buffer and do not take effect until the server is rebooted. We recommend that you verify the support for BIOS settings in the server that you want to configure. Some settings, such as Mirroring Mode and Sparing Mode for RAS Memory, are not supported by all Cisco UCS servers.

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Right-click **BIOS Policies** and choose **Create BIOS Policy**.

Step 4 In the **Create BIOS Policy** dialog box, enter the **Name** and optional description.

Note To create a BIOS policy quickly, you can click **Finish** after specifying the name. Cisco UCS Central creates a new BIOS policy with the specified name and all system default values.

Step 5 (Optional) In the **Main** panel, choose the main BIOS settings such as, **Reboot on BIOS Change**, **Quiet Boot**, **Post Error Pause**, **Resume Ac on Power Loss**, and **Front Panel Lockout**, then click **Next**.

Step 6 (Optional) In the **Processor** panel, choose the processor settings, then click **Next**.

Step 7 (Optional) In the **Intel Directed IO** panel, choose the IO settings, then click **Next**.

Step 8 (Optional) In the **RAS Memory** panel, choose the memory settings, then click **Next**.

Step 9 (Optional) In the **Serial Port** panel, choose the **Serial Port A** settings, then click **Next**.

Step 10 (Optional) In the **Processor** panel, choose the processor settings information, then click **Next**.

Step 11 (Optional) In the **USB** panel, choose the USB settings such as, **Make Device Non Bootable**, **Legacy USB Support**, **USB Idle Power Optimizing Setting**, and **USB Front Panel Access Lock**, then click **Next**.

Step 12 (Optional) In the **PCI Configuration** panel, choose the PCI configuration settings such as, **Max Memory Below 4GB** and **Memory Mapped IO Above 4GB Config**, then click **Next**.

Step 13 (Optional) In the **Boot Options** panel, choose the boot settings such as, **Boot Option Retry**, **Intel Entry SAS RAID**, **Intel Entry SAS RAID Module**, and **Onboard SCU Storage Support**, then click **Next**.

Step 14 (Optional) In the **Server Manager** panel, choose the non-maskable interrupt settings and the **OS Boot Watchdog Timer**, specify the **Console Redirection** settings, then click**Finish**.

Modifying a BIOS Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **BIOS Policies**.

Step 4 Click the BIOS policy that you want to modify.

Step 5 In the **Work** pane, click the appropriate tab and then click the desired radio button or make a choice from the drop-down list to modify the BIOS settings.

Step 6 Click **Save**.

Deleting a BIOS Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **BIOS Policies**.

Step 4 Right-click the policy that you want to delete and choose **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

IPMI Access Profile

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

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

Creating an IPMI Access Profile

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

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Right-click **IPMI Access Profiles** and choose **Create IPMI Access Profile**.

Step 4 In the **Create IPMI Access Profile** dialog box, enter the **Name** and optional description.

Step 5 Click **Create IPMI User** to add IPMI users to the IPMI Access Profile.

Step 6 Click **OK**.

What to Do Next

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

Adding an IPMI User to an IPMI Access Profile

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **IPMI Access Profiles**.

Step 4 Click the IPMI access profile for which you want to add an IPMI user.

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

Step 6 In the **IPMI Users** area, click **Create IPMI User**.

Step 7 In the **Create IPMI Users** dialog box, enter the **Name** and **Password**, confirm the password, and choose a **Serial over LAN State**.

Step 8 Click **OK**.

Deleting an IPMI Access Profile

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **IPMI Access Profiles**.

Step 4 Right-click the IPMI access profile that you want to delete and choose **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Deleting an IPMI User from an IPMI Access Profile

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **IPMI Access Profiles**.

Step 4 Click the IPMI access profile for which you want to delete an IPMI user.

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

Step 6 In the **IPMI Users** table, click the IPMI user you want to delete.

Step 7 In the **IPMI Users** toolbar, click **Delete**.

Local Disk Configuration Policy

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

The local disk modes include the following:

- **No Local Storage—**For a diskless server or a SAN only configuration. If you select this option, you cannot associate any service profile which uses this policy with a server that has a local disk.
- **RAID 0 Striped—**Data is striped across all disks in the array, providing fast throughput. There is no data redundancy, and all data is lost if any disk fails.
- **RAID 1 Mirrored—**Data is written to two disks, providing complete data redundancy if one disk fails. The maximum array size is equal to the available space on the smaller of the two drives.
- **Any Configuration—**For a server configuration that carries forward the local disk configuration without any changes.
- **No RAID—**For a server configuration that removes the RAID and leaves the disk MBR and payload unaltered.

  If you choose **No RAID** and you apply this policy to a server that already has an operating system with RAID storage configured, the system does not remove the disk contents. Therefore, there may be no visible differences on the server after you apply the **No RAID** mode. This can lead to a mismatch between the RAID configuration in the policy and the actual disk configuration shown in the **Inventory** > **Storage** tab for the server.

  To make sure that any previous RAID configuration information is removed from a disk, apply a scrub policy that removes all disk information after you apply the **No RAID** configuration mode.

- **RAID 5 Striped Parity—**Data is striped across all disks in the array. Part of the capacity of each disk stores parity information that can be used to reconstruct data if a disk fails. RAID 5 provides good data throughput for applications with high read request rates.
- **RAID 6 Striped Dual Parity—**Data is striped across all disks in the array and two parity disks are used to provide protection against the failure of up to two physical disks. In each row of data blocks, two sets of parity data are stored.
- **RAID 10 Mirrored and Striped—**RAID 10 uses mirrored pairs of disks to provide complete data redundancy and high throughput rates.
- **RAID 50 Striped Parity and Striped —**Data is striped across multiple striped parity disk sets to provide high throughput and multiple disk failure tolerance.
- **RAID 60 Striped Dual Parity and Striped —**Data is striped across multiple striped dual parity disk sets to provide high throughput and greater disk failure tolerance.

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

Boot Policy

The Cisco UCS Manager boot policy overrides the boot order in the BIOS setup menu, and determines the following:

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

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

You must include this policy in a service profile, and that service profile must be associated with a server for it to take effect. If you do not include a boot policy in a service profile, Cisco UCS Manager applies the default boot policy.

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

Creating a Boot Policy

You can also create a local boot policy that is restricted to a service profile or service profile template. However, except for iSCSI boot, we recommend that you create a global boot policy that can be included in multiple service profiles or service profile templates.

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Right-click **Boot Policies** and choose **Create Boot Policy**.

Step 4 In the **Create Boot Policy** dialog box, enter the **Name**and optional description.

Step 5 (Optional) To reboot all servers that use this boot policy after you make changes to the boot policy, check the**Reboot on Boot Order Change** check box.

Step 6 (Optional) To enforce that the vNICs, vHBAs, or iSCSI vNICs listed in the **Qualifications** table match the server configuration in the service profile, check the **Enforce vNIC/vHBA/iSCSI Name** check box.

Step 7 In the **Actions** area, configure one or more of the following boot options for the boot policy and set their boot order:

- Local device boot—Click **Add CD/DVD ROM Boot** or **Add Local Disk** to add local devices to the boot policy.
- LAN Boot—Click **Add LAN Boot** to boot from a centralized provisioning server.
- SAN Boot—Click **Add SAN Boot** to boot from an operating system image on the SAN.

  If the vHBA points to a bootable SAN image, click **Add SAN Boot Target** to configure it.
- iSCSI vNICs—Click **Add iSCSI Boot** to boot from an iSCSI LUN.

Step 8 (Optional) Click the up and down arrows in the **Qualifications** table to change the boot order.

Step 9 Click **OK**.

What to Do Next

Include the boot policy in a service profile and/or template.

After a server is associated with a service profile that includes this boot policy, you can verify the actual boot order in the Boot Order Details area on the General tab for the server.

Modifying a Boot Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Boot Policies**.

Step 4 Click the boot policy that you want to modify.

Step 5 In the **Work** pane, click the **General** tab and make the appropriate changes to the boot options and boot order.

Step 6 Click **Save**.

Deleting a Boot Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Boot Policies**.

Step 4 Right-click the policy that you want to delete and choose **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

LAN Boot

You can configure a boot policy to boot one or more servers from a centralized provisioning server on the LAN. A LAN (or PXE) boot is frequently used to install operating systems on a server from that LAN server.

You can add more than one type of boot device to a LAN boot policy. For example, you could add a local disk or virtual media boot as a secondary boot device.

Configuring a LAN Boot for a Boot Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Boot Policies**.

Step 4 Click the boot policy for which you want to configure a LAN boot.

Step 5 In the **Work** pane, on the **General** tab, click **Add LAN Boot**.

Step 6 In the **Add LAN Boot** dialog box, enter the **vNIC** and select primary or secondary from the **Type** drop-down list.

Step 7 Click **OK** to close the dialog box.

Step 8 Click **Save** to save the boot policy.

SAN Boot

You can configure a boot policy to boot one or more servers from an operating system image on the SAN. The boot policy can include a primary and a secondary SAN boot. If the primary boot fails, the server attempts to boot from the secondary.

We recommend that you use a SAN boot, because it offers the most service profile mobility within the system. If you boot from the SAN when you move a service profile from one server to another, the new server boots from the exact same operating system image. Therefore, the new server appears to be the exact same server to the network.

To use a SAN boot, ensure that the following is configured:

- The Cisco UCS domain must be able to communicate with the SAN storage device that hosts the operating system image.
- A boot target LUN on the device where the operating system image is located.

Note SAN boot is not supported on Gen-3 Emulex adapters on Cisco UCS blade & rack servers.

Configuring a SAN Boot for a Boot Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Boot Policies**.

Step 4 Click the boot policy for which you want to configure a SAN boot.

Step 5 In the **Work** pane, on the **General** tab, click **Add SAN Boot**.

Step 6 In the **Add SAN Boot** dialog box, enter the **vHBA** and choose primary or secondary from the **Type** drop-down list.

Step 7 Click **OK** to close the dialog box.

Step 8 Click **Save** to save the boot policy.

Adding a SAN Boot Target

You must have configured a SAN boot for a boot policy before you can add a SAN boot target.

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Boot Policies**.

Step 4 Click the boot policy for which you want add a SAN boot target.

Step 5 In the **Work** pane, on the **General** tab, click **Add SAN Boot Target**.

Step 6 In the **Add SAN Boot Target** dialog box, enter the **Boot Target LUN** and the **Boot Target WWPN**, and select primary or secondary from the **Type** drop-down list.

Step 7 Click **OK** to close the dialog box.

Step 8 Click **Save** to save the boot policy.

iSCSI Boot

iSCSI boot enables a server to boot its operating system from an iSCSI target machine located remotely over a network.

iSCSI boot is supported on the following Cisco UCS hardware:

- Cisco UCS blade servers that have the Cisco UCS M51KR-B Broadcom BCM57711 network adapter and use the default MAC address provided by Broadcom.
- Cisco UCS M81KR Virtual Interface Card
- Cisco UCS VIC-1240 Virtual Interface Card
- Cisco UCS VIC-1280 Virtual Interface Card
- Cisco UCS rack servers that have the Cisco UCS M61KR-B Broadcom BCM57712 network adapter.
- Cisco UCS P81E Virtual Interface Card

- Cisco UCS VIC1225 Virtual Interface Card

There are prerequisites that must be met before you configure iSCSI boot. For a list of these prerequisites, see iSCSI Boot Guidelines and Prerequisites, on page 197.

iSCSI Boot Process

Cisco UCS Central uses the iSCSI vNIC and iSCSI boot information created for the service profile in the association process to program the adapter, located on the server. After the adapter is programmed, the server reboots with the latest service profile values. After the power on self-test (POST), the adapter attempts to initialize using these service profile values. If the adapter can use the values and log in to its specified target, the adapter initializes and posts an iSCSI Boot Firmware Table (iBFT) to the host memory and a valid bootable LUN to the system BIOS. The iBFT that is posted to the host memory contains the initiator and target configuration that is programmed on the primary iSCSI VNIC.

Note Previously, the host would see only one of the boot paths configured, depending on which path completed the LUN discovery first, and would boot from that path. Now, when there are two iSCSI boot vNICs configured, the host will see both of the boot paths. So for multipath configurations, a single IQN needs to be configured on both the boot vNICs If there are different IQNs configured on the boot vNICs on a host, the host will boot with the IQN that is configured on the boot vNIC with the lower PCI order.

The next step, which is the installation of the operating system (OS), requires an OS that is iBFT capable. During installation of the OS, the OS installer scans the host memory for the iBFT table and uses the information in the iBFT to discover the boot device and create an iSCSI path to the target LUN. In some OS's a NIC driver is required to complete this path. If this step is successful, the OS installer finds the iSCSI target LUN on which to install the OS.

Note The iBFT works at the OS installation software level and might not work with HBA mode (also known as TCP offload). Whether iBFT works with HBA mode depends on the OS capabilities during installation. Also, for a server that includes a Cisco UCS M51KR-B Broadcom BCM57711 adapter, the iBFT normally works at a maximum transmission unit (MTU) size of 1500, regardless of the MTU jumbo configuration. If the OS supports HBA mode, you might need to set HBA mode, dual-fabric support, and jumbo MTU size after the iSCSI installation process.

iSCSI Boot Guidelines and Prerequisites

These guidelines and prerequisites must be met before configuring iSCSI boot:

- After the iSCSI boot policies have been created, a user with ls-compute privileges can include them in a service profile or service profile template. However, a user with only ls-compute privileges cannot create iSCSI boot policies.
- To set up iSCSI boot from a Windows 2008 server where the second vNIC (failover vNIC) must boot from an iSCSI LUN, consult Microsoft Knowledge Base Article 976042. Microsoft has a known issue where Windows might fail to boot from an iSCSI drive or cause a bugcheck error if the networking hardware is changed. To work around this issue, follow the resolution recommended by Microsoft.

- The storage array must be licensed for iSCSI boot and the array side LUN masking must be properly configured.
- Two IP addresses must be determined, one for each iSCSI initiator. If possible, the IP addresses should be on the same subnet as the storage array. The IP addresses are assigned statically or dynamically using the Dynamic Host Configuration Protocol (DHCP).
- You cannot configure boot parameters in the Global boot policy. Instead, after configuring boot parameters, you need to include the boot policy in the appropriate service profile.
- The operating system (OS) must be iSCSI Boot Firmware Table (iBFT) compatible.
- For Cisco UCS M51KR-B Broadcom BCM57711 network adapters:
  - Servers that use iSCSI boot must contain the Cisco UCS M51KR-B Broadcom BCM57711 network adapter. For information on installing or replacing an adapter card, see the *Cisco UCS B250 Extended Memory Blade Server Installation and Service Note*. The service note is accessible from the *Cisco UCS B-Series Servers Documentation Roadmap* at http://www.cisco.com/go/unifiedcomputing/b-series-doc.
  - Set the MAC addresses on the iSCSI device.
  - If you are using the DHCP Vendor ID (Option 43), configure the MAC address of an iSCSI device in /etc/dhcpd.conf.
  - HBA mode (also known as TCP offload) and the boot to target setting are supported. However, only Windows OS supports HBA mode during installation.
  - Before installing the OS, disable the boot to target setting in the iSCSI adapter policy, then after installing the OS, reenable the boot to target setting.

    Note Each time you change an adapter policy setting, the adapter reboots to apply the new setting.

  - When installing the OS on the iSCSI target, the iSCSI target must be ordered *before* the device where the OS image resides. For example, if you are installing the OS on the iSCSI target from a CD, the boot order should be the iSCSI target and then the CD.
  - After the server has been iSCSI booted, do not modify the Initiator Name, Target name, LUN, iSCSI device IP, or Netmask/gateway using the Broadcom tool.
  - Do not interrupt the POST (power on self-test) process or the Cisco UCS M51KR-B Broadcom BCM57711 network adapter will fail to initialize.
- For Cisco UCS M81KR Virtual Interface Card and Cisco UCS VIC-1240 Virtual Interface Card:
  - Do not set MAC addresses on the iSCSI device.
  - HBA mode and the boot to target setting are *not* supported.
  - When installing the OS on the iSCSI target, the iSCSI target must be ordered *after* the device where the OS image resides. For example, if you are installing the OS on the iSCSI target from a CD, the boot order should be the CD and then the iSCSI target.
  - If you are using the DHCP Vendor ID (Option 43), the MAC address of the overlay vNIC needs to be configured in /etc/dhcpd.conf.

- After the server has been iSCSI booted, do not modify the IP details of the overlay vNIC.

- The VMware ESX/ESXi operating system does not support storing a core dump file to an iSCSI boot target LUN. Dump files must be written to a local disk.

Configuring an iSCSI Boot for a Boot Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Boot Policies**.

Step 4 Click the boot policy for which you want to configure an iSCSI boot.

Step 5 In the **Work** pane, on the **General** tab, click **Add iSCSI Boot**.

Step 6 In the **Add iSCSI Boot** dialog box, enter the **iSCSI vNIC** and choose primary or secondary from the **Type** drop-down list.

Step 7 Click **OK** to close the dialog box.

Step 8 Click **Save** to save the boot policy.

Creating an iSCSI Adapter Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Right-click **Adapter Policies** and choose **Create iSCSI Adapter Policy**.

Step 4 In the **Create iSCSI Adapter Policy** dialog box, enter the **Name**, optional description, the **Connection Timeout**, **LUN Busy Retry Count**, and **DHCP Timeout**.

Step 5 Choose the **Enable TCP Timestamp**, **HBA Mode**, and **Boot To Target** checkboxes.

Step 6 Click **OK**.

Deleting an iSCSI Adapter Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Adapter Policies**.

Step 4 Right-click the policy that you want to delete and choose **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Creating an iSCSI Authentication Profile

For iSCSI boot, you need to create both an initiator and a target authentication profile

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Right-click **iSCSI Authentication Profile** and choose **Create iSCSI Authentication Profile**.

Step 4 In the **Create iSCSI Authentication Profile** dialog box, enter the **Name**, **User ID**, optional description, and **Password**, then confirm the password.

Step 5 Click **OK**.

What to Do Next

Include the authentication profile in a service profile and/or template.

Deleting an iSCSI Authentication Profile

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **iSCSI Authentication Profile**.

Step 4 Right-click the iSCSI authentication profile that you want to delete and choose **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Guidelines for all Local Disk Configuration Policies

Before you create a local disk configuration policy, consider the following guidelines:

No Mixed HDDs and SSDs

Do not include HDDs and SSDs in a single server or RAID configuration.

Do Not Assign a Service Profile with the Default Local Disk Configuration Policy from a B200 M1 or M2 to a B200 M3

Due to the differences in the RAID/JBOD support provided by the storage controllers of B200 M1 and M2 servers and those of the B200 M3 server, you cannot assign or re-assign a service profile that includes the default local disk configuration policy from a B200M1 or M2 server to a B200 M3 server. The default local disk configuration policy includes those with Any Configuration or JBOD configuration.

JBOD Mode Support

Note Only B200 M1, B200 M2, B200 M3, B250 M1, B250 M2 and B22 M3 blade servers support the JBOD mode for local disks.

Guidelines for Local Disk Configuration Policies Configured for RAID

Configure RAID Settings in Local Disk Configuration Policy for Servers with MegaRAID Storage Controllers

If a blade server or integrated rack-mount server has a MegaRAID controller, you must configure RAID settings for the drives in the Local Disk Configuration policy included in the service profile for that server. You can do this either by configuring the local disk configuration policy in the service profile using one of the defined RAID modes for that server, or you can use the **Any Configuration** mode with the LSI Utilities toolset to create the RAID volumes.

If you do not configure your RAID LUNs before installing the OS, disk discovery failures might occur during the installation and you might see error messages such as “No Device Found.”

Server May Not Boot After RAID1 Cluster Migration if Any Configuration Mode Specified in Service Profile

After RAID1 clusters are migrated, you need to associate a service profile with the server. If the local disk configuration policy in the service profile is configured with **Any Configuration** mode rather than **RAID1**, the RAID LUN remains in "inactive" state during and after association. As a result, the server cannot boot.

To avoid this issue, ensure that the service profile you associate with the server contains the identical local disk configuration policy as the original service profile before the migration and does not include the **Any Configuration** mode.

Do Not Use JBOD Mode on Servers with MegaRAID Storage Controllers

Do not configure or use JBOD mode or JBOD operations on any blade server or integrated rack-mount server with a MegaRAID storage controllers. JBOD mode and operations are not intended for nor are they fully functional on these servers.

Maximum of One RAID Volume and One RAID Controller in Integrated Rack-Mount Servers

A rack-mount server that has been integrated with Cisco UCS Manager and is registered with Cisco UCS Central can have a maximum of one RAID volume irrespective of how many hard drives are present on the server.

All the local hard drives in an integrated rack-mount server must be connected to only one RAID Controller. Integration with Cisco UCS Manager does not support the connection of local hard drives to multiple RAID Controllers in a single rack-mount server. We therefore recommend that you request a single RAID Controller configuration when you order rack-mount servers to be integrated with Cisco UCS Manager.

In addition, do not use third party tools to create multiple RAID LUNs on rack-mount servers. Cisco UCS Manager does not support that configuration.

Maximum of One RAID Volume and One RAID Controller in Blade Servers

A blade server can have a maximum of one RAID volume irrespective of how many drives are present in the server. All the local hard drives must be connected to only one RAID controller. For example, a B200 M3 server has an LSI controller and an Intel Patsburg controller, but only the LSI controller can be used as a RAID controller.

In addition, do not use third party tools to create multiple RAID LUNs on blade servers. Cisco UCS Central does not support that configuration.

Number of Disks Selected in Mirrored RAID Should Not Exceed Two

If the number of disks selected in the Mirrored RAID exceed two, RAID 1 is created as a RAID 10 LUN. This issue can occur with the Cisco UCS B440 M1 and B440 M2 servers.

License Required for Certain RAID Configuration Options on Some Servers

Some Cisco UCS servers require a license for certain RAID configuration options. When Cisco UCS Central associates a service profile containing this local disk policy with a server, Cisco UCS Central verifies that the selected RAID option is properly licensed. If there are issues, Cisco UCS Central displays a configuration error during the service profile association.

For RAID license information for a specific Cisco UCS server, see the *Hardware Installation Guide* for that server.

B420 M3 Server Does Not Support All Configuration Modes

The B420 M3 server does not support the following configuration modes in a local disk configuration policy:

- No RAID
- RAID 6 Striped Dual Parity

In addition, the B420 M3 does not support JBOD modes or operations.

Single-Disk RAID 0 Configurations Not Supported on Some Blade Servers

A single-disk RAID 0 configuration is not supported in the following blade servers:

- Cisco UCS B200 M1
- Cisco UCS B200 M2
- Cisco UCS B250 M1
- Cisco UCS B250 M2

Creating a Local Disk Configuration Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Right-click **Local Disk Config Policies** and choose **Create Local Disk Config Policy**.

Step 4 In the **Create Local Disk Config Policy** dialog box, enter the **Name** and other optional details.

Step 5 Click **OK**.

Deleting a Local Disk Configuration Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Local Disk Config Policies**.

Step 4 Right-click the policy that you want to delete and choose **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Power Control Policy

Cisco UCS uses the priority set in the power control policy, along with the blade type and configuration, to calculate the initial power allocation for each blade within a chassis. During normal operation, the active blades within a chassis can borrow power from idle blades within the same chassis. If all blades are active and reach the power cap, service profiles with higher priority power control policies take precedence over service profiles with lower priority power control policies.

Priority is ranked on a scale of 1-10, where 1 indicates the highest priority and 10 indicates lowest priority. The default priority is 5.

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

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

Creating a Power Control Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Right-click **Power Control Policies** and choose **Create Power Control Policy**.

Step 4 In the **Create Power Control Policy** dialog box, enter the **Name** and optional description, choose whether to use **Power Capping**, and enter the **Power Priority**.

Step 5 Click **OK**.

What to Do Next

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

Deleting a Power Control Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.

If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Power Control Policies**.

Step 4 Right-click the policy that you want to delete and choose **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Step 6

Scrub Policy

This policy determines what happens to local data and to the BIOS settings on a server during the discovery process, when the server is reacknowledged, or when the server is disassociated from a service profile.

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

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

Disk scrub

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

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

BIOS Settings Scrub

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

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

FlexFlash Scrub

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

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

Note

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

Creating a Scrub Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Right-click **Scrub Policies** and choose **Create Scrub Policy**.

Step 4 In the **Create Scrub Policy** dialog box, enter the **Name** and optional description, and choose whether to use **Disk Scrub** and **BIOS Setting Scrub**.

Step 5 Click **OK**.

Deleting a Scrub Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Scrub Policies**.

Step 4 Right-click the policy that you want to delete and choose **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Serial over LAN Policy

This policy sets the configuration for the serial over LAN connection for all servers associated with service profiles that use the policy. By default, the serial over LAN connection is disabled.

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

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

Creating a Serial over LAN Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Right-click **Serial over LAN Policies** and choose **Create Serial over LAN Policy**.

Step 4 In the **Create Serial over LAN Policy** dialog box, enter the **Name** and optional description, choose the **Serial over LAN State**, and choose a **Speed** from the drop-down list.

Step 5 Click **OK**.

Deleting a Serial over LAN Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Serial over LAN Policies**.

Step 4 Right-click the policy that you want to delete and choose **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Server Pool Policy

This policy is invoked during the server discovery process. It determines what happens if server pool policy qualifications match a server to the target pool specified in the policy.

If a server qualifies for more than one pool and those pools have server pool policies, the server is added to all those pools.

Creating a Server Pool Policy

Before You Begin

This policy requires that one or more of the following resources already exist in the system:

- A minimum of one server pool
- Server pool policy qualifications, if you choose to have servers automatically added to pools

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Right-click **Server Pool Policies** and choose **Create Policy**.

Step 4 In the **Create Policy** dialog box, enter the **Name**, choose a **Target Pool** and **Qualification** from the drop-down lists, and enter an optional description.

Step 5 Click **OK**.

Deleting a Server Pool Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Server Pool Policies**.

Step 4 Right-click the policy that you want to delete and choose **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Server Pool Policy Qualifications

This policy qualifies servers based on the inventory of a server conducted during the discovery process. The qualifications are individual rules that you configure in the policy to determine whether a server meets the selection criteria. For example, you can create a rule that specifies the minimum memory capacity for servers in a data center pool.

Qualifications are used in other policies to place servers, not just by the server pool policies. For example, if a server meets the criteria in a qualification policy, it can be added to one or more server pools or have a service profile automatically associated with it.

You can use the server pool policy qualifications to qualify servers according to the following criteria:

- Adapter type
- Chassis location
- Memory type and configuration
- Power group
- CPU cores, type, and configuration
- Storage configuration and capacity
- Server model

Depending upon the implementation, you might need to configure several policies with server pool policy qualifications including the following:

- Autoconfiguration policy
- Chassis discovery policy
- Server discovery policy
- Server inheritance policy
- Server pool policy

Creating Server Pool Policy Qualifications

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Right-click **Server Pool Policy Qualifications** and choose **Create Policy Qualification**.

Step 4 In the **Create Policy Qualification** dialog box, enter the **Name** and optional description.

Step 5 In the **Actions** area, configure one or more of the policy qualification options:

- **Create Domain Qualification**
- **Create Adapter Qualification**
- **Create Memory Qualification**
- **Create Processor Qualification**
- **Create Storage Qualification**
- **Create Server PID Qualification**

Step 6 Click **OK**.

Creating a Domain Qualification

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Server Pool Policy Qualifications**.

Step 4 Click the policy qualification that you want to modify.

Step 5 In the **Work** pane, on the **General** tab, click **Create Domain Qualification**.

Step 6 In the **Create Domain Qualification** dialog box, enter the **Name**.

Step 7 In the **Actions** area, configure one or more of the domain qualification options:

- **Create Chassis/Server Qualification**
- **Create Address Qualification**
- **Create Owner Qualification**
- **Create Site Qualification**
- **Create Rack Qualification**

Step 8 Click **OK** to close the dialog box.

Step 9 Click **Save** to save the policy qualification.

Creating an Adapter Qualification

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Server Pool Policy Qualifications**.

Step 4 Click the policy qualification that you want to modify.

Step 5 In the **Work** pane, on the **General** tab, click **Create Adapter Qualification**.

Step 6 In the **Create Adapter Qualification** dialog box, choose the **Type** and enter the **PID (RegEx)**.

Step 7 In the **Units** area, enter a number of units or click the **Unspecified** check box.

Step 8 Click **OK** to close the dialog box.

Step 9 Click **Save** to save the policy qualification.

Creating a Memory Qualification

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Server Pool Policy Qualifications**.

Step 4 Click the policy qualification that you want to modify.

Step 5 In the **Work** pane, on the **General** tab, click **Create Memory Qualification**.

Step 6 In the **Create Memory Qualification** dialog box, enter values for **Clock (MHz)**, **Min Cap (MB)**, **Width**, **Speed**, **Latency (ns)**, **Max Cap (MB)**, and **Units**, or leave them unspecified.

Step 7 Click **OK** to close the dialog box.

Step 8 Click **Save** to save the policy qualification.

Creating a Processor Qualification

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Server Pool Policy Qualifications**.

Step 4 Click the policy qualification that you want to modify.

Step 5 In the **Work** pane, on the **General** tab, click **Create Processor Qualification**.

Step 6 In the **Create Processor Qualification** dialog box, choose the **Processor Architecture**, then enter values for **Min Number of Cores**, **Max Number of Cores**, **Min Number of Threads**, **Max Number of Threads**, **CPU Speed (MHz)**, **CPU Stepping**, **Min Number of Procs**, and **Max Number of Procs**, or leave them unspecified.

Step 7 Click **OK** to close the dialog box.

Step 8 Click **Save** to save the policy qualification.

Creating a Storage Qualification

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Server Pool Policy Qualifications**.

Step 4 Click the policy qualification that you want to modify.

Step 5 In the **Work** pane, on the **General** tab, click **Create Storage Qualification**.

Step 6 In the **Create Storage Qualification** dialog box, choose the **Diskless** state, then enter values for **Number of Blocks**, **Block Size (Bytes)**, **Min Cap (MB)**, **Max Cap (MB)**, **Per Disk Cap (MB)** and **Units**, or leave them unspecified.

Step 7 Click **OK** to close the dialog box.

Step 8 Click **Save** to save the policy qualification.

Creating a Server PID Qualification

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Server Pool Policy Qualifications**.

Step 4 Click the policy qualification that you want to modify.

Step 5 In the **Work** pane, on the **General** tab, click **Create Server PID Qualification**.

Step 6 In the **Create Server PID Qualification** dialog box, enter the **PID (RegEx)**.

Step 7 Click **OK** to close the dialog box.

Step 8 Click **Save** to save the policy qualification.

Creating a Chassis/Server Qualification

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Server Pool Policy Qualifications**.

Step 4 Click the policy qualification that you want to modify.

Step 5 In the **Work** pane, on the **General** tab, click **Create Domain Qualification**.

Step 6 In the **Create Domain Qualification** dialog box, click **Create Chassis/Server Qualification**.

Step 7 In the **Create Chassis/Server Qualification** dialog box, enter the **First Chassis Id** and the **Number of Chassis**.

Step 8 Click **Create Server Qualification** to add a service qualification to the **Server Qualifications** table.

Step 9 Click **OK** to close the dialog box.

Step 10 Click **OK** to close the **Domain Qualification** dialog box.

Creating a Server Qualification

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Server Pool Policy Qualifications**.

Step 4 Click the policy qualification that you want to modify.

Step 5 In the **Work** pane, on the **General** tab, click **Create Domain Qualification**.

Step 6 In the **Create Domain Qualification** dialog box, click **Create Chassis/Server Qualification**.

Step 7 In the **Create Chassis/Server Qualification** dialog box, click **Create Server Qualification**.

Step 8 In the **Create Server Qualification** dialog box, enter the **First Slot Id** and **Number of Slots**.

Step 9 Click **OK** to close the dialog box.

Step 10 Click **OK** to close the **Create Domain Qualification** dialog box.

Step 11 Click **OK** to close the **Domain Qualification** dialog box.

Creating an Address Qualification

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Server Pool Policy Qualifications**.

Step 4 Click the policy qualification that you want to modify.

Step 5 In the **Work** pane, on the **General** tab, click **Create Domain Qualification**.

Step 6 In the **Create Domain Qualification** dialog box, click **Create Address Qualification**.

Step 7 In the **Create Address Qualification** dialog box, enter the **Minimum Address** and the **Maximum Address**.

Step 8 Click **OK** to close the dialog box.

Step 9 Click **OK** to close the **Domain Qualification** dialog box.

Creating an Owner Qualification

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Server Pool Policy Qualifications**.

Step 4 Click the policy qualification that you want to modify.

Step 5 In the **Work** pane, on the **General** tab, click **Create Domain Qualification**.

Step 6 In the **Create Domain Qualification** dialog box, click **Create Owner Qualification**.

Step 7 In the **Create Owner Qualification** dialog box, enter the **First Chassis Id** and the **Number of Chassis**.

Step 8 Click **OK** to close the dialog box.

Step 9 Click **OK** to close the **Domain Qualification** dialog box.

Creating a Rack Qualification

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Server Pool Policy Qualifications**.

Step 4 Click the policy qualification that you want to modify.

Step 5 In the **Work** pane, on the **General** tab, click **Create Domain Qualification**.

Step 6 In the **Create Domain Qualification** dialog box, click **Create Rack Qualification**.

Step 7 In the **Create Rack Qualification** dialog box, enter the **First Slot Id** and the **Number of Slots**.

Step 8 Click **OK** to close the dialog box.

Step 9 Click **OK** to close the **Domain Qualification** dialog box.

Creating a Site Qualification

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Server Pool Policy Qualifications**.

Step 4 Click the policy qualification that you want to modify.

Step 5 In the **Work** pane, on the **General** tab, click **Create Domain Qualification**.

Step 6 In the **Create Domain Qualification** dialog box, click **Create Site Qualification**.

Step 7 In the **Create Site Qualification** dialog box, enter the **Name** and the **Regex**.

Step 8 Click **OK** to close the dialog box.

Step 9 Click **OK** to close the **Domain Qualification** dialog box.

Deleting Server Pool Policy Qualifications

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Server Pool Policy Qualifications**.

Step 4 Right-click the policy qualification that you want to delete and choose **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Deleting a Domain Qualification from a Policy Qualification

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Server Pool Policy Qualifications**.
Step 4 Click the policy qualification that you want to modify.
Step 5 In the **Work** pane, click the **General** tab.
Step 6 Expand **Domain Qualifications**.
Step 7 Right-click the qualification that you want to delete and choose **Delete**.
Step 8 Click **Save** to save the policy qualification.

Deleting a Chassis/Server Qualification from a Domain Qualification

Procedure

Step 1 On the menu bar, click **Servers**.
Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.
Step 3 Expand **Server Pool Policy Qualifications**.
Step 4 Click the policy qualification that you want to modify.
Step 5 In the **Work** pane, click the **General** tab.
Step 6 Expand **Domain Qualifications**.
Step 7 In the **Qualifications** table, expand the domain qualification that you want to modify.
Step 8 Expand **Chassis/Server Qualifications**.
Step 9 Right-click the qualification that you want to delete and choose **Delete**.
Step 10 Click **Save** to save the policy qualification.

Deleting a Server Qualification from a Chassis/Server Qualification

Procedure

Step 1 On the menu bar, click **Servers**.
Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Server Pool Policy Qualifications**.
Step 4 Click the policy qualification that you want to modify.
Step 5 In the **Work** pane, click the **General** tab.
Step 6 Expand **Domain Qualifications**.
Step 7 In the **Qualifications** table, expand the domain qualification that you want to modify.
Step 8 Expand **Chassis Qualifications**.
Step 9 Expand the chassis qualification that you want to modify.
Step 10 Right-click the server qualification that you want to delete and choose **Delete**.
Step 11 Click **Save** to save the policy qualification.

Deleting an Address Qualification from a Domain Qualification

Procedure

Step 1 On the menu bar, click **Servers**.
Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.
Step 3 Expand **Server Pool Policy Qualifications**.
Step 4 Click the policy qualification that you want to modify.
Step 5 In the **Work** pane, click the **General** tab.
Step 6 Expand **Domain Qualifications**.
Step 7 In the **Qualifications** table, expand the domain qualification that you want to modify.
Step 8 Expand **Address Qualifications**.
Step 9 Right-click the qualification that you want to delete and choose **Delete**.
Step 10 Click **Save** to save the policy qualification.

Deleting an Owner Qualification from a Domain Qualification

Procedure

Step 1 On the menu bar, click **Servers**.
Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Server Pool Policy Qualifications**.
Step 4 Click the policy qualification that you want to modify.
Step 5 In the **Work** pane, click the **General** tab.
Step 6 Expand **Domain Qualifications**.
Step 7 In the **Qualifications** table, expand the domain qualification that you want to modify.
Step 8 Expand **Owner Qualifications**.
Step 9 Right-click the qualification that you want to delete and choose **Delete**.
Step 10 Click **Save** to save the policy qualification.

Deleting a Rack Qualification from a Domain Qualification

Procedure

Step 1 On the menu bar, click **Servers**.
Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.
Step 3 Expand **Server Pool Policy Qualifications**.
Step 4 Click the policy qualification that you want to modify.
Step 5 In the **Work** pane, click the **General** tab.
Step 6 Expand **Domain Qualifications**.
Step 7 In the **Qualifications** table, expand the domain qualification that you want to modify.
Step 8 Expand **Rack Qualifications**.
Step 9 Right-click the qualification that you want to delete and choose **Delete**.
Step 10 Click **Save** to save the policy qualification.

Deleting a Site Qualification from a Domain Qualification

Procedure

Step 1 On the menu bar, click **Servers**.
Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Server Pool Policy Qualifications**.
Step 4 Click the policy qualification that you want to modify.
Step 5 In the **Work** pane, click the **General** tab.
Step 6 Expand **Domain Qualifications**.
Step 7 In the **Qualifications** table, expand the domain qualification that you want to modify.
Step 8 Expand **Site Qualifications**.
Step 9 Right-click the qualification that you want to delete and choose **Delete**.
Step 10 Click **Save** to save the policy qualification.

Deleting an Adapter Qualification from a Policy Qualification

Procedure

Step 1 On the menu bar, click **Servers**.
Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.
Step 3 Expand **Server Pool Policy Qualifications**.
Step 4 Click the policy qualification that you want to modify.
Step 5 In the **Work** pane, click the **General** tab.
Step 6 Expand **Adapter Qualifications**.
Step 7 Right-click the qualification that you want to delete and choose **Delete**.
Step 8 Click **Save** to save the policy qualification.

Deleting a Memory Qualification from a Policy Qualification

Procedure

Step 1 On the menu bar, click **Servers**.
Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Server Pool Policy Qualifications**.
Step 4 Click the policy qualification that you want to modify.
Step 5 In the **Work** pane, click the **General** tab.
Step 6 Right-click the qualification that you want to delete and choose **Delete**.
Step 7 Click **Save** to save the policy qualification.

Deleting a Processor Qualification from a Policy Qualification

Procedure

Step 1 On the menu bar, click **Servers**.
Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.
Step 3 Expand **Server Pool Policy Qualifications**.
Step 4 Click the policy qualification that you want to modify.
Step 5 In the **Work** pane, click the **General** tab.
Step 6 Right-click the qualification that you want to delete and choose **Delete**.
Step 7 Click **Save** to save the policy qualification.

Deleting a Storage Qualification from a Policy Qualification

Procedure

Step 1 On the menu bar, click **Servers**.
Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.
Step 3 Expand **Server Pool Policy Qualifications**.
Step 4 Click the policy qualification that you want to modify.
Step 5 In the **Work** pane, click the **General** tab.
Step 6 Right-click the qualification that you want to delete and choose **Delete**.
Step 7 Click **Save** to save the policy qualification.

Deleting a Server Qualification from a Policy Qualification

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Server Pool Policy Qualifications**.

Step 4 Click the policy qualification that you want to modify.

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

Step 6 Right-click the qualification that you want to delete and choose **Delete**.

Step 7 Click **Save** to save the policy qualification.

vNIC/vHBA Placement Policies

vNIC/vHBA placement policies are used to determine the following:

- How the virtual network interface connections (vCons) are mapped to the physical adapters on a server.
- What types of vNICs or vHBAs can be assigned to each vCon.

Each vNIC/vHBA placement policy contains four vCons that are virtual representations of the physical adapters. When a vNIC/vHBA placement policy is assigned to a service profile, and the service profile is associated with a server, the vCons in the vNIC/vHBA placement policy are assigned to the physical adapters and the vNICs and vHBAs are assigned to those vCons.

For blade or rack servers that contain one adapter, Cisco UCS assigns all vCons to that adapter. For servers that contain four adapters, Cisco UCS assigns vCon1 to Adapter1, vCon2 to Adapter2, vCon3 to Adapter3, and vCon4 to Adapter4.

For blade or rack servers that contain two or three adapters, Cisco UCS assigns the vCons based on the type of server and the selected virtual slot mapping scheme, which can be **Round Robin** or **Linear Ordered**. For details about the available mapping schemes, see vCon to Adapter Placement, on page 223.

After Cisco UCS assigns the vCons, it assigns the vNICs and vHBAs based on the **Selection Preference** for each vCon. This can be one of the following:

- **—**All configured vNICs and vHBAs can be assigned to the vCon, whether they are explicitly assigned to it, unassigned, or dynamic. This is the default.
- **—**vNICs and vHBAs must be explicitly assigned to the vCon. You can assign them explicitly through the service profile or the properties of the vNIC or vHBA.
- **—**Dynamic vNICs and vHBAs cannot be assigned to the vCon. The vCon can be used for all static vNICs and vHBAs, whether they are unassigned or explicitly assigned to it.

- —Unassigned vNICs and vHBAs cannot be assigned to the vCon. The vCon can be used for dynamic vNICs and vHBAs and for static vNICs and vHBAs that are explicitly assigned to it.

If you do not include a vNIC/vHBA placement policy in the service profile, Cisco UCS Central defaults to the **Round Robin** vCon mapping scheme and the **All** vNIC/vHBA selection preference, distributing the vNICs and vHBAs between the adapters based on the capabilities and relative capacities of each adapter.

Creating a vNIC/vHBA Placement Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Right-click **vNIC/vHBA Placement Policies** and choose **Create Placement Policy**.

Step 4 In the **Create Placement Policy** dialog box, enter the **Name** and other optional details.

Step 5 Click **OK**.

Deleting a vNIC/vHBA Placement Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Servers** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **vNIC/vHBA Placement Policies**.

Step 4 Right-click the policy that you want to delete and choose **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

vCon to Adapter Placement

Cisco UCS maps every vCon in a service profile to a physical adapter on the server. How that mapping occurs and how the vCons are assigned to a specific adapter in a server depends on the following:

- The type of server. N20-B6620-2 and N20-B6625-2 blade servers with two adapter cards use a different mapping scheme than other supported rack or blade servers.

- The number of adapters in the server.
- The setting of the virtual slot mapping scheme in the vNIC/vHBA placement policy, if applicable.

You must consider this placement when you configure the vNIC/vHBA selection preference to assign vNICs and vHBAs to vCons.

Note vCon to adapter placement is not dependent upon the PCIE slot number of the adapter. The adapter numbers used for the purpose of vCon placement are not the PCIE slot numbers of the adapters, but the ID assigned to them during server discovery.

vCon to Adapter Placement for N20-B6620-2 and N20-B6625-2 Blade Servers

In N20-B6620-2 and N20-B6625-2 blade servers, the two adapters are numbered left to right while vCons are numbered right to left. If one of these blade servers has a single adapter, Cisco UCS assigns all vCons to that adapter. If the server has two adapters, the vCon assignment depends upon the virtual slot mapping scheme:

- —Cisco UCS assigns vCon2 and vCon4 to Adapter1 and vCon1 and vCon3 to Adapter2. This is the default.
- —Cisco UCS assigns vCon3 and vCon4 to Adapter1 and vCon1 and vCon2 to Adapter2.

vCon to Adapter Placement for All Other Supported Servers

For all other servers supported by Cisco UCS besides the N20-B6620-2 and N20-B6625-2 blade servers, the vCon assignment depends on the number of adapters in the server and the virtual slot mapping scheme.

For blade or rack servers that contain one adapter, Cisco UCS assigns all vCons to that adapter. For servers that contain four adapters, Cisco UCS assigns vCon1 to Adapter1, vCon2 to Adapter2, vCon3 to Adapter3, and vCon4 to Adapter4.

For blade or rack servers that contain two or three adapters, Cisco UCS assigns the vCons based on the selected virtual slot mapping scheme: **Round Robin** or **Linear Ordered**.

Table 3: vCon to Adapter Placement Using the Round Robin Mapping Scheme

Number of Adapters	vCon1 Assignment	vCon2 Assignment	vCon3 Assignment	vCon4 Assignment
1	Adapter1	Adapter1	Adapter1	Adapter1
2	Adapter1	Adapter2	Adapter1	Adapter2
3	Adapter1	Adapter2	Adapter3	Adapter2
4	Adapter1	Adapter2	Adapter3	Adapter4

Round Robin is the default mapping scheme.

Table 4: vCon to Adapter Placement Using the Linear Ordered Mapping Scheme

Number of Adapters	vCon1 Assignment	vCon2 Assignment	vCon3 Assignment	vCon4 Assignment
1	Adapter1	Adapter1	Adapter1	Adapter1
2	Adapter1	Adapter1	Adapter2	Adapter2
3	Adapter1	Adapter2	Adapter3	Adapter3
4	Adapter1	Adapter2	Adapter3	Adapter4

vNIC/vHBA to vCon Assignment

Cisco UCS Central provides two options for assigning vNICs and vHBAs to vCons through the vNIC/vHBA placement policy: explicit assignment and implicit assignment.

Explicit Assignment of vNICs and vHBAs

With explicit assignment, you specify the vCon and, therefore, the adapter to which a vNIC or vHBA is assigned. Use this assignment option when you need to determine how the vNICs and vHBAs are distributed between the adapters on a server.

To configure a vCon and the associated vNICs and vHBAs for explicit assignment, do the following:

- Set the vCon configuration to any of the available options. You can configure the vCons through a vNIC/vHBA placement policy or in the service profile associated with the server. If a vCon is configured for **All**, you can still explicitly assign a vNIC or vHBA to that vCon.
- Assign the vNICs and vHBAs to a vCon. You can make this assignment through the virtual host interface placement properties of the vNIC or vHBA or in the service profile associated with the server.

If you attempt to assign a vNIC or vHBA to a vCon that is not configured for that type of vNIC or vHBA, Cisco UCS Central displays a message advising you of the configuration error.

During service profile association, Cisco UCS Central validates the configured placement of the vNICs and vHBAs against the number and capabilities of the physical adapters in the server before assigning the vNICs and vHBAs according to the configuration in the policy. Load distribution is based upon the explicit assignments to the vCons and adapters configured in this policy.

If the adapters do not support the assignment of one or more vNICs or vHBAs, Cisco UCS Central raises a fault against the service profile.

Implicit Assignment of vNICs and vHBAs

With implicit assignment, Cisco UCS Central determines the vCon and, therefore, the adapter to which a vNIC or vHBA is assigned according to the capability of the adapters and their relative capacity. Use this assignment option if the adapter to which a vNIC or vHBA is assigned is not important to your system configuration.

To configure a vCon for implicit assignment, do the following:

- Set the vCon configuration to **All**, **Exclude Dynamic**, or **Exclude Unassigned**. You can configure the vCons through a vNIC/vHBA placement policy or in the service profile associated with the server.
- Do not set the vCon configuration to **Assigned Only**. Implicit assignment cannot be performed with this setting.
- Do not assign any vNICs or vHBAs to a vCon.

During service profile association, Cisco UCS Central verifies the number and capabilities of the physical adapters in the server and assigns the vNICs and vHBAs accordingly. Load distribution is based upon the capabilities of the adapters, and placement of the vNICs and vHBAs is performed according to the actual order determined by the system. For example, if one adapter can accommodate more vNICs than another, that adapter is assigned more vNICs.

If the adapters cannot support the number of vNICs and vHBAs configured for that server, Cisco UCS Central raises a fault against the service profile.

Implicit Assignment of vNICs in a Dual Adapter Environment

When you use implicit vNIC assignment for a dual slot server with an adapter card in each slot, Cisco UCS Central typically assigns the vNICs/vHBAs as follows:

- If the server has the same adapter in both slots, Cisco UCS Central assigns half the vNICs and half the vHBAs to each adapter.
- If the server has one non-VIC adapter and one VIC adapter, Cisco UCS Central assigns two vNICs and two vHBAs to the non-VIC adapter and the remaining vNICs and vHBAs to the VIC adapter.
- If the server has two different VIC adapters, Cisco UCS Central assigns the vNICs and vHBAs proportionally, based on the relative capabilities of the two adapters.

The following examples show how Cisco UCS Central would typically assign the vNICs and vHBAs with different combinations of supported adapter cards:

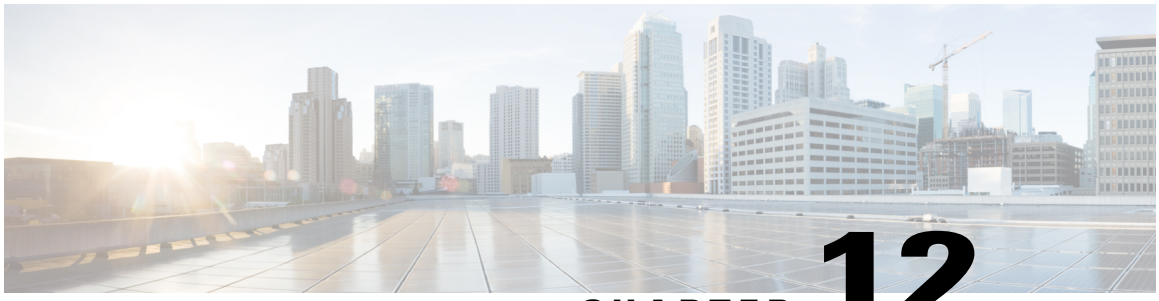
- If you want to configure four vNICs and the server contains two Cisco UCS M51KR-B Broadcom BCM57711 adapters (with two vNICs each), Cisco UCS Central assigns two vNICs to each adapter.
- If you want to configure 50 vNICs and the server contains a Cisco UCS CNA M72KR-E adapter (2 vNICs) and a Cisco UCS M81KR Virtual Interface Card adapter (128 vNICs), Cisco UCS Central assigns two vNICs to the Cisco UCS CNA M72KR-E adapter and 48 vNICs to the Cisco UCS M81KR Virtual Interface Card adapter.
- If you want to configure 150 vNICs and the server contains a Cisco UCS M81KR Virtual Interface Card adapter (128 vNICs) and a Cisco UCS VIC-1240 Virtual Interface Card adapter (256 vNICs), Cisco UCS Central assigns 50 vNICs to the Cisco UCS M81KR Virtual Interface Card adapter and 100 vNICs to the Cisco UCS VIC-1240 Virtual Interface Card adapter.

Note Exceptions to this implicit assignment occur if you configure the vNICs for fabric failover and if you configure dynamic vNICs for the server.

For a configuration that includes vNIC fabric failover where one adapter does not support vNIC failover, Cisco UCS Central implicitly assigns all vNICs that have fabric failover enabled to the adapter that supports them. If the configuration includes only vNICs that are configured for fabric failover, no vNICs are implicitly assigned to the adapter that does not support them. If some vNICs are configured for fabric failover and some

are not, Cisco UCS Central assigns all failover vNICs to the adapter that supports them and a minimum of one nonfailover vNIC to the adapter that does not support them, according to the ratio above.

For a configuration that includes dynamic vNICs, the same implicit assignment would occur. Cisco UCS Central assigns all dynamic vNICs to the adapter that supports them. However, with a combination of dynamic vNICs and static vNICs, at least one static vNIC is assigned to the adapter that does not support dynamic vNICs.



CHAPTER 12

Network Policies

This chapter includes the following sections:

- vNIC Template, page 229
- Default vNIC Behavior Policy, page 230
- LAN and SAN Connectivity Policies, page 231
- Network Control Policy, page 235
- Dynamic vNIC Connection Policy, page 237
- Quality of Service Policy, page 238

vNIC Template

This policy defines how a vNIC on a server connects to the LAN. This policy is also referred to as a vNIC LAN connectivity policy.

Cisco UCS Central does not automatically create a VM-FEX port profile with the correct settings when you create a vNIC template. If you want to create a VM-FEX port profile, you must configure the target of the vNIC template as a VM.

You need to include this policy in a service profile for it to take effect.

Note If your server has two Emulex or QLogic NICs (Cisco UCS CNA M71KR-E or Cisco UCS CNA M71KR-Q), you must configure vNIC policies for both adapters in your service profile to get a user-defined MAC address for both NICs. If you do not configure policies for both NICs, Windows still detects both of them in the PCI bus. Then because the second eth is not part of your service profile, Windows assigns it a hardware MAC address. If you then move the service profile to a different server, Windows sees additional NICs because one NIC did not have a user-defined MAC address.

Creating a vNIC Template

Procedure

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

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Right-click **vNIC Templates** and choose **Create vNIC Template**.

Step 4 In the **Create vNIC Template** dialog box, enter the **Name** and optional description.

Step 5 Choose the **Fabric ID** and **Template Type**, enter the **MTU**, and choose a **Type**.
You can also create a MAC pool from this area.

Step 6 In the **VLANs** table, select the VLANs that you want to use.

Step 7 In the **Policies** area, choose a **MAC Pool**, **QoS Policy**, **Network Control Policy**, and **Stats Threshold Policy** from the drop-down lists, and enter the **Pin Group Name**.
You can also create a MAC pool, a QoS policy, a network control policy, and a threshold policy from this area.

Step 8 Click **OK**.

Deleting a vNIC Template

Procedure

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

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **vNIC Templates**.

Step 4 Right-click the vNIC template that you want to delete and choose **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Default vNIC Behavior Policy

Default vNIC behavior policy allows you to configure how vNICs are created for a service profile. You can choose to create vNICS manually, or you can allow them to be created automatically

You can configure the default vNIC behavior policy to define how vNICs are created. This can be one of the following:

- **None—**Cisco UCS Central does not create default vNICs for a service profile. All vNICs must be explicitly created.
- **HW Inherit—**If a service profile requires vNICs and none have been explicitly defined, Cisco UCS Central creates the required vNICs based on the adapter installed in the server associated with the service profile.

Note If you do not specify a default behavior policy for vNICs, **HW Inherit** is used by default.

Configuring Default vNIC Behavior

If you do not specify a default behavior policy for vNICs, **HWInherit** is used by default.

Procedure

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

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
You can only configure the default vNIC behavior policy in the root organization. You cannot configure the default vNIC behavior policy in a sub-organization.

Step 3 Right-click **Default vNIC Behavior** and choose **Properties**.

Step 4 In the **Properties (Default vNIC Behavior)** dialog box, choose the **Action** and the optional **vNIC Template**.

Step 5 Click **OK**.

LAN and SAN Connectivity Policies

Connectivity policies determine the connections and the network communication resources between the server and the LAN or SAN on the network. These policies use pools to assign MAC addresses, WWNs, and WWPNs to servers and to identify the vNICs and vHBAs that the servers use to communicate with the network.

Note We do not recommend that you use static IDs in connectivity policies, because these policies are included in service profiles and service profile templates and can be used to configure multiple servers.

Privileges Required for LAN and SAN Connectivity Policies

Connectivity policies enable users without network or storage privileges to create and modify service profiles and service profile templates with network and storage connections. However, users must have the appropriate network and storage privileges to create connectivity policies.

Privileges Required to Create Connectivity Policies

Connectivity policies require the same privileges as other network and storage configurations. For example, you must have at least one of the following privileges to create connectivity policies:

- admin—Can create LAN and SAN connectivity policies
- ls-server—Can create LAN and SAN connectivity policies
- ls-network—Can create LAN connectivity policies
- ls-storage—Can create SAN connectivity policies

Privileges Required to Add Connectivity Policies to Service Profiles

After the connectivity policies have been created, a user with ls-compute privileges can include them in a service profile or service profile template. However, a user with only ls-compute privileges cannot create connectivity policies.

Creating a LAN Connectivity Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Right-click **LAN Connectivity Policies** and choose **Create LAN Connectivity Policy**.

Step 4 In the **Create LAN Connectivity Policy** dialog box, enter the **Name** and optional description.

Step 5 Click **Create vNIC** in the **vNICs** area to add vNICs to the LAN connectivity policy.
The vNICs you create will be added to the **vNIC** table.

Step 6 Click **Create iSCSI vNIC** in the **iSCSI vNICs** area to add iSCSI vNICs to the LAN connectivity policy.
The iSCSI vNICs you create will be added to the **iSCSI vNIC** table.

Step 7 Click **OK**.

Creating a vNIC for a LAN Connectivity Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **LAN Connectivity Policies**.

Step 4 Select the LAN connectivity policy for which you want to create a vNIC.

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

Step 6 In the **vNICs** area, click **Create vNIC**.

Step 7 In the **Create vNIC** dialog box, enter the name, select a **MAC Address Assignment**, and check the **Use vNIC Template** check box if you want to use an existing vNIC template.
You can also create a MAC pool from this area.

Step 8 In the **Details** area, choose the **Fabric ID**, select the VLANs you want to use, and enter the **MTU**.

Step 9 In the **Pin Group** area, choose a **Pin Group Name**.

Step 10 In the **Operational Parameters** area, choose a **Stats Threshold Policy**.
You can also create a threshold policy from this area.

Step 11 In the **Adapter Performance Profile** area, choose an **Adapter Policy**, **QoS Policy**, and a **Network Control Policy**.
You can also create an ethernet adapter policy, a QoS policy, and a network control policy from this area.

Step 12 Click **OK**.

Creating an iSCSI vNIC for a LAN Connectivity Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **LAN Connectivity Policies**.

Step 4 Select the LAN connectivity policy for which you want to create an iSCSI vNIC.

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

Step 6 In the **iSCSI vNICs** area, click **Create iSCSI vNIC**.

Step 7 In the **Create iSCSI vNIC** dialog box, enter the name, choose the **Overlay vNIC**, **iSCSI Adapter Policy**, and **VLAN** from the drop-down lists, and select a **MAC Address Assignment**.
You can also create an iSCSI adapter policy and a MAC pool from this dialog box.

Step 8 Click **OK**.

Deleting a LAN Connectivity Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **LAN Connectivity Policies**.

Step 4 Right-click the policy that you want to delete and choose **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Deleting a vNIC from a LAN Connectivity Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **LAN Connectivity Policies**.

Step 4 Select the policy for which you want to delete the vNIC.

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

Step 6 In the **vNICs** table, click the vNIC you want to delete.

Step 7 On the **vNICs** table icon bar, click **Delete**.

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

Deleting an iSCSI vNIC from a LAN Connectivity Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **LAN Connectivity Policies**.

Step 4 Select the policy for which you want to delete the iSCSI vNIC.

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

Step 6 In the **iSCSI vNICs** table, click the vNIC you want to delete.

Step 7 On the **iSCSI vNICs** table icon bar, click **Delete**.

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

Network Control Policy

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

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

Action on Uplink Fail

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

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

MAC Registration Mode

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

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

Creating a Network Control Policy

MAC address-based port security for Emulex converged Network Adapters (N20-AE0102) is not supported. When MAC address-based port security is enabled, the fabric interconnect restricts traffic to packets that contain the MAC address that it first learns. This is either the source MAC address used in the FCoE Initialization Protocol packet, or the MAC address in an ethernet packet, whichever is sent first by the adaptor. This configuration can result in either FCoE or Ethernet packets being dropped.

Procedure

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

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Right-click **Network Control Policies** and choose **Create Network Control Policy**.

Step 4 In the **Create Network Control Policy** dialog box, enter the **Name** and optional description.

Step 5 Choose the **CDP**, **MAC Register Mode**, and **Action on Uplink Fail**.

Step 6 In the **MAC Security** area, choose whether to allow or deny forged MAC addresses.

Step 7 Click **OK**.

Deleting a Network Control Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Network Control Policies**.

Step 4 Right-click the policy that you want to delete and choose **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Dynamic vNIC Connection Policy

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

Ethernet Adapter Policy

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

Server Migration

Note If you migrate a server that is configured with dynamic vNICs or another migration tool, the dynamic interface used by the vNICs fails and Cisco UCS Central notifies you of that failure.

When the server comes back up, Cisco UCS Central assigns new dynamic vNICs to the server. If you are monitoring traffic on the dynamic vNIC, you must reconfigure the monitoring source.

Creating a Dynamic vNIC Connections Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Right-click **Dynamic vNIC Connection Policies** and choose **Create Dynamic vNIC Connection Policy**.

Step 4 In the **Create Dynamic vNIC Connection Policy** dialog box, enter the **Name**, optional description, **Naming Prefix**, and **Number of Dynamic vNICs**.

Step 5 Choose the **Adapter Policy** from the drop-down list, and set the **Protection** level.

Step 6 Click **OK**.

Deleting a Dynamic vNIC Connections Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Dynamic vNIC Connections Policies**.

Step 4 Right-click the policy that you want to delete and choose **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Quality of Service Policy

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

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

Creating a QoS Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Right-click **QoS Policies** and choose **Create QoS Policy**.

Step 4 In the **Create QoS Policy** dialog box, enter the **Name** and optional description.

Step 5 In the **Egress** area, choose a **Priority**, enter the **Burst(Bytes)** and **Rate(Kbps)**, and choose the **Host Control**.

Step 6 Click **OK**.

What to Do Next

Include the QoS policy in a vNIC or vHBA template.

Deleting a QoS Policy

Procedure

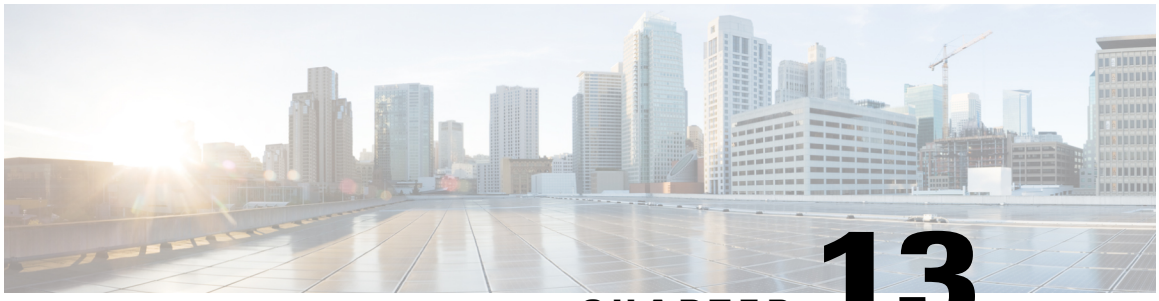
Step 1 On the menu bar, click **Network**.

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **QoS Policies**.

Step 4 Right-click the policy that you want to delete and choose **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.



CHAPTER 13

Storage Policies

This chapter includes the following sections:

- vHBA Template, page 241
- Default vHBA Behavior Policy, page 242
- Ethernet and Fibre Channel Adapter Policies, page 243
- LAN and SAN Connectivity Policies, page 245

vHBA Template

This template is a policy that defines how a vHBA on a server connects to the SAN. It is also referred to as a vHBA SAN connectivity template.

You must include this policy in a service profile for it to take effect.

Creating a vHBA Template

Procedure

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

Step 2 In the **Navigation** Pane, expand **Storage** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Right-click **vHBA Templates** and choose **Create vHBA Template**.

Step 4 In the **Create vHBA Template** dialog box, enter the **Name** and optional description.

Step 5 Choose the **Fabric ID**, **Select VSAN**, and **Template Type**.

Step 6 Choose the **WWPN Pool**, **QoS Policy**, and **Stats Threshold Policy** from the drop-down lists.
You can also create a WWPN pool, QoS policy, and threshold policy from this dialog box.

Step 7 Click **OK**.

Deleting a vHBA Template

Procedure

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

Step 2 In the **Navigation** Pane, expand **Storage** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **vHBA Templates**.

Step 4 Right-click the vHBA Template that you want to delete and choose **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Default vHBA Behavior Policy

Default vHBA behavior policy allow you to configure how vHBAs are created for a service profile. You can choose to create vHBAs manually, or you can allow them to be created automatically.

You can configure the default vHBA behavior policy to define how vHBAs are created. This can be one of the following:

- **None—**Cisco UCS Central does not create default vHBAs for a service profile. All vHBAs must be explicitly created.
- **HW Inherit—**If a service profile requires vHBAs and none have been explicitly defined, Cisco UCS Central creates the required vHBAs based on the adapter installed in the server associated with the service profile.

Note If you do not specify a default behavior policy for vHBAs, **none** is used by default.

Configuring Default vHBA Behavior

If you do not specify a default behavior policy for vHBAs, **none** is used by default.

Procedure

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

Step 2 In the **Navigation** Pane, expand **Storage** > **Policies** > **root**.

You can only configure the default vHBA behavior policy in the root organization. You cannot configure the default vHBA behavior policy in a sub-organization.

Step 3 In the **Navigation** Pane, expand **Storage** > **Policies** > **root**.

Step 4 Right-click **Default vHBA Behavior** and choose **Properties**.

Step 5 In the **Properties (Default vHBA Behavior)** dialog box, choose the **Action** and the optional **vHBA Template**.

Step 6 Click **OK**.

Ethernet and Fibre Channel Adapter Policies

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

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

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

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

Operating System Specific Adapter Policies

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

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

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

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

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

Completion Queues = 1 + 8 = 9
Interrupt Count = (9 + 2) rounded up to the nearest power of 2 = 16

Creating a Fibre Channel Adapter Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Storage** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Right-click **Fibre Channel Adapter Policies** and choose **Create Fibre Channel Adapter Policy**.

Step 4 In the **Create Fibre Channel Adapter Policy** dialog box, enter the **Name** and optional description.

Step 5 In the **Resources** area, enter the **Ring Size** for the **Transmit Queues**, **Receive Queues**, and **SCSI I/O Queues**.

Step 6 In the **Options** area, choose the **FCP Error Recovery** and **Interrupt Mode**, and enter the **Flogi Retries**, **Flogi Timeout (ms)**, **Plogi Retries**, **Plogi Timeout (ms)**, **Port Down Timeout (ms)**, **Port Down IO Retry**, **Link Down Timeout (ms)**, **IO Throttle Count**, and **Max LUNs Per Target**.

Step 7 Click **OK**.

Deleting a Fibre Channel Adapter Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Storage** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Fibre Channel Adapter Policies**.

Step 4 Right-click the policy that you want to delete and choose **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

LAN and SAN Connectivity Policies

Connectivity policies determine the connections and the network communication resources between the server and the LAN or SAN on the network. These policies use pools to assign MAC addresses, WWNs, and WWPNs to servers and to identify the vNICs and vHBAs that the servers use to communicate with the network.

Note We do not recommend that you use static IDs in connectivity policies, because these policies are included in service profiles and service profile templates and can be used to configure multiple servers.

Privileges Required for LAN and SAN Connectivity Policies

Connectivity policies enable users without network or storage privileges to create and modify service profiles and service profile templates with network and storage connections. However, users must have the appropriate network and storage privileges to create connectivity policies.

Privileges Required to Create Connectivity Policies

Connectivity policies require the same privileges as other network and storage configurations. For example, you must have at least one of the following privileges to create connectivity policies:

- admin—Can create LAN and SAN connectivity policies
- ls-server—Can create LAN and SAN connectivity policies
- ls-network—Can create LAN connectivity policies
- ls-storage—Can create SAN connectivity policies

Privileges Required to Add Connectivity Policies to Service Profiles

After the connectivity policies have been created, a user with ls-compute privileges can include them in a service profile or service profile template. However, a user with only ls-compute privileges cannot create connectivity policies.

Creating a SAN Connectivity Policy

Procedure

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

Step 2 In the **Navigation** Pane, expand **Storage** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Right-click **SAN Connectivity Policies** and choose **Create SAN Connectivity Policy**.

Step 4 In the **Create SAN Connectivity Policy** dialog box, enter the **Name** and optional description.

Step 5 In the **WWNN Assignment** area, choose the **Global Pool** or **OUI**.

Step 6 In the **vHBA** table, click **Create vHBA** to add vHBAs to the SAN Connectivity Policy.

Step 7 Click **OK**.

Deleting a SAN Connectivity Policy

Procedure

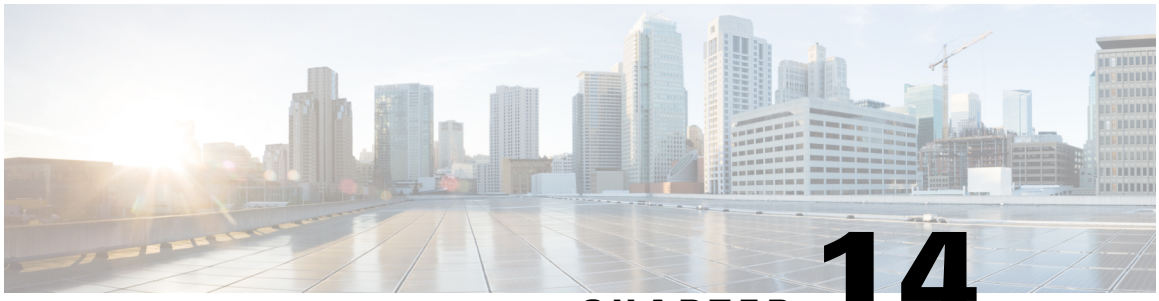
Step 1 On the menu bar, click **Storage**.

Step 2 In the **Navigation** Pane, expand **Storage** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **SAN Connectivity Policies**.

Step 4 Right-click the policy that you want to delete and choose **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.



CHAPTER 14

Statistics Management

This chapter includes the following sections:

- Statistics Management, page 247
- Standard Reports, page 250
- Custom Reports, page 254

Statistics Management

Cisco UCS Central enables you to generate standard and customized reports from the **Statistics** tab. You can generate reports on the following data in the registered Cisco UCS domains:

- Cooling
- Network
- Power
- Temperature

Important You must be logged in as an admin or as a user with statistics privilege to create, modify or delete a report. Other users can only run reports and view available data.

When you generate a report, you can specify the option to view the report either in the format of a table or a chart. Using the display options, you can select top or bottom domains for a specific report type. You can also use overlay to overlay the data for a report type. The following are the two report options:

- **Standard Reports**: Predefined reports on Peak Fan Speed, Receive Traffic(Rx), Transmit Traffic (Tx), Average Power, and Peak Temperature. You can run any of these predefined reports any time to view reports. You can also modify the predefined configurations, but cannot create any new standard report.
- **Custom Reports**: Option to create customized reports from any of the available report options. Based on your requirements, you can create either create individual reports in the **Ungrouped Reports** or create **Report Group**s and then create reports under the groups or sub-groups. You can create, edit or delete the custom report groups at anytime.

Statistics Data Collection in Cisco UCS Central

Cisco UCS Central collects and aggregates statistics data on **Network**, **Temperature**, **Cooling** and **Power** from the registered Cisco UCS domains. During Cisco UCS Central installation, you must specify a default location to store the statistics data. You can store the statistics data in the internal PostgreSQL database called "ucscentral-stats-db" or in an external database such as Oracle 11g, MSSQL, or Postgre SQL. If you have chosen internal storage as the default location during installation, the statistics data is stored only for a maximum of two weeks. If you want to retain the collected data for more than two weeks, it is recommended that you set up an external database, see External Database for Statistics, on page 248.

The collected data is aggregated based on daily, hourly, weekly and real time records and stored in tables. You can run SQL query in this database to retrieve data specific to each of the report components, see Retrieving Data from the External Database. Cisco UCS Central database is the default database to store the data.

You can set up statistics collection interval using Cisco UCS Central CLI, to collect information from the registered Cisco UCS domains at a specified interval. When a new Cisco UCS domain is registered in Cisco UCS Central, Cisco UCS Central subscribes the new domain to the statistics collection interval you have specified. If you reconfigure the collection interval, the data is updated in the registered domains. The registered Cisco UCS domains send statistics to Cisco UCS Central based on the specified collection interval.

Statistics collection interval can be one of the following:

- 15 minutes (default)
- 30 minutes
- never—disables statistics collection

Important You can specify the statistics collection interval only in the Cisco UCS Central CLI. You cannot set it from the Cisco UCS Central GUI. You can view the statistics reports only in the Cisco UCS Central GUI and not in the Cisco UCS Central CLI.

External Database for Statistics

You can set up an external database to retain the collected data for more than two weeks or to collect statistics data from more than 5 registered Cisco UCS domains. The following are the two supported databases that you can use as external database from Cisco UCS Central:

- Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - 64-bit Production or higher
- PostgreSQL Server 9.1.8 64-bit or higher
- Microsoft SQL Server 2012 (SP1) - 11.0.3000.0 (X64) or higher
- Microsoft SQL Server 2008 R2 10.50.1600.1 (X64) SP1 or higher

Make sure you have the following information to access and setup either of these databases as your external database:

- Database server host name
- Database name

- Username
- Password
- Port number

Note You must open the firewall ports in the database server so that Cisco UCS Central can access the configured external database.

Setting up an External Database

You can set up the external database either during initial Cisco UCS Central set up or at anytime you have a requirement to set up an external database for statistics collection:

- **Setting up external database with initial setup**: When you are doing the initial set up for Cisco UCS Central, you are prompted to enable statistics collection. If you choose **Yes**, you are prompted to enter information on the external database. If you choose **No**, the collection of statistics data from registered Cisco UCS domains is disabled.
- **Anytime**: You can use the Cisco UCS Central CLI to connect to the external database and set up statistics collection for registered Cisco UCS domains. For information on setting up an Oracle database, see Connecting to an External Oracle Database. For information on setting up an PostgreSQL database, see Connecting to an External PostgreSQL Database.

The external database stores statistical data on network traffic, temperature, cooling and power from the registered Cisco UCS domains. You can run queries on the external database to retrieve statistics data on network, temperature, cooling and power. For information on running queries on the database, see Retrieving Data from the External Database.

Note When you set up an external database to store the statistical data, you must determine the time interval to purge old records from the database. You are responsible for maintaining the external database.

Guidelines for Configuring an External Database

When you configure the database for statistics collection, make sure to restart the Cisco UCS Central services. You must restart the services in the following scenarios:

- After upgrading to the latest version of Cisco UCS Central using the ISO image

  Earlier versions of Cisco UCS Central did not have the capability for statistics collection. After the upgrade process is complete, you can use the Cisco UCS Central CLI to set up an external database for statistics data collection.
- You set up an external database for statistics collection after installing Cisco UCS Central. The external database can be either an Oracle database or a PostgreSQL database.
- After switching from an Oracle database to a PostgreSQL database or switching from a PostgreSQL database to an Oracle database.

Backing up and Restoring Cisco UCS Central Statistics Database

The Cisco UCS Central database is not backed up during a full state backup. If you have set up an external database to store statistical data, then you must follow standard database backup and restore procedures. However, prior to restoring an external database, you must stop the Cisco UCS Central service. To stop this service, you must login to the Cisco UCS Central CLI, and run the **pmon stop** command in the **local-mgmt** command mode. After the database is restored, start the Cisco UCS Central service by running the **pmon start** command in the Cisco UCS Central CLI.

Troubleshooting Faults with the External Database

When Cisco UCS Central fails to connect to an external database, a fault is raised. You can view the fault details in the Cisco UCS Central CLI using the **show fault** command or in the Cisco UCS Central GUI, **Fault** panel.. When the problem is resolved ,Cisco UCS Central automatically retries to connect to the external database. If the connection is established, the fault is cleared from the Cisco UCS Central CLI.

Standard Reports

Standard Reports are pre-defined reports in Cisco UCS Central. You can use these standard reports to view top and bottom 10 transmitted (Tx) or received (Rx) data aggregated at the domain, chassis or server level. While you cannot create any additional standard reports in Cisco UCS Central, you can modify the parameters for these standard reports.

Important You must be logged in as an administrator user or as a user with statistics privilege to modify the parameters of the standard reports. Other users can only run the currently available reports, and cannot edit any of the report parameters.

The following table describes a standard network report in Cisco UCS Central.

Name	Description
Default View	The view of the report. It can be one of the following: • **Chart** • **Table** By default, the **Chart** option is selected.
Display	The nature of the data to be included in the report. It can be one of the following: • **Top Tx or Rx** • **Bottom Tx or Rx** By default, the **Top Tx or Rx** option is selected.

Name	Description
For	The endpoints for the report. It can be one of the following: • **FI Ethernet Ports** • **FI FC Ports** • **HBAs** • **NICs** By default, **Fi Ethernet Ports** is selected.
Duration	The specified time period for which the report is run. It can be one of the following: • **Customized date and time range** • **Last 3 hours** • **Last 6 hours** • **Last 12 hours** • **Last 24 hours** • **Last 48 hours** By default, **Last 12 hours** is selected.
Overlay	To include overlay information in the report.

Name	Description
Context	The context for the report. It can be one of the following: • **Domains** • **Chassis** • **Servers** You can specify a context for the report, only when you have specified the endpoint as **HBAs** or **NICs**. By specifying a context, you can view server NIC or HBA traffic at the domain, chassis or server level. For the other endpoints, such as **FI Ethernet Ports** or **FI FC Ports**, you cannot change the default selection of **Domains** for the context. When you specify **Domains** as the context, the chart renders the report at the domain level, which can be further drilled down to the chassis level of a selected domain. From a specific chassis level, you can further drill down to a server. When you specify **Chassis** as the context, the data is rendered at the chassis level, which can be further drilled down to the server level. When you specify **Servers** as the context, the data is rendered at the server level, and you cannot drill down further.

If you run a standard network report with the default selections, the generated report will show top and bottom transmitted (Tx) or received (Rx) data for Fi Ethernet Ports in Cisco UCS domains, for the last 12 hours, in a chart format.

Related Topics

- Generating a Network Report, on page 252

Generating a Network Report

Before You Begin

You must be logged in as an administrative user or as a user with statistics privilege to modify the parameters of the standard reports. Other users can only run the currently available reports, and cannot edit any of the report parameters.

Procedure

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

Step 2 In the navigation pane, expand **Standard Reports**.

Step 3 Expand **Network** and click one of the following options to generate the type of network report that you want to generate.

- **Receive Traffic (Rx)**
- **Transmit Traffic (Tx)**

Step 4 (Optional) In the work pane, click **Configure** if you want to modify the parameters for the report.

Step 5 In the work pane, click **Run/Refresh**.
The work pane displays the report. If you selected the chart type display, you can mouse over the chart to view total transmitted traffic (Tx) or total received traffic (Rx) bytes. If you selected **NICs** or **HBAs** as the endpoint and Domains or Chassis as the context for the report, then you can drill down by clicking on the bars of the report.

Generating a Peak Fan Speed Report

You can a generate peak fan speed report on the following end points, **Chassis Fans**, **Fabric Interconnect Fans** or **Rack Unit Fans**. You can overlay **Average Fan Speed** in the peak fan speed report. The **Context** is **Domains**.

Before You Begin

You must be logged in as an administrator user or as a user with statistics privilege to create a report, or modify the parameters of a report. Users, other than administrators, or users without the statistics privilege can only run the currently available reports.

Procedure

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

Step 2 In the navigation pane, expand **Standard Reports** > **Cooling** and click **Peak Fan Speed**.

Step 3 If you want to run the report with existing options, click **Run Report To Load Data**.

Step 4 If you want to modify existing configuration, click **Configure**. In the **Configure Peak Fan Speed** dialog box, modify the options and click **Save & Run**.

Generating a Peak Temperature Report

You can a generate reports on the **Server Inlet Temperature** in the registered Cisco UCS **Domains**. You can choose to overlay **Average Temperature** in the peak temperature report.

Before You Begin

You must be logged in as an administrator user or as a user with statistics privilege to create a report, or modify the parameters of a report. Users, other than administrators, or users without the statistics privilege can only run the currently available reports.

Procedure

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

Step 2 In the navigation pane, expand **Standard Reports** > **Temperature** and click **Peak Temperature**.

Step 3 If you want to run the report with existing options, click **Run Report To Load Data**.

Step 4 If you want to modify existing configuration, click **Configure**. In the **Configure Peak Temperature** dialog box, modify the options and click **Save & Run**.

Generating an Average Power Report

You can a generate average power report on the following end points,**Chassis (Input Power - AC)**, **Blade (Consumed Power - DC)** or **Rack (Input Power - AC)**. You can overlay **Peak Power** in the average power report. The **Context** is **Domains**.

Before You Begin

You must be logged in as an administrator user or as a user with statistics privilege to create a report, or modify the parameters of a report. Users, other than administrators, or users without the statistics privilege can only run the currently available reports.

Procedure

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

Step 2 In the navigation pane, expand **Standard Reports** > **Power** and click **Average Power**.

Step 3 If you want to run the report with existing options, click **Run Report To Load Data**.

Step 4 If you want to modify existing configuration, click **Configure**. In the **Configure Average Power** dialog box, modify the options and click **Save & Run**.

Custom Reports

Custom reports are reports that you can create in Cisco UCS Central. To create these reports, you must be logged in as an administrator or as a user with stats-privilege. If you are not an administrator, or a user without the stats-privilege, you cannot access the **Statistics** tab in the UCS Central GUI. You can create, modify and delete a custom report in UCS Central.

You an create custom reports based on your requirements either in **Report Groups** or in **Ungrouped Reports**. A report group functions as a container for grouping custom reports. Custom reports have the same report type options as the standard reports, such as **Network**, **Cooling**, **Power** and **Temperature**.

Creating a Custom Report Group

Custom report groups in Cisco UCS Central act like folders within which you can create custom reports. You can also create a report group within a report group.

Before You Begin

You must be logged in as an administrator user or as a user with statistics privileges.

Procedure

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

Step 2 In the navigation pane, right-click **Custom Reports** and select **Create Group**.

Step 3 (Optional) In the work pane, click **Create Group**.

Step 4 In the **Create Group** dialog box, specify the **Name** and **Description** for the report group.

Step 5 Click **OK**.
The report group is displayed in the navigation pane under **Custom Reports**.

What to Do Next

You can create custom reports within this report group.

Deleting a Report Group

Important When you delete a report group from the Cisco UCS Central GUI, all reports you created within this group are also deleted.

Before You Begin

- You must be logged in as an administrator user or as a user with statistics privileges to perform this task.
- Evaluate the list of custom reports created within the report group.

Procedure

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

Step 2 In the navigation pane, expand **Custom Reports**.
The list of report groups you created are displayed.

Step 3 Right-click on the report group you want to delete, and click **Delete**.

A dialog box appears prompting you to confirm the deletion of the report group.

Step 4 Click **Yes**.
The report group, along with the custom reports within it, is deleted from the Cisco UCS Central GUI.

Creating a Custom Report

You can create a customized report to view specific statistics data of the registered UCS domains. In Cisco UCS Central, you can create a custom report group and create a report within it.

Before You Begin

You must be logged in as an admin user or a user with stats-privilege to create a custom report.

Procedure

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

Step 2 In the navigation pane, expand **Custom Reports**.

Step 3 Right-click on **Ungrouped Reports** and select **Create Report**.
To create a report within a report group, right-click the desired report group in the navigation pane and select **Create Report**.

For information on creating a report group, see Creating a Custom Report Group, on page 255.

Step 4 In the **Create Report** dialog box, specify the **Name** for the report.

Step 5 (Optional) Specify a description for the report.

Step 6 In the **Properties** area, specify the required information.
Based on the report type you select, the required data in the **Properties** area changes. Make sure to specify all required information for the type of report you want to generate.

Step 7 Click **OK**.
The report is listed under **Custom Reports** in the navigation pane and in the work area.

What to Do Next

You can run the report to view the data.

Running a Custom Report

Before You Begin

You must be logged in as an administrator user or as a user with statistics privilege to create a report, or modify the parameters of a report. Users, other than administrators, or users without the statistics privilege can only run the currently available reports.

Procedure

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

Step 2 In the navigation pane, expand **Custom Reports**.

Step 3 (Optional) If the report you want to run is in a report group, then expand the report group name.
If the report you want to run is not in a report group, then expand **Ungrouped Reports**.

Step 4 Select the name of the report, and click **Run/Refresh** in the work pane.

Step 5 (Optional) You can toggle between chart and table display by clicking the respective option on the report.
In the Table view of the report, you may see values such as 0 and -1. The 0 value indicates that the data displayed in the report is actual data collected from a registered UCS domain. The -1 value indicates that Cisco UCS Central did not receive statistical information from the UCS domain for the specified time period or for the specified endpoint. This occurs when the connection to the UCS domain was lost and statistical data for the domain was not collected till the connection was restored. In the Chart view, this is indicated by broken lines on the report.

Deleting a Custom Report

Before You Begin

You must be logged in as an administrator user or as a user with statistics privileges to perform this task.

Procedure

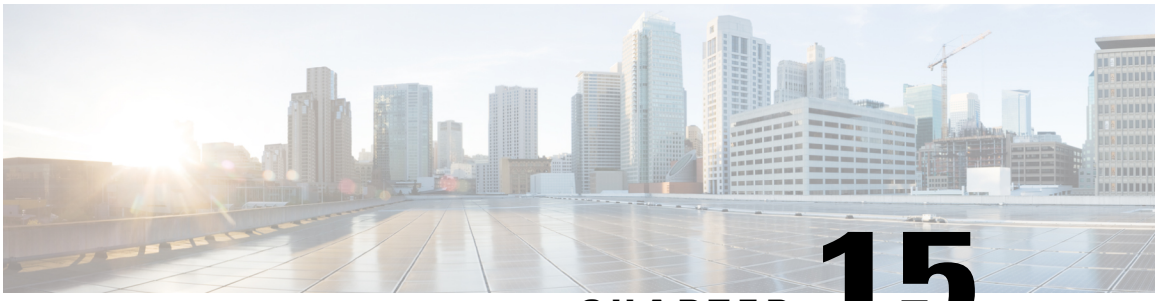
Step 1 On the menu bar, click **Statistics**.

Step 2 In the navigation pane, expand **Custom Reports**.
The list of report groups you created are displayed.

Step 3 Expand the report group which contains the report you need to delete.
If there are no report groups, then expand **Ungrouped Reports**.

Step 4 Right-click on the report name, and click **Delete**.
A dialog box appears prompting you to confirm the deletion of the report.

Step 5 Click **Yes**.
The report is deleted from the Cisco UCS Central GUI.



CHAPTER 15

System Management

This chapter includes the following sections:

- Managing DNS Policies, page 259
- Managing Power Policies, page 261
- Managing Time Zones, page 263
- SNMP Policies, page 266
- About High Availability in Cisco UCS Central, page 274

Managing DNS Policies

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

Configuring a DNS Policy

Before You Begin

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

Procedure

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, 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.
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, 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, 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.
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, 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**.

Managing Power Policies

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

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, 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.
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, 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 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, 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.
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, 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**.

Managing Time Zones

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

Configuring a Date and Time Policy

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, 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.
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, 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 and 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, 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 IPv4 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 from 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, 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**.

SNMP Policies

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

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

SNMP Functional Overview

The SNMP framework consists of three parts:

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

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

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

SNMP Support in Cisco UCS Central

Support for MIBs

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

- SNMP MIB-2 System
- HOST-RESOURCES-MIB
  - hrSystem
  - hrStorage
  - hrDevice
  - hrSWRun

    - hrSWRunPerf
- UCD-SNMP-MIB
    - Memory
    - dskTable
    - systemStats
    - fileTable
- SNMP MIB-2 Interfaces
    - ifTable
- IP-MIB
- SNMP-FRAMEWORK-MIB
    - snmpEngine
- IF-MIB
- DISMAN-EVENT-MIB
- SNMP MIB-2 snmp

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

Authentication Protocols for SNMPv3 Users

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

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

AES Privacy Protocol for SNMPv3 Users

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

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

SNMP Notifications

A key feature of SNMP is the ability to generate notifications from an SNMP agent. These notifications do not require that requests be sent from the SNMP manager. Notifications can indicate improper user

authentication, restarts, the closing of a connection, loss of connection to a neighbor router, or other significant events.

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

SNMP Security Features

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

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

SNMP Security Levels and Privileges

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

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

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

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

SNMP Security Models and Levels

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

Table 5: SNMP Security Models and Levels

Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for authentication.
v3	authNoPriv	HMAC-MD5 or HMAC-SHA	No	Provides authentication based on the Hash-Based Message Authentication Code (HMAC) Message Digest 5 (MD5) algorithm or the HMAC Secure Hash Algorithm (SHA).
v3	authPriv	HMAC-MD5 or HMAC-SHA	DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard.

Configuring an SNMP Policy

Before You Begin

Before configuring a SNMP policy under a domain group, ensure that a SNMP policy is first created. Policies under the Domain Groups root which were already created by the system and are 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**, or the **Domain Group** name where you want to create the policy.

Step 3 Under the **Domain Groups root** node, 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 **Enabled** to choose the **Admin State**.
If **Enabled**, Cisco UCS Central uses SNMP to monitor the Cisco UCS Central system. Cisco UCS uses SNMP in all Cisco UCS domains included in the domain group if the groups themselves are not configured with SNMP.

The default state is **Disabled** with no fields displayed. Leaving the default state disables the SNMP policy

b) Enter the community or the username in the **Community/Username** field.
You can use 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.

c) Enter the system contact person information in the **System Contact** field.
The **System Contact** person is responsible for the SNMP implementation. Enter a string of up to 255 characters, such as an email address or a name and telephone number.

d) Enter the system location in the **System Location** field.
The **System Location** defines the location of the host on which the SNMP agent (server) runs. Enter an alphanumeric string up to 510 characters.

Step 7 Click **Save**.

What to Do Next

Create SNMP traps and SNMP users.

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 in the **Create SNMP Trap** dialog box.

a) Enter the SNMP host IP in the **IP Address** field.
Cisco UCS sends the trap to the defined IP address.

b) Enter the community or the username in the **Community/Username** field.
You can use 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.

c) Enter the port number in the **Port** field.
Cisco UCS uses the defined port to communicate with the SNMP host for the trap. Enter an integer between 1 and 65535. The default port is 162.

d) Click **v1**, **v2c**, or **v3** to choose the SNMP **Version**.

e) Click **trap** to choose the SNMP trap**Type**.

f) Click **auth**, **no auth**, or **priv** to define the **v3Privilege**.

g) Click **OK**.

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 in the **Create SNMP User** dialog.

a) Enter the SNMP username in the **Name** field.
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 locally authenticated username.

b) Click **md5** or **sha** to chose the authorization type.
c) Check the **AES-128** checkbox.
If checked, this user uses AES-128 encryption.
d) Enter the user password in the **Password** field.
e) Re-enter the user password in the **Confirm Password** field.
f) Enter the privacy password for this user in the **Privacy Password** field.
g) Re-enter the privacy password for this user in the **Confirm Privacy Password** field.
h) Click **OK**.

Step 6 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, 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**.

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**.

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**.

About High Availability in Cisco UCS Central

Cisco UCS Central provides high availability in a cluster setup when you deploy Cisco UCS Central in two virtual nodes. High availability provides stability and redundancy directly to your Cisco UCS Central and indirectly to your Cisco UCS Domains management. The high availability in Cisco UCS Central provides you the following:

- Simplified large scale Cisco UCS deployments with an increased number of servers, chassis, fabric interconnects, and data centers.
- UCS Central VM redundancy in a Hypervisor independent environment.
- A shared storage device to house database and image repositories.
- Built-in failure detection (DME, VM, host, or network failures) and automatic failover to ensure continuous operation.

High Availability Architecture

You will deploy Cisco UCS Central in two VMs on separate hosts to enable high availability. High availability -

- Requires at least one Cisco UCS Manager be registered with Cisco UCS Central for a cluster to support high availability
- Uses the same subnet for individual VMs and VIP addresses
- Allows you to configure a mirrored, multi-path shared storage disk on each VM that is accessible from both hosts
- Uses UCS Manager to store quorum data and determine primary node.

- Exchanges information such as heartbeat and election protocols in the same way as Cisco UCS Manager. This results in a simpler design, more code reusability, and easy to define failover conditions

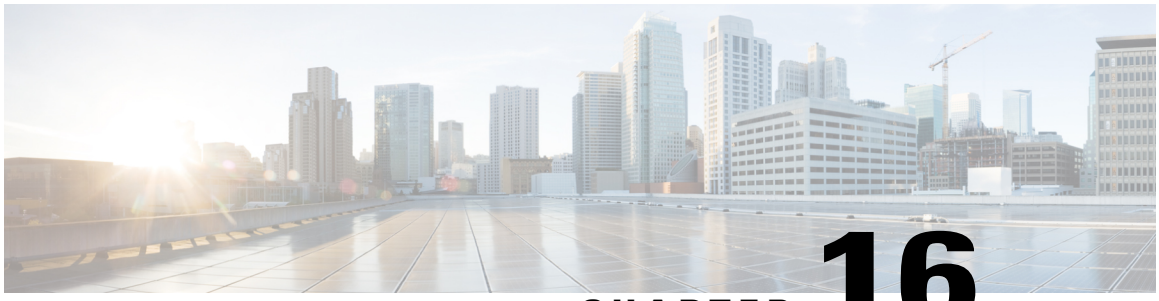
Cautions and Guidelines for Using High Availability

The following are the guidelines to setup Cisco UCS Central in high availability:

- Make sure both VMs in the cluster should never be on the same server. Otherwise, a single host failure would end up bringing down the cluster.
- Each node in the cluster must have the following:
  - A primary NIC connected to the production network that is used for communicating with Cisco UCS Manager, and for heartbeat communications, with the peer node in the cluster.
  - A host bus adapter connected to the Storage Area Network (SAN), that is used to access the storage target.
- **Separate network path for management and storage network**: Make sure the management network used communications between the two Cisco UCS Central nodes are not on the same network as the network that the nodes use to access the shared disk array. The primary heartbeat mechanism relies on exchanging datagrams across the management network. The secondary heartbeat mechanism uses quorum data on Cisco UCS Manager. When you use separate network paths for management and shared disk access, that provides redundant paths between the two nodes making it easier to distinguish node failures from link failures.

Note High availability is supported only in IPv4 addressing without the DHCP. You must configure the node IPs and cluster VIPs statically during the installation. These IP addresses are allocated from the production network over which the UCS Central cluster communicates with UCSMs.

- Both VMs must be configured on IP addresses that belongs to the same subnet.
- Make sure the cluster node infrastructure does not have a single point of failure. You can connect the cluster nodes my multiple, distinct networks. You can also construct the network with redundant switches and routers or similar hardware that removes single points of failure.
- For high availability Cisco UCS Central supports the most commonly used bus types, such as SAS , Fiber Channel (FC), and iSCSI. SCSI compatibility with Persistent Reservations (PRs) is recommended. LUN masking or zoning should be used to isolate the storage volumes accessed by the cluster from other hosts on the network.



CHAPTER 16

Monitoring Logs

This chapter includes the following sections:

- System Event Log, page 277
- Configuring Settings for Faults, Events and Logs, page 279

System Event Log

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

System Event Log

The system event log (SEL) resides on the CIMC in NVRAM. It records most server-related events, such as over and under voltage, temperature events, fan events, and events from BIOS. The SEL is mainly used for troubleshooting purposes.

The SEL file is approximately 40KB in size, and no further events can be recorded when it is full. It must be cleared before additional events can be recorded.

You can use the SEL policy to backup the SEL to a remote server, and optionally clear the SEL after a backup operation occurs. Backup operations can be triggered based on specific actions, or they can occur at regular intervals. You can also manually backup or clear the SEL.

The backup file is automatically generated. The filename format is sel-*SystemName-ChassisID-ServerID-ServerSerialNumber-Timestamp*; for example, sel-UCS-A-ch01-serv01-QCI12522939-20091121160736.

Tip For more information about the SEL, including how to view the SEL for each server and configure the SEL policy, see the Cisco UCS Manager configuration guides, which are accessible through the Cisco UCS B-Series Servers Documentation Roadmap.

Configuring 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, 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, fill in the required fields.
b) In the **Backup Configuration** area, fill in the required fields.

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, 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**.

Configuring Settings for Faults, Events and Logs

Configuring Global Fault Policies

Configuring a Global Fault Debug Policy

Before You Begin

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

Procedure

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, 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.
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, 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.

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, 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.
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, 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.
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, 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.
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, 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.
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, 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.
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**.

Viewing Logs and Faults

You can view faults, events, and audit logs generated in one or more registered domains under the **Logs and Faults** tab in Cisco UCS Central. Information for each of these items is categorized and displayed under the following tabs:

- **mgmt-controller —** Management controller
- **policy-mgr —** Policy manager
- **resource-mgr —** Resource manager
- **identifier-mgr —** Identifier manager
- **operation-mgr —** Operation manager
- **service-reg —** Service registry

Additionally, you can view and terminate active user sessions (for local and remote users), view core files located at specified locations on the server, internal services for providers, controllers and service registries, and a categorized list of registered domains.

Active Sessions

You can view active sessions for remote and local users in Cisco UCS Central and choose to terminate those sessions from the server.

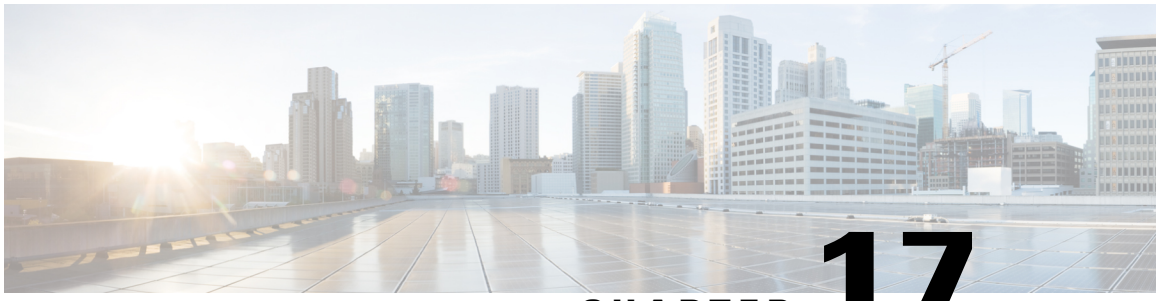
Procedure

Step 1 On the menu bar, Click **Logs and Faults**.

Step 2 By default, the **Active Sessions** pane is highlighted.

Step 3 In the **Work** pane, click the **Local** and/or **Remote** tabs to display a list of active sessions under each category.

Step 4 Right click the individual session you wish to remove and select Terminate Session.



CHAPTER 17

User Management

This chapter includes the following sections:

- Cisco UCS Central User Accounts, page 289
- Role-Based Access Control, page 302
- User Locales, page 308
- User Organizations, page 312

Cisco UCS Central User Accounts

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

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

Admin Account

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

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

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

Locally Authenticated User Accounts

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

Remotely Authenticated User Accounts

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

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

Expiration of User Accounts

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

By default, user accounts do not expire.

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

Guidelines for Creating Usernames

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

- The login ID can contain between 1 and 32 characters, including the following:
  - Any alphabetic character
  - Any digit
  - _ (underscore)
  - - (dash)
  - . (dot)
- The login ID must be unique within Cisco UCS Central.
- The login ID must start with an alphabetic character. It cannot start with a number or a special character, such as an underscore.
- The login ID is case-sensitive.
- You cannot create an all-numeric login ID.
- After you create a user account, you cannot change the login ID. You must delete the user account and create a new one.

Guidelines for Creating Passwords

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

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

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

Password Profile for Locally Authenticated Users

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

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

Password History Count

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

A user must create and use the number of passwords configured in the password history count before being able to reuse one. For example, if you set the password history count to 8, a locally authenticated user cannot reuse the first password until after the ninth password has expired.

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

If necessary, you can clear the password history count for a locally authenticated user and enable reuse of previous passwords.

Password Change Interval

The password change interval enables you to restrict the number of password changes a locally authenticated user can make within a given number of hours. The following table describes the two configuration options for the password change interval.

Interval Configuration	Description	Example
No password change allowed	This option does not allow passwords for locally authenticated users to be changed within a specified number of hours after a password change. You can specify a no change interval between 1 and 745 hours. By default, the no change interval is 24 hours.	For example, to prevent passwords from being changed within 48 hours after a locally authenticated user changes his or her password, set the following: • Change during interval to disable • No change interval to 48
Password changes allowed within change interval	This option specifies the maximum number of times that passwords for locally authenticated users can be changed within a pre-defined interval. You can specify a change interval between 1 and 745 hours and a maximum number of password changes between 0 and 10. By default, a locally authenticated user is permitted a maximum of 2 password changes within a 48 hour interval.	For example, to allow to be changed a maximum of once within 24 hours after a locally authenticated user changes his or her password, set the following: • Change during interval to enable • Change count to 1 • Change interval to 24

Configuring the Maximum Number of Password Changes for a Change Interval

You must have admin 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**.

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.
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.

Name	Description
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.
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**.

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

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**.

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**.

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**.

Web Session Limits for User Accounts

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

Monitoring User Sessions

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.

Name	Description
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.

Role-Based Access Control

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

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

User Roles

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

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

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

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

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

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

Default User Roles

The system contains the following default user roles:

AAA Administrator

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

Administrator

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

Facility Manager

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

Network Administrator

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

Operations

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

Read-Only

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

Server Compute

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

Server Equipment Administrator

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

Server Profile Administrator

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

Server Security Administrator

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

Storage Administrator

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

Privileges

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

Table 6: User Privileges

Privilege	Description	Default Role Assignment
aaa	System security and AAA	AAA Administrator
admin	System administration	Administrator
domain-group-management	Domain Group Management	Domain Group Administrator
ext-lan-config	External LAN configuration	Network Administrator
ext-lan-policy	External LAN policy	Network Administrator
ext-lan-qos	External LAN QoS	Network Administrator
ext-lan-security	External LAN security	Network Administrator
ext-san-config	External SAN configuration	Storage Administrator
ext-san-policy	External SAN policy	Storage Administrator
ext-san-qos	External SAN QoS	Storage Administrator
ext-san-security	External SAN security	Storage Administrator
fault	Alarms and alarm policies	Operations
operations	Logs and Smart Call Home	Operations
org-management	Organization management	Operations
pod-config	Pod configuration	Network Administrator
pod-policy	Pod policy	Network Administrator
pod-qos	Pod QoS	Network Administrator
pod-security	Pod security	Network Administrator
power-mgmt	Read-and-write access to power management operations	Facility Manager

Privilege	Description	Default Role Assignment
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
service-profile-qos	Service profile QoS	Network Administrator
service-profile-qos-policy	Service profile QoS policy	Network Administrator
service-profile-security	Service profile security	Server Security Administrator
service-profile-security-policy	Service profile security policy	Server Security Administrator
service-profile-server	Service profile server management	Server Profile Administrator
service-profile-server-oper	Service profile consumer	Server Profile Administrator
service-profile-server-policy	Service profile pool policy	Server Security Administrator
service-profile-storage	Service profile storage	Storage Administrator
service-profile-storage-policy	Service profile storage policy	Storage Administrator
stats	Statistics Management	Statistics Administrator

Creating a User Role

Procedure

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**.

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

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**.

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**.

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**.