

Cisco UCS Director Administration Guide, Release 6.9

First Published: 2024-05-07

Last Modified: 2026-05-05

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2024–2026 Cisco Systems, Inc. All rights reserved.



CONTENTS

Full Cisco Trademarks with Software License ?

PREFACE

Preface xix

Audience xix

Conventions xix

Documentation Feedback xxi

Obtaining Documentation and Submitting a Service Request xxi

CHAPTER 1

New and Changed Information for this Release 1

New and Changed Information for this Release 1

CHAPTER 2

Overview 5

Cisco UCS Director 5

Features and Benefits 6

Physical and Virtual Management Features 7

Model-Based Orchestration 8

User Interface of Cisco UCS Director 9

Landing Page 10

Common Icons 12

Converged View 14

Generating Additional Reports for a Cloud Account 14

Guided Setup Wizards in Cisco UCS Director 14

Creating a Wizard from a Workflow 15

Setting up Non-Secure Connection to the Cisco UCS Director User Interface 16

Initial Login 17

Generating a Self-Signed Certificate 17

Initial System Setup 18
Recommended Order of System Setup 20
Configuring the Host Name for Cisco UCS Director 22
Working with Ciphers 23
Editing Cipher Usage 23

CHAPTER 3 **Managing Users and Groups** 25
User Roles 25
Adding a User Role 27
Adding Users 28
Modifying Users 30
Deleting Users 30
Viewing User Management Activities in Syslog Server 31
Managing User Types 31
Default User Permissions 31
User Roles and Permissions 31
Permissions for Server Management 34
All Policy Admin 35
Billing Admin 37
Computing Admin 38
Group Admin 40
IS Admin 42
Network Admin 43
Operator 45
Service End User 47
Storage Admin 48
Viewing User Role Information for Users 50
Reviewing Recent Login History of Users 50
Configuring Session Limits for Users 51
Managing User Account Status 52
Unassigning Resources From a User 52
Disabling a User Account in Cisco UCS Director 53
Disabling User Accounts within a Group 53
MSP Administrator Role 54

Managing Groups 55
Creating a User Group 55
Using the Global Dashlet Setup Option 56
Creating an MSP Organization 57
Creating a Customer Organization 58
Password Policy 59
Creating a Password Policy 60
Group Budget Policy 61
Viewing and Editing a Group Budget Policy 61
Resource Limits 62
Viewing Resource Limits 63
Editing Resource Limits 63
Configuring the Administration Profile 66
Creating the Admin Profile 66
Editing Your Administrative Profile 67
Sending a Broadcast Message 68
Changing the Admin Password 69
Viewing Current Online Users 69
Viewing Workflow Task Details 69
Managing User Access Profiles 70
Multi-Role Access Profiles 70
Creating a User Access Profile 70
Logging in to a Profile 71
Default Profile 71
Changing a Default Profile 72
Authentication and LDAP Integration 72
Configuring Authentication Preferences 72
LDAP Integration 73
Viewing LDAP Directory Sync Status 88
Single Sign On with OneLogin 88
Authentication and Cisco Identity Services Engine (Cisco ISE) 94
Cisco Identity Services Engine (Cisco ISE) Integration 94
Configuring Cisco Identity Services Engine (Cisco ISE) Server Integration 95
Branding for Customer Organizations 98

Branding User Groups 99
Branding Customer Organizations 100
Login Page Branding 101
Configuring a Custom Domain Logo 101

CHAPTER 4 **Setting Up the End User Portal** 103
End User Portal 103
Summary of Tasks to Set Up the End User Portal 103
Setting Up User Accounts for the End User Portal 104
Creating a User Group 104
Adding Users 105
Setting Permissions for the End User Portal 107
Permissions Required for Approvals 107
Permissions Required for Catalogs 108
Permissions Required for Budget Entries 108
Physical Resources 109
Permissions Required for CloudSense Reports 109
Permissions Required for Rack Servers 109
Permissions Required for Servers 109
Permissions Required for Service Profiles 109
Permissions Required for SnapMirrors 110
Permissions Required for Storage Virtual Machines 110
Permissions Required for vFilers 110
Permissions Required for SVM Initiator Groups 110
Permissions Required for SVM LUNs 111
Permissions Required for SVM CIFS Shares 111
Permissions Required for SVM Export Policies 111
Permissions Required for SVM Export Rules 111
Permissions Required for SVM Initiators 112
Permissions Required for SVM Port Sets 112
Permissions Required for SVM SIS Policies 112
Permissions Required for SVM Snapshot Policies 112
Permissions Required for SVM WWPN Aliases 112
Permissions Required for SVM Volume Snapshots 113

Permissions Required for SVM Volumes 113
Permissions Required for vFiler Volumes 114
Services 114
Permissions Required for Service Requests 114
Permissions Required for User OVF Management 115
Virtual Resources 115
Permissions Required for Application Containers 115
Permissions Required for VMs 116
Permissions Required for Images 116
Setting Up the User Interface of the End User Portal 117
Configuring Dashlets 117
Changing Colors of Dashlet Reports 118
Selecting Catalogs for End User Portal 119

CHAPTER 5 **Managing System Administration Settings** 121
Setting up the Outgoing Mail Server 121
Working with Email Templates 122
Adding an Email Template 123
Previewing an Email Template 124
Setting a Default Email Template 124
Configuring System Parameters (Optional) 125
Configuring System Parameters 125
Configuring Infrastructure System Parameters (Optional) 126
Configuring Proxy Settings 127
Running an Object Search 127
Viewing Workflow Tasks in the Workflow Designer 128
Working with Licenses in Cisco UCS Director 129
Limitations on Using NFR and Permanent Physical Server Licenses 131
Applying Upgrade License 132
Migrating a License 132
Replacing a License 133
Updating the License 133
Verifying License Utilization 134
Viewing License Utilization History 134

Viewing Deactivated License Information 135
Viewing License Key Information 135
Viewing License Status 136
Viewing Resource Usage Data 136
Application Categories 136
Adding Application Categories 137
Customizing the Portal 138
Customizing the Login Page and Background Images 138
Customizing the Application Logo 139
Customizing Favicons 140
Customizing Application Header 141
Customizing Date Display 142
Customizing the Color Theme 142
Customizing Logout Redirect 142
Customizing Reports 142
Enabling Advanced Controls 143
Enabling the Service Provider Feature 145
User Menus 145
Setting User Menus 145
Setting User Permissions 146
System Tasks 146
Creating a Node Pool 147
Creating a System Task Policy 147
Assigning a Node Pool to a System Task Policy 148
Creating a Service Node 148
Assigning a System Policy to a System Task 149
Executing System Tasks 150
Disabling or Enabling a System Task 150
Scheduling a System Task 151
Resetting a System Task 152
System Tasks with Fixed Rate Option 153
Managing Icons in the Cisco UCS Director User Interface 153
Modifying an Icon in the Cisco UCS Director User Interface 154
Editing an Icon 155

Deleting an Icon 156
Previewing an Icon 156
Tag Library 156
Creating a Tag 157
Support Information 158
Viewing System Information 159
Showing Logs 160
Downloading Logs 160
Starting the Debug Log 161
Generating API Logs 161
Database Audit Logging 162
Enabling Audit Logging 162
Device Connector 163
Configuring Device Connector 163
Launching Cisco UCS Director from Cisco Intersight 164
Connector Pack Management 165
Upgrading Connector Packs 167
Viewing Connector Pack Upgrade Information 168
Base Platform Pack and System Update Manager 169
Upgrading Base Platform Pack 169
Upgrading the System Update Manager 170
Upgrade Process Validation and Failure Scenarios 171
Alert About Insecure Protocols 173
Viewing Details About Insecure Protocols 173

CHAPTER 6 **Managing Integration Settings** 175
About Integration Settings 175
Configuration Management Database Integration 176
Setting Up CMDB Integration 176
Metering Data Export 177
Setting Up Metering Data Export 177
Change Records 178
Viewing Change Records 178
System Logs 179

Setting up System Logs 179
Storage and OVF Upload 179
Multiple Language Support 180
Choosing a Language for Cisco UCS Director 180
Setting a Locale for the User Interface 180
Adding a Repository 181

CHAPTER 7 Managing a Physical Infrastructure 183
About Managing a Physical Infrastructure 183
Using the Converged View 183
Adding a Site 184
Adding a Pod 184
Adding a Physical Account 186
Adding a Multi-Domain Manager Account 188
Adding a Network Element 189
Enabling DHCP Logging 190
Configuring Inventory Data Collection Schedule for Physical Accounts 191
Testing Connectivity 192
Testing Connectivity of Managed Network Elements 192
Testing the Connection to a Physical Account 193
Enabling Device Discovery 193

CHAPTER 8 Managing a Virtual Infrastructure 195
About Managing VMware Clouds 195
Creating a VMware Cloud 196
Configuring Inventory Data Collection Schedule for Virtual Accounts 199
Downloading the PowerShell Agent Installer 201
Creating a PowerShell Agent 202
Verifying Cloud Discovery and Connectivity 202
Testing the Connection 202
Viewing vCenter Plug-ins 203
Provisioning Virtual Machines in Cisco UCS Director 203

CHAPTER 9 Managing Policies 207

Policies 207
Computing Policies 208
Creating a Computing Policy 208
Configuring a Bare Metal Server Provisioning Policy 211
Validating a Bare Metal Server Provisioning Policy 215
Data Collection Policy 215
Configuring a Data Collection Policy for a Virtual Account 216
Associating the Data Collection Policy for a Virtual Account 217
About Group Share Policy 218
Creating a Group Share Policy 218
Storage Policies 219
Storage Policies for Multiple VM Disks 219
Adding and Configuring a Storage Policy 219
Virtual Storage Catalogs 225
Configuring a Virtual Storage Catalog 225
Credential Policies 226
Configuring a Credential Policy 227
Network Policies 227
Adding a Static IP Pool Policy 227
Configuring a IP Subnet Pool Policy 229
Adding a Network Policy 230
Networking Provisioning Policies 233
Configuring a Network Provisioning Policy 233
VLAN Pool Policies 235
Configuring a VLAN Pool Policy 235
System Policies 235
Configuring a System Policy 235
OS Licenses 241
Adding an OS License 241
End User Self-Service Policy 242
Creating an End User Policy 243
Configuring a VM Management Policy 243

CHAPTER 10 **Managing Virtual Data Centers** 247

Virtual Data Centers 247
VDC Actions 248
Adding a Virtual Data Center 248
Viewing a Virtual Data Center 251
Managing Application Categories in a Virtual Data Centers 252
Assigning an Application Category to Multiple VDCs 252
Virtual Data Center Service Profiles 253
Adding a Virtual Data Center Service Profile 253

CHAPTER 11 **Managing Resource Groups** 257
Resource Groups 257
Environment Variables 257
Adding a Custom Environment Variable 266
Adding a Resource Group 268
Editing a Resource Group 276
Adding a Pod to a Resource Group 277
Managing Tags of a Resource Group 278
Deleting a Resource Group 279
Tenant 280
Service Offerings 281
Adding a Service Offering 281
Cloning a Service Offering 285
Editing a Service Offering 289
Deleting a Service Offering 293
Tenant Profiles 293
Adding a Tenant Profile 293
Troubleshooting a Service Offering List 295
Cloning a Tenant Profile 296
Editing a Tenant Profile 297
Deleting a Tenant Profile 298

CHAPTER 12 **Managing Catalogs** 299
About Managing Catalogs 299
Publishing a Catalog 300

About Publishing Advanced Catalogs 308
Publishing Advanced Catalogs 308
Creating a Bare Metal Server Catalog 310
Reordering Catalogs Within a Folder 312
Accessing Hosts for Deployment 312
Reordering Catalog Folders 313

CHAPTER 13 **Using Self-Service Provisioning** 315
Self-Service Provisioning 315
Service Requests 315
Creating a Service Request with Catalog Type—Standard 316
Creating a Service Request with Catalog Type—Advanced 323
Creating a Service Request with Catalog Type—Bare Metal 324
Service Request Workflow and Details 327
Service Request Workflow 327
Service Request Details 329
Viewing the Workflow Status of a Service Request 330
Viewing Log Details for a Service Request 330
About Scheduling a Service Request 331
Scheduling Service Requests 331
About Resubmitting a Service Request 331
Resubmitting a Service Request 332
Other Service Request Functions 332
Canceling a Service Request 332
Rolling Back a Service Request 332
Archiving a Service Request 333
Bulk Archiving Service Requests 334
Deleting Service Requests 335
Viewing Service Requests for a Particular Group 336
Searching the Records of Service Requests for a Group 337
Exporting a Report of Service Requests for a Group 337
Reinstating an Archived Service Request 338
Launching the Service Request Quick View 338
Service Request Approval Process 339

Approving a Service Request 339
Rejecting a Service Request 339
Viewing Approval Information on Service Requests 340
Searching the Records of Service Request Approvals 340
Exporting a Report of Service Request Approvals 340
Service Request Budgeting 341
Viewing the Current Month Budget Availability 341
Viewing Budget Entries 341
Adding a Budget Entry 341

CHAPTER 14 **Multiple Disk VM Provisioning** 343
About Multiple Disk VM Provisioning 343
Overview of the Procedure for Multiple Disk VM Provisioning 344
About Templates with Multiple Disks 344
Assigning Disk Categories 344
Defining Storage Policies 345
Creating a Storage Policy 345
Creating a Catalog 351
Adding a Catalog 351
Creating a VM Disk 359

CHAPTER 15 **Using the Chargeback Module** 363
About Chargeback Features 363
Budget Policies 364
Configuring a Budget Policy 364
Creating a Tag-Based Cost Model 364
Cost Models 365
Creating a Cost Model 366
Creating a Bare Metal Cost Model 369
Modifying a VDC to Include a Cost Model 370
Adding a Cost Model to a VDC 370
Editing a VDC to Include a Cost Model 372
Package-Based Cost Models 372
Creating a Package-Based Cost Model 373

Storage Tier Cost Models 374
Assigning a Cost to a Tier 374
About Assigning a Datastore to Tiers 375
Assigning a Datastore to a Tier 375
Chargeback Reports 375
Viewing the Current Month Summary 377
Viewing the Previous Month's Summary 377
Viewing Monthly Resource Accounting Information 377
Viewing the VM Level Resource Accounting Details 377
Viewing the VM Level Chargeback Details 378
Exporting the Monthly Resource Accounting Details 378
Exporting VM Level Resource Accounting Details 379
Exporting VM Level Chargeback Details 379
About Change Records 380
Accessing Change Records 380
Chargeback Calculations 380

CHAPTER 16 **System Monitoring and Reporting** 383
Dashboard 383
Enabling the Dashboard 383
Creating Additional Dashboards 384
Deleting a Dashboard 384
Adding Report Widgets 385
Refreshing Widget Data 385
Summary 385
Viewing Virtual Machine, Cloud, and System Summary Information 385
Customizing Summary Report Widgets 386
Inventory Management 386
Accessing System Inventory Details 386
Resource Pools 387
Accessing Resource Details 387
Clusters 387
Accessing Clusters 387
Images 388

Accessing Images 388
Assigning VM Images to Users or Groups 388
Host Nodes 389
Accessing Host Nodes 389
Virtual Machines (VMs) 389
Accessing VMs 389
Accessing Group Level VMs 390
Topology 390
Accessing Topology Types 390
Assessment 391
Accessing Assessments 391
Reports 391
Accessing Reports 392
Diagnostic System Messages 392
Viewing Diagnostic System Messages 392
Compatibility Matrix Information 393
Viewing Compatibility Matrix Information 393

CHAPTER 17 **Managing Lifecycles** 395
Managing VM Power Settings 395
Managing VM Snapshots 396
Creating VM Snapshots 397
Reverting to a Snapshot 397
Marking a Golden Snapshot 398
Deleting a Snapshot 398
Deleting All Snapshots 399
Configuring the Lease Time for a Virtual Machine 399
Managing VM Actions 400
Viewing VM Details 401
Resizing VMs 401
Using the Stack View Option 402
Creating a VM Disk 403
Resizing a VM Disk 405
Locking VMs in Cisco UCS Director 405

Adding vNICs 406
Replacing a vNIC 408
Launching the VM Client 409
Enabling the VNC Console on a VM 409
Automatically Unconfiguring the VNC Console on a VM 410
Accessing VM Console Using VNC Client 411
Configuring ESX/ESXi Server for VNC Access to VM Console 411
Accessing VMRC Console 412
Assigning a VM 413
VM Credentials 415
Viewing VM Credentials 415
Initiating Inventory Collection for a VM 416
Testing VNC Connectivity 416
Cloning a VM 417
Moving a VM to VDC 421
Resynchronizing a VM 422
Applying a Tag to a VM 423
Mounting an ISO Image as a CD/DVD Drive 423
Unmounting an ISO Image as a CD/DVD Drive 424

CHAPTER 18 **Managing CloudSense Analytics** 425
CloudSense Analytics 425
Generating a Report 426
Generating an Assessment 428
Report Builder for Custom Report Templates 428
Creating a Report Builder Template 429
Generating a Report from a Template 430
Viewing Reports Generated From a Template 431
Emailing Reports Generated From a Template 432



Preface

This preface contains the following sections:

- Audience, on page xix
- Conventions, on page xix
- Documentation Feedback, on page xxi
- Obtaining Documentation and Submitting a Service Request, on page xxi

Audience

This guide is intended primarily for data center administrators who use Cisco UCS Director and who have responsibilities and expertise in one or more of the following:

- Server administration
- Storage administration
- Network administration
- Network security
- Virtualization and virtual machines

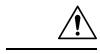
Conventions

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.



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



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



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



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

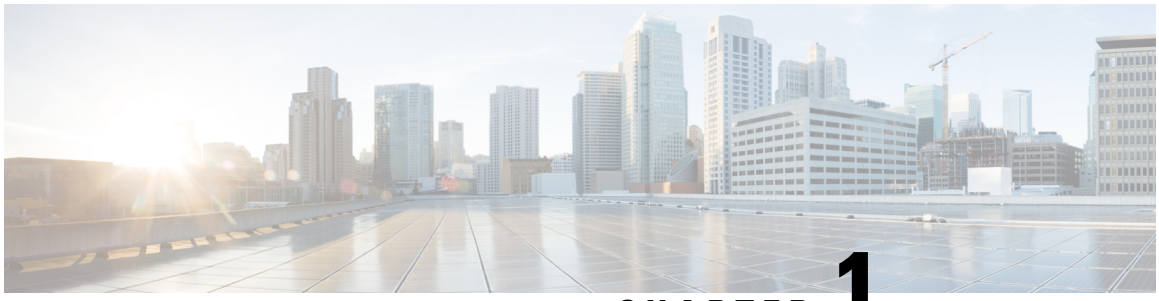
Documentation Feedback

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

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation.

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.



CHAPTER 1

New and Changed Information for this Release

This chapter contains the following section:

- New and Changed Information for this Release, on page 1

New and Changed Information for this Release

The following tables provides an overview of the significant changes to this guide for this current release. The table does not provide an exhaustive list of all changes made to this guide or of all new features in this release.

Table 1: New and Changed Information in Cisco UCS Director, Release 6.9(4.0)

Feature	Description	Where Documented
Enforcement of default values for specific password policy parameters	Allows you to select default values for specific parameters, which are enforced to improve the password strength and enhance security.	Password Policy
Viewing log messages for user management activities	Allows you to view messages generated when user management activities are performed.	Viewing User Management Activities in Syslog Server
Enabling LDAP redundancy	Allows you to enable dynamic lookup of active LDAP servers associated with the domain name. Due to this, if the primary LDAP server is unavailable, the secondary LDAP server is used to synchronize the data.	Configuring LDAP Servers
Support for SFTP and SCP protocols	Allows you to choose SFTP and SCP protocols for exporting change information and trend data to a target server.	• Setting Up CMDB Integration • Setting Up Metering Data Export

Feature	Description	Where Documented
Details about the usage of insecure protocols	Allows you to view details about the insecure protocols used in different areas of Cisco UCS Director.	Viewing Details About Insecure Protocols

Table 2: New and Changed Information in Cisco UCS Director, Release 6.9(3.0)

Feature	Description	Where Documented
Viewing compatibility matrix information	Allows you to view details about software and hardware components compatible with the Cisco UCS Director.	Compatibility Matrix Information
Viewing critical alerts	Allows you to view critical alerts based on advance predictions of potential failure scenarios.	Viewing Diagnostic System Messages
Defining expiry period for approval tasks	Allows you to define the number of days an approval task must remain active.	Configuring System Parameters
Resetting system task	Allows you to quickly reset and reschedule a system task that has been stuck in the in-progress state for a long time, causing inventory failure.	Resetting a System Task
Discontinuation of support for NFR and permanent physical server licenses	The support for permanent and subscription-based NFR licenses, and permanent physical server licenses is discontinued. However, the physical server licenses with valid expiry dates will remain supported until their expiry.	Limitations on Using NFR and Permanent Physical Server Licenses

Table 3: New and Changed Information in Cisco UCS Director, Release 6.9(2.0)

Feature	Description	Where Documented
Change of default account to access Cisco UCS Director	The root user access is disabled, and ucsdadmin access is enabled by default. You must log in to the Cisco UCS Director as the ucsdadmin user.	Initial Login

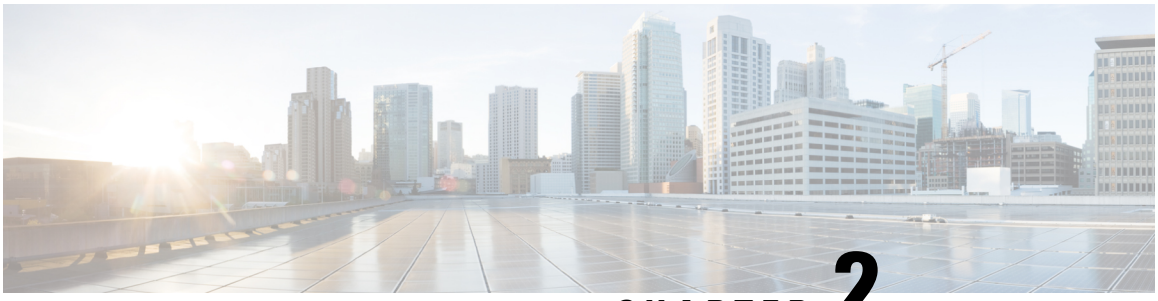
Table 4: New and Changed Information in Cisco UCS Director, Release 6.9(1.0)

Feature	Description	Where Documented
BigData personality	The BigData personality and the Cisco BigData Express connector have been removed.	Working with Licenses in Cisco UCS Director

Table 5: New and Changed Information in Cisco UCS Director, Release 6.9

Feature	Description	Where Documented
CSV format reports.	In this release, you can generate, export and email CloudSense reports in CSV format.	• Viewing Reports Generated From a Template, on page 431 • Emailing Reports Generated From a Template, on page 432
GUI edit of LDAP server IP.	The LDAP server IP address in LDAP Integration can be edited in this release.	Modifying LDAP Server Details, on page 83
Custom User input for resizing the memory of a VM.	In this release of Cisco UCS Director 6900, users have a provision to Resize their VM(s) using a Custom User Input via both GUI action and Workflow Task.	Resizing VMs, on page 401

New and Changed Information for this Release



CHAPTER 2

Overview

This chapter contains the following sections:

- Cisco UCS Director, on page 5
- Setting up Non-Secure Connection to the Cisco UCS Director User Interface, on page 16
- Initial Login, on page 17
- Initial System Setup, on page 18
- Recommended Order of System Setup, on page 20
- Configuring the Host Name for Cisco UCS Director, on page 22
- Working with Ciphers, on page 23

Cisco UCS Director

Cisco UCS Director is a complete, highly secure, end-to-end management, orchestration, and automation solution for a wide array of Cisco and non-Cisco data infrastructure components, and for the industry's leading converged infrastructure solutions based on the Cisco UCS and Cisco Nexus platforms. For a complete list of supported infrastructure components and solutions, see the Cisco UCS Director Compatibility Matrix.

Cisco UCS Director is a 64-bit appliance that uses the following standard templates:

- Open Virtualization Format (OVF) and Open Virtual Appliance (OVA) for VMware vSphere
- Virtual Hard Disk (VHD) for Microsoft Hyper-V

Management through Cisco UCS Director

Cisco UCS Director extends the unification of computing and networking layers through Cisco UCS to provide you with comprehensive visibility and management of your data center infrastructure components. You can use Cisco UCS Director to configure, administer, and monitor supported Cisco and non-Cisco components. The tasks you can perform include the following:

- Create, clone, and deploy service profiles and templates for all Cisco UCS servers and compute applications.
- Monitor organizational usage, trends, and capacity across a converged infrastructure on a continuous basis. For example, you can view heat maps that show virtual machine (VM) utilization across all your data centers.
- Deploy and add capacity to converged infrastructures in a consistent, repeatable manner.

- Manage, monitor, and report on data center components, such as Cisco UCS domains or Cisco Nexus network devices.
- Extend virtual service catalogs to include services for your physical infrastructure.
- Manage secure multi-tenant environments to accommodate virtualized workloads that run with non-virtualized workloads.

Automation and Orchestration with Cisco UCS Director

Cisco UCS Director enables you to build workflows that provide automation services, and to publish the workflows and extend their services to your users on demand. You can collaborate with other experts in your company to quickly and easily create policies. You can build Cisco UCS Director workflows to automate simple or complex provisioning and configuration processes.

Once built and validated, these workflows perform the same way every time, no matter who runs the workflows. An experienced data center administrator can run them, or you can implement role-based access control to enable your users and customers to run the workflows on a self-service basis, as needed.

With Cisco UCS Director, you can automate a wide array of tasks and use cases across a wide variety of supported Cisco and non-Cisco hardware and software data center components. A few examples of the use cases that you can automate include, but are not limited to:

- VM provisioning and lifecycle management
- Network resource configuration and lifecycle management
- Storage resource configuration and lifecycle management
- Tenant onboarding and infrastructure configuration
- Application infrastructure provisioning
- Self-service catalogs and VM provisioning
- Bare metal server provisioning, including installation of an operating system

Features and Benefits

The features and benefits of Cisco UCS Director are as follows:

Feature	Benefit
Central management	• Provides a single interface for administrators to provision, monitor, and manage the system across physical, virtual, and bare metal environments • Provides unified dashboards, reports, and heat maps, which reduce troubleshooting and performance bottlenecks
Self-service catalog	• Allows end users to order and deploy new infrastructure instances conforming to IT-prescribed policies and governance
Adaptive provisioning	• Provides a real-time available capability, internal policies, and application workload requirements to optimize the availability of your resources

Feature	Benefit
Dynamic capacity management	• Provides continuous monitoring of infrastructure resources to improve capacity planning, utilization, and management • Identifies underutilized and overutilized resources
Multiple hypervisor support	• Supports VMware ESX, ESXi, Microsoft Hyper-V, and Red Hat hypervisors
Computing management	• Provisions, monitors, and manages physical, virtual, and bare metal servers, as well as blades • Allows end users to implement virtual machine life-cycle management and business continuance through snapshots • Allows administrators to access server utilization trend analysis
Network management	• Provides policy-based provisioning of physical and virtual switches and dynamic network topologies • Allows administrators to configure VLANs, virtual network interface cards (vNICs), port groups and port profiles, IP and Dynamic Host Control Protocol (DHCP) allocation, and access control lists (ACLs) across network devices
Storage management	• Provides policy-based provisioning and management of filers, virtual filers (vFilers), logical unit numbers (LUNs), and volumes • Provides unified dashboards that allow administrators comprehensive visibility into organizational usage, trends, and capacity analysis details.

Physical and Virtual Management Features

Physical Server Management	Virtual Computing Management
• Discover and collect configurations and changes • Monitor and manage physical servers • Perform policy-based server provisioning • Manage blade power • Manage server life cycle • Perform server use trending and capacity analysis • Perform bare metal provisioning using preboot execution environment (PXE) boot management	• Discover, collect, and monitor virtual computing environments • Perform policy-based provisioning and dynamic resource allocation • Manage the host server load and power • Manage VM life cycle and snapshots • Perform analysis to assess VM capacity, sprawl, and host utilization

Physical Storage Management	Virtual Storage Management
• Discover, collect, and monitor storage filers • Perform policy-based provisioning of vFilers • Provision and map volumes • Create and map Logical Unit Number (LUN) and iGroup instances • Perform SAN zone management • Monitor and manage network-attached storage (NAS) and SAN-based storage • Implement storage best practices and recommendation	• Discover, collect, and monitor storage of vFilers and storage pools • Perform policy-based storage provisioning for thick and thin clients • Create new datastores and map them to virtual device contexts (VDCs) • Add and resize disks to VMs • Monitor and manage organizational storage use • Perform virtual storage trend and capacity analysis
Physical Network Management	**Virtual Network Management**
• Discover, collect, and monitor physical network elements • Provision VLANs across multiple switches • Configure Access Control Lists (ACLs) on network devices • Configure storage network s • Implement dynamic network topologies	• Add networks to VMs • Perform policy-based provisioning with IP and DHCP allocation • Configure and connect Virtual Network Interface Cards (vNICs) to VLANs and private VLANs • Create port groups and port profiles for VMs • Monitor organizational use of virtual networks

Model-Based Orchestration

Cisco UCS Director includes a task library containing over 1000 tasks and out-of-the-box workflows. Model-based orchestration and a workflow designer enable you to customize and automate the infrastructure administrative and operational tasks. You can extend and customize the system to meet individual needs.

The following table shows the maintenance and update activities of the task library from day1 through day 3:

Day-1	Day-2	Day-3
• Add tenants • Migrate or add applicants • Integrate with enterprise systems • Use End User Portal	• Monitor performance • Start meeting and billing • Manage tenant change • Self-service Infrastructure as a Service (IaaS)	• Add/upgrade hardware • Repurpose

User Interface of Cisco UCS Director

Cisco UCS Director introduces a new user interface for the administrative portal. This section introduces you to some of the key features of this new user interface.

Change in Navigation

In earlier releases, you could access screens using the main menu bar. Starting with this release, all navigation options are now available from a side bar, and not from the horizontal main menu bar. As a result, the main menu bar is no longer visible in the user interface. You can use your mouse or the cursor to hover over an option on the side navigation bar, and then click on any of the menu options.

Absence of User Interface Labels

The user interface no longer includes labels for actions such as Add, Edit, Delete, Export, and Filter. These actions are represented only with icons. If you use your mouse or cursor to hover over the icon, the label will display the action you can perform using that icon. You can also modify the icons in the user interface for all actions and status messages. For more information, see Modifying an Icon in the Cisco UCS Director User Interface, on page 154.

Using Dashboard to Access Detailed Reports

If you have enabled the **Dashboard**, then it is the first screen that you will see when you login to Cisco UCS Director. Typically, you can use this dashboard to add important or frequently accessed report widgets. Now, you can click on any of the reports that are displayed on the **Dashboard**, and immediately access the screen in the user interface where more detailed information is displayed.

For more information, see Enabling the Dashboard, on page 383

In addition, you can create multiple dashboards and delete them when you no longer need them. For more information, see Creating Additional Dashboards, on page 384 and Deleting a Dashboard, on page 384.

Enhanced Capabilities with Tabular Reports

Following are some of the enhanced capabilities with tabular reports available in the user interface:

- Right-click to view additional options

  After you select a row, if you right-click on your mouse, a list of options relevant to the row you selected are displayed.

- Filter and Search

  You can use a **Filter** option or a **Search** option with tabular reports in the Cisco UCS Director interface. On any page with a tabular report, you can use the **Filter** option that allows you to narrow down the tabular report results with a specific criteria. You can use this **Filter** option on tabular reports that do not span across pages. For tabular reports that do span across multiple pages, you can use the **Search** option to narrow down your search result.

- Adding tabular reports to the **Favorites** menu

  You can add any tabular report displayed in the user interface as a Favorite. By adding a report as a favorite, you can access this report from the **Favorites** menu.

- Resizing of columns

You can resize all the columns that are displayed in the tabular report, including the last column. After you expand the columns, you can use the horizontal scroll bar to view the complete screen.

- Informational message displayed in the absence of data

  If there is no information to be displayed in a report, the following message is displayed.

  No Data

Removing and Restoring Tabs

On any screen that has multiple tabs available, you can choose the number of tabs that you would like to see on that screen. If you close a tab on a screen, it will no longer be displayed in the row of tabs displayed in the user interface. If you would like to bring it back on the screen, then click the arrow facing downwards that is visible on the far right of the screen. It displays a drop-down list of tabs that are available but hidden from view. Choose the tab you would like to restore.



Note You can remove and restore tabs on a screen only when there are a minimum of two tabs. This functionality is not available when there is only one tab displayed on a screen in the interface.

Enhancements to Reporting Capabilities

Following are some of the enhanced reporting capabilities available in the user interface:

- Introduction of pie charts and bar graphs

  Each individual pie chart or bar graph can be exported out of the system in PDF, CSV or XLS format, or can be added to the **Dashboard**.

- Availability of **More Reports** option

  Using the **More Reports** option, you can now generate reports on specific data for the resources in the cloud accounts. For more information, see Generating Additional Reports for a Cloud Account, on page 14.

Landing Page

The landing page opens when you log in to the Cisco UCS Director administrator portal. The elements that you see on the landing page depend upon how you have configured the display. By default, the Converged View is displayed when you login to the portal.

The following are the available elements for your landing page:

- Header—Displays across the top of the screen.
- Navigation menu—The main navigation bar is no longer on the top of the screen. It is now available as a vertical menu on the left-side of the screen.



Note The menu does not have a scroll bar. The menu only displays the number of options that fit in the space available. Some options may not appear if you minimize your screen or zoom in. You can click **Site Map** to view all available options.



Number	Name	Description
1	Header	Contains frequently accessed elements, including the menu. The header is always visible.
2	Link	Provides a link to the Cisco website from where you can access information on using the software.
3	Search icon	Allows you to search for and navigate directly to a specific report in the portal.
4	Diagnostic System Messages icon	Displays the number of diagnostic system messages that have been logged. Clicking on this link takes you to the **Diagnostic System Messages** screen from where you can view detailed information.
5	Claim Status icon	Displays the claim status of the device in Cisco Intersight.
6	Service Request Quick View Panel	Launches the Service Request Quick View panel that displays the recent in-progress, completed and failed service requests. This feature is not available in Cisco UCS Director instances that have been cross-launched from Cisco Intersight.
7	New Upgrade Notification	Displays the list of connector packs available for upgrade. Clicking on this link takes you to the **Available System Upgrades** screen from where you can view detailed information.

Number	Name	Description
8	Help icon	Links to the online help system for the administrator portal.
9	About icon	Displays information about the software, and the version that is currently installed.
10	Home icon	Returns you to the landing page from any location in the user interface.
11	User icon	Allows you to edit your profile, enable or disable the dashboard, and log out.
12	Navigation menu	The vertical navigation menu using which you can access different screens in the interface.

Common Icons

The following table provides information about the common icons used in the user interface. You can see the name of an icon when you hover over it with your mouse. Some icons may have a different name, depending upon the context in which they're used.

Icon	Name	Description
	Search	Search is available on the header and on individual screens. Click **Search** on the header to find a report in the user interface. Click **Search** on an individual screen to find one or more items in the report.
	Alert	Alert is available on the header. Click **Alert** to view your diagnostic system messages.
	User	User is available on the header. Click **User** to access your profile, or to log out of the user interface.
	Export	Export is available on individual screens. Click **Export** to export the content of the report that is visible on the screen.
	Import	Import is available on individual screens. Click **Import** to import a file.
	Refresh	Refresh is available on individual screens. Click **Refresh** to refresh the data that is visible on the screen.
	View Details	View Details is available on individual screens. Click **View Details** to see details about the selected row in the table.
	Table View	Table view is available for your application containers and catalogs. Click **Table View** to view your application containers or catalogs in a table with details about each application container or catalog displayed.

Icon	Name	Description
	Tile View	Tile view is available for your catalogs and application containers. **Tile View** to view your catalogs and application containers in a tiled view of icons. With this view, you must click on an icon to see details about that catalog item or application container.
	Create	Create is available on individual screens. Click **Create** to create a new object, such as a VM disk.
	Add	Add is available on individual screens. Click **Add** to add an item to an existing object, such as adding a catalog item to an existing catalog folder. The name of this icon may also include the item that you want to add, such as **Add Catalog**.
	Expand a list of values	Lists of values are available in forms when you must select one (single select) or more (multi select) items, for example IP addresses or VMs. **Tip** A *multi-select* list displays a check box in the upper left corner of the table next to the first column label. Click this check box to select all items in the table. The item label appears to the right of the **Expand** icon. Click the **Expand** icon to display the list, then select an item or items. Once an item is selected, its value appears in parentheses to the right of the **Expand** icon and label.
	Collapse a list of values	Once a list of values is expanded, the **Expand** icon changes to a **Collapse** icon. Click the **Collapse** icon to hide the list of values, for example to see what is beneath the list.
	Edit	Edit is available on individual screens. Click **Edit** to modify an existing object, such as a catalog item or a VM disk.
	Delete	Delete is available on individual screens. Click **Delete** to delete an object, such as a catalog item or a VM disk.
	Custom Actions	This icon represents additional tasks that do not have an associated icon. It also represents the default icon available in the user interface.
	Favorites	Adds a page to the **Favorites** menu. You can use this option to view frequently accessed pages more quickly.
	Filter	Provides filtering parameters on the page.



Note You can view the complete list of icons and the details from the **Administration** > **User Interface Settings** > **Icon Management** screen. These icons are listed in the **Action Icon Set** category.

Converged View

When you login to the administrator portal for the first time, by default, the **Converged** screen is displayed. This screen displays the currently configured pods in your environment. From this screen, you can add additional pods, or you can select a pod and view additional details on the resources within the pod. Typically, the additional details displayed include the following:

- Virtual resources
- Compute resources
- Network resources
- Storage resources

You can click on any of these resources, and the screen loads additional information.

Cisco UCS Director allows you to configure the Dashboard as the first screen to be displayed when you login to the user interface. For more information, see Enabling the Dashboard, on page 383.

Generating Additional Reports for a Cloud Account

You can use the **More Reports** option to generate specific reports for either a virtual cloud account or for a physical pod account. The type of reports that are generated using this **More Reports** option varies based on the type of account.

If there is no information available to generate this report, then a message stating that there is no data is displayed.

Procedure

Step 1 Navigate to the cloud account that you want to generate additional reports for.

Step 2 From the **More Actions** drop-down menu, click **More Reports**.

Step 3 From the **Type** drop-down list, and **Report** drop-down list, choose the type of report that you want to generate.

The report is generated and displayed in the user interface.

Step 4 (Optional) Click **Settings** > **Export Report** to choose the format in which you want the report to be exported in.

Guided Setup Wizards in Cisco UCS Director

Cisco UCS Director includes a set of wizards that guide you through configuring important features. The following are the available guided setup wizards:

- Device Discovery—This wizard enables you to discover devices and assign them to a pod.
- Initial System Configuration—This wizard helps you complete initial tasks to set up Cisco UCS Director, such as uploading licenses, and setting up SMTP, NTP, and DNS servers.
- vDC Creation—This wizard enables you to configure the policies required to provision VMs in private clouds.

- FlexPod Configuration—This wizard helps you set up a FlexPod account.
- Vblock Pod Configuration—This wizard enables you to discover and assign accounts to Vblock pods.
- VSPEX Pod Configuration—This wizard enables you to discover and assign accounts to VSPEX pods.
- Virtual SAN Pod Configuration—This wizard enables you to set up a Virtual SAN Pod and add devices.

When you first log into Cisco UCS Director, a **Wizard Explorer** window is displayed. From this window, you can view the details of the available guided setup wizards and choose to launch any of them. If you do not want this **Wizard Explorer** to appear every time you log in, you can check the **Do not show this page again** checkbox. To launch these wizards later on, click **Administration** > **Guided Setup**.

In addition to these system-provided wizards, you can create a wizard from a workflow that you have previously configured. For more information, see Creating a Wizard from a Workflow, on page 15.

Creating a Wizard from a Workflow

You can convert valid workflows into wizards, and save them in Cisco UCS Director.

Before you begin

You must have created valid workflows in Cisco UCS Director.

Procedure

Step 1 Choose **Administration** > **Guided Setup**.

Step 2 On the **Guided Setup** page, click **Setup**.

Step 3 From the **More Actions** drop-down menu, click **Create from Workflow**.

Step 4 In the **Create Wizard from Workflow** screen, complete the required fields, including the following:

Name	Description
Select Workflow field	Click **Select** to view a list of available workflows in the **Select Workflow** screen. Check the check boxes of the workflows that you want to convert to a wizard and click **Select**.
Carry over static field values check box	Check this check box if you want the static values from the selected workflow tasks to be carried over into the wizard pages.
Label field	The name of the wizard. This is the primary name of the wizard.
Second Label field	A secondary name of the wizard.
Description field	A description of the wizard.

Name	Description
Icon Image field	Click **Select** to view a list of available icons in the **Icon Image** screen. Check the check box of the icon that you want to associate with this workflow and click **Select**.

Step 5 Click **Submit**.

What to do next

You can perform the following tasks:

- Launch the wizard.
- Edit the wizard.
- View details of the wizard.
- Re-order the wizard in the interface.
- Delete the wizard.

Setting up Non-Secure Connection to the Cisco UCS Director User Interface

By default, the Cisco UCS Director user interface launches in the secure mode. If you want to bypass the secure mode, and launch the user interface in a non-secure mode (HTTP), you must follow this procedure.

Procedure

Step 1 Log in to the Shell Admin.

Step 2 Enable the shell admin option 28--Enable/Disable HTTP. For more information, see *Enabling HTTP Access* section in the Cisco UCS Director Shell Guide, Release 6.9.

Step 3 Restart the services.

Step 4 Launch the user interface and log in to the system.

You can now log into the system in the non-secure mode using the following URL format:

http://<IP-Address>:8080 or http://<IP-Address>

You can launch the user interface in both, secure and non-secure modes.

Initial Login

Starting with Cisco UCS Director Release 6.9(2.0), the 'root' access is disabled and 'ucsdadmin' access is enabled by default. You must log in to Cisco UCS Director using 'ucsdadmin' as the login ID and password.

When you access the Cisco UCS Director using the hostname or IP address for the first time, you will be prompted to change your password according to the password policy. However, you cannot save the new password information unless you have also reset the default SSH password for root and shelladmin users.

To reset these passwords, connect to Cisco UCS Director using SSH and perform the password reset. After you reset the SSH root and shelladmin passwords, the **Save** button on the GUI screen is enabled.

For more information, see 'Managing ucsdadmin Access' section in the Cisco UCS Director Shell Guide, Release 6.9.



Important We recommend you to access the Cisco UCS Director using 'ucsdadmin' account. However, you can also perform the necessary operations using 'root' account. If you want to access the Cisco UCS Director using 'root' account, you must enable the 'root' account as it is disabled by default. For more information, see 'Enabling root Access' section in the Cisco UCS Director Shell Guide, Release 6.9.



Note We recommend that you delete the startup admin account after you create the first admin account. To access the End User Portal, you must have a valid email address.

Generating a Self-Signed Certificate

Prior versions of Cisco UCS Director required a Cisco-signed SSL certificate. Cisco UCS Director now requires a user-signed certificate instead of a Cisco-signed certificate. After installing or upgrading Cisco UCS Director, if the SSL certificate in the system is identified as a Cisco-signed certificate, you will be prompted post login to generate a self-signed certificate. After you generate the self-signed certificate, the Tomcat service is restarted to associate with the new certificate. After the Tomcat service is restarted, you are prompted to re-login to the user interface.



Note Do not use this self-signed certificate for the Device Connector.

To generate the self-signed certificate, do the following:

Procedure

Step 1 Log into the Cisco UCS Director user interface.

Step 2 In the **Generate Self-Signed Certificate** screen, complete the required fields, including the following:

Field	Description
Local Domain field	Enter the domain name. For example, cisco.com.
Certificate Validity (in days) field	Enter the number of days that you want the self-signed certificate to be valid. For example, 1825. We recommend that you enter a number between 1825 days (5 years) and 5475 days (15 years).
Keystore Password field	Enter the Java KeyStore (JKS) password to generate the self-signed certificate. The Java KeyStore (JKS) file is a repository for certificates used by the Tomcat service, and is password protected. Enter this password for this field.
Confirm Keystore Password field	Confirm the Java KeyStore (JKS) password to generate the self-signed certificate.

Step 3 Click **Save**.

Initial System Setup



Note When **Skip** is selected, the optional steps will be bypassed and the default or existing settings for the particular screen will be retained automatically.

Although the Guided Setup wizard allows you to uncheck and skip steps, the recommended approach is to perform all steps in the process.

Procedure

Step 1 Log in to Cisco UCS Director.

Step 2 Choose **Administration** > **Guided Setup**.

Step 3 On the **Guided Setup** page, double-click **Initial System Configuration**.

Step 4 Read the information given in the **Overview** page to know the prerequisites and sequence of steps.

Step 5 Click **Next**.

Step 6 On the **License** screen, perform one of the following to apply the license:

- If you want to upload a license file, drag and drop it into the license upload area, or click the **Select a File** button, choose the license file, and then click **Open**.
- Select the **Enter License Text** check box, enter the license text in the **License Text** field, and click **Next**.

Note

If you have uploaded license file already according to the procedure given in Updating the License section, click **Skip**.

Step 7 After the license upload is complete, click **Next**.

Step 8 From the **Language** drop-down list, choose your preferred language.

Note
After completing all the tasks in the wizard, you must log out and log back into the system for the locale changes to take effect.

Step 9 Click **Next**.

Step 10 On the **DNS Server** screen, enter the IP address of one or more DNS servers.

Step 11 Click **Next**.

Step 12 On the **Mail Server** screen, configure the following mail server settings. This configuration allows Cisco UCS Director to send email notifications to administrators and users.

- **SMTP Server**—Hostname or IP address of the outgoing mail server used to send emails.
- **SMTP Port**—Port number used by the SMTP server for sending emails.
- **Outgoing Email Address**—Email address that appears as the sender in outgoing system-generated emails.
- **System IP Address**—IP address of the system that sends email notifications. This may be used by the mail server for identification or access control.
- **User**—Username required to authenticate with the SMTP server.
- **Password**—Password associated with the SMTP username for authentication.
- **Send a Test Email**—When selected, sends a test email using the configured SMTP settings to verify that the email configuration is working correctly.
- **Test Email Address**—Recipient email address for the test email. This field appears only when the **Send a Test Email** check box is selected.

Note
Consider naming the outgoing email address with Cisco UCS Director nomenclature so that administrators and users can easily identify the source of email messages.

Step 13 On the **Email Address** screen, enter your email address in the **Administrator Email Address** field to receive notification and approval messages from the system.

Step 14 Click **Next**.

Step 15 On the **NTP Servers** field, enter the IP address of one or more Network Time Protocol (NTP) servers, separated by commas.
The following warning message is displayed:

```
It is strongly recommended to configure NTP authentication to ensure that the system time
is synchronized only with trusted, legitimate NTP servers. Use the Shelladmin option Time
Sync to configure NTP authentication.
```

Note
5Cisco UCS Director provides a symmetric key-based authentication mechanism for time synchronization with the NTP server, preventing modified, fake, or redirected packets from being accepted.

Step 16 Click **Next**.

Step 17 On the **Summary** screen, review the summary and status for each step you performed in the wizard. Navigate to the different Initial System Configuration options and configure the settings as needed.

Step 18 Click **Next**.

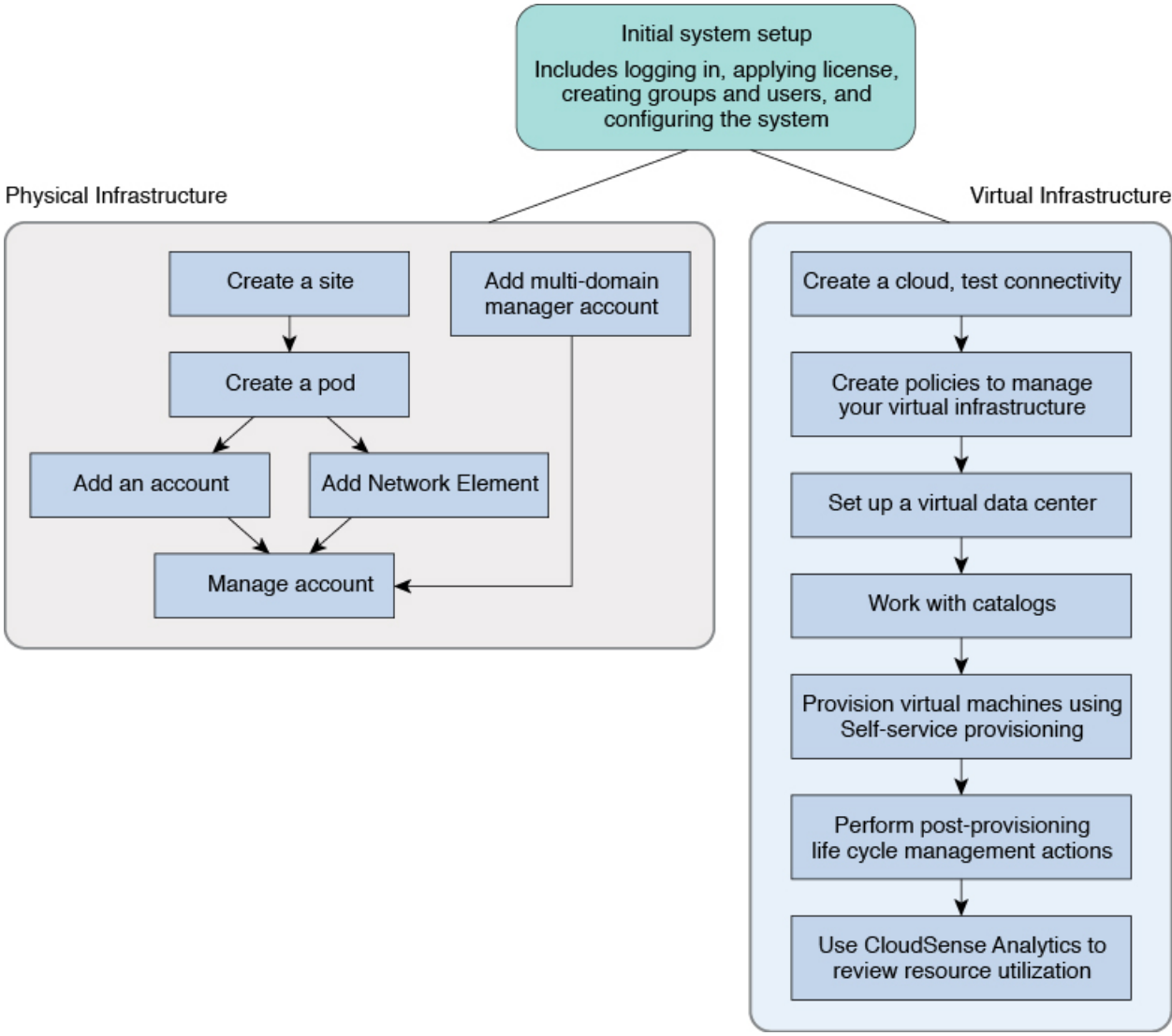
Step 19 On the Wizard selection screen, click the **Launch** button to select the **FlexPod** wizard or **Pod Discovery** wizard, and then proceed further based on the selection of wizard.

Step 20 Click **Close** to save the configurations.

Recommended Order of System Setup

The following figure illustrates the workflow to set up your environment using Cisco UCS Director:

Figure 1: Sample Workflow to Set up Your Environment



The following table describes the chapters available in this book using which you can complete setting up your environment.

Name	Chapter	Description
Initial set up	2, 3, 4 and 5	Describes how to apply a license, set up the Admin profile, create groups, and create users. You will learn how to access language support, apply portal customization, and system settings
Physical Infrastructure	6	Describes how to optionally add a pod and physical account, add network elements, test the connections, and verify account discovery. **Note** You can create the virtual infrastructure before the physical infrastructure if you want.

Name	Chapter	Description
Virtual Infrastructure	7	Describes how to create a cloud, verify cloud discovery and connectivity, test the connections, and view vCenter plug ins.
Policies	8	Describes how to create and manage computing policies, storage policies, network policies, and system policies. You will learn how to add OS licenses for Microsoft Windows catalogs.
Virtual Data Centers	9	Describes how to set up VDCs to manage specific environments for groups. policies, and cost models, and how resource limits are configured and managed at the VDC level.
Catalogs	10	Describes how to set up catalog items, attach groups with access to a catalog, and publish catalog items.
Self-Service Provisioning	11	Describes how you can create and manage provisioning service requests.
Multi-Disk Provisioning	12	Describes how to configure VM disk provisioning on a preferred single datastore or multiple datastores. It also provides instructions on how to configure individual disk policies for each additional disk in a template.
Chargeback	13	Describes how to create chargeback summary reports, detailed reports, and resource accounting reports. It shows how cost models are defined and assigned to policies within departments and organizations.
Cloud Management	14	Describes how you can get complete cloud visibility, monitor resource usage, and manage the cloud stack—clouds, clusters, host servers, and virtual machines.
Life Cycles	15	Describes how to perform post provisioning life cycle management actions on VMs, such as VM power management, VM resizing, VM snapshot management, and other VM actions.
CloudSense	16	Describes the analytical reports about the underlying physical and virtual infrastructure that Cisco UCS Director can generate.

Configuring the Host Name for Cisco UCS Director

If you changed the default host name of the appliance of Cisco UCS Director using the command prompt, then you must follow this procedure to ensure that the name is updated in the `/etc/hosts` file.

Procedure

Step 1 Log in to Cisco UCS Director as 'ucsdadmin' using your SSH terminal client.

Step 2 Execute the following command to obtain write permission for the `hosts` file.

```
sudo chmod o+w /etc/hosts
```

Step 3 Edit the `/etc/hosts` file to update the new host name.

In a single node environment, you must update the file in the following format:

```
vi /etc/hosts
198.51.100.1 new_hostname
```

In a multi-node environment, if the host names of other nodes are changed, then you must update the IP address and the new host name on the primary node, service nodes and database nodes. For example:

```
vi /etc/hosts
198.51.100.1 new_hostname
Ex:
198.51.100.2 UCSD_Primary
198.51.100.3 UCSD_Service
198.51.100.4 UCSD_Inv_DB
198.51.100.5 UCSD_Mon_DB
```

Step 4 Restart the appliance services.

Working with Ciphers

As an administrator in Cisco UCS Director, you have the capability to enable or disable ciphers from the property file. In the event that you enable a cipher with a potential security risk, a warning message is logged in the Cisco UCS Director log file. By default, all ciphers that pose a risk are disabled. You can configure specific ciphers from the `defaultEnabledCipherSuites.properties` file, located in the `/opt/infra/inframgr` folder. For more information, see Editing Cipher Usage, on page 23.

In addition, you can change the preference order of the standard set of ciphers, based on your system requirements. By default, the standard ciphers are listed according to the preference order.

Editing Cipher Usage

CipherSuites are maintained in the `defaultEnabledCipherSuites.properties` file. You can edit the list of ciphers in this file, based on the application requirements for your network.

We recommend that you always use the standard ciphers and not enable any broken or risky ciphers for your application.

Procedure

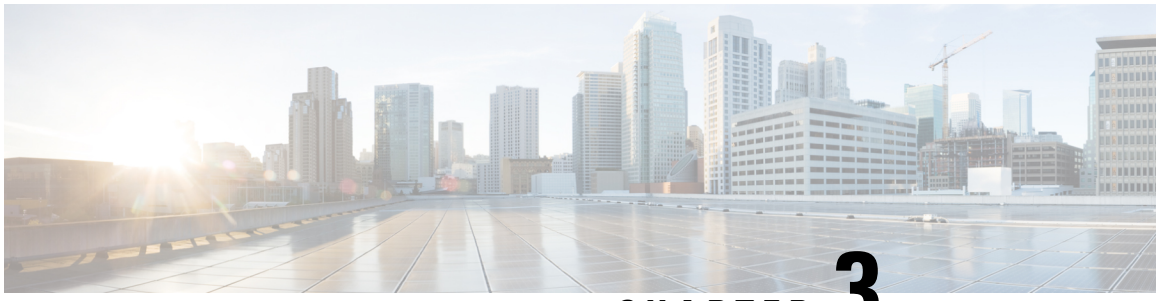
Step 1 Open the `defaultEnabledCipherSuites.properties` file.

It is available in the `opt/infra/inframgr/` directory.

Step 2 To use a broken cipher, locate the cipher in the file, and uncomment it.

Step 3 Save the file.

Step 4 Restart the service.



CHAPTER 3

Managing Users and Groups

This chapter contains the following sections:

- User Roles, on page 25
- Adding a User Role, on page 27
- Adding Users, on page 28
- Modifying Users, on page 30
- Deleting Users, on page 30
- Viewing User Management Activities in Syslog Server, on page 31
- Managing User Types, on page 31
- Default User Permissions, on page 31
- Managing User Account Status, on page 52
- MSP Administrator Role, on page 54
- Managing Groups, on page 55
- Configuring the Administration Profile, on page 66
- Managing User Access Profiles, on page 70
- Authentication and Cisco Identity Services Engine (Cisco ISE), on page 94
- Branding for Customer Organizations, on page 98
- Branding User Groups, on page 99
- Branding Customer Organizations, on page 100
- Login Page Branding, on page 101

User Roles

Cisco UCS Director supports the following user roles:

- All Policy Admin
- Billing Admin
- Computing Admin
- Group Admin—An end user with the privilege of adding users. This user can use the End User Portal.
- IS Admin
- MSP Admin

- Network Admin
- Operator
- Service End User—This user can only view and use the End User Portal.
- Storage Admin
- System Admin

These user roles are system-defined and available in Cisco UCS Director by default. You can determine if a role is available in the system by default, if the **Default Role** column in the **Users** page is marked with **Yes**.



Note As an administrator in Cisco UCS Director, you can assign users to system-provided user roles or to custom-defined user roles. In addition, at a later point in time, you can view information on the role that a user is assigned to. For more information, see Viewing User Role Information.

As an administrator in the system, you can perform the following tasks with user roles:

- Create a custom user role in the system, and create user accounts with this role or assign the role to existing users.

  When you create a new user role, you can specify if the role is that of an administrator or an end user. For more information on creating a user role, see Adding a User Role, on page 27. For information on creating user accounts for a role, see Adding Users, on page 105.

- Modify existing user roles, including default roles, to change menu settings and read/write permissions for users associated with that role.

  The procedure to modify menu settings and permissions for a role is the same as the procedure to add a user role.

Defining Permissions to Perform VM Management Tasks to Users

Previously, user permissions for VM management tasks could only be created by defining them in an end-user self-service policy. As an administrator in the system, you can now map permissions to perform VM management tasks to any user role. Users that are mapped to the given role can complete the selected VM management related tasks. However, to assign VM management tasks to end users using the end-user self service policy, you must first disable all VM management actions for this user role, and then enable all other management tasks.

For any user in the system, the capability to perform VM management tasks is determined by the following:

- The permissions assigned to the user role that the user is mapped to
- The end user self-service policy that is mapped to the VDC.

If you have upgraded to the current release, then the permissions to perform VM management tasks is retained in the end user self service policy that was created with the previous release version. However, the permissions that you defined or set for the user role after upgrading to the current release, takes precedence.

Note You can provide permissions to perform VM management tasks to other administrators, such as MSP Admin or Group Admin, by defining them in the user role only.

Adding a User Role

You can create any number of user roles in Cisco UCS Director and define the menu settings for the users created with these roles.

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **User Roles**.

Step 3 Click **Add**.

Step 4 In the **Add User Role** screen, complete the required fields, including the following:

Name	Description
User Role field	Name of the user role.
Role Type drop-down list	Choose the type of role that you are adding. It can be one of the following: • **Admin** • **End user**
Description field	The description of the role being added.
Deny Role List	Click **Select** to view a list of user roles in the **Deny Role List** screen. Check the roles that you want to deny for users created with this role and click **Select**. For example, as an administrator, you are creating a new group admin role in the system using the clone feature, and this group admin role must include the capability to create users with privileges higher than the group admin role. However, by default, the Group Admin role does not allow creating users with privilege higher than the group admin. So in this situation, as the administrator, you will need to select the default group admin role in the deny list.

Step 5 Click **Next**.

Step 6 In the **Menu Settings** pane, check the menu options that will be visible to users who are defined in this role.

Step 7 Click **Next**.

Step 8 In the **User Permissions** pane, choose the read or write permissions associated with various available user tasks.

Step 9 Click **Submit**.

What to do next

Create a user account with this role type.

Adding Users

Before you begin

Ensure that you have created a group before you add a user to it.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **Users**.

Step 3 Click **Add**.

Step 4 On the **Add User** screen, complete the required fields:

Field Name	Description
User Role drop-down list	Choose the role type for the user. **All Policy Admin** is selected by default. **Note** This drop-down list displays all the available user roles in Cisco UCS Director. In addition to the user roles available by default, you can also create additional user roles. For more information on creating user roles, see Adding a User Role, on page 27.
User Group drop-down list	This field appears when you select **Service End-User** or **Group Admin** from the **User Role** drop-down list. Select an existing group from the drop-down list. If you want to add a new group to the drop-down list, click the **Add** icon and proceed further. For more information on how to create a user group, see Creating a User Group.
Login Name field	Enter the login name of the user. The login name can contain uppercase letters (A–Z), lowercase letters (a–z), and digits (0–9).

Field Name	Description
Password field	Enter the password that meets the following requirements: • Upper case characters (A-Z) • Lower case characters (a-z) • Numbers (0-9) **Note** If Lightweight Directory Access Protocol (LDAP) authentication is configured for the user, the password is validated only at the LDAP server, and not at the local server.
Confirm Password field	Enter the password again for confirmation.
User Contact Email field	The email address of the user.
First Name field	First name of the user.
Last Name field	Last name of the user.
Phone field	Enter the phone number of the user.
Address field	The office address of the user.
Set user disable date check box	Check this check box to specify the date and time when the user account is disabled. After the configured disable time is reached, the user cannot log in to the system. A week prior to the specified date, an email message stating that the account will be disabled is sent to the user. On the specified date and time, the user account is disabled automatically. If the user is logged in to the system on the date specified, then the login session is terminated automatically.
Disable Date field	This field appears when you select the **Set user disable date** check box. Click the **Calendar** icon and the associated drop-down list to specify the date and time when the user account must be disabled.
Locale drop-down list	Choose a preferred language for the user. The language is set to English (United States) by default. When the user logs in, the user interface is displayed in the language you selected.

Step 5 Click **Add**.

What to do next

Click a row with a user and click **Manage Profiles**, to optionally assign multiple roles for that user.

Modifying Users

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **Users**.

Step 3 Right-click the user, and select **Edit**.

Step 4 On the **Edit User** page, modify the required fields. For more information on fields related to user account, see Adding Users.

Note
You cannot edit **User Role** field for **System Admin** user. You cannot edit **Login Name** field for any user.

Step 5 Click **Save**.

Deleting Users



Important Before deleting an user, consider the impact of that user in the management of Cisco UCS Director.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **Users**.

Step 3 Right-click the user, and click **Delete**.
A deletion confirmation message is displayed.

Step 4 Click **Delete**.

Viewing User Management Activities in Syslog Server

When you perform user management activities, such as User account creation, modification, and deletion performed in Cisco UCS Director and external identity management systems such as Active Directory and Cisco Identity Services Engine, a corresponding message is generated and sent to the configured Syslog servers. You can log in to the Syslog servers to view messages and other details related to user management activities.

Managing User Types

As the system administrator, you have full privileges to manage Cisco UCS Director, including adding users, viewing users and user permissions, and modifying individual user read/write permissions for different system components.

Most users access the Administrative portal when they log in.

Default User Permissions

Each admin user has a set of permissions to access Cisco UCS Director. The types of user permissions are as follows:

- Read—An admin user with Read permission has the ability to only read a file.
- Write—An admin user with Write permission has the ability to read, write, and modify a file. This permission includes the ability to delete or rename files.
- Read/Write—An admin user with Read/Write permission has the ability to read and write a file.

User Roles and Permissions

The following table shows a list of the permissions that are mapped to each user role:

Permission	All Policy Admin	Billing Admin	Computing Admin	Group Admin	IS Admin	MSP Admin	Network Admin	Operator	Service End User	Storage Admin
Virtual Computing	Read		Read	Read / Write	Read	Write	Read	Read	Read / Write	Read
VM Label	Write		Write	Write	Write	Write	Write	Write	Write	Write
Assign VM to vDC	Write				Write			Write		
Virtual Storage	Read		Read		Read		Read	Read		Read

Permission	All Policy Admin	Billing Admin	Computing Admin	Group Admin	IS Admin	MSP Admin	Network Admin	Operator	Service End User	Storage Admin
Virtual Network	Read		Read		Read		Read	Read		Read
Physical Computing	Read / Write		Read / Write		Read		Read	Read	Read	Read
Physical Storage	Read / Write		Read	Read / Write	Read		Read	Read	Read	Read / Write
Physical Network	Read / Write		Read		Read		Read / Write	Read / Write		Read
Group Service Request	Read / Write	Read	Read	Read / Write	Read	Read / Write	Read	Read / Write	Read / Write	Read
Create Service Request	Write			Write		Write		Write	Write	
Approver Service Request	Read / Write		Read / Write	Read /Write	Read / Write	Read / Write	Read / Write	Read	Read / Write	Read / Write
Budgeting	Read	Read / Write	Read		Read	Read / Write	Read	Read		Read
Resource Accouting	Read	Read	Read	Read	Read	Read	Read	Read	Read	Read
Chargeback	Read	Read	Read	Read	Read	Read	Read	Read	Read	Read
System Admin	Read		Read		Read		Read	Read		Read
Users and Groups	Read		Read		Read		Read	Read		Read
Virtual Accounts	Read		Read		Read		Read	Read		Read
Catalogs	Read		Read	Read	Read	Read	Read	Read	Read	Read
vDC	Read		Read	Read	Read / Write	Read	Read	Read	Read	Read
Computing Policy	Read / Write		Read / Write		Read		Read	Read		Read
Storage Policy	Read / Write		Read		Read		Read	Read		Read / Write

Permission	All Policy Admin	Billing Admin	Computing Admin	Group Admin	IS Admin	MSP Admin	Network Admin	Operator	Service End User	Storage Admin
Network Policy	Read / Write		Read		Read		Read / Write	Read		Read
Deployment Policy	Write		Read		Read / Write		Read	Read		Read
Service Delivery	Read / Write		Read		Read / Write		Read	Read		Read
Resource Limit Report	Read	Read	Read	Read	Read	Read	Read	Read	Read	Read
Group Users	Read		Read	Read / Write	Read	Read / Write	Read	Read		Read
Cloudsense Reports	Read	Read / Write	Read	Read / Write	Read		Read	Read	Read	Read
Cloudsense Assessment Reports	Read	Read / Write	Read				Read			Read
Orchestration	Read / Write		Read / Write		Read / Write		Read / Write			Read / Write
Discovery	Read	Read	Read		Write		Read / Write			Read / Write
Open Automation Modules										
CS Shared Reports				Read / Write		Read			Read	
CS Shared Assessments				Read / Write						
Remote VM Access										
Mobile Access Settings										
End User Chargeback				Read		Read			Read	

Permission	All Policy Admin	Billing Admin	Computing Admin	Group Admin	IS Admin	MSP Admin	Network Admin	Operator	Service End User	Storage Admin
UCSD Cluster										
Resource Groups			Read / Write		Read / Write		Read / Write			Read / Write
Tag Library			Read / Write		Read / Write		Read / Write			Read / Write
Allow Deployability Assessment	True	True	True	True	True	True	True	True	True	True
Write CloupiaScript	Read / Write	Read / Write	Read / Write	Read / Write	Read / Write	Read / Write	Read / Write	Read / Write	Read / Write	Read / Write
Execute CloupiaScript	Read / Write	Read / Write	Read / Write	Read / Write	Read / Write	Read / Write	Read / Write	Read / Write	Read / Write	Read / Write

Permissions for Server Management

In prior releases, to manage physical servers, Cisco UCS Director only provided the following options:

- **Read Physical Computing**
- **Write Physical Computing**

As an administrator, if you enabled the write permission, then users had the capability to manage all Cisco UCS physical servers in the environment. With this release, within the **Write Physical Computing** permission, the following new categories of permissions have been introduced:

- **Physical Server Management**
- **Other Physical Compute Management**

Enabling **Physical Server Management** implies enabling management of Cisco UCS Servers only. This category includes the following actions:

- Power Management (Power On and Power Off)
- Group Management (Assign Group and Unassign Group)
- Inventory Management
- Server Management
- Server Access

If you enable these tasks for users, then those users can view these actions or tasks in the portal. However, for end users, even if you enable these tasks, they can only perform the following tasks on Cisco UCS servers:

- Power on and off servers
- Associate and disassociate groups
- KVM console

Enabling **Other Physical Compute Management** implies enabling management tasks for other UCS servers in the environment. Uses from whom this permission is enabled can perform tasks such as working with service profiles or VLANs.

All Policy Admin

The following table shows a list of operations that an **All Policy** admin can perform:

Operations	Permissions	
	Read	**Write**
Virtual Computing	Yes	
VM Label		Yes
Assign VM to vDC		Yes
Virtual Storage	Yes	
Virtual Network	Yes	
Physical Computing	Yes	Yes
Physical Storage	Yes	Yes
Physical Network	Yes	Yes
Group Service Request	Yes	Yes
Create Service Request		Yes
Approver Service Request	Yes	Yes
Budgeting	Yes	
Resource Accounting	Yes	
Chargeback	Yes	
System Admin	Yes	
Users and Groups	Yes	
Virtual Accounts	Yes	
Catalogs	Yes	

Operations	Permissions	
vDC	Yes	
Computing Policy	Yes	Yes
Storage Policy	Yes	Yes
Deployment Policy		Yes
Network Policy	Yes	Yes
Service Delivery	Yes	Yes
Resource Limit Report	Yes	
Group Users	Yes	
Cloudsense Reports	Yes	
Cloudsense Assessment Reports	Yes	
Orchestration	Yes	Yes
Discovery	Yes	
Open Automation Modules		
CS Shared Reports		
CS Shared Assessments		
Remote VM Access		
Mobile Access Settings		
End User Chargeback		
Write Resource Accounting		
UCSD Cluster		
Resource Groups		
Tag Library		
Allow Deployability Assessment		True

Billing Admin

The following table show a list of operations that a Billing admin can perform:

Operation	Permission	
	Read	**Write**
Virtual Computing		
VM Label		
Assign VM to vDC		
Virtual Storage		
Virtual Network		
Physical Computing		
Physical Storage		
Physical Network		
Group Service Request	Yes	
Approver Service Request		
Budgeting	Yes	Yes
Resource Accounting	Yes	
Chargeback	Yes	
System Admin		
Users and Groups		
Virtual Accounts		
Catalogs		
vDC		
Computing Policy		
Storage Policy		
Deployment Policy		
Network Policy		
Service Delivery		
Resource Limit Report	Yes	
Group Users		

Operation	Permission	
Cloudsense Reports	Yes	Yes
Cloudsense Assessment Reports	Yes	Yes
Orchestration		
Discovery	Yes	
Open Automation Modules		
CS Shared Reports		
CS Shared Assessments		
Remote VM Access		
Mobile Access Settings		
End User Chargeback		
Write Resource Accounting		Yes
UCSD Cluster		
Resource Groups		
Tag Library		
Allow Deployability Assessment		True

Computing Admin

The following table shows a list of operations that a **Computing** admin can perform:

Operation	Permission	
	Read	**Write**
Virtual Computing	Yes	
VM Label		Yes
Assign VM to vDC		
Virtual Storage	Yes	
Virtual Network	Yes	
Physical Computing	Yes	Yes
Physical Storage	Yes	

Operation	Permission	
Physical Network	Yes	
Group Service Request	Yes	
Approver Service Request	Yes	Yes
Budgeting	Yes	
Resource Accounting	Yes	
Chargeback	Yes	
System Admin	Yes	
Users and Groups	Yes	
Virtual Accounts	Yes	
Catalogs	Yes	
vDC	Yes	
Computing Policy	Yes	Yes
Storage Policy	Yes	
Deployment Policy	Yes	
Network Policy	Yes	
Service Delivery	Yes	
Resource Limit Report	Yes	
Group Users	Yes	
Cloudsense Reports	Yes	
Cloudsense Assessment Reports	Yes	
Orchestration	Yes	Yes
Discovery	Yes	
Open Automation Modules		
CS Shared Reports		
CS Shared Assessments		

Operation	Permission	
Remote VM Access		
Mobile Access Settings		
End User Chargeback		
Write Resource Accounting		
UCSD Cluster		
Resource Groups	Yes	Yes
Tag Library	Yes	Yes
Allow Deployability Assessment		True

Group Admin

The following table shows a list of operations that a **Group** admin can perform:

Task	Permission	
	Read	**Write**
Virtual Computing	Yes	Yes
VM Label		Yes
Assign VM to vDC		
Virtual Storage		
Virtual Network		
Physical Computing		
Physical Storage	Yes	Yes
Physical Network		
Group Service Request	Yes	Yes
Create Service Request		Yes
Approver Service Request	Yes	Yes
Budgeting		
Resource Accounting	Yes	

Task	Permission	
Chargeback	Yes	
System Admin		
Users and Groups		
Virtual Accounts		
Catalogs	Yes	
vDC	Yes	
Computing Policy		
Storage Policy		
Deployment Policy		
Network Policy		
Service Delivery		
Resource Limit Report	Yes	
Group Users	Yes	Yes
Cloudsense Reports	Yes	Yes
Cloudsense Assessment Reports		
Orchestration		
Discovery		
Open Automation Modules		
CS Shared Reports	Yes	Yes
CS Shared Assessments		
Remote VM Access		
Mobile Access Settings		
End User Chargeback	Yes	
Write Resource Accounting		
UCSD Cluster		
Resource Groups		
Tag Library		

Task	Permission	
Allow Deployability Assessment		True

IS Admin

The following table shows a list of operations that an **IS** admin can perform:

Task	Permission	
	Read	**Write**
Virtual Computing	Yes	
VM Label		Yes
Assign VM to vDC		Yes
Virtual Storage	Yes	
Virtual Network	Yes	
Physical Computing	Yes	
Physical Storage	Yes	
Physical Network	Yes	
Group Service Request	Yes	
Approver Service Request	Yes	Yes
Budgeting	Yes	
Resource Accounting	Yes	
Chargeback	Yes	
System Admin	Yes	
Users and Groups	Yes	
Virtual Accounts	Yes	
Catalogs	Yes	
vDC	Yes	Yes
Computing Policy	Yes	
Storage Policy	Yes	
Deployment Policy	Yes	Yes
Network Policy	Yes	

Task	Permission	
Service Delivery	Yes	Yes
Resource Limit Report	Yes	
Group Users	Yes	
Cloudsense Reports	Yes	
Cloudsense Assessment Reports	Yes	
Orchestration	Yes	Yes
Discovery		Yes
Open Automation Modules		
CS Shared Reports		
CS Shared Assessments		
Remote VM Access		
Mobile Access Settings		
End User Chargeback		
Write Resource Accounting		
UCSD Cluster		
Resource Groups	Yes	Yes
Tag Library	Yes	Yes
Allow Deployability Assessment		True

Network Admin

The following table shows a list of operations that a **Network** admin can perform:

Task	Permission	
	Read	**Write**
Virtual Computing	Yes	
VM Label		Yes
Assign VM to vDC		
Virtual Storage	Yes	

Task	Permission	
Virtual Network	Yes	
Physical Computing	Yes	
Physical Storage	Yes	
Physical Network	Yes	Yes
Group Service Request	Yes	
Approver Service Request	Yes	Yes
Budgeting	Yes	
Resource Accounting	Yes	
Chargeback	Yes	
System Admin	Yes	
Users and Groups	Yes	
Virtual Accounts	Yes	
Catalogs	Yes	
vDC	Yes	
Computing Policy	Yes	
Storage Policy	Yes	
Deployment Policy	Yes	
Network Policy	Yes	Yes
Service Delivery	Yes	
Resource Limit Report	Yes	
Group Users	Yes	
Cloudsense Reports	Yes	
Cloudsense Assessment Reports	Yes	
Orchestration	Yes	Yes
Discovery	Yes	Yes
Open Automation Modules		
CS Shared Reports		

Task	Permission	
CS Shared Assessments		
Remote VM Access		
Mobile Access Settings		
End User Chargeback		
Write Resource Accounting		
UCSD Cluster		
Resource Groups	Yes	Yes
Tag Library	Yes	Yes
Allow Deployability Assessment		True

Operator

The following table shows a list of operations that an **Operator** can perform:

Task	Permission	
	Read	**Write**
Virtual Computing	Yes	
VM Label		Yes
Assign VM to vDC		Yes
Virtual Storage	Yes	
Virtual Network	Yes	
Physical Computing	Yes	
Physical Storage	Yes	
Physical Network	Yes	
Group Service Request	Yes	Yes
Create Service Request		Yes
Approver Service Request	Yes	Yes
Budgeting	Yes	
Resource Accounting	Yes	
Chargeback	Yes	

Task	Permission	
System Admin	Yes	
Users and Groups	Yes	
Virtual Accounts	Yes	
Catalogs	Yes	
vDC	Yes	
Computing Policy	Yes	
Storage Policy	Yes	
Deployment Policy	Yes	
Network Policy	Yes	
Service Delivery	Yes	
Resource Limit Report	Yes	
Group Users	Yes	
Cloudsense Reports	Yes	
Cloudsense Assessment Reports	Yes	
Orchestration		
Discovery		
Open Automation Modules		
CS Shared Reports		
CS Shared Assessments		
Remote VM Access		
Mobile Access Settings		
End User Chargeback		
Write Resource Accounting		
UCSD Cluster		
Resource Groups		
Tag Library		
Allow Deployability Assessment		True

Service End User

The following table shows a list of operations that a **Service End User** can perform:

Task	Permission	
	Read	**Write**
Virtual Computing	Yes	Yes
VM Label		Yes
Assign VM to vDC		
Virtual Storage		
Virtual Network		
Physical Computing	Yes	
Physical Storage	Yes	
Physical Network		
Group Service Request	Yes	Yes
Create Service Request		Yes
Approver Service Request	Yes	Yes
Budgeting		
Resource Accounting	Yes	
Chargeback	Yes	
System Admin		
Users and Groups		
Virtual Accounts		
Catalogs	Yes	
vDC	Yes	
Computing Policy		
Storage Policy		
Deployment Policy		
Network Policy		
Service Delivery		
Resource Limit Report	Yes	

Task	Permission	
Group Users		
Cloudsense Reports	Yes	
Cloudsense Assessment Reports		
Orchestration		
Discovery		
Open Automation Modules		
CS Shared Reports	Yes	
CS Shared Assessments		
Remote VM Access		
Mobile Access Settings		
End User Chargeback	Yes	
Write Resource Accounting		
UCSD Cluster		
Resource Groups		
Tag Library		
Allow Deployability Assessment		True

Storage Admin

The following table shows a list of operations that a **Storage** admin can perform:

Task	Permission	
	Read	**Write**
Virtual Computing	Yes	
VM Label		Yes
Assign VM to vDC		
Virtual Storage	Yes	
Virtual Network	Yes	
Physical Computing	Yes	

Task	Permission	
Physical Storage	Yes	Yes
Physical Network	Yes	
Group Service Request	Yes	
Approver Service Request	Yes	Yes
Budgeting	Yes	
Resource Accounting	Yes	
Chargeback	Yes	
System Admin	Yes	
Users and Groups	Yes	
Virtual Accounts	Yes	
Catalogs	Yes	
vDC	Yes	
Computing Policy	Yes	
Storage Policy	Yes	Yes
Deployment Policy	Yes	
Network Policy	Yes	
Service Delivery	Yes	
Resource Limit Report	Yes	
Group Users	Yes	
Cloudsense Reports	Yes	
Cloudsense Assessment Reports	Yes	
Orchestration	Yes	Yes
Discovery	Yes	Yes
Open Automation Modules		
CS Shared Reports		
CS Shared Assessments		
Remote VM Access		

Task	Permission	
Mobile Access Settings		
End User Chargeback		
Write Resource Accounting		
UCSD Cluster		
Resource Groups	Yes	Yes
Tag Library	Yes	Yes
Allow Deployability Assessment		True

Viewing User Role Information for Users

As an administrator in the system, you can assign users to system-provided user roles or to custom-defined user roles. You can view this information at a later point in time for all users in a group.

Procedure

Step 1 Choose **Organizations** > **Summary**.

Step 2 On the **Summary** page, choose the user group.

Step 3 Click **Users**.

From this page, you can view detailed information on the users that belong to the selected group. The **Access Level** column displays the roles, system-defined or custom-defined roles, that the users are assigned to. Optionally, you can choose **Administration** > **User and Groups** > **Users** to view all user information. If you are a group administrator, then to view this information, choose **Organizations** > **Users**.

If you are a group administrator, then this page displays the password expiry date and time for each user. This information is derived from the Password policy that is configured in the system. This page also graphically represents the password expiry status for each user. The column titled **Password Expiry Status** displays a green icon for passwords that have not yet expired, and a red icon for passwords that have expired.

Reviewing Recent Login History of Users

As an administrator in the system, you can review the login history for all users. The system records the following details for every login attempt:

- Login Name—The user name of the logged in user.
- Remote Address—The IP address of the system or the server that the user has logged in from.
- Client Detail—The browser information.

- Client Type—Information on whether the user logged in to the brower or the REST API.
- Authentication Status—Information on whether the login action resulted in success or failure.
- Comments—The cause for authentication failure.
- Accessed On—The date and time of the login activity for the user.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **All Users Login History**.

Step 3 Review the information displayed on the screen.

Configuring Session Limits for Users

You can configure the number of user interface sessions and REST API requests that users can initiate on the system.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **Session Management**.

Step 3 In the **Session Management** screen, complete the required fields, including the following:

Name	Description
Maximum Concurrent Sessions Per User field	The maximum number of concurrent GUI sessions that are supported for each user. Enter a number between 1 and 128. The default value is 16.
Maximum Concurrent REST API Requests Per User field	The maximum number of concurrent REST API requests that are supported for each user. Enter a number between 1 and 256. The default value is 128.

Step 4 Click **Submit**.

What to do next

When users initiate a GUI session or a REST API request to exceed the limit specified on this screen, an error message is displayed in the **System Messages** screen. In this scenario, either users should clear their sessions

and API requests, or as an administrator, you can use the Shell utility and clear the sessions and requests for a user. For more information, see *Cisco UCS Director Shell Guide*, Release 6.5.

Managing User Account Status

Cisco UCS Director provides you with the capability to enable and disable users in the system. When you disable a user record, the user cannot log in to the system, and cannot use the APIs. In addition, the disabled user record is no longer present in any of the **User** fields that are displayed while performing administrative actions, such as assigning VMs or port groups. However, the records of all system users, whether enabled or disabled, are listed in the **Users** tab. In this tab, view the **Status** column to see if a user account status is **Disabled** or **Enabled**.

You can disable a user in one of the following ways:

- At account creation, you can set a date for disabling the user. For more information, see Adding Users, on page 105.
- Disable a user from the **Users** page. For more information, see Disabling a User Account in Cisco UCS Director, on page 53.
- Disable all users in an MSP Organization or a Customer Organization. For more information, see Disabling User Accounts within a Group, on page 53.

Note After you disable a user account, you can re-enable the account at a later point.

Unassigning Resources From a User

Cisco UCS Director allows you to unassign resources from a user.

Note You can unassign resources from a user prior to disabling the user account in the system.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **Users**.

Step 3 Choose a user from the report, and click **View**.

Step 4 From the **User Details** screen, choose the resources you want to unassign from the user.

You can select multiple resources.

Step 5 Click **Unassign**.

Step 6 In the **Unassign Resource** screen, click **Unassign**.

Step 7 Click **OK**.

What to do next

You can assign this resource to another user in the system.

Disabling a User Account in Cisco UCS Director

Perform this procedure to disable a specific user account in Cisco UCS Director.

Procedure

Step 1 On the menu bar, choose **Administration** > **Users and Groups**.

Step 2 Click the **Users** tab.

Step 3 Choose the user account from the table.

You can choose multiple users.

Step 4 On the toolbar, choose **Disable**.

Step 5 In the **Disable User** dialog box, click **Disable**.

Step 6 Click **OK**.

If the user whose account that you disabled is currently logged in to the system through the graphical user interface or the API, then that user session is terminated immediately. The disabled user cannot log in to the application.

What to do next

You can choose to enable the user's account at a later point in time. To do so, return to the **Users** page, select the user and click **Enable**.

Disabling User Accounts within a Group

Perform this procedure to disable user accounts within an MSP organization or a customer organization.

Procedure

Step 1 On the menu bar, choose **Administration** > **Users and Groups**.

Step 2 Click the **MSP Organizations** tab or the **Customer Organizations** tab.

These tab names are only indicative. If you have enabled the **Service Provider Feature**, you have to specify the names of the organization at the first and second level. The names that you specify are displayed as tabs in the interface.

Step 3 Select a group from the table.

You can select multiple groups.

Step 4 Click **Disable Users**.

Step 5 In the **Disable Users** dialog box, click **Disable Users**.

Step 6 Click **OK**.

What to do next

You can enable all the user accounts in this group by returning to **MSP Organizations** tab or the **Customer Organizations** tab, selecting the group, and clicking **Enable Users**.

MSP Administrator Role

A Managed Service Provider (MSP) organization is a type of customer group in Cisco UCS Director. It can be considered as a parent organization in the system. Within this MSP organization, multiple sub-categories or child organizations can be grouped. For example, a company name such as 'Cisco Systems' would represent an MSP organization. Within this MSP organization, you can create multiple customer groups, such as HR, Finance, and Operations. These groups would be considered as customer groups within an MSP organization.

An administrator is required for each MSP in Cisco UCS Director. This administrator is referred to as the MSP Admin. This administrator manages the MSP organization and all the customer organizations within the MSP organization.

If you are a global administrator in Cisco UCS Director, following is the recommended sequence of steps to create an MSP organization and an MSP administrator:

1. Enable the Service Provider Feature in Cisco UCS Director. For more information, see Enabling the Service Provider Feature, on page 145.
2. Create the MSP organization. For more information, see Creating an MSP Organization, on page 57.
3. Create the customer groups within the MSP organization. For more information, see Creating a Customer Organization, on page 58.
4. Create a user account with MSP administrator role privileges in Cisco UCS Director. While creating this user account, you can also select the MSP organizations that this user can manage and you can create a new MSP organization. For information on creating a user account with a specific role, see Adding Users, on page 105.

   The role defines the menus and tabs that this user can view in Cisco UCS Director. Typically, an MSP administrator will require the following menus:

   - Organization
   - Policies
   - CloudSense

In addition to creating MSP organizations and MSP administrator roles, you can also brand these organizations with customized logos and application labels. For more information, see Branding Customer Organizations, on page 100.

Note Cisco UCS Director supports branding at the global level, MSP organization level, and customer organization level. However, the branding details visible to a user are limited by certain guidelines. For more information, see Branding for Customer Organizations, on page 98.

If you are an MSP administrator, then the following table lists the tasks that you can perform in Cisco UCS Director. It also lists sections in this guide where you can find procedural information.

Task	Link to the information in the guide
Create customer organizations to manage	Creating a Customer Organization, on page 58
Apply specific branding to customer organizations.	Branding Customer Organizations, on page 100
Create and manage policies to provision VMs	Managing Policies, on page 207
Use CloudSense Analytics to generate reports	Managing CloudSense Analytics, on page 425

Managing Groups

Creating a User Group

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **User Groups**.

Step 3 Click **Add**.

Step 4 On the **Add Group** screen, complete the following fields:

Field Name	Description
Name field	The name of the group or the customer organization. You can include special characters such as ( ). & - _ `~ $% ^ {}! '@
Description field	The description of the group or the customer organization, if required.
Code field	A shorter name or code name for the group. This name is used in VM and hostname templates.
Cost Center field	(Optional) The cost center name or number if required. This name or number represents a cost center that a group is associated with. This name can be used in a VMware System policy for the VM naming convention. For more information about using a cost center for naming conventions, see Managing Policies, on page 207.

Field Name	Description
Contact Email field	The email used to notify the group owner about the status of service requests and request approvals if necessary.
First Name field	The contact's first name.
Last Name field	The contact's last name.
Phone field	The contact's phone number.
Address field	The contact's address.
Group Share Policy drop-down list	Choose the group share policy for the users in this group. This drop-down list is populated only when you have created group share policies. For more information on creating this policy, see Creating a Group Share Policy, on page 218.
Allow Resource Assignment To Users check box	If checked, the users of this group can have resources assigned to them and can own these resources. Also, these users can view resources belonging to the group. However, the resources among these users cannot be shared.

Step 5 Click **Add**.

What to do next

Repeat this procedure if you want to add more groups. For each group that you add, you can edit resource limits, manage tags, and customize the logo and application labels.

Using the Global Dashlet Setup Option

This procedure describes how you can customize the number of dashlets that all end users in all groups can view in the End User Portal. In addition, you can customize the number of dashlets that end users in a specific group can view. For more information on customizing the dashlets for a specific group, see Configuring Dashlets, on page 117.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **Global Dashlet Setup**.

Step 3 In the **Dashlets Report** screen, click **Select**.

Step 4 In the **Dashlet Name** screen, uncheck the check boxes of the dashlets that should not be displayed for all end users of all groups in the system.

Step 5 Click **Select**.

Step 6 In the **Dashlets Report** screen, click **Submit**.

Creating an MSP Organization

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 Click **MSP Organizations**.

These tab names are only indicative. If you have enabled the **Service Provider Feature**, you must specify the names of the organization at the first and second level. The names that you specify are displayed as tabs in the interface.

Step 3 Click **Add**.

Step 4 In the **Add MSP Organizations** screen, complete the required fields, including the following:

Field Name	Description
Name field	The name of the MSP organization. You can include special characters such as ( ). & - _ `~ $% ^ {}! '
Description field	The description of the MSP organization, if necessary.
Code field	A shorter name or code name for the group. This name is used in VM and hostname templates.
Cost Center field	The cost center name or number if required. This name or number represents a cost center that a group is associated with. This name can be used in a VMware System policy for the VM naming convention. For more information about using a cost center for naming conventions, see Managing Policies, on page 207.
Contact Email field	The email used to notify the MSP administrator about the status of service requests and request approvals, if necessary.
First Name field	The contact's first name.
Last Name field	The contact's last name.
Phone field	The contact's phone number.
Address field	The contact's address.

Step 5 Click **Add**.

What to do next

For each MSP organization that you create, you can edit resource limits, manage tags, and customize the logo and application labels. You can also create customer organizations within each MSP organization.

Creating a Customer Organization

You can follow this procedure to create a customer organization within an MSP organization.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 Click **Customer Organizations**.

This tab name is only indicative. If you have enabled the **Service Provider Feature**, you must specify the names of the organization at the first and second level. Those names are displayed as tabs in the interface. If you have disabled the **Service Provider Feature**, then only the **Customer Organizations** tab is displayed.

Step 3 Click **Add**.

Step 4 In the **Add Group** screen, complete the required fields, including the following:

Field Name	Description
Name field	The name of the group or the customer organization. You can include special characters such as ( ). & - _ `~ $% ^ {}! '
Description field	The description of the group or the customer organization, if necessary.
MSP Group Name field	Select the MSP organization name from the drop-down list. This list includes all the groups that you can currently manage. For example, if you are a global administrator of the system, then this list displays all the organizations that you manage. But, if you are an MSP administrator, then this list displays only the organization that you have administrative privileges for.
Code field	A shorter name or code name for the group. This name is used in VM and hostname templates.
Cost Center field	(Optional) The cost center name or number if required. This name or number represents a cost center that a group is associated with. This name can be used in a VMware System policy for the VM naming convention. For more information about using a cost center for naming conventions, see Managing Policies, on page 207.
Contact Email field	The email used to notify the group owner about the status of service requests and request approvals, if necessary.
First Name field	The contact's first name.
Last Name field	The contact's last name.

Field Name	Description
Phone field	The contact's phone number.
Address field	The contact's address.
Group Share Policy drop-down list	Choose the group share policy for the users in this group. This drop-down list is populated only when you have created group share policies. For more information on creating this policy, see Creating a Group Share Policy, on page 218.
Allow Resource Assignment To Users check box	If checked, the users of this group can have resources assigned to them and can own these resources. Also, these users can view resources belonging to the group. However, the resources among these users cannot be shared.

Step 5 Click **Add**.

What to do next

Repeat this procedure to add more customer organizations. For each customer organization that you add, you can edit resource limits, manage tags, and customize the logo and application labels.

Password Policy

The password policy applies to all users and is enforced when you add a user or change the password for all user types. This policy enables the following password constraints:

- Password length
- Whether the previous password can be set as a new password
- Whether the new password can be the user's login password
- Minimum number of different character types a password must contain
- Whether certain regular expressions are disallowed in a password
- Number of previous passwords that can be remembered by the system
- Validity of the password
- Additional days allowed to login after a password has expired
- How many days in advance a warning message must be displayed before expiry of the password.

Starting with Cisco UCS Director Release 6.9(4.0), the default values for some parameters are changed to improve the password strength and enhance security. For more information, see the table below.

Table 6: Password Policy Settings Changes for Cisco UCS Director 6.9(4.0)

Parameters	Value for Cisco UCS Director releases earlier than 6.9(4.0)	Value for Cisco UCS Director 6.9(4.0)
Minimum Password Length	Default: 4	Default: 8
Minimum Character Classes	Default: 1	Default: 4
Disallow Login in Password	Default: Unchecked	Default: Checked
Disallow Previous Password	Default: Unchecked	Default: Checked
Previous Passwords Counts	1	3

Creating a Password Policy



Important Refer to the table for the recommended settings for some parameters specific to Cisco UCS Director 6.9(4.0).

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **Password Policy**.

Step 3 In the **Password Policy** screen, complete the required fields, including the following:

Name	Description
Minimum Password Length drop-down list	Choose the minimum number of characters for the password.
Maximum Password Length drop-down list	Choose the maximum number of characters for the password. **Note** The maximum length of a password can be up to 127 characters.
Minimum Character Classes drop-down list	Choose the minimum number of character classes, such as uppercase, lowercase, numbers, and special characters.
Disallow Login in Password check box	Check the check box to disallow passwords that are the same as the login password.
Disallow Previous Password check box	Check the check box to disallow the previous password from being used as the new password.
Previous Passwords Counts drop-down list	Choose the number of previous passwords that must be stored in the system.

Name	Description
Disallow Passwords that match Regular Expression field	The regular expressions (one per line) that are not allowed for passwords. For example,.*abc.* specifies that a given password cannot contain the string “abc”.
Password expiry (in days) field	Specify the number of days for which the password will remain active. By default, the value for this field is set to 180.
Warn Password expiry (in Days) drop-down list	Specify how many days in advance a warning message must be displayed before expiry of the password.
Grace Period for Password (in Days) drop-down list	Specify the number of days, after password expiration, that a user can use the password to log in to the system.

Step 4 Click **Submit**.

Group Budget Policy

Resources are accounted for by using the Chargeback feature. For resource usage by a group or customer organization, you associate the entity with a budget policy.

You can configure a group or customer organization with a budget watch, and configure a group or customer organization to stay within or exceed the provisioned budget.

Viewing and Editing a Group Budget Policy

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **User Groups**.

Step 3 Choose a group from the list.

Step 4 From the **More Actions** drop-down menu, click **Budget Policy**.

Step 5 In the **Budget Policy** screen, complete the required fields, including the following:

Name	Description
Enable Budget Watch check box	Check the check box to monitor the budget usage for the group. Uncheck the box to ignore all budget entries for this group.
Allow Over Budget check box	Check the check box to allow group members to exceed the provisioned budget. Uncheck the box to reject requests, once the budget is exhausted, until a new budget is added.

Step 6 Click **Save**.

Resource Limits

You can configure resource limits for a group, a customer organization, or a tenant, to manage resource utilization. You can specify limits for the following:

- Virtual resources
- Operating system resources
- Physical resources

Note Configuration of operating system resource and physical resource limits are not supported for public clouds.

Guidelines for Resource Limits with Service Provider Enabled

If you have enabled the Service Provider feature in Cisco UCS Director, keep in mind the following considerations while configuring resource limits:

- The limit set for the parent organization determines the limits that you can set for customer groups and containers within the parent organization.
- If you have not added resource limits to a specific customer group but have specified limits for containers within that group, you must consider the total resource limits before setting a limit for another customer group within the parent organization.
- The total number of resource limits configured for all customer groups and containers within those groups cannot exceed the resource limit set for the parent organization.
- If you do not add resource limits to a specific customer group but do specify resource limits for containers within that group, you must consider the total of all container resource limits before you set a limit for the parent organization.

For example, the parent organization, Tenant 1, includes three customer groups: Group A, Group B, and Group C. If you configure a resource limit of ten for Tenant 1, the cumulative resource limits specified for all customer groups within Tenant 1 must not exceed ten. The cumulative resource limits include resource limits applied to customer groups and containers.

Group A includes containers C1 and C2, and has a resource limit of 4 assigned to the customer group. Group B includes containers C3 and C4, and each of these containers has a resource limit of two. This configuration means that two is the maximum available resource limit you can configure for Group C and all its containers (the resource limit for Tenant 1, minus the total resource limits for Group A, Group, B, and containers C1, C2, C3, and C4).

Guidelines for Resource Limits with Service Provider Disabled

If you have disabled the Service Provider feature, there is only one parent organization. Therefore, if you set a resource limit for the parent organization, the total of the limits specified for all customer groups must not exceed the parent resource limit.

For example, the parent organization includes two customer groups: Group A and Group B. If you set a limit of ten for the parent organization and five for Group A. The resource limit that you set for Group B, must not exceed five (the resource limit for the parent organization minus the resource limit for Group A).

Viewing Resource Limits

Procedure

Step 1 Choose **Organizations** > **Summary**.

Step 2 On the **Summary** page, choose the user group.

Step 3 Click **Resource Limits** to view the current limit, usage, pending SR usage, and status of the resources for the selected group.

Editing Resource Limits

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 If you are editing a resource limit for an organization or a customer group, choose **Customer Organization**, or **MSP Organization**.

Important
These tab names are only indicative. If you have enabled the **Service Provider Feature**, you have to specify the names of the organization at the first and second level. The names that you specify are displayed as tabs in the interface.

Step 3 To edit the resource limit for a user group, choose **User Groups**.

Step 4 Choose a group from the table, and click **Edit Resources Limits**. The **Resource Limit** screen appears.

Step 5 In the **Resource Limit** screen, check **Enable Resource Limits** and complete the required fields, including the following:

Field Name	Description
Group field	The group name that you selected.
Enable Resource Limits check box	Check the check box to enable the resource limits or uncheck the check box to disable the resource limits. If checked, the user is provided with the option to set resource limits for a group and all nonzero resource limits are applied.
Maximum Active VM Count field	The maximum number of active VMs.
Maximum Total VM Count field	The total number of VMs.

Field Name	Description
Maximum Total VDC Count field	The total number of VDCs. While provisioning a VM, if the number of VDCs you specify exceeds the number you specify in this field, then an error message is displayed.
Provisioned vCPUs Limit field	The maximum number of provisioned vCPUs.
Provisioned Memory (GB) Limit field	The provisioned memory limit, in gigabytes.
Provisioned Disk (GB) Limit field	The provisioned limit for disks, in gigabytes.
Reserved CPU (GHz) Limit field	The reserved limit of CPUs, in gigahertz.
Reserved Memory (GB) Limit field	The reserved memory limit, in gigabytes
Maximum Snapshot (GB) Limit field	The maximum limit for snapshots, in gigabytes.
Count CPU and Memory for Inactive VMs check box	Check the box to include the group's inactive VM CPU or memory data in the computation of resource limits. Uncheck the box to exclude inactive VM CPU or memory data from the computation of resource limits.
OS Resource Limits **Note** The configuration of OS resource limits and physical resource limits is not supported for public clouds.	
CentOS field	The maximum number of CentOS (Community Enterprise Operating System) servers.
Windows Server 2003 field	The maximum number of Windows 2003 servers.
Windows Server 2008 field	The maximum number of Windows 2008 servers.
Windows Server 2012 field	The maximum number of Windows 2012 servers.
Windows Server 2016 field	The maximum number of Windows 2016 servers.
Windows 7 field	The maximum number of Windows 7 machines.
Windows XP field	The maximum number of Windows XP machines.
Red Hat field	The maximum number of Red Hat machines.
Ubuntu field	The maximum number of Ubuntu machines.
FreeBSD field	The maximum number of FreeBSD machines.
Other Linux field	The maximum number of other Linux OS.
Other field	The maximum number of other OS.

Field Name	Description
Physical Resource Limits	
Maximum Physical Server Count field	The maximum number of servers.
Maximum Full Width Physical Server Count field	The maximum number of full length physical servers. The number of servers specified in this field, when added with the number of servers specified for the **Maximum Half Width Physical Server Count** field must be less than or equal to the number of servers specified in the **Maximum Physical Server Count** field. **Important** This field is applicable only for Cisco UCS blade servers.
Maximum Half Width Physical Server Count field	The maximum number of half length physical servers. The number of servers specified in this field, when added with the number of servers specified for the **Maximum Full Width Physical Server Count** field must be less than or equal to the number of servers specified in the **Maximum Physical Server Count** field. **Important** This field is applicable only for Cisco UCS blade servers.
Maximum Physical Server Memory (GB) field	The maximum amount of server memory.
Maximum Physical Server CPU Count field	The maximum number of server CPUs.
Maximum vFiler Count field	The maximum number of vFilers.
Maximum Physical Storage Space (GB) field	The maximum amount of storage space.

Step 6 Click **Save**.

Configuring the Administration Profile

Creating the Admin Profile

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **Users**.

Step 3 Click **Add**.

Step 4 In the **Add User** screen, complete the required fields, including the following:

Field Name	Description
User Type drop-down list	Choose the user type option as **System Admin**. The system administrator has full privileges.
Login Name field	The login name. The default is admin.
Password field	The admin password.
Confirm Password field	The admin password that is entered again for confirmation.
User Contact Email field	The administrator's email address.
First Name field	The administrator's first name.
Last Name field	The administrator's last name.
Phone field	The administrator's phone number.
Address field	The administrator's address.
Set user disable date check box	Check to set the date and time when the user account must be disabled in the system. Disabling a user account means that the user can no longer log in into the system. A week prior to this date, an email message stating that the account will be disabled is sent to the user. This automatic email message is generated and sent by the **PeriodicNotificationToUserTask** system task. On the specified date and time, the user account is disabled automatically. If the user is logged in to the system on the date specified, then the login session is terminated automatically.

Field Name	Description
Locale drop-down list	Choose a language for the system specifically for this user. By default, the language is set to English. When this user logs in, the user interface is displayed in the language you selected. This locale selection applies only to this user.

Step 5 Click **Add**.

Editing Your Administrative Profile

As an administrator in the system, you can edit your own profile in the system.

Procedure

Step 1 Mouse-over your login name on the top right corner of the screen.

Step 2 Choose **Edit My Profile**.

All information that was specified while creating the account is displayed.

Step 3 In the **Edit My Profile** screen, complete the required fields, including the following:

Name	Description
Language drop-down list	Choose a new language for the user interface
Old Password field	Enter your current password.
New Password field	Enter your new password.
Confirm Password field	Re-enter your new password.
Access Profiles	Choose a new profile as the default profile.
Enable Dashboard check box	Check this check box to view the **Dashboard** screen soon after logging into the system.

Step 4 Click **Show Advanced Settings** and complete the required fields, including the following:

Name	Description
REST API Access Key field	Choose either **Copy Key Value** or **Regenerate Key** option.

Name	Description
Enable Developer Menu check box	Check this check box to enable the Developer menu on the system. You must restart the system for this change to take effect.
System Broadcast Message field	Enter a message that must be broadcast on the system.

Step 5 Click **Save**.

Step 6 Restart the system.

All changes that require a system restart are available in the interface.

Sending a Broadcast Message

As an administrator on the system, you can send a broadcast message to all the users that are currently logged into Cisco UCS Director. While configuring this message, you can either choose to have this message set with or without a timer.

Procedure

Step 1 Move the cursor over your login name on the top right corner of the screen.

Step 2 Choose **Edit My Profile**.

Step 3 Choose **Show Advanced Settings** and complete the required fields, including the following:

Name	Description
System Broadcast Message field	Enter the message that you want to send as a broadcast to all users.
Dismiss Message Automatically check box	Check this check box to dismiss the message automatically after a specific period of time. If you do not check this check box, the user will necessarily have to close the message.
Number of Minutes to Display drop-down list	Choose the number of minutes that the message must be visible to users, after which it automatically closes.

Step 4 Click **Send**.

Changing the Admin Password

Procedure

Step 1 Choose **Administration** > **Users and Groups**.
Step 2 On the **Users and Groups** page, click **Users**.
Step 3 Choose the administrator user account from the list of accounts.
Step 4 From the **More Actions** drop-down menu, click **Change Password.**
Step 5 In the **Change Password** screen, enter a new password for the **admin** user and confirm it.
Step 6 Click **Save**.

Viewing Current Online Users

Procedure

Step 1 Choose **Administration** > **Users and Groups**.
Step 2 Choose **Current Online Users** to view a list of online users. The list displays each user's username, IP address, session start time, last data access, and client.

Viewing Workflow Task Details

Before you begin

You must have read-only privileges for Orchestration assigned to your administrator user role. For information on creating or or modifying user roles, see Adding a User Role, on page 27.

Procedure

Step 1 Choose **Orchestration**.
Step 2 On the **Orchestration** page, click **Workflows**.
Step 3 Choose a workflow task from the list.
Step 4 Choose **View**.

The subsequent screen displays a textual summary of the entire workflow task and the inputs provided.

Step 5 Review the information and click **Close**.

Managing User Access Profiles

Multi-Role Access Profiles

A user can be assigned to more than one role, which is reflected in the system as a user access profile. For example, a user might log into Cisco UCS Director as a group administrator and as an all-policy administrator, if both types of access are appropriate.

Access profiles also define the resources that can be viewed by a user. With Cisco UCS Director Release 5.4, support for multiple profiles for a single user was introduced. So when you install version 5.4, and if a user account is associated with multiple groups, the system creates multiple profiles for the user account. But if you upgrade the system from a prior version to version 5.4, and if the **LDAPSyncTask** system task is not yet run, then, by default, only one profile is listed for a user account in the system.

When LDAP users are integrated with Cisco UCS Director, if a user belongs to more than one group, then the system creates a profile for each group. But by default, the domain users profile is added for LDAP users.

Note The **Manage Profiles** feature enables you to add, log into, edit, or delete a user access profile.

The **Authentication Type** column in the **Manage Profiles** screen indicates the authentication mechanism specified for the user accounts. It can be Local, LDAP or TACACS.

Creating a User Access Profile

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **Users**.

Step 3 Choose a user from the list.

Step 4 From the **More Actions** drop-down menu, click **Manage Profiles**.

Step 5 In the **Manage Profile** screen, click **Add**.

Step 6 In the **Add Entry to Access Profiles** screen, complete the required fields, including the following:

Field Name	Description
Name field	The profile name.
Description field	The description of the profile.
Type drop-down list	Choose the user role type.
Customer Organizations drop-down list	Choose the organization to which this user profile applies.

Field Name	Description
Show Resources From All Other Groups the User Has Access check box	Select this checkbox to specify that the user can view resources from all other groups that they have access to or are a part of.
Shared Groups field	Click **Select** to choose the groups to which the user profile applies. The user will be able to access all the resources associated with the selected groups.
Default Profile check box	Check the check box if this is the default user access profile. Uncheck the check box if it is not the default.

Step 7 Click **Submit**.

What to do next

Create additional user access profiles as needed.

Logging in to a Profile

As a user in the system, if you have multiple profiles for your account, then you can log in to the system with a specific profile.

Procedure

Step 1 In the **Cisco UCS Director login** dialog box, enter your username in the **Username** field, in the format Username: Access Profile Name.

For example, Alex: GrpAdmin

Step 2 In the **Password** field, enter your password.

Step 3 Click **Login**.

Default Profile

The default profile is the first profile that you created in the system. You can change the default to another profile. Using the new default profile, you log in by entering the username and password.

Changing a Default Profile

Procedure

Step 1 In the user interface, click the username displayed on the top right corner.

Step 2 In the drop-down menu, click **Edit My Profile**.

Step 3 In the **Edit My Profile** screen, select the profile that you want to set as a default profile.

Note
A profile can also be set as default while it is being added, or being edited.

Authentication and LDAP Integration

As an administrator, you can specify an authentication mechanism for the user accounts in the system. You can configure an authentication preference with a fallback choice for LDAP.



Important Starting with Release 6.6, configuring an LDAP authentication preference using the Verisign Identity Protection authentication service is no longer supported.

Name	Description
Local First, fallback to LDAP	Authentication is done first at the local server (Cisco UCS Director). If the user record is not found in the local server, then the authentication process shifts to the LDAP server.

Configuring Authentication Preferences

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **Authentication Preferences**.

Step 3 In the **Authentication Preferences** screen, complete the required field:

Name	Description
Authentication Preferences drop-down list	• **Local First, fallback to LDAP** If you select this option, then you must configure the LDAP servers. For more information, see Configuring LDAP Servers, on page 77.

Step 4 Click **Save.**

LDAP Integration

You can use LDAP integration to synchronize the LDAP server's groups and users with Cisco UCS Director. LDAP authentication enables synchronized users to authenticate with the LDAP server. You can synchronize LDAP users and groups automatically or manually. While adding an LDAP account, you can specify a frequency at which the LDAP account is synchronized automatically with Cisco UCS Director. Optionally, you can manually trigger the LDAP synchronization by using the **LDAPSyncTask** system task.

After you configure an LDAP account and after the synchronization process is run, either manually or automatically, the recently added LDAP information is displayed in Cisco UCS Director. This information is displayed in a tree view that depicts the hierarchical structure of all organizational units (OUs), groups, and users that have been added to the system. You can view this information by choosing **Administration** > **LDAP Integration**. You can select and expand an OU in the left pane to view all the groups within it. If you select a group in this left pane, you can view a list of users that are associated with that group. If an OU has several sub OUs within it, then you can click the **Organization** tab in the right pane to view detailed information. In addition, the **Groups** and **Users** tabs in the right pane display groups and users respectively that are synchronized within the selected OU.



Note Please note that we provide support for a total of 10,000 users and groups. It is not recommended to synchronize a number exceeding this limit.

In addition to running a system task, Cisco UCS Director also provides an additional option for you to synchronize the LDAP directory with the system:

- **Cleanup LDAP Users** system task—This system task determines if the synchronized users in the system are deleted from the LDAP directories or not. If there are user records that have been deleted from the LDAP directories, then after this system task is run, these user accounts are marked as disabled in the system. As an administrator, you can unassign resources of these disabled user accounts. By default, this task is in the enabled state. After the second system restart, this system task is changed to the disabled state. This applies to both, a standalone and multi-node setup.

  In a multi-node setup, this system task runs only on the primary node, even if there is a service node configured.

Important Users that do not belong to a group or to a domain user's group display in LDAP as **Users with No Group**. These users are added under the domain user's group in Cisco UCS Director.

You can add LDAP users with the same name in different LDAP server accounts. The domain name is appended to the login user name to differentiate multiple user records. For example: abc@vxedomain.com. This rule is applicable to user groups as well.

Appending the domain name to the user name to login to the system is only applicable to LDAP users. It does not apply to local users. All local users can login to the system with the user names.

When a single LDAP account is added, and a user logs in by specifying only the user name, Cisco UCS Director first determines if the user is a local user or is an LDAP user. If the user is identified as a local user and as an external LDAP user, then at the login stage, if the user name matches the local user name, then the local user is authenticated into Cisco UCS Director. Alternatively, if the user name matches that of the external user, then the LDAP user is authenticated into Cisco UCS Director.

LDAP Integration Rules and Limitations

Note Recommended version for security PSB is TLS: 1.2 and above.

If you do not want to upgrade and break the existing functionality, you need to update the `service.properties` manually and configure to the older version.The path for the `service.properties` file is **/resources/properties/service.properties**.The supported versions of **ldap.ssl.socket.protocols** for Cisco UCS Director, Release 6.8 are TLSv1.2 and TLSv1.3.

Group Synchronization Rules

- If a chosen LDAP group already exists in Cisco UCS Director and the source is type **Local**, the group is ignored during synchronization.
- If a chosen LDAP group already exists in Cisco UCS Director and the group source is type **External**, the group's description and email attributes are updated in Cisco UCS Director.
- While adding an LDAP server, you can now specify user filters and group filters. When you specify a group filter, all users that belong to the specified group are added to the system. In addition, the following actions are also performed:
  - If the specified group includes sub-groups, then the group, the sub-groups and the users in those sub-groups are added to the system (only applicable when you manually synchronize the LDAP directory).
  - If the user is part of multiple groups, and the other groups do not match the group specified as the group filter, then those additional groups are not added to the system.
- A user can be part of multiple user groups. However, the group that is mentioned first in the list of groups that the user is part of is set as the default primary group for the user. If the user is not part of any group, then the default primary group is set as **Domain Users**.

Note You can view information on all the groups that a user is part of only after the **LDAPSyncTask** system task is run.

- When an LDAP group is synchronized, all users that are in the group are first added to the system. Also, if users in the specified LDAP group are associated with other groups that are in the same OU or in a different OU, then those groups are also retrieved and added to the system.
- The LDAP synchronization process will retrieve the specified LDAP groups for the system, along with nested groups, if any.
- Prior to this release, a user was part of only one group. After an upgrade to the current release, and only after the **LDAPSyncTask** system task is run, the **Manage Profiles** dialog box displays the other groups that the user is part of. This is applicable only when the other groups match the group filters that you specified while configuring the LDAP server.

User Synchronization Rules

- LDAP users that have special characters in their names are now added to Cisco UCS Director.
- While adding an LDAP server, you can now specify user filters and group filters. When you specify a user filter, all the users that match the filter you specified, and the groups that they belong to, are retrieved for the system.
- An LDAP user can have multiple group memberships. When the LDAP user is synchronized with the system, this multiple group membership information is retained. Cisco UCS Director provides you with an option to view this information for every user. For more information, see Viewing Group Membership Information, on page 87. In addition, multiple access profiles are also automatically created for the user.

Note You can view this information only when the groups match the filter you specified while configuring the LDAP server, and when the groups have been assimilated into the system.

- Cisco UCS Director now displays the User Principal Name (UPN) for each user that is added into the system. This is applicable for users that have been added into the system in prior releases. Users can log in to the system using their login name or their user principal name. Logging in using the user principal name along with the profile name is not supported.
- If a chosen LDAP user already exists in Cisco UCS Director and the source type is **External**, then that user is ignored at synchronization. The user's name, description, email, and other attributes are not updated again.
- If a user account is created in two different LDAP directories, then the user details of the LDAP directory that was synchronized first are displayed. The user details from the other LDAP directory are not displayed.
- After multiple LDAP directories are synchronized, the LDAP external users must log in to Cisco UCS Director by specifying the complete domain name along with their user name. For example: vxedomain.com\username. However, this rule does not apply if there is only one LDAP server directory added to Cisco UCS Director.

Note After an LDAP synchronization process, verify that the user is assigned to the correct group.

Managing LDAP Integration

Procedure

Step 1 Choose **Administration** > **LDAP Integration**.

Step 2 Required: Choose an LDAP server and click the following buttons, as needed, to manage LDAP integration:

Name	Description
Search BaseDN button	Enables you to choose a distinguished domain name to search. All users and groups from the chosen organization units are fetched into Cisco UCS Director when the LDAP synchronization process is completed. This action is also considered to be an automatic synchronization process. **Note** You can initiate LDAP server synchronization as a system task. For more information, see Executing the LDAP Synchronization System Task, on page 83.
Request Manual LDAP Sync	Displays a dialog box that enables you to specify either basic or advanced search criteria to fetch LDAP users and groups.

Step 3 (Optional) If you chose **Request Manual LDAP Sync**, complete the following fields:

Name	Description
Manual Search Base check box	Enables search on the manually added organization units. When you check this check box, the manually added OUs are displayed.
Basic Search check box	Enables basic search by organization unit.
Advanced Search check box	Enables advanced search.

Important
When you use either of the search options, if users and groups that match the search criteria already exist in Cisco UCS Director, then they are not displayed as part of the search results.

Step 4 For basic search, click **Select** to specify the search base.

Step 5 Choose the search base DN, click **Select**, and continue to Step 9.

Step 6 For advanced search, in the **Advanced Filtering Options** pane add or edit attribute names for **User Filters** and **Group Filters**.

Step 7 Click **Next**.

Step 8 In the **Select Users and Groups** pane, complete the following fields:

Name	Description
LDAP Groups field	The LDAP groups from which the users must be synchronized.
LDAP Users field	The LDAP users that must be synchronized.

Step 9 Click **Submit** to synchronize the LDAP server.

Configuring LDAP Servers

You can configure multiple LDAP servers and accounts in Cisco UCS Director. While adding LDAP accounts, you can specify the following:

- An organization unit (OU) that is part of the search base DN.
- A frequency at which the LDAP account is automatically synchronized with the system.
- A group or user filter to narrow down the results, and specify an LDAP role filter on the groups and users

Soon after an LDAP server account is added, a system task for this account is created automatically, and it immediately begins to synchronize the data. All the users and groups in the LDAP server account are added to the system. By default, all the users from the LDAP account are automatically assigned to the service end-user profile.

Before you begin

You should have set the authentication preferences to the following:

- **Local First, fallback to LDAP**

Procedure

Step 1 Choose **Administration** > **LDAP Integration**.

Step 2 Click **Add**.

Step 3 In the **LDAP Server Configuration** screen, complete the required fields, including the following:

Name	Description
Account Name field	The name of the account. This name must be unique.

Name	Description
Server Type field	The type of LDAP server. It can be one of the following: • Open LDAP • Microsoft Active Directory
Enable LDAP Redundancy check box	**Important** As a prerequisite, you must configure DNS servers to use the LDAP redundancy option. For more information on how to configure DNS servers using the Shelladmin option **Configure DNS**, see the **Configuring DNS** section in the Cisco UCS Director Shell Guide, Release 6.9. This field appears only when **Microsoft Active Directory** is selected in the **Server Type** field. Check this check box to enable LDAP redundancy support. When this check box is selected, the system performs DNS-based discovery of LDAP servers based on the domain. If the primary LDAP server is unavailable, the other LDAP servers associated with the domain are used to synchronize the data. **Note** When this check box is selected, the **Server** field disappears.
Server field	The IP address or host name of the LDAP server.
Enable SSL check box	Enables a secure connection to the LDAP server. **Important** This check box must always be selected to ensure secure data transmission, just as it is essential to use secure protocols such as HTTPS, SSH, SFTP, and SCP to protect data during transit.
Port field	The port number. It is automatically set to 636 for SSL, and 389 for non-secure mode.
Domain Name field	The domain name. If you selected **Open LDAP** as the Server Type, then this domain name must match the domain specified with the user name. **Important** You must specify the complete domain name. For example: vxedomain.com.

Name	Description
User Name field	The user name of the selected server. You can specify the user name in one of the following formats: • <username>@domain.com • Distinguished Name of the user in the following format: **CN=PowerUser,CN=Users,DC=domain,DC=com** If you selected **Open LDAP** as the Server Type, then specify the user name in the following format: **uid=users,ou=People,dc=ucsd,dc=com** where the **ou** corresponds to the organizational unit in which the users are located within the directory hierarchy.
Password field	The server password.
Synchronization Frequency drop-down list	Select the frequency (hours) at which the LDAP server must be synchronized. It can be one of the following: • 1 • 4 • 12 • 24
Enable Manual Search Base check box	Check this check box to manually enter the search base organization units (OU). If you do not check this check box, then the search base organization units (OU) are retrieved from the LDAP server automatically.
Enable TACACS Authentication check box	Check this check box to enable TACACS authentication for user accounts in Cisco Identity Services Engine (Cisco ISE). This option is not displayed if you have not added a Cisco ISE server in Cisco UCS Director.
ISE Server drop-down list	Choose the Cisco ISE server from the list.

Step 4 Click **Next**.

Step 5 If you checked the **Enable Manual Search Base** check box, the **Add Entry to Search Base** screen is displayed. In this screen, enter the organization units (OU) and click **Submit**.

You can enter multiple organization units (OU) from this screen.

a) After the OU is added to the system, click **Next** to configure user and group filters.

Step 6 If you did not check the **Enable Manual Search Base** check box, the **LDAP Search Base** pane is displayed. In this pane, click **Select** to specify LDAP search base entries and click **Select**.

All organization units (OU) that are available in Cisco UCS Director are displayed in this list.

Step 7 Click **Next**.

Step 8 In the **Configure User and Group Filters** pane, complete the following fields:

Name	Description
User Filters	Click the + sign to select specific users that must be synchronized with the system. All groups that the selected users are part of are retrieved and added into the system.
Group Filters	Click the + sign to select groups that must be synchronized with the system. All users that are part of the selected group filters are retrieved and added into the system. However, if the users in the selected group are also part of other groups, then those groups are not retrieved and added to the system unless you select them.
Add Entry to Group Filters dialog box	
Attribute Name drop-down list	Choose either **Group Name** or **User Name**.
Operator drop-down list	Choose the filter to retrieve groups and users. It can be one of the following: • **Equals to** • **Starts with**
Attribute Value field	Specify a keyword or a value that must be included in the search.

Based on the filters, the groups or users are retrieved.

Step 9 Click **Next**.

Step 10 In the **LDAP User Role Filter** pane, click the **(+)** sign to add a user role filter.

Step 11 In the **Add Entry to User Role Filters** dialog box, complete the following fields:

Name	Description
Attribute Name field	The name of the attribute. It can be **Group Name**.
Operator drop-down list	It can be one of the following: • **Equal to** • **Starts with**

Name	Description
Attribute Value field	Specify a value in this field. All users that match the values of the **Operator** field and the **Attribute Value** field are assigned to the user role you select in the **Map User Role** drop-down list.
Map User Role drop-down list	Select a user role that you want the users mapped to. You can choose a role that was available by default, or you can choose a role that you created in the system. Following are the roles that are available by default in Cisco UCS Director: • All Policy Admin • Billing Admin • Computing Admin • Service End-User • Group Admin • IS Admin • Network Admin • Operator Admin • Storage Admin • System Admin
Enable TACACS Authentication check box	Check this check box to enable TACACS-based authentication for users configured in Cisco ISE.

Step 12 Click **Submit**.

Step 13 Click **OK**.

The user role filters are added to the **User Role Filters** table.

Note
If you have multiple user role filters specified, then the filter specified in the first row is processed.

If you manually update a user role for a user from the **Login Users** tab, then the user role that you mapped the group to is no longer applied to the user.

What to do next

If you have not set the authentication preference to LDAP, then you are prompted to modify the authentication preference. For more information on changing the authentication preference, see Configuring Authentication Preferences, on page 72.

Test the LDAP server connectivity. For more information, see Testing LDAP Server Connectivity.

Testing LDAP Server Connectivity

Procedure

Step 1 Choose **Administration** > **LDAP Integration**.
Step 2 In the **LDAP Integration** tab, choose an LDAP account name from the table.
Step 3 Click **Test Connection**.
Step 4 In the **Test LDAP Connectivity** screen, click **Close**.

Viewing LDAP Directory Sync Status

Procedure

Step 1 Choose **Administration** > **LDAP Integration**.
Step 2 In the **LDAP Integration** tab, choose an LDAP account name from the table.
Step 3 From the **More Actions** drop-down list, select **Results**.
The following information is displayed:

- Start Time—The time when the LDAP discovery started
- Status—Indicates the result of the LDAP discovery
- Message—Displays details about LDAP groups and users, along with the final synchronization status after the LDAP discovery is completed. When the **Enable LDAP Redundancy** check box is selected during LDAP server configuration, the details about the server or domain controller used for data synchronization are also displayed.
- End Time—The time when the LDAP discovery ended.

Viewing LDAP Server Summary Information

Procedure

Step 1 Choose **Administration** > **LDAP Integration**.
Step 2 In the **LDAP Integration** tab, choose an LDAP account name from the table.
Step 3 Click **View**.
The **View LDAP Account Information** screen displays summary information of the LDAP account.
Step 4 Click **Close**.

Adding LDAP Search BaseDN Entries

Procedure

Step 1 Choose **Administration** > **LDAP Integration**.

Step 2 In the **LDAP Integration** tab, choose an LDAP account name from the table.

Step 3 Click **Search BaseDN**.

Step 4 If you have not checked **Enable Manual Search Base** while configuring the LDAP server, then in the **LDAP Search Base** screen, click **Select** to view the list of search base entries that are currently added.

a) Check the check boxes of the search base entries you want to include.
b) Click **Select**.
c) Click **Submit**.

Step 5 If you have checked **Enable Manual Search Base** while configuring the LDAP server, then in the **LDAP Search Base** screen, click **+** to add a new entry to the search base table.

For search base entries that are already added in the system, you can either edit, delete or re-order them using the options displayed on the screen.

Step 6 Click **Submit**.

Executing the LDAP Synchronization System Task

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **System Tasks**.

Step 3 Enter **LDAP** in the Filter field.

Step 4 Select **LDAPSyncTask** from the **System Tasks** table.

Step 5 Click **Run Now**.

Step 6 (Optional) Click **Manage Task** to enable or disable the synchronization process.

What to do next

The results of the synchronization process are displayed in Cisco UCS Director. Select an LDAP account on the **LDAP Integration** pane, and click **Results** to view the summary of the synchronization process.

Modifying LDAP Server Details

You can only modify the following details for a configured LDAP server:

- Enable or disable LDAP redundancy
- Port numbers and SSL configuration
- Server

- User name and password
- Synchronization frequency
- Search BaseDN selections
- User roles and groups that are mapped

Procedure

Step 1 Choose **Administration** > **LDAP Integration**.

Step 2 In the **LDAP Integration** tab, choose an LDAP account name from the table.

Step 3 From the **More Actions** drop-down list, select **Modify**.

Step 4 In the **LDAP Server Configuration** screen, edit the required fields:

Name	Description
Enable LDAP Redundancy check box	**Important** As a prerequisite, you must configure DNS servers to use the LDAP redundancy option. For more information on how to configure DNS servers using the Shelladmin option **Configure DNS**, see the **Configuring DNS** section in the Cisco UCS Director Shell Guide, Release 6.9. This field appears only when **Microsoft Active Directory** is selected in the **Server Type** field. Check this check box to enable LDAP redundancy support. When this check box is selected, the system performs DNS-based discovery of LDAP servers based on the domain. If the primary LDAP server is unavailable, the other LDAP servers associated with the domain are used to synchronize the data. **Note** When this check box is selected, the **Server** field disappears.
Server field	The IP address or host name of the LDAP server.
Enable SSL check box	Enables a secure connection to the LDAP server.
Port field	The port number. It is automatically set to 636 for SSL, and 389 for non-secure mode.

Name	Description
User Name field	The user name of the selected server. You can specify the user name in one of the following formats: • <username>@domain.com • Distinguished Name of the user in the following format: **CN=PowerUser,CN=Users,DC=domain,DC=com** If you selected **Open LDAP** as the Server Type, then specify the user name in the following format: **uid=users,ou=People,dc=ucsd,dc=com** where the **ou** corresponds to the organizational unit in which the users are located within the directory hierarchy.
Password field	The server password.
Synchronization Frequency drop-down list	Select the frequency (hours) at which the LDAP server must be synchronized. It can be one of the following: • 1 • 4 • 12 • 24
Enable Manual Search Base check box	Check this check box to manually enter the search base organization units (OU). If you do not check this check box, then the search base organization units (OU) are retrieved from the LDAP server automatically.

Step 5 Click **Next**.

Step 6 In the **LDAP Search Base** pane, click **Select** to specify the LDAP search base entries. and then click **Select**.

Step 7 Click **Next**.

Step 8 In the **Configure User and Group** pane, complete the following fields:

Name	Description
User Filters	Click the + sign to select specific users that must be synchronized with the system.
Group Filters	Click the + sign to select groups that must be synchronized with the system.

Step 9 Click **Next**.

Step 10 In the **LDAP User Role Filter** pane, click the **(+)** sign to add a user role filter.

Step 11 In the **Add Entry to User Role Filters** dialog box, complete the following fields:

Name	Description
Attribute Name field	The name of the attribute. It can be **Group Name**.
Operator drop-down list	It can be one of the following: • **Equal to** • **Starts with**
Attribute Value field	Specify a value in this field. All users that match the values of the **Operator** field and the **Attribute Value** field are assigned to the user role you select in the **Map User Role** drop-down list.
Map User Role drop-down list	Select a user role that you want the users mapped to. You can choose a role that was available by default, or you can choose a role that you created in the system. Following are the roles that are available by default in Cisco UCS Director: • All Policy Admin • Billing Admin • Computing Admin • Service End-User • Group Admin • IS Admin • Network Admin • Operator • Storage Admin • System Admin

Step 12 Click **Submit**.

The user role filters are added to the **User Role Filters** table.

Note

- If you have multiple user role filters specified, then the filter specified in the first row is processed.
- Users and groups synced manually will retain their LDAP Server IP settings even if the LDAP server IP is modified. During auto-sync, manually synced users and groups will be ignored.

Step 13 Click **Submit**.

Viewing Group Membership Information

Any user in the system can be part of multiple user groups. When a user is added to the system, all groups that the user is part of are also added to the system. However, the group that the user was most recently added to is set as the default primary group for the user. If the user is not part of any group, then the default primary group is set as **Domain Users**. While you can use the **Manage Profiles** option to view and modify group membership for users, Cisco UCS Director also provides you with an additional option to view a list of all groups that a specific user is part of.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **Users**.

Step 3 Select a user from the table.

Step 4 From the **More Actions** drop-down menu, click **Group Membership**.

The **MemberOf** screen displays all the groups that the user is part of.

Step 5 Click **Close**.

Deleting LDAP Server Information

When you delete an LDAP server account, the following actions are initiated:

- Resources that have been assigned to LDAP users are un-assigned.
- VMs that have been assigned to the LDAP users are un-assigned.
- Resources that have been assigned to LDAP groups are un-assigned.
- VMs that have been assigned to the LDAP groups are un-assigned.
- VM share policies that have been assigned to LDAP users are un-assigned.
- Tags that have been applied to the LDAP users and groups are cleared
- Users and groups are immediately deleted from the database.
- The LDAP server details are removed from the tree view.

Procedure

Step 1 Choose **Administration** > **LDAP Integration**.

Step 2 In the **LDAP Integration** tab, choose an LDAP account name from the table.

Step 3 Click **Delete**.

Step 4 In the **Delete LDAP Account** screen, click **Delete**.

Step 5 Click **OK**.

This initiates the deletion of the LDAP account in Cisco UCS Director. Based on the number of users and groups in the LDAP account, this deletion process could take a few minutes to complete. During such time, the LDAP account may still be visible in Cisco UCS Director. Click **Refresh** to ensure that the account has been deleted.

Viewing LDAP Directory Sync Status

Procedure

Step 1 Choose **Administration** > **LDAP Integration**.

Step 2 In the **LDAP Integration** tab, choose an LDAP account name from the table.

Step 3 From the **More Actions** drop-down list, select **Results**.
The following information is displayed:

- Start Time—The time when the LDAP discovery started
- Status—Indicates the result of the LDAP discovery
- Message—Displays details about LDAP groups and users, along with the final synchronization status after the LDAP discovery is completed. When the **Enable LDAP Redundancy** check box is selected during LDAP server configuration, the details about the server or domain controller used for data synchronization are also displayed.
- End Time—The time when the LDAP discovery ended.

Single Sign On with OneLogin

Cisco UCS Director provides a Single Sign-On (SSO) service based on SAML 2.0. To enable SSO, Cisco UCS Director must be registered as a Service Provider (SP) with the OneLogin Identity Provider (IDP). SSO enables users to access multiple systems seamlessly without having to log in to individual systems. With SSO configured and enabled between the SP and IDP, a user can log in to the OneLogin portal and then access Cisco UCS Director without having to log in again.

To enable Single Sign-On with OneLogin, you must complete the following:

1. Create a user account at the OneLogin site.
2. Map the Cisco UCS Director appliance details in the OneLogin site.

   For more information, see Mapping the Cisco UCS Director Appliance at the OneLogin Site, on page 89
3. Generate a Single Sign-On certificate at the OneLogin site.

   For more information, see Generating a OneLogin Certificate, on page 90.

4. Create a user account in Cisco UCS Director with the same credentials as the account created at the OneLogin site. The user account must be created on the same appliance that was mapped in the OneLogin site.

   For information on adding a user, see Adding Users, on page 105.

5. Enable Single Sign-on by uploading the certificate on the appliance that you referenced in the OneLogin site.

   For more information, see Enabling Single Sign-On, on page 91.

After you complete this procedure, when you return to the OneLogin site and click on Cisco UCS Director, the user will no longer be prompted to enter their user name and password information.

Mapping the Cisco UCS Director Appliance at the OneLogin Site

To enable Single Sign-On, you must first map the system that is running Cisco UCS Director.

Before you begin

You must have a OneLogin account.

Procedure

Step 1 Access the OneLogin site from the following link: https://www.onelogin.com.

Step 2 Log in to the site using your account details.

Step 3 From the menu bar, choose **Apps** > **Add Apps**.

Step 4 In the **Find Applications** field, enter `SAML`.

Step 5 In the search results that are displayed, select and double-click **OneLogin SAML Test (IdP) SAML 2.0**.

The **Info** pane is displayed.

Step 6 In the **Info** pane, enter the following information:

Field	Description
Display Name field	Enter a unique name for the system that is running Cisco UCS Director. This name is displayed on the home page of the OneLogin portal. You can register multiple Cisco UCS Director appliances at this portal. Be sure to enter a name that helps you identify the system accurately.

Step 7 Click **Save**.

Step 8 Choose **Configuration** from the menu bar, and enter the following information:

Field	Description
SAML Consumer URL field	Enter the URL of the system that is running Cisco UCS Director. **Important** Enter the URL that is displayed after a user logs into the Cisco UCS Director user interface. It should look similar to the following: https://<ip_address>/app/cloudmgr/cloudmgr.jsp. For example: https://10.10.10.10/app/cloudmgr/cloudmgr.jsp. For releases 6.0 and later, the URL should look similar to the following: https://<ip_address>/app/ux/index.html. For example: https://10.10.10.10/app/ux/index.html.

Step 9 Click **Save**.

On the home page of this site, an icon is created for the server details that you specified. For every appliance that you register at the OneLogin site, an icon is displayed on the home page. If you click this icon, you are automatically directed to the Cisco UCS Director user interface.

What to do next

Generate a OneLogin certificate and enable SSO on the Cisco UCS Director appliance.

Generating a OneLogin Certificate

Before you begin

- You must have a OneLogin account
- The Cisco UCS Director application must be registered with the OneLogin website.

Procedure

Step 1 Access the OneLogin site from the following link: https://www.onelogin.com.

Step 2 Log in to the site using your account details.

Step 3 From the menu bar, choose **Settings** > **SAML**.

Step 4 Select **Standard Strength Certificate (2048-bit)**.

Step 5 Click **Download**.

Step 6 Click **OK**.

A file with the name `onelogin.pem` is downloaded to your system.

What to do next

You must upload this certificate on the Cisco UCS Director appliance.

Enabling Single Sign-On

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **Single Sign-On**.

Step 3 Check **Enable Single Sign-On**.

Step 4 In the **File** field, either drag and drop a file, or click **Select a File** to browse and select the OneLogin certificate file on your system.

The OneLogin certificate file is saved on your system with the name `onelogin.pem`.

Step 5 Click **Upload**.

Step 6 When the upload is complete, click **Submit**.

When you launch Cisco UCS Director from the OneLogin site, you are not prompted to log in to the system.

Single Sign-on with Ping Federate

You can enable Single Sign-on (SSO) for Cisco UCS Director with Ping Federate. SSO enables users to access multiple systems seamlessly without having to log in to individual systems.

To enable Single Sign-On with Ping Federate, you must complete the following:

1. Create an adaptor.

   See Creating an Adapter in Ping Federate, on page 92

2. Create Service Provider (SP) connectors.

   See Creating Service Provider Connections, on page 93

3. Upload the certificate on the Cisco UCS Director appliance.
4. Navigate to the URL specified while creating the SP connection, and login using the credentials you had specified.

Creating a User in Ping Federate

Procedure

Step 1 Launch the Ping Federate user interface.

Step 2 Click **Server Configuration**.

Step 3 Click **Password Credential Validators** displayed under Authentication.

Step 4 Click **Create New Instance** and complete the following:

a) In the **Type** tab, enter unique values for **INSTANCE NAME** and **INSTANCE ID** fields.
b) In the **TYPE** drop-down list, choose **Simple Username Password Credential Validator**.
c) In the **PARENT INSTANCE** drop-down list, choose **None**.
d) In the **Instance Configuration** tab, click **Add a new row to Users**.

Step 5 Add a new user and click **Update**.
Step 6 Click **Next**.
Step 7 Review the summary.
Step 8 Click **Done**.

Creating LDAP Users

Procedure

Step 1 Launch the Ping Federate user interface.
Step 2 Click **Server Configuration**.
Step 3 Click **Password Credential Validators** link displayed below **Authentication**.
Step 4 Click **Create New Instance** and complete the following fields:
a) In the **Type** tab, enter unique values for **INSTANCE NAME** and **INSTANCE ID** fields and click **Next**.
b) In the **TYPE** drop-down list, choose **LDAP Username Password Credential Validator**.
c) In the **Parent Instance** drop-down list, choose **None**.
d) In the **Instance Configuration** tab, click **Manage Data Stores** displayed at the botton of the page.
e) Choose **Add New Data Store**.
f) In the **Data Store Type** drop-down list, choose **LDAP**.
g) Add appropriate values for the LDAP configuration fields.
h) Click **Done**.

Creating an Adapter in Ping Federate

Before you begin

You must create a user in Ping Federate with the same credentials of the user created in Cisco UCS Director. You can create a user in multiple ways in Ping Federate. Following are the commonly used procedures to create a user:

- Create a single user.

  See Creating a User in Ping Federate, on page 91

- Configure LDAP users.

  See Creating LDAP Users, on page 92

Procedure

Step 1 Launch the Ping Federate user interface.

Step 2 Choose **Adapter** > **Type**.

Step 3 Complete the following fields on the **Type** screen:

a) Enter unique values for the **INSTANCE NAME** and **INSTANCE ID** fields.
b) Choose **HTML Form IDP Adapter or LDAP** from the **Type** drop-down list.
c) Choose **None** from the **Parent Instance** drop-down list.
d) Click **Next**.

Step 4 Complete the following fields on the **IDP Adapter** screen:

a) Click **Add a new row to Credential Validators** and select the form that you created earlier.
b) Click **Update**.
c) Click **Next**.

Step 5 In the **Extended Contract** screen, click **Next**.

Step 6 In the **Adapter Attributes** screen, choose the user name as the pseudonym.

Step 7 Click **Next**.

Step 8 In the **Adapter Contract Mapping** screen, click **Next**.

Step 9 Review the information displayed in the **Summary** screen, and click **Done**.

Step 10 Click **Save**.

What to do next

Configure Service Provider (SP) connections.

Creating Service Provider Connections

Procedure

Step 1 Launch the Ping Federate user interface.

Step 2 Click **SP Connections**.

Step 3 Click **Create New**.

Step 4 In the **Connection Type** tab, check the **Browser SSO Profiles** check box and click **Next**.

Step 5 In the **Connection Options** tab, check the **Browser SSO** check box and click **Next**.

Step 6 In the **Import Metadata** tab, click the **None** radio button for the **METADATA** field.

Step 7 In the **General Info** tab, enter the values for the following fields:

- **Connection ID**
- **Connection Name**
- **BASE URL**—Enter the URL of Cisco UCS Director.

Step 8 Click **Next**.

Step 9 In the **Browser SSO** tab, choose **Configure Browser SSO** and complete the following:

a) In the **SAML Profiles** tab, check the **IDP-INITIATED SSO** checkbox and click **Next**.
b) In the **Assertion Lifetime** tab, retain the default values and settings, and click **Next**.
c) In the **Assertion Creation** tab, choose **Configure Assertion Creation** and complete the following:

1. In the **Identity Mapping** tab, choose the **Standard** option and click **Next**.
2. In the **Attribute Contract** tab, retain the default values and click **Next**.
3. In the **Authentication Source Mapping** tab, choose **Map New Instance** tab.

   You must select the adapter instance you previously created, and and click **Next**.
4. In the **Mapping Method** tab, retain the default values and click **Next**.
5. In the **Attributes Contract Fulfillment** tab, choose **Adapter** in the **Source** column and **username** in the **Value** column. Retain the default values for other columns, and and click **Next**.

Step 10 In the **Protocol Setting** tab, choose **New Protocol**, and complete the following:

a) In the **Assertion Consumer Service URL** screen, choose **POST** in the **Binding** column and enter the Cisco UCS Director URL in the **Endpoint URL** column and click **Next**.
b) Choose the default values in the subsequent screen and click **Done**.

Step 11 In the **Credentials** tab, create a certificate and download it. Click **Next**.

Step 12 In the **Activation and Summary** screen, choose **Active** as the **Connection Status** and click **Done**.

Step 13 Upload the certificate in Cisco UCS Director.

The user name you specify must be the same as the user name specified in Ping Federate.

Step 14 Navigate to the URL you specificed as the SSO Application Endpoint and login to complete enabling single sign-on.

Authentication and Cisco Identity Services Engine (Cisco ISE)

Cisco Identity Services Engine (Cisco ISE) Integration

You can integrate a Cisco Identity Services Engine (Cisco ISE) server into Cisco UCS Director using TACACS to synchronize Cisco ISE users and user groups. With this integration, users configured in Cisco ISE are retrieved and integrated in Cisco UCS Director. Following are the prerequisites to configuring the Cisco ISE server in Cisco UCS Director:

- Add Cisco UCS Director as a network device in Cisco ISE and enable TACACS authentication.

  The shared secret key that you enter in Cisco ISE to enable TACACS authentication must be entered in Cisco UCS Director when you add the Cisco ISE server.

- Specify an authentication protocol in Cisco ISE. It can either be PAP/ASCII or CHAP.

  The authentication protocol that you select in Cisco ISE must be selected in Cisco UCS Director as well.

- Enable the External RESTful Services (ERS) APIs in Cisco ISE.

  In a cluster-setup, you must enable ERS for the primary administration node and for all the other nodes.

Note You can integrate a Cisco ISE server that is running release version 2.6.0.156 or later.

For information on completing these prerequisites, see the *Cisco Identity Services Engine Administrator Guide*.

After addng the Cisco ISE server in Cisco UCS Director, you can synchronize the users and groups automatically or manually. While adding the Cisco ISE account, you can specify a frequency at which the account is synchronized automatically with Cisco UCS Director. Optionally, you can manually trigger the synchronization by using the **ISE Sync Task** system task. After the system task runs, all user accounts are retrieved and displayed on the **Users** page, and **User Groups** page. By default, a user group called TACACS Users Group is available on the **User Groups** page. Cisco ISE users that do not belong to any user group are automatically added to this user group when their accounts are retrieved in Cisco UCS Director.

Cisco UCS Director also includes the **Cleanup ISE Users** system task to disable accounts of users that have been removed from Cisco ISE. By default, this system task is disabled. If you enable this system task, it runs automatically every day.

Configuring Cisco Identity Services Engine (Cisco ISE) Server Integration

Before you begin

- Add Cisco UCS Director as a network device in Cisco ISE and enable TACACS authentication.

  The shared secret key that you enter in Cisco ISE to enable TACACS authentication will have to be entered in Cisco UCS Director when you add the Cisco ISE server.

- Specify an authentication protocol in Cisco ISE.

  It can either be Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP). The authentication protocol that you select in Cisco ISE must be selected in Cisco UCS Director when you add the Cisco ISE server.

- Enable the External RESTful Services (ERS) APIs in Cisco ISE.

  In a cluster-setup, you must enable ERS for the primary administration node and for all the other nodes.

For information on completing these prerequisites, see the *Cisco Identity Services Engine Administrator Guide*.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **ISE Server Integration**.

Step 3 Click **Add**.

Step 4 In the **ISE Configuration** screen, complete the required fields, including the following:

Name	Description
Account Name field	The name of the account. This name must be unique.
Server field	The IP address or the host name of the Cisco ISE server.
Port field	The port number. By default this port number is set to 49.
Username field	The user name of the user who has access to the REST APIs of the Cisco Identity Services Engine (ISE).
Password field	The password of the user who has access to the REST APIs of the Cisco Identity Services Engine (Cisco ISE).
Authentication Type	The authentication type to be used. It can be one of the following: • Password Authentication Protocol (PAP) or • Challenge Handshake Authentication Protocol (CHAP)—not supported for LDAP users.
Secret Key	The shared secret key you configured in Cisco ISE.
Connection Timeout	The time (in seconds) that the system waits after which the connection is timed out.
Synchronization Interval field	Select the frequency (hours) at which the ISE server must be synchronized. It can be one of the following: • 4 • 12 • 24

Step 5 Click **Next**.

Step 6 In the **Configure User and Group Filters** pane, complete the following fields:

Name	Description
User Filters	Click the + sign to select specific users that must be synchronized with the system. All groups that the selected users are part of are retrieved and added into the system.

Name	Description
Group Filters	Click the + sign to select groups that must be synchronized with the system. All users that are part of the selected group filters are retrieved and added into the system. However, if the users in the selected group are also part of other groups, then those groups are not retrieved and added to the system unless you select them.
Add Entry to Group Filters dialog box	
Attribute Name drop-down list	Choose either **Group Name** or **User Name**.
Operator drop-down list	Choose the filter to retrieve groups and users. It can be one of the following: • **Equal to** • **Starts with**
Attribute Value field	Specify a keyword or a value that must be included in the search and click **Submit**.

Based on the filters, the groups or users are retrieved.

Step 7 Click **Next**.

Step 8 In the **Configure User Role Filters** pane, click the **(+)** sign to add a user role filter.

Step 9 In the **Add Entry to User Role Filters** dialog box, complete the following fields:

Name	Description
Attribute Name field	The name of the attribute. It can be **Group Name**.
Operator drop-down list	It can be one of the following: • **Equal to** • **Starts with**
Attribute Value field	Specify a value in this field. All users that match the values of the **Operator** field and the **Attribute Value** field are assigned to the user role you select in the **Map User Role** drop-down list.

Name	Description
Map User Role drop-down list	Select a user role that you want the users mapped to. You can choose a role that was available by default, or you can choose a role that you created in the system. Following are the roles that are available by default in Cisco UCS Director: • All Policy Admin • Billing Admin • Computing Admin • Service End-User • Group Admin • IS Admin • Network Admin • Operator Admin • Storage Admin • System Admin

Step 10 Click **Submit**.

Step 11 Click **Submit** in the **Configure User Role Filters** page.

Branding for Customer Organizations

Cisco UCS Director supports branding and customizing the portal at the following levels:

- Global level—This system-level branding can be modified by the global administrator.
- MSP Organization level or the tenant level—The branding at this level can be modified by the administrator or the MSP administrator.
- Customer organization level—Customer organizations are usually grouped with an MSP organization. An MSP administrator or a global administrator can modify the branding details.

With the introduction of branding support at the MSP organization level, certain rules apply to what branding changes users may view. The settings that are applied depend on the following:

- User role—Is the user an end user, a group administrator, or an MSP administrator?
- User's customer organization and the branding set for it.
- MSP Organization branding settings.

The following table elaborates the branding behavior in Cisco UCS Director.

Table 7: Branding Behavior in Cisco Cisco UCS Director

Branding set at MSP Organization Level	Branding set at Customer Organization Level	MSP Administrator	Group Administrator	End User
Yes	Yes	Branding details set at the MSP organization level are displayed.	Branding details set at the customer organization level is displayed.	Branding details set at the customer organization level to which this user belongs to is displayed.
No	Yes	Global branding details are displayed.	Branding details set at the customer organization level is displayed.	Branding details set at the customer organization level to which this user belongs to is displayed.
Yes	No	Branding details set at the MSP organization level are displayed.	Branding details set at the MSP organization level to which this customer organization belongs to is displayed.	Branding details set at the MSP organization level to which the customer organization belongs to is displayed.
No	No	Global branding details are displayed.	Global branding details are displayed.	Global branding details are displayed.

Branding User Groups

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **User Groups**.

Step 3 Choose the group to brand.

Step 4 From the **More Actions** drop-down menu, click **Branding**.

The **Group Branding** screen displays the options that you can customize.

Step 5 Check **Logo image** to customize the image that is displayed on the top left corner of the user interface.

a) Click **Upload** to browse to a logo image file and choose it.

Note

Make sure that the logo image is in PNG, JPG, or GIF format. The optimal image size is 200 pixels in width and 100 pixels in height. We recommend that you use a small file size to enable faster download.

b) Click **Submit**.

Step 6 Check **Application Labels** to specify a label that is displayed on the top header of the user interface.

a) Enter at least one application label in the **Label 1** and **Label 2** fields.

Step 7 Check **URL Forwarding on Logout** to re-direct users to a specific URL after logging out of the user interface.

a) In the **URL** field, enter the **URL**.

Step 8 Required: Check **Custom Links** to specify the links that appear on the top right corner of the user interface.

a) Complete at least the first two fields.

Name	Description
Custom Link 1 Label field	The label for custom link 1.
Custom Link 1 URL field	The URL for custom link 1.
Custom Link 2 Label field	The label for custom link 2.
Custom Link 2 URL field	The URL for custom link 2.

Step 9 Click **Submit**.

Branding Customer Organizations

You can customize the logo and application labels for customer organizations in Cisco UCS Director.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 Choose the **Customer Organizations** tab or the **MSP Organizations** tab.

These tab names are only indicative. If you have enabled the **Service Provider Feature**, you have to specify the names of the organization at the first and second level. The names that you specify are displayed as tabs in the interface. If you have disabled the **Service Provider Feature**, then only the **Customer Organizations** tab is displayed.

Step 3 Choose the customer organization to brand.

Step 4 From the **More Actions** drop-down menu, click **Branding**.

The **Group Branding** screen displays the options that you customize.

Step 5 Check **Logo image** to customize the image that is displayed on the top left corner of the user interface.

a) Click **Upload** to browse to a logo image file and choose it.

Note

Make sure that the logo image is in PNG, JPG, or GIF format. The optimal image size is 200 pixels in width and 100 pixels in height. We recommend that you use a small file size to enable faster download.

b) Click **Submit**.

Step 6 Check **Application Labels** to specify a label that is displayed on the top header of the user interface.

a) Enter at least one application label in the **Label 1** and **Label 2** fields.

Step 7 Check **URL Forwarding on Logout** to re-direct users to a specific URL after logging out of the user interface.

a) In the **URL** field, enter the **URL**.

Step 8 Required: Check **Custom Links** to specify the links that appear on the top right corner of the user interface.

a) Complete at least the first two fields.

Name	Description
Custom Link 1 Label field	The label for custom link 1.
Custom Link 1 URL field	The URL for custom link 1.
Custom Link 2 Label field	The label for custom link 2.
Custom Link 2 URL field	The URL for custom link 2.

Step 9 Click **Submit**.

Login Page Branding

A login page can be configured to display a logo that is associated with a domain name. When the end user logs in from that domain, the user sees the custom logo on the login page. The optimal image size for a logo is 890 pixels wide and 470 pixels high, with 255 pixels allowed for white space. Cisco recommends that you keep the image size small to enable faster downloads.



Note The group or customer organization login page must first be configured (enabled) for branding.

Configuring a Custom Domain Logo

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

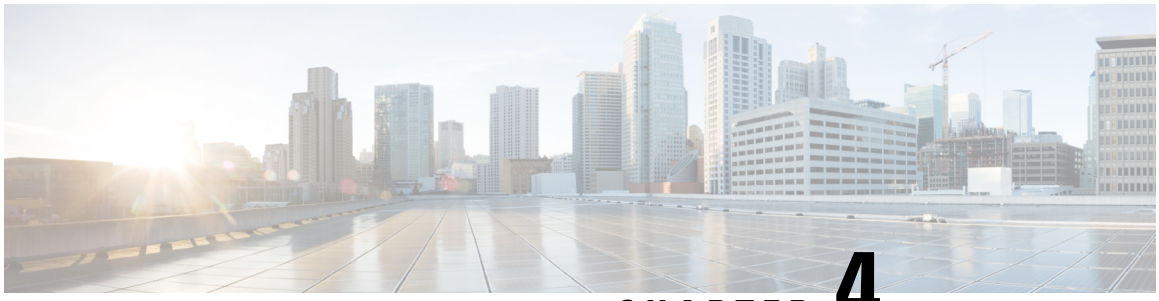
Step 2 On the **Users and Groups** page, click **Login Page Branding**.

Step 3 Click **Add**.

Step 4 In the **Domain Branding** screen, complete the required fields, including the following:

Name	Description
Domain Name field	The domain name to brand.
Custom Domain Logo check box	Check the check box to enable login page branding from a specified domain name.
File field	The logo file to upload. You can either drag and drop a file in this field, or you can click **Select a File** to browse and select the file to upload. **Note** The optimal image size for a logo is 890 pixels wide by 470 pixels high, with 255 pixels for white space. We recommend that you keep the image size small to enable faster downloads.

Step 5 Click **Submit**.



CHAPTER 4

Setting Up the End User Portal

- End User Portal, on page 103
- Summary of Tasks to Set Up the End User Portal, on page 103
- Setting Up User Accounts for the End User Portal, on page 104
- Setting Permissions for the End User Portal, on page 107
- Setting Up the User Interface of the End User Portal, on page 117

End User Portal

The End User Portal is a self-service portal that includes a catalog of services that you provide to the user. After an end user requests one of the services available, the End User Portal completes the service request workflow that you have configured for the user. This workflow may include approvals of the self-service provisioning request, assignment of the necessary compute, storage and network resources, and configuration of security and performance settings. After the service is provisioned, the end user can track the status of the services using the summary dashlets and summary reports on the landing page and through the reports available within the End User Portal.

Following are tasks that an end user can perform in the End User Portal:

- Provision virtual machines (VMs), application specific infrastructure, and bare metal servers
- Review and manage your service requests
- Upload and deploy OVFs and other images
- Monitor and create reports for your provisioned virtual and physical resources
- Approve service requests to provision infrastructure

Summary of Tasks to Set Up the End User Portal

As an administrator, following are the tasks you must complete to set up the End User Portal:

- Add user groups
- Add user accounts
- Set up end user permissions for specific tasks

- Set up the user interface of the portal

Setting Up User Accounts for the End User Portal

Creating a User Group

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **User Groups**.

Step 3 Click **Add**.

Step 4 On the **Add Group** screen, complete the following fields:

Field Name	Description
Name field	The name of the group or the customer organization. You can include special characters such as ( ). & - _ `~ $% ^ {}! '@
Description field	The description of the group or the customer organization, if required.
Code field	A shorter name or code name for the group. This name is used in VM and hostname templates.
Cost Center field	(Optional) The cost center name or number if required. This name or number represents a cost center that a group is associated with. This name can be used in a VMware System policy for the VM naming convention. For more information about using a cost center for naming conventions, see Managing Policies, on page 207.
Contact Email field	The email used to notify the group owner about the status of service requests and request approvals if necessary.
First Name field	The contact's first name.
Last Name field	The contact's last name.
Phone field	The contact's phone number.
Address field	The contact's address.
Group Share Policy drop-down list	Choose the group share policy for the users in this group. This drop-down list is populated only when you have created group share policies. For more information on creating this policy, see Creating a Group Share Policy, on page 218.

Field Name	Description
Allow Resource Assignment To Users check box	If checked, the users of this group can have resources assigned to them and can own these resources. Also, these users can view resources belonging to the group. However, the resources among these users cannot be shared.

Step 5 Click **Add**.

What to do next

Repeat this procedure if you want to add more groups. For each group that you add, you can edit resource limits, manage tags, and customize the logo and application labels.

Adding Users

Before you begin

Ensure that you have created a group before you add a user to it.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **Users**.

The **Users** page displays the following information for all user accounts currently available in the system:

- Status
- Login name and access level
- Email address
- Date when the user account will be disabled
- Current status of the password, and the date on which the password will expire

Step 3 Click **Add**.

Step 4 On the **Add User** screen, complete the required fields, including the following:

Field Name	Description
User Role drop-down list	Choose the role type for the user. **Note** This drop-down list displays all the available user roles in Cisco UCS Director. In addition to the user roles available by default, you can create additional user roles. For more information on creating user roles, see Adding a User Role, on page 27.

Field Name	Description
User Group drop-down list	Select the group that the user will have access to. You can either select a group already available, or you can add a new group. **Note** This field is visible only when you select Service End-User or Group Admin as the user role.
MSP Organization drop-down list	Select the MSP organization that the user will manage. You can either select an organization that is currently available, or you can add a new organization. **Note** This field is visible only when you select **MSP Admin** as the user role.
Login Name field	The login name. You can include special characters such as ( ). & - _ `~ $% ^ {}! ' @
Password field	The password. **Note** If Lightweight Directory Access Protocol (LDAP) authentication is configured for the user, the password is validated only at the LDAP server, and not at the local server.
Confirm Password field	The password is entered again for confirmation.
User Contact Email field	The email address. **Note** The email address is required to notify the group owner about the service request status and to request approval.
First Name field	The first name.
Last Name field	The last name.
Phone field	The phone number of the user.
Address field	The office address of the user.

Field Name	Description
Set user disable date check box	Check to set the date and time when the user account must be disabled in the system. Disabling a user account means that the user can no longer log in into the system. A week prior to this date, an email message stating that the account will be disabled is sent to the user. This automatic email message is generated and sent by the **PeriodicNotificationToUserTask** system task. On the specified date and time, the user account is disabled automatically. If the user is logged in to the system on the date specified, then the login session is terminated automatically.
Locale drop-down list	Choose a language for the system specifically for this user. By default, the language is set to English. When this user logs in, the user interface is displayed in the language you selected. This locale selection applies only to this user.

Step 5 Click **Add**.

What to do next

Click a row with a user and click **Manage Profiles**, to optionally assign multiple roles for that user.

Setting Permissions for the End User Portal

After you create user accounts for the End User Portal, you must provide these accounts with permissions to perform specific tasks. The subsequent sections list out the permissions that you need to able for end users to perform tasks such as managing catalogs or managing VMs.

Permissions Required for Approvals

The following table shows a list of the available approval actions and permissions required:

Task	End User Permissions
Viewing Service Request Details	Default
Approving a Service Request	Default
Rejecting a Service Request	Default
Canceling a Service Request	Default
Resubmitting a Service Request	Default

Task	End User Permissions
Archiving a Service Request	Default
Adding Notes to a Service Request	Default
Rolling Back a Service Request	Default

Permissions Required for Catalogs

The following table shows a list of the available catalog actions and permissions required:

Task	End User Permissions
Viewing Catalog Details	Default
Creating a Service Request for a Standard Catalog	Default
Creating a Service Request for an Advanced Catalog	Default
Creating a Service Request for a Service Container Catalog	Default
Creating a Service Request for a Bare Metal Catalog	Default
Running a Deployability Assessment	Default
Adding a Standard Catalog Item	Additional permissions required
Adding an Advanced Catalog Item	Additional permissions required
Adding a Service Container Catalog Item	Additional permissions required
Adding a Bare Metal Catalog Item	Additional permissions required
Cloning a Catalog Item	Additional permissions required
Editing a Catalog	Additional permissions required
Deleting a Catalog	Additional permissions required

Permissions Required for Budget Entries

You can perform actions on the budget entries. For some actions, additional permissions are required. The following table shows a list of the available budget entry management actions and permissions required:

Task	End User Permissions
Adding a Budget Entry	Additional permissions required
Viewing a Budget Entry	Additional permissions required

Physical Resources

Permissions Required for CloudSense Reports

The following table shows a list of the available CloudSense management actions and permissions required:

Task	End User Permissions
Generating a CloudSense Report	Default
Opening a CloudSense Report	Additional permissions required
Emailing a CloudSense Report	Additional permissions required
Deleting a CloudSense Report	Additional permissions required

Permissions Required for Rack Servers

The following table shows a list of the available rack server management actions and permissions required:

Task	End User Permissions
Powering a Rack Server On or Off	Additional permissions required
Shutting Down a Rack Server	Additional permissions required
Performing a Hard Reset on a Rack Server	Additional permissions required
Power Cycling a Rack Server	Additional permissions required
Launching the KVM Console for a Rack Server	Additional permissions required

Permissions Required for Servers

The following table shows a list of the available server management actions and permissions required:

Task	End User Permissions
Powering a Server On or Off	Additional permissions required
Associating a Server with a Service Profile	Additional permissions required
Disassociating a Server	Additional permissions required
Launching the KVM Console for a Server	Additional permissions required

Permissions Required for Service Profiles

The following table shows a list of the available service profile management actions and permissions required:

Task	End User Permissions
Viewing Service Profile Details	Default

Task	End User Permissions
Disassociating a Service Profile from a Server	Additional permissions required
Requesting an Inventory Collection	Additional permissions required

Permissions Required for SnapMirrors

The following table shows a list of the available SnapMirror actions and permissions required:

Task	End User Permissions
Viewing SnapMirror Details	Default

Permissions Required for Storage Virtual Machines

The following table shows a list of the available SVM management actions and permissions required:

Task	End User Permissions
Viewing SVM Details	Default

Permissions Required for vFilers

The following table shows a list of the available NetApp vFiler actions and permissions required:

Task	End User Permissions
Viewing vFiler Details	Default
Setting up a vFiler	Additional permissions required
Setting up CIFS on a vFiler	Additional permissions required

Permissions Required for SVM Initiator Groups

The following table shows a list of the available SVM initiator group actions and permissions required:

Task	End User Permissions
Creating an SVM Initiator Group	Additional permissions required
Renaming an SVM Initiator Group	Additional permissions required
Binding a Port Set to an SVM Initiator Group	Additional permissions required
Unbinding a Port Set from an SVM Initiator Group	Additional permissions required

Permissions Required for SVM LUNs

The following table shows a list of the available SVM LUN actions and permissions required:

Task	End User Permissions
Viewing SVM LUN details	Default
Creating an SVM LUN	Additional permissions required
Resizing an SVM LUN	Additional permissions required
Cloning an SVM LUN	Additional permissions required
Taking an SVM LUN Offline or Online	Additional permissions required
Mapping an SVM LUN to an Initiator Group	Additional permissions required
Unmapping an SVM LUN from an Initiator Group	Additional permissions required
Toggling the Space Reservation on an SVM LUN	Additional permissions required

Permissions Required for SVM CIFS Shares

The following table shows a list of the available CIFS share actions and permissions required:

Task	End User Permissions
Creating a CIFS Share on an SVM	Additional permissions required
Setting CIFS Share Access on an SVM	Additional permissions required

Permissions Required for SVM Export Policies

The following table shows a list of the available SVM export policy actions and permissions required:

Task	End User Permissions
Creating an Export Policy for an SVM	Additional permissions required

Permissions Required for SVM Export Rules

The following table shows a list of the available SVM export rule actions and permissions required:

Task	End User Permissions
Creating an SVM Export Rule	Additional permissions required

Permissions Required for SVM Initiators

The following table shows a list of the available SVM initiator actions and permissions required:

Task	End User Permissions
Creating an SVM Initiator	Additional permissions required

Permissions Required for SVM Port Sets

The following table shows a list of the available SVM port set actions and permissions required:

Task	End User Permissions
Creating an SVM Port Set	Additional permissions required
Destroying an SVM Port Set	Additional permissions required
Adding a Port to an SVM Port Set	Additional permissions required
Removing a Port from an SVM Port Set	Additional permissions required

Permissions Required for SVM SIS Policies

The following table shows a list of the available SVM SIS policy actions and permissions required:

Task	End User Permissions
Creating an SIS Policy for an SVM	Additional permissions required

Permissions Required for SVM Snapshot Policies

The following table shows a list of the available SVM snapshot policy actions and permissions required:

Task	End User Permissions
Viewing SVM Snapshot Policy Details	Default
Creating a Snapshot Policy on an SVM	Additional permissions required
Enabling and Disabling a Snapshot Policy on an SVM	Additional permissions required
Creating a Snapshot Policy Schedule for an SVM Snapshot Policy	Additional permissions required

Permissions Required for SVM WWPN Aliases

The following table shows a list of the available SVM WWPN alias actions and permissions required:

Task	End User Permissions
Creating a WWPN Alias on an SVM	Additional permissions required

Permissions Required for SVM Volume Snapshots

The following table shows a list of the available SVM volume snapshot actions and permissions required:

Task	End User Permissions
Creating a Snapshot for an SVM Volume	Additional permissions required
Restoring an SVM Volume from a Snapshot	Additional permissions required
Using a Snapshot to Restore a File on an SVM Volume	Additional permissions required
Using a Snapshot to Partially Restore a File on an SVM Volume	Additional permissions required

Permissions Required for SVM Volumes

The following table shows a list of the available SVM volume actions and permissions required:

Task	End User Permissions
Viewing SVM Volume Details	Default
Creating an SVM Volume	Additional permissions required
Taking an SVM Volume Offline or Online	Additional permissions required
Resizing an SVM Volume	Additional permissions required
Cloning an SVM Volume	Additional permissions required
Creating a Multi-Volume Snapshot	Additional permissions required
Moving an SVM Volume	Additional permissions required
Mounting and Unmounting an SVM Volume	Additional permissions required
Enabling and Disabling Deduplication on an SVM Volume	Additional permissions required
Starting Deduplication on an SVM Volume	Additional permissions required
Stopping Deduplication on an SVM Volume	Additional permissions required
Creating a Qtree on an SVM Volume	Additional permissions required
Running Inventory Collection on an SVM Volume	Additional permissions required
Setting the Snapshot Reserve for an SVM Volume	Additional permissions required
Assigning an SVM Volume to a Group	Additional permissions required
Unassigning an SVM Volume from a Group	Additional permissions required

Permissions Required for vFiler Volumes

The following table shows a list of the available vFiler volume actions and permissions required:

Task	End User Permissions
Viewing vFiler Volume Details	Default
Creating a vFiler Volume	Additional permissions required
Resizing a vFiler Volume	Additional permissions required
Taking a vFiler Volume Offline or ONline	Additional permissions required
Enabling and Disabling Deduplication on a vFiler Volume	Additional permissions required
Exporting a vFiler Volume using NFS	Additional permissions required
Creating a vFiler Volume Snapshot	Additional permissions required
Resizing the Snapshot Reserve for a vFiler Volume	Additional permissions required
Creating a CIFS Share on a vFiler Volume	Additional permissions required
Setting CIFS Share Access on a vFiler Volume	Additional permissions required
Creating a Qtree on a vFiler Volume	Additional permissions required

Services

Permissions Required for Service Requests

The following table shows a list of the available service request actions and permissions required:

Task	End User Permissions
Viewing Service Request Details	Default
Creating a Service Request for a Standard Catalog	Default
Creating a Service Request for an Advanced Catalog	Default
Creating a Service Request for a Service Container	Default
Creating a Service Request for a Bare Metal Catalog	Default
Canceling a Service Request	Default
Resubmitting a Service Request	Default
Archiving a Service Request	Default
Adding Notes to a Service Request	Default

Task	End User Permissions
Rolling Back a Service Request	Default

Permissions Required for User OVF Management

The following table shows a list of the available OVF management actions and permissions required:

Task	End User Permissions
Uploading an OVF File	Default
Deploying an OVF File	Default

Virtual Resources

Permissions Required for Application Containers

The following table shows a list of the available application container actions and permissions required:

Task	End User Permissions
Viewing Application Container Details	Default
Viewing Application Container Reports	Default
Managing an Application Container's Power	Default
Decommissioning an Application Container	Default
Cloning an Application Container	Default
Adding a VM to an Application Container	Default
Adding a Bare Metal Server to a Deployed APIC Application Container	Default
Deleting an Application Container	Default
Accessing a VM Console	Default
Editing Resource Limits	Default
Editing a Cost Model	Default
Adding an Application Container Contract	Default

Permissions Required for VMs

The following table shows a list of the available VM lifecycle management actions and permissions required:

Task	End User Permissions
Viewing VM Details	Default
Requesting Inventory Collection on a VM	Default
Launching the VM Client	Additional permissions required
Launching the VNC Console	Additional permissions required
Launching the VMRC HTML5 Console	Additional permissions required
Configuring the Lease Time for a VM	Additional permissions required
Managing a VM's Power	Additional permissions required
Creating a Snapshot	Additional permissions required
Reverting a Snapshot	Additional permissions required
Marking a Snapshot as Golden	Additional permissions required
Cloning a VM	Additional permissions required
Resizing a VM	Additional permissions required
Resynchronizing a VM	Additional permissions required
Creating a VM Disk	Additional permissions required
Adding a vNIC to a VM	Additional permissions required
Assigning a VM to a VDC	Additional permissions required
Moving a VM to a VDC	Additional permissions required
Cloning a VM as an Image	Additional permissions required
Converting a VM as an Image	Additional permissions required
Enabling and Disabling the VMRC Console on a VM	Additional permissions required
Mounting an ISO Image as a CD/DVD Drive	Additional permissions required
Unmounting an ISO Image as a CD/DVD Drive	Additional permissions required

Permissions Required for Images

The following table shows a list of the available image actions and permissions required:

Task	End User Permissions
Converting an Image to a VM	Additional Permissions Required
Deploying a VM from a Template	Additional Permissions Required

Setting Up the User Interface of the End User Portal

In addition to enabling permissions for end users, you can also enable certain elements in the End User Portal. These include:

- Configuring dashlets
- Configuring colors of dashlet reports
- Selecting catalogs

Configuring Dashlets

A dashlet is a report that you can display on the dashboard of End User Portal.

The available dashlets include:

- VMs
- UCS Servers
- Orders
- Catalogs
- Approvals

As an administrator, you can choose to display some or all of dashlets on the End User Portal to all users in all groups in the system, or to all users in specific user groups in the system. This procedure describes how to configure the dashlets for users within a specific group. To configure dashlets for all user groups, see Using the Global Dashlet Setup Option, on page 56.

Note All available dashlets are added to a user group only when the user group contains a user. When a user group does not have even one user, dashlets do not appear for the user group.

To configure dashlets for a specific user group, do the following:

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **User Groups**.

Step 3 Click the row with the user group for which you want to configure the dashlets.

Step 4 From the **More Actions** drop-down list, choose **Dashlet Setup**.
The **Dashlets Report** screen appears with all the available dashlets.

Note
When the user group does not have any users, dashlets do not appear in the **Dashlets Report** screen. Add a user to the user group to configure the dashlets.

Step 5 On the **Dashlets Report** screen, select the dashlet you do not want for the user group and click the **X (Delete)** icon.

Step 6 To add a dashlet to the user group, click the **+ (Add)** icon. On the **Add Entry** screen, do the following:

a) From the Dashlet Name list, select the dashlet type.
b) In the Dashlet Data Report section, click the **+ (Add)** icon.
c) In the Add Entry to Dashlet Data Report, select the entry (status, type, or state depending on the dashlet type you chose), assign a color to the entry, and click **Submit**.
d) Assign colors to the rest of the entries.
e) After assigning colors to the entries for the dashlet, click **Submit**.

Step 7 On the **Dashlets Report** screen, make sure the **Publish to end users** box is checked.

This option enables the dashlets to appear on the End User Portal for users of this group.

Step 8 Click **Submit**.

Changing Colors of Dashlet Reports

As an administrator, you can choose to change the color for each entry in the dashlet reports that appear on the End User Portal. An entry might be a status (In Progress or Completed), a category type (Standard or Advanced), or a power state (on or off) depending on the dashlet. For example, for the VMs dashlet, you can assign red for the ON state and gray for the Off state.

To change colors for entries in a dashlet report, do the following:

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **User Groups**.

Step 3 Click the row with the user group for which you want to configure the dashlet.

Step 4 From the **More Actions** drop-down list, choose **Dashlet Setup**.
The **Dashlets Report** screen appears with all the available dashlets.

Step 5 On the **Dashlets Report** screen, select the dashlet and click **Edit**.
The **Add Entry screen** appears.

Step 6 On the **Add Entry** screen, do the following:

a) In the Add Entry to Dashlet Data Report area, select the entry, assign a color to the entry, and click **Submit**.
b) Assign colors for the rest of the entries.
c) After assigning colors to the entries for the dashlet, click **Submit**.

Step 7 Make sure the **Publish to end users** box is checked.

This option enables the changes in the dashlet to appear on the End User Portal for users of this group.

Step 8 Click **Submit**.

Selecting Catalogs for End User Portal

As an administrator, you can enable folders and catalogs within these folders to appear on the dashboard of the end user portal. You can enable a maximum of 25 catalog folders and a maximum of 25 catalogs within a folder to appear on the dashboard of the end user portal.

To configure catalogs to appear on the dashboard of the end user portal, do the following:

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **User Groups**.

Step 3 If you have MSP-mode enabled, then choose the **Customer Organizations** tab.

Step 4 Click the row with the user group for which you want to configure the catalogs.

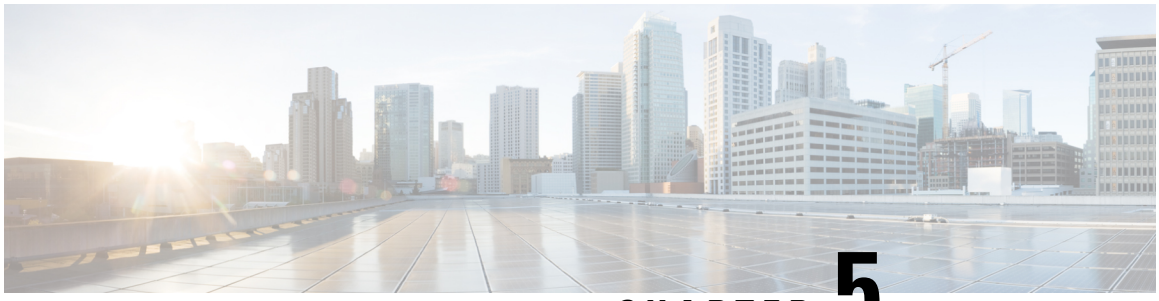
Step 5 From the **More Actions** drop-down list, choose **Catalog Setup**.
The **Configure Catalog** screen appears with the list of catalogs available for the user group.

Note
If catalogs have not been assigned to the user group, the **Configure Catalog** screen is empty.

Step 6 On the **Configure Catalog** screen, check the catalogs that must appear on the End User Portal dashboard.

Step 7 Click **Submit**.

When users that belong to the group login to the end user portal, the dashboard is populated with the selected catalogs and catalog folders.



CHAPTER 5

Managing System Administration Settings

This chapter contains the following sections:

- Setting up the Outgoing Mail Server, on page 121
- Working with Email Templates, on page 122
- Configuring System Parameters (Optional), on page 125
- Running an Object Search, on page 127
- Viewing Workflow Tasks in the Workflow Designer, on page 128
- Working with Licenses in Cisco UCS Director, on page 129
- Application Categories, on page 136
- Customizing the Portal, on page 138
- Customizing Reports, on page 142
- Enabling Advanced Controls, on page 143
- Enabling the Service Provider Feature, on page 145
- User Menus, on page 145
- Setting User Permissions, on page 146
- System Tasks, on page 146
- Managing Icons in the Cisco UCS Director User Interface, on page 153
- Tag Library , on page 156
- Support Information, on page 158
- Database Audit Logging, on page 162
- Device Connector, on page 163
- Launching Cisco UCS Director from Cisco Intersight, on page 164
- Connector Pack Management, on page 165
- Alert About Insecure Protocols , on page 173

Setting up the Outgoing Mail Server

All outgoing emails from Cisco UCS Director require an SMTP server.

Note In the case of configuring an Outgoing Email Server with an SMTP FQDN, the DNS IP for the mail server remains cached indefinitely. Consequently, if the IP for the SMTP FQDN changes, UCSD fails to send emails as it continues to send them to the original IP address.

Although the returned IP has a TTL (Time to Live), UCS-Director does not utilize it. Instead, it caches the IP indefinitely until UCS-Director is restarted.

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **Mail Setup**.

Step 3 On the **Mail Setup** screen, complete the following fields:

Name	Description
Outgoing Email Server (SMTP) field	The outgoing SMTP server address.
Outgoing SMTP Port field	The outgoing SMTP server port number.
Outgoing SMTP User field	The user ID.
Outgoing SMTP Password field	The user password.
Outgoing Email Sender Email Address field	The sender's email address
Server IP address field	The IP address or DNS name of the Cisco UCS Director virtual appliance. This field is used to create proper links in emails for user workflow actions.
Send Test Email check box	Check this check box to test the current email settings.

Step 4 Click **Save**.

Working with Email Templates

Cisco UCS Director has a notification mechanism that enables you to configure emails to be sent to an administrator when specific events occur, such as when a VM is provisioned. In addition, if approvals are required for any task, an email notification can be sent to an administrator or to the group administrator.

Note You can specify multiple recipients for an email notification. Use a comma as a separator for multiple email addresses.

Cisco UCS Director provides a set of email templates in the HTML format that cover different scenarios. The following are some of the tasks that you can perform with email templates library:

- Add a new email template
- Edit an existing email template—You can edit the subject and message details, or the formatting and presentation fields of an email template. Do not modify any Java-related information in the template.
- Preview an email template—You can preview the email content and determine if the email template needs modification.
- Set an email template as default—You can set email notifications to be sent based on the default email template.
- Delete an email template—You can delete the templates that you have added. However, you cannot delete a template if it meets one of the following criteria:
  - You added a template and set it as a default template.
  - It is a system-provided template.

Adding an Email Template

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **Email Templates**.

Step 3 Click **Add**.

Step 4 On the **Add Template** screen, complete the following fields:

Name	Description
Email Template Name field	The name of the email template.
Template Description field	The description of the email template.
Template Type drop-down list	Select the type of email template that you are adding. This drop-down list is populated with the system-provided templates.
Subject field	The subject line for the email template.
Reset to Default Subject check box	If you check this check box, the subject line you entered is cleared, and the system-provided subject line is populated in the **Subject** field.
Body field	The HTML code that defines the email template, such as the email content, font size and color, the notification triggers, and so on.

Name	Description
Reset to Default Body check box	If you check this box, the HTML code used in the system-provided email template is populated in the **Script** field. After the HTML code is populated, to retain the changes you made to the code, you must uncheck this box.

Step 5 Click **Submit**.

What to do next

Preview the email template to determine if you need to make more changes.

Previewing an Email Template

After you create a new email template in Cisco UCS Director, you can preview the email content to determine if you need to make any additional changes.

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **Email Templates**.

Step 3 Expand the folder with the email template type, and click the row with the email template that you want to preview.

Step 4 Click **Preview Template**.

Step 5 On the **Launch Report** screen, click **Submit**.

Note
The preview mode of an email template displays only static information. Dynamic information such as the customer name, or resources, is not displayed.

What to do next

If necessary, you can return to the email template to make additional changes.

Setting a Default Email Template

Usually, a system template is set as the default email template. If you have added multiple templates for a specific scenario, you can choose to select one of these templates as a default template. Setting a template as default means that the selected template is used for notification.

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **Email Templates**.

Step 3 Expand the folder with the email template type, and click the row with the email template that you want to set as the default.

Step 4 Click **Set As Default Email Template**.

Configuring System Parameters (Optional)

Configuring System Parameters

You should edit the system parameters only if you need to change the default values.

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **System Parameters**.

Step 3 On the **System** screen, complete the following fields:

Name	Description
Number of Days to Keep Deleted VMs Data field	The user-defined number of days that the system retains VM data.
Number of Days to Keep Events field	The user-defined number of days that the system retains all events. **Note** Events older than the specified time period are deleted.
Number of Days to Keep Trend Data field	The user-defined number of days that the system retains trend data or historical data of the inventory (such as CPU, storage, and memory usage). **Note** This data is used for reporting.
Number of Days to Keep Metering Data drop-down list	Choose the number of days that the system retains VM metering records. **Note** This data is specific to VMs and their resources.

Name	Description
Number of Days to Keep User-Created Files drop-down list	Choose the number of days that the system retains user-created files. **Note** The Clean Up User Created Files task deletes the unused files created while generating reports, uploading files, and exporting content. The task deletes files that are older than the number of days you configure.
Download VM Locking Controls from URL field	The URL of the VM locking controls file that is hosted on a server that is accessible from the system that is running Cisco UCS Director. **Note** This file must be in XML format. For more information on creating this VM locking controls file, see Locking VMs in Cisco UCS Director, on page 405.
Currency drop-down list	Choose the type of currency to use. Available currencies are USD, EURO, GBP, KRW, CAD, CHF, CLP, INR, JPY, AUD, NZD, SGD, HKD, MYR, MXN, BRL, AED, DKK, SEK, KWD, CYN, RUB, ZAR, and Other.
Other Currency field	Enter the currency name (one only). **Note** This field appears when **Other** is chosen as the Currency.
Currency Precision drop-down list	Refers to the number of decimal places used to display the currency values. Available precision is from 0 to 5 decimal points.
Approval Task Expiry Days drop-down list	Choose the number of days an approval task must remain available for action by approvers. The available options are Never, 7, 15, and 30 days. Once the selected period expires, the system automatically cancels the approval task. **Never** is set as the default value. When **Never** is selected, the task will not expire and will remain active indefinitely.

Step 4 Click **Save**.

Configuring Infrastructure System Parameters (Optional)

You can set parameters for polling the virtual and physical system infrastructure resources.

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **Infrastructure System Parameters**.

Step 3 On the **Infrastructure System Parameters** screen, enter the number of days to keep trend data for the system infrastructure. The default is 30 days.

Step 4 Click **Save**.

Configuring Proxy Settings

Perform this procedure when you want to configure proxy settings.

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **Proxy Configuration**.

Step 3 Complete the required fields, including the following, to configure proxy on the system:

Field	Description
Enable Proxy Configuration check box	(Optional) Check this check box to enable proxy and complete the following: • **Host Name** field - Enter a host name for the proxy configuration. • **Port** field - Enter the port for the proxy configuration.
Enable Proxy Authentication check box	(Optional) Check this check box to enable proxy authentication and complete the following: • **Proxy User Name** field - Enter a proxy user name for the proxy authentication. • **Proxy Password** field - Enter the password for the proxy user name.

Step 4 Click **Save**.

Running an Object Search

Use the object search feature to locate a specific report from the following screens in the user interface:

- **Physical**
- **Virtual**
- **Workflows**
- **Custom Tasks**

Procedure

Step 1 Choose **Sitemap**.

Step 2 On the **Sitemap** screen, click **Object Search**.

Step 3 To determine the tabs that the search should run on, choose **Advanced Search**.

Any report that contains the searchable objects in the **Physical** and **Virtual** screens are displayed, along with the options to choose **Workflows** and **Custom Tasks**.

By default, all these options are selected.

Step 4 Clear the check boxes of the tabs that you do not want the search to include.

Step 5 In the **Search** field, we recommend that you enter 3 characters of the object you want to locate.

The search field is case sensitive.

Step 6 Click the **Search** icon or press **Enter** on your keyboard.
All reports that match the search criteria are displayed.

Viewing Workflow Tasks in the Workflow Designer

Before you begin

You must have read-only privileges for Orchestration assigned to your administrator user role. For information on creating or or modifying user roles, see Adding a User Role, on page 27.

Procedure

Step 1 Choose **Orchestration**.

Step 2 On the **Orchestration** page, click **Workflows**.

Step 3 Choose a workflow task from the list.

Step 4 Choose **Workflow Designer**.

The subsequent screen displays the details of the workflow. All information on this screen is read-only. You cannot edit the workflow tasks.

Step 5 Double-click on a workflow task in the **Workflow Designer** to review the detailed information.

Step 6 Review the information on the screen, and click **Close**.

Working with Licenses in Cisco UCS Director

Licenses enable you to add or manage resources in your environment. The Cisco UCS Director supports the following licenses:

- Evaluation license—Free trial license with an expiry date. This license is also referred to as the default license. It is valid for 90 days.
- Production License—With this license, you can add server, storage and network licenses in your environment.
- ELA license—With this license, you can provided unlimited count of resources. For example, if you add a server license to an ELA license, then you can manage an unlimited number of servers in your environment.

These licenses are also referred as the base license, using which users can access resources such as Users, Groups, VDCs, and Catalogs in the Cisco UCS Director. In addition to the base licenses, the Cisco UCS Director supports the use of subscription licenses. These subscription licenses may or may not include a base license.

The administrator user interface of Cisco UCS Director provides you with a number of options and reports, using which, you can perform several administrative tasks with licenses.

Following are the options that you can use to perform specific tasks:

Option Name	Description	Additional Information Available in
Update License	Use this option to add a new license to your system.	Updating the License, on page 133
Apply Upgrade License	Use this option to upgrade a specific license to get server, storage, network, and VM counts.	Applying Upgrade License, on page 132
Replace License	Use this option to deactivate and delete all existing licenses, including the base license, and replace it with a new license. However, the new license must include a base license. For example: Use the **Replace Option** if you have a base license currently installed, and have to install a subscription license that includes a base license within it.	Replacing a License, on page 133

Option Name	Description	Additional Information Available in
Migrate License	Use this option to delete all existing system licenses, except the base license, and add a new license. The new license that you want to migrate to must be of the same license type. For example, you can migrate from one production license to another production license. But you cannot migrate from a production license to an Evaluation license. You can also use this option if you have a base license currently installed, and have to install a subscription license that does not include a base license.	Migrating a License, on page 132

Following are some of the reports that you can view to understand license utilization and usage in Cisco UCS Director:

Report Name	Displays Information On	Additional Information in
License Keys	Lists all available license keys in the system. It also lists the license features, the license count and the expiry date.	Viewing License Key Information, on page 135
License Utilization	Lists all the licenses that are in use, available licenses, and the actual license limit of all resources. This screen is populated with results from the **License Audit** task. This task collects license usage and license limit of all resources and displays it on the **License Utilization** screen. The **License Audit** task runs every 4 hours, by default.	Verifying License Utilization, on page 134
License Status	Displays information on license violations, if any. For example, violations such as exceeding license limit for a resource, or the absence of a permanent license in the system are displayed on this screen.	Viewing License Status, on page 136

Report Name	Displays Information On	Additional Information in
License Utilization History	Displays periodic license utilization for Network controllers, storage controllers, servers, server VMs, desktop VMs, small pods and medium pod resources. This screen is populated with results from the System resource Util Snapshot scheduler task that runs every 24 hours.	Viewing License Utilization History, on page 134
Resource Usage Data	Displays the resource usage of different resources in the system, such as users, VDCs, service requests, public and private clouds, and physical servers. Every time you add or delete a resource from the system, this report is updated.	Viewing Resource Usage Data, on page 136
Deactivated Licenses	Displays all the licenses that were deleted when you used the Replace Licenses option. This screen also displays the user who replaced the license, and the time when the license was deactivated.	Viewing Deactivated License Information, on page 135



Important The Cisco UCS Director 6.9(1.0) does not have BigData personality. When you upgrade from Cisco UCS Director 6.9(0.0) or migrate from Cisco UCS Director 6.7(4.3)/6.8(x.x) to Cisco UCS Director 6.9(1.0), ensure that the **BigData** check box is unchecked under the **Manage Personalities** field in the **License Keys** pane.

The migration process fails when you upgrade or migrate to Cisco UCS Director 6.9(1.0) with **BigData** personality enabled and the following error message is displayed:

```
ERROR: Cisco UCS Director personality mismatch. Configure correct personality for current
appliance and try migration.
Exiting the migration process.
```

Limitations on Using NFR and Permanent Physical Server Licenses

Physical server licenses with valid expiry dates will remain supported until their expiry. Starting with Cisco UCS Director Release 6.9(3.0), the support for permanent and subscription-based NFR licenses, and permanent physical server licenses is discontinued. However, you can continue using these licenses for up to 90 days from the activation date of Cisco UCS Director Release 6.9(3.0). During this 90-day grace period, the system will display a warning message indicating the limited support for these licenses.

Procedure

Step 1 Choose **Administration** > **License**.

Step 2 On the **License** page, click **License Keys**.

The following warning message is displayed:

License is no longer supported and will expire in 90 days. Please contact your sales representative to purchase a valid license.

Note After 90 days, provisioning of accounts will not be allowed.

Applying Upgrade License

Use this option to upgrade a specific license to get server, storage, network, and VM counts. You can convert small pod or medium pod licenses to server, storage, network or VM counts. 1 pod license provides 8 physical servers, 8 storage resources, 8 network resources, 400 VMs and 8 other resources.

Procedure

Step 1 Choose **Administration** > **License**.

Step 2 On the **License** page, click **License Keys**.

Step 3 Choose **Apply Upgrade License**.

Step 4 Choose an option from the **Select Upgrade Type** drop-down list.

Step 5 Specify the number of pods to upgrade.

Step 6 Click **Apply**.

Migrating a License

Use this procedure to delete all exiting licenses, except the base license, and add a new license to the system.

Important When you migrate to a subscription-based license, ensure that the subscription license quantity is less than or equal to the perpetual license quantity allocated for physical servers. Otherwise, the following error message is displayed:

```
Migration to a subscription-based license failed. Subscription license quantity is more
than the existing perpetual license quantity. Please make sure the new subscription license
quantity is accurate.
```

Procedure

Step 1 Choose **Administration** > **License**.
Step 2 On the **License** page, click **License Keys**.
Step 3 Choose **Migrate License**.
Step 4 In the **File** field, you can either drag and drop a PAK file or click **Select a File** to browse and select a file.
Step 5 (Optional) Check **Enter License Text** to copy and paste the license text.
Step 6 Click **Submit**.

Replacing a License

You can use this procedure to replace a license in the system. This action will deactivate all other existing licenses on the systems.

Procedure

Step 1 Choose **Administration** > **License**.
Step 2 On the **License** page, click **License Keys**.
Step 3 Choose **Replace License**.
Step 4 In the **File** field, you can either drag and drop a PAK file or click **Select a File** to browse and select a file.
Step 5 (Optional) Check **Enter License Text** to copy and paste the license text.
Step 6 Click **Submit**.

All existing licenses are replaced with the new license.

Updating the License

You can update the license using the Product Authorization Key (PAK). However, you cannot mix license types in your environment. For example, you cannot use this option to update a permanent license with a subscription license.

Procedure

Step 1 Choose **Administration** > **License**.
Step 2 On the **License** page, click **License Keys**.
Step 3 Click **Update License**.
The **Update License** screen is displayed.
Step 4 Click **Select a File** to navigate and to choose the PAK license file.

Step 5 Click **Upload** to upload the PAK license file.

Note
If the license file does not upload, check the check box and copy and paste the license text into the license text field.

Step 6 Click **Submit**.
The license is updated.

Verifying License Utilization

The **License Utilization** page shows the licenses in use and details about each license, including license limit, available quantity, status, and remarks. License audits can also be run from this page.

Procedure

Step 1 Choose **Administration** > **License**.
Step 2 On the **License** page, click **License Utilization**.
Step 3 Click the row with the license that you want to verify.
Step 4 (Optional) To run a license audit, click **Run License Audit**.
Step 5 On the **Run License Audit** screen, click **Submit**.

This process takes several minutes to run.

Viewing License Utilization History

The number of licensed network and storage controllers, servers, server and desktop VMs, and small and medium pods can be tracked over time to see how network resources are being utilized.

Procedure

Step 1 Choose **Administration** > **License**.
Step 2 On the **License** page, click **License Utilization History**.

The license utilization history is displayed for the following resource categories, with timestamp:

- Network Controllers
- Storage Controllers
- Servers
- Server VMs

- Desktop VMs
- Small pods
- Medium pods

Viewing Deactivated License Information

You can view the list of deactivated licenses from the user interface. You can view the following information on deactivated licenses:

- PAK file name
- File ID
- License Entry
- Licence Value
- Expiry Date
- Deactivated Time
- Name of user who deactivated the license

Procedure

Step 1 Choose **Administration** > **License**.
Step 2 On the **License** page, click **Deactivated Licenses**.
Step 3 Review the information displayed for all the deactivated licenses.

Viewing License Key Information

The **License Keys** screen lists all available license keys in the system. It also lists the license features, the license count and the expiry date.

Procedure

Step 1 Choose **Administration** > **License**.
Step 2 On the **License** page, click **License Keys**.
Step 3 Review the information displayed on the screen.

Viewing License Status

The **License Status** page displays information on license violations, if any.

Procedure

Step 1 Choose **Administration** > **License**.

Step 2 On the **License** page, click **License Status**.

Step 3 Review the information displayed in the screen.

Viewing Resource Usage Data

You can view how resources are being utilized in your environment.

Procedure

Step 1 Choose **Administration** > **License**.

Step 2 On the **License** page, click **Resource Usage Data**.

Following are the available report categories:

- Resource Name—Name of the available resources associated with Cisco UCS Director.
- Resource Count—Quantity of each available resource.

Application Categories

Application categories are an optional configuration that enable you to define the type of workload for a VM. If you do not use application categories, Cisco UCS Director assumes that all VMs provisioned for your users are generic VMs and configures them to handle CPU-intensive workloads. Whether you choose to use the default application categories or to create your own, you can provide your users with a pre-defined set of workloads that match their application needs.

The workload options for application categories include the following:

- CPU intensive
- Network I/O intensive
- Disk I/O intensive
- Memory intensive
- Any combination of the above

After you create your application categories, you can go to the desired cloud account and assign the vDC policies to the application categories. This assignment determines the boundaries of the infrastructure where the application can be provisioned. You can also use application categories to allocate clusters based on the type of application. For example, Cluster 1 is allocated for Web applications and Cluster 2 is allocated for database applications.

When an application category is chosen by a user, Cisco UCS Director uses the vDC assignment to determine which location, within the boundary of the vDC, best meets the application's workload needs. For example, if the user chooses a CPU-intensive application category, Cisco UCS Director provisions the application in the available infrastructure with the least CPU utilization.

Adding Application Categories

By default, Cisco UCS Director provides the following application categories for you to use or edit:

- Discovered VM
- Generic VM
- Web Server
- Application Server
- Database
- App—CPU Intensive
- App—Memory Intensive
- App—Disk Intensive
- App—Network Intensive
- Other App 1
- Other App 2
- Other App 3

Cisco UCS Director allows you to create application categories for multiple virtual data centers at a system level. This capability eliminates the repetitive task of selecting individual virtual data centers and assigning policies for categories.

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **Application Categories**.

Step 3 Click **Add**.

Step 4 On the **Add Category** screen, complete the following fields:

Name	Description
Category Label field	A unique name for the category.

Name	Description
Category Code field	Specify a code for the category. You can use this code in the VM or host name templates.
Category Description field	A description of the category.
Category Enabled check box	Check this check box to enable the category. Enabling a category implies that you can select this category during VDC assignment. If you do not check this check box, then this category cannot be used in the system.
Default Smart Allocation Algorithm drop-down list	Choose a default algorithm that must be applied during VM provisioning.

Step 5 Click **Submit**.

The application category is displayed when you click the **Manage Categories** option for a virtual data center.

What to do next

After you have created an application category, you can perform the following tasks:

- Edit or clone the application category
- Assign the application category to multiple virtual data centers. For more information, see Managing Application Categories in a Virtual Data Centers, on page 252.

Customizing the Portal

Organizations can customize the End User Portal. The logo, login page, home page, and so on can be customized for branding and user interface-related changes.

Customizing the Login Page and Background Images

You can change the login page and background images by uploading custom images.

Procedure

Step 1 Choose **Administration** > **User Interface Settings**.

Step 2 On the **User Interface Settings** page, click **Login Page**.

Step 3 Check **Use customizable Login page**.

Step 4 In the **Logo Images** section, click **Add** and complete the following fields:

Field	Description
Image Label field	A name for the image.
Description field	A description for the image that you upload.
Select a file for upload field	Click **Browse** to search and select an image file. **Important** An optimal image is 200 pixels in width and 100 pixels in height and is in the PNG format.
Upload option	Click this option to upload the image. This option is enabled only after you have browsed and selected an image.
Submit option	Click **Submit** after the image is uploaded.

Step 5 In the **Background Images** section, choose an item or click **Add** and complete the following fields:

Field	Description
Image Label field	A name for the image.
Description field	A description for the image that you upload.
Select a file for Upload field	Click **Browse** to search and select an image file. **Important** An optimal image is 890 pixels in width, 470 pixels in height, and has 255 pixels of white space. In addition, the image must be in the PNG format.
Upload option	Click this option to upload the image. This option is enabled only after you have browsed and selected an image.

Step 6 Click **Submit**.

Customizing the Application Logo

You can customize the application logo on the home page by uploading a custom image.

Procedure

Step 1 Choose **Administration** > **User Interface Settings**.

Step 2 On the **User Interface Settings** page, click **Application Logo**.

Step 3 In the **Images** section, click **Add** to add a new image that is not listed, and complete the following fields:

Field	Description
Image Label field	A name for the image.
Description field	A description for the image that you upload.
Select a file for upload field	Click **Browse** to search and select an image file. **Important** Supported image formats are PNG, JPG, and GIF. An optimal image size is 100 pixels in width and 50 pixels in height.
Upload option	Click this option to upload the image. This option is enabled only after you have browsed and selected an image.

Step 4 Click **Submit**.

Customizing Favicons

You can customize a favorites icon (Favicon) that is displayed in the browser's address bar or next to the page name, if it is bookmarked.

Procedure

Step 1 Choose **Administration** > **User Interface Settings**.

Step 2 On the **User Interface Settings** page, click **Favicon**.

Step 3 In the **Images** section, click **Add** to add a new image not listed and complete the following fields:

Field	Description
Image Label field	A name for the image.
Description field	A description for the image that you upload.
Select a file for upload field	Click **Browse** to search and select an image file. **Important** Supported image format is PNG. An optimal image size is 16x16 pixels.
Upload option	Click this option to upload the image. This option is enabled only after you have browsed and selected an image.

Step 4 Click **Submit**.

Customizing Application Header

You can customize the End User Portal labels, next to the customer logo, by modifying existing labels.

Procedure

Step 1 Choose **Administration** > **User Interface Settings**.

Step 2 On the **User Interface Settings** page, click **Application Header**.

Step 3 Complete the following fields:

Name	Description
Hide Entire Header check box	Check to hide the header section. If checked, the header that contains the logo image, application name, and links, such as **Logout**, are hidden.
Product Name field	The product name that must be displayed in the header.
Product Name 2nd Line field	The second title of the product.
Enable About Dialog check box	Check to enable the **About** link in the header. Uncheck to disable the **About** link in the header.
Administrator Portal	
Custom Link 1 Label field	The custom link label 1 for the administrator portal.
Custom Link 1 URL field	The custom link URL 1 for the administrator portal.
Custom Link 2 Label field	The custom link label 2 for the administrator portal.
Custom Link 2 URL field	The custom link URL 2 for the administrator portal.
End User Portal	
Custom Link 1 Label field	The custom link label 1 for the End User Portal.
Custom Link 1 URL field	The custom link URL 1 for the End User Portal
Custom Link 2 Label field	The custom link label 2 for the End User Portal.
Custom Link 2 URL field	The custom link URL 2 for the End User Portal.

Step 4 Click **Save**.

Customizing Date Display

Numerous data display formats are supported.

Procedure

Step 1 Choose **Administration** > **User Interface Settings**.
Step 2 On the **User Interface Settings** page, click **Date Display**.
Step 3 Edit the date format.
Step 4 If required, check **Hide Timezone** to hide the time zone display from the user interface.
Step 5 Click **Save**.

Customizing the Color Theme

Procedure

Step 1 Choose **Administration** > **User Interface Settings**.
Step 2 On the **User Interface Settings** page, click **Color Theme**.
Step 3 From the drop-down list, choose from the available theme styles.
Step 4 Click **Save**.

Customizing Logout Redirect

Procedure

Step 1 Choose **Administration** > **User Interface Settings**.
Step 2 On the **User Interface Settings** page, click **Logout Redirect**.
Step 3 In the **Logout Redirect** field, enter the URL.
Step 4 Click **Save**.

Customizing Reports

Report customization enables you to make a custom label or hide the available reports.

Note You cannot customize or hide reports for users and groups. You can customize the report table on all other pages. You can customize only those reports that are identified as **Tabular with actions**.

Procedure

Step 1 Choose **Administration** > **User Interface Settings**.

Step 2 On the **User Interface Settings** page, click **Reports Customization**.

Step 3 Click the row with the report that you want to customize.

Step 4 Click **Edit**.

Step 5 On the **Customize Report** screen, complete the following fields:

Name	Description
Hide Report check box	Check to hide the report. Uncheck to show the report.
New Label field	A new label for the report, if required.

Step 6 Click **Save**.

Enabling Advanced Controls

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **Advanced Controls**.

Step 3 Check the required fields:

Name	Description
Performance Monitoring check box	Check to enable virtual infrastructure monitoring, physical infrastructure monitoring, and external cloud monitoring. Check all additional check boxes under this category, as needed.
Resource Metering check box	Check to enable monitoring of VM metering functions. **Note** If the VM metering function is disabled, chargeback does not work.

Name	Description
Event Monitoring check box	Check to enable virtual and physical infrastructure events.
Auto Support check box	Check to enable automatic support.
Heat Map Report Computing check box	Check to enable generation of heat map reports for the virtual infrastructure.
Automatic Assessment check box	Check to generate reports on virtual assessment.
Adaptive Provisioning Indexing check box	Check to enable and compute the load indices for hosts for various host parameters every 4 hours. These indices are used in adaptive provisioning of the catalogs. A lower index indicates a better chance for the host being chosen for provisioning. This process works according to the computing policy of a specific VDC.
Delete Inactive VMs Based on VDC Policy check box	Check to enable and delete the inactive (powered off) VMs under a VDC after a time that is specified by the administrator. The deletion of these inactive VMs is also based on the VM management policy defined by the administrator. Before an inactive VM is is deleted, an email notification is sent to the user. This property is associated with the **Delete after inactive VM days** field in the VM management policy. See Configuring a VM Management Policy, on page 243. **Note** By default, the property box is not checked.
System Task Remoting check box	Check to administratively enable the remote execution.
Force User Password Reset check box	Check to make password reset mandatory for new users at first login. A user, whose password is changed by any other user, will be forced to reset the password upon his successive login. **Note** **Force User Password Reset** is applicable for Local users only.

Step 4 Click **Submit**.

Enabling the Service Provider Feature

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **Service Provider Feature**.

Step 3 Complete the following fields:

Name	Description
Enable Service Provider Feature (Requires System Restart) check box	Check to enable service providers in Cisco UCS Director.
Organization Name (First Level) field	The name of the parent organization for which this feature should be enabled.
Organization Name (Second Level) field	The name of the child organization for which this feature should be enabled.

Step 4 Click **Submit**.

User Menus

You can enable customized menu operations for individual user roles. The menu settings that users can view and access in the application is dependent on the user roles that they have been assigned, and the menu operations that you set for the roles.

Setting User Menus

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **User Roles**.

Step 3 Click the row with the user role for which you want to edit the user menus.

Step 4 Click **Edit**.

Step 5 On the **Edit User Role** screen, click **Next**.

Step 6 On the **Menu Settings** screen, you can view the menu settings for the chosen user role.

Step 7 Check or uncheck the menu check boxes to allow menus for that role, or check **Reset to Defaults**.

Step 8 Click **Submit**.

Setting User Permissions

Procedure

Step 1 Choose **Administration** > **System**.
Step 2 On the **System** page, click **User Roles**.
Step 3 Click the row with the user role for which you want to edit the user permissions.
Step 4 Click **Edit**.
Step 5 On the **Edit User Role** screen, click **Next**.
Step 6 On the **User Permissions** screen, you can view the read and write operations for the chosen user role.
Step 7 Check or uncheck the check boxes to allow read and write operations for an individual role, or check **Reset to Defaults**.
Step 8 Click **Submit**.

System Tasks

The **System Tasks** screen displays all the system tasks that are currently available in Cisco UCS Director. However, this list of system tasks is linked to the type of accounts that you have created in Cisco UCS Director. For example, if you have logged in for the first time, then only a set of general system-related tasks or VMware related tasks are visible on this page. When you add accounts, such as rack accounts or Cisco UCS Manager accounts, system tasks related to these accounts are populated on this page.

Following are the tasks that you can complete from the **System Tasks** screen:

- View the available systems tasks—You can use the **Expand** and **Collapse** options to view all the system tasks that are available on this page. The tasks are categorized according to the accounts available in Cisco UCS Director. For example: Cisco UCS Tasks or NetApp Tasks.
- Manage system tasks—You can select a system task on the **System Tasks** screen, and click **Manage Task**. From this **Manage Task** screen, you can perform the following tasks:
  - Disable and enable system tasks—In circumstances when there are multiple processes or tasks running on the appliance, you can choose to disable a system task. If you do so, then until such time that you manually enable it, the system task will not run. This will affect the data populated in other reports. For example, if you disable an inventory collection system task, then reports that require this data may not display accurate data. In this case, you will have to manually run an inventory collection process, or enable the system task.

    For more information, see Disabling or Enabling a System Task, on page 150.

- Modify the schedule for the system task—You can modify the schedule type for a system task, or you can configure a custom frequency for the task. For more information, see Scheduling a System Task, on page 151

In a single-node setup, where there is only one server, all system tasks run on this server. In a multi-node setup, where there are multiple servers configured, all system tasks run on the primary server by default. However, you can specify system tasks to run on the secondary servers. Following are the recommended steps to perform this task:

1. Ensure that the secondary servers are available in Cisco UCS Director as nodes. If the servers are not available, then you must add the servers as nodes. See Creating a Service Node, on page 148.
2. Create a node pool from the available servers. See Creating a Node Pool, on page 147.
3. Create a system task policy, and associate it with a node policy. See Creating a System Task Policy, on page 147.
4. Associate a node pool with the system task policy. See Assigning a Node Pool to a System Task Policy, on page 148.
5. Select a system task, and associate it with a system-task policy. See Assigning a System Policy to a System Task, on page 149.

Creating a Node Pool

Procedure

Step 1 Choose **Administration** > **System**.
Step 2 On the **System** page, click **Service Nodes**.
Step 3 Click **Service Node Pools**.
Step 4 On the **Service Node Pool** screen, click **Add**.
Step 5 On the **Add Entry to Service Node Pools** screen enter the node pool name in the **Name** field.
Step 6 (Optional) In the **Description** field, enter a description of the node pool name.
Step 7 Click **Submit**. The node pool is created.

Creating a System Task Policy

As an administrator, you can choose to combine a few policies and create a system task policy, in addition to the default system task policy. You can group system tasks into a system task policy to later determine which system tasks are running on which node.

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **System Task Policy**.
Step 3 Click **Add**.
Step 4 On the **Add** screen, enter the name that you gave the system task policy in the **Name** field.
Step 5 (Optional) In the **Description** field, enter a description of the system task policy.
Step 6 From the **Node Pool** drop-down list, choose the node pool to which this system task policy belongs.
Step 7 Click **Submit**.

The selected node pool now belongs to the newly created system task policy.

Assigning a Node Pool to a System Task Policy

Procedure

Step 1 Choose **Administration** > **System**.
Step 2 On the **System** page, click **System Task Policy**.
Step 3 Click the row with the system task policy to which you want to assign a node pool.
Step 4 Click **Edit**.

Note
If the default system task policy is used, you can assign service nodes to this policy. See Creating a System Task Policy, on page 147, if you want to configure a policy that is different from the default.

Step 5 From the **Node Pool** drop-down list, choose a node pool that you want to assign to the system task policy.
Step 6 Click **Submit**.

The selected node pool now belongs to the system task policy.

Creating a Service Node

Procedure

Step 1 Choose **Administration** > **System**.
Step 2 On the **System** page, click **Service Nodes**.
Step 3 Click **Add**.
Step 4 On the **Service Node** screen, complete the following fields:

Name	Description
Node Name field	The name of the service node.

Name	Description
Role field	You cannot edit this field. By default, this field displays **Service** as the role of this node.
Service Node Pool drop-down list	By default, the **default-service-node-pool** is displayed.
DNS Name field	Enter either the DNS name or IP address of the service node. **Note** This field cannot use the Primary Node's IP address. Ensure that a valid Service Node DNS name or IP address is entered.
Description field	The description of the of the service node.
Protocol drop-down list	Choose either http (default) or https.
Port field	The default TCP port for the Hypertext Transfer Protocol (HTTP) 80 is entered by default. Enter a different TCP port if necessary.
UserName field	The **infraUser** user name is entered by default. The infraUser is a user account created by default. To find this user account on the menu bar, choose **Administration** > **Users and Groups**. Click **Login Users** to find the **infraUser** user account in the **Login Name** column. **Note** The InfraUser user name is not the default administrator user to login to the system. Another user name can be added to this field. This user's API key is used to authenticate with the Service Node.

Step 5 Click **Submit**.

Assigning a System Policy to a System Task

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **System Tasks**.

Step 3 Choose a folder that contains system tasks. Click the folder arrow to expand its tasks.

Note
128 system tasks are available.

Step 4 Choose the task and click **Manage Task**.

The **Manage Task** screen appears.

Step 5 From the **Task Execution** drop-down list, choose **Enable**.

Step 6 From the **System Task Policy** drop-down list, choose a system policy.

Step 7 Click **Submit**.

The system task is assigned to the selected system policy.

Executing System Tasks

Cisco UCS Director includes a few system tasks that cannot be run remotely on a service node. Also, you can assign a system policy remotely from the local host or the primary node.

In addition, you can search and select a specific system task, and run it immediately in the system.

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **System Tasks**.

Step 3 Choose a task from the list.

Step 4 Click **Run Now**.

The result of the executed system task is updated in the user interface.

Disabling or Enabling a System Task

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **System Tasks**.

Step 3 Choose a folder that contains one or more system tasks. Click the folder arrow to expand its tasks.

Note
128 system tasks are available.

Step 4 Choose the task and click **Manage Task**.

The **Manage Task** screen appears.

Step 5 To disable a system task, from the **Task Execution** drop-down list, choose **Disable**.

Step 6 To enable a system task, from the **Task Execution** drop-down list, choose **Enable**.

Step 7 Click **Submit**.

Scheduling a System Task

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **System Tasks**.

Step 3 Choose a system task and click **Manage Task**.

Step 4 In the **Manage Task** screen, complete the following fields to schedule the system task:

Name	Description
Schedule Type drop-down list	Specify the schedule type for the system task. It can be one of the following options: • **Fixed Delay**—Implies the time period between the completion of one task execution and the initiation of the next task execution. • **Fixed Rate**—Implies the time period between successive tasks executions. If there is a delay in the execution of one task or if one task takes longer to execute than its scheduled time, it results in delays in subsequent task executions. Systems tasks that are configured with this setting will not run concurrently. These tasks will not run concurrently.
Minutes or **Hours** or **Days** **Note** The field label is **Minutes**, **Hours** or **Days** depending upon the System Task you choose.	Choose a number from the drop-down list. If you chose **Fixed Delay** as the schedule type, then this number indicates the time gap, in hours, between the completion of one task exection and the initiation of the next task execution. IF you chose **Fixed Rate**, then this number indicates time period, in hours, between successive task executions.
Enable Custom Frequency check box	Check this check box to enable a custom frequency for the system task.

Name	Description
Recurrence Type drop-down list	Specify the recurrence schedule for the system task.It can be one of the following: • **No End** • **Only Once**
Start Time field	Specify the date and time for the recurrence schedule.
Frequency drop-down list	Choose a frequency for the system task. It can be one of the following: • **Hourly** • **Daily** • **Weekly** • **Monthly** **Note** This field is displayed only when you select **No End** in the **Recurrence Type** drop-down list.
Frequency Interval drop-down list	Choose a frequency interval from the drop-down list. The values in this list vary depending on the frequency you have specified.

Step 5 Click **Submit**.

Resetting a System Task

The inventory process fails when a system task remains stuck in a running state and fails to complete due to various reasons, such as network issues, connectivity failure, device configuration setup, and so on. The **Reset Task** option allows you to quickly reset the particular system task and schedule it automatically.



Note You can only reset a system task that is in the in-progress state.

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **System Tasks**.

Step 3 Right-click a system task and select **Reset Task**.
A popup message 'Selected task is in progress. Are you sure you want to reset the task ?' is displayed.

Step 4 Click **Submit**.
A popup message 'Reset of the task <system task name> was successful' is displayed, and the **Execution Status** is changed from **In Progress** to **Scheduled**.

System Tasks with Fixed Rate Option

The following table lists the system tasks that run only with the **Fixed Rate** option.

Category	System Task Label
Compute	Deleted UCSCentralAccount CleanUp Task
	UCS Daily Historical DataPurge Task
	Deleted UCSAccount CleanUp Task
	UCS Historical Data Aggregator Task
	UCS Monthly Historical DataPurge Task
	UCS Event Record Purge Task
	UCS Event Subscription Task
	UCS Fault Record Purge Task
	UCS Server Transition State Manager
	Virtual SAN Ready Node Qualification Task
Admin	VM Metering Data Aggregator Task
	VM Metering Task
	VM LifeCycle Manager
Virtualization	UsageData Aggregator
	Performance Data Collector

Managing Icons in the Cisco UCS Director User Interface

Cisco UCS Director supports customization and management of catalog icons, action-related icons, and status-related icons. Each icon set in the system contains several images that are available by default. You can change the icons that are displayed for either the catalogs, actions or status. You can either upload a new image and set it as the icon, or you can choose a different icon from the set of system-provided icons

Important

- While uploading an icon, ensure that the icon is in either the .SVG format or in the .PNG format. If you are uploading a .SVG image, ensure that the pixel compression is as follows:
  - For action icons— 24px x 24px
  - For table icons—16px x 16px
  - For status icons—16px x 16px
  - For header icons— 20px x 20px (except for the alert icon)
- After you select an icon, you must log out and log in again to the system for the new icon to be visible in the user interface.

Following are the pre-populated icon sets in Cisco UCS Director:

- Standard Catalog Icon Set
- Status Icon Set
- Bare Metal Catalog Icon Set
- Advanced Catalog Icon Set
- Container Catalog Icon Set
- Catalog Folder Icon Set
- Action Icon Set

In addition to modifying an icon in the user interface, you can also revert to the default icon.

Modifying an Icon in the Cisco UCS Director User Interface

Procedure

Step 1 Choose **Administration** > **User Interface Settings**.

Step 2 On the **User Interface Settings** page, click **Icon Management**.

Step 3 Select an icon set category.

It can be one of the following:

- Standard Catalog Icon Set
- Status Icon Set
- Bare Metal Catalog Icon Set
- Advanced Catalog Icon Set
- Container Catalog Icon Set

- Catalog Folder Icon Set
- Action Icon Set

Step 4 Click **Icon Images**.

Step 5 Expand **Icon Images**.

Step 6 Select an icon image from the list of icons.

Step 7 Click edit.

Step 8 In the **Edit Icon Images Entry** page, complete one of the following steps:

a) Choose an image that currently exists in the system using the **Use Existing icon** drop-down list.

b) Upload a new image to the system by either dragging the image into the **File** field or by browsing and selecting an image using the **Select a File** option.

Important
While uploading an icon, ensure that the icon is in either the .SVG format or in the .PNG format. If you are uploading a .SVG image, ensure that the pixel compression is as follows:

- For action icons— 24px x 24px
- For table icons—16px x 16px
- For status icons—16px x 16px
- For header icons— 20px x 20px (except for the alert icon)

Step 9 Click **Submit**.

What to do next

You must log out and log in again to the system for the new icon to be visible in the user interface.

Editing an Icon

Procedure

Step 1 Choose **Administration** > **User Interface Settings**.

Step 2 On the **User Interface Settings** page, click **Icon Management**.

Step 3 Choose the row with the icon category that contains the icon that you want to edit.

Step 4 Click **Icon Images**.

Step 5 On the **Manage Icon Images** screen, choose an icon image to edit.

Step 6 Click **Edit**.

Step 7 On the **Edit Icon Images Entry** screen, edit the **Description**.

Step 8 Choose a replacement file to upload by clicking **Browse** and browsing to an image.

Step 9 Click **Upload**.

Step 10 Once the upload is finished, click **Submit**.

Deleting an Icon

Procedure

Step 1 Choose **Administration** > **User Interface Settings**.
Step 2 On the **User Interface Settings** page, click **Icon Management**.
Step 3 Choose the row with the icon category that contains the icon that you want to delete.
Step 4 Click **Icon Images**.
Step 5 On the **Manage Icon Images** screen, choose an icon image and click **Delete**.
Step 6 Click **Submit**.

Previewing an Icon

Procedure

Step 1 Choose **Administration** > **User Interface Settings**.
Step 2 On the **User Interface Settings** page, click **Icon Management**.
Step 3 Choose the row with the icon category that you want to preview.
Step 4 Click **Icon Images**.
Step 5 On the **Manage Icon Images** screen, choose an icon image to preview.
Step 6 Click the **Information** icon to preview the image.

Tag Library

Tagging is when you assign a label to an object. As an administrator, you can decide to tag objects such as resource groups and user groups, in Cisco UCS Director. You can assign tags to a category such as Compute, Storage, Network, and Virtual. You can also apply a tag to a specific type of account in the selected category. For information on how to apply and remove tags on resource groups, see the *Managing Tags of a Resource Group* section in the *Cisco UCS Director APIC Management Guide*.

Once the tag is created, based on the defined applicability rules, the tags are filtered and displayed in an object report. You can associate the tag to an object such as resource group. To view the resource entities that are associated with a tag, choose the tag and click **View Details**. Alternatively, you can double click the tag.

Note If resource entity is not associated with the tag, the table is empty.

Creating a Tag

You can use the **Create** action on the **Tag Library** screen to create a tag that can be assigned to one or more objects in report page.

Procedure

Step 1 Choose **Policies** > **Tag Library**.

Step 2 Click **Create**.

Step 3 On the **Create Tag** screen, complete the following fields:

Name	Description
Name field	The name for the tag.
Description field	The description of the tag.
Type drop-down list	Choose **INTEGER** or **STRING** as the type of the tag.
Possible Tag Values field	The possible values for the tag.

Step 4 Click **Next**.

Step 5 On the **Applicability Rules** screen, complete the following fields:

Name	Description
Visible to End User field	Checko make the tag visible to end user.

Name	Description
Taggable Entities field	Choose the entities on which the tag need to be applied. To add an entity, do the following: **a.** Click the + icon. **b.** From the **Category** drop-down list, choose the category. It can be one of the following: • **Virtual_Compute** • **Virtual_Storage** • **Virtual_Network** • **Physical_Compute** • **Physical_Storage** • **Physical_Network** • **Administration** **c.** Choose the taggable entities. **d.** Click **Submit**. **Note** The tags are displayed under the respective category according to the set taggable entities.

Step 6 Click **Submit**.

What to do next

After creating a tag, you can edit, clone and delete it by selecting the respective option in the user interface.

Support Information

Cisco UCS Director support provides basic and advanced system information, including the license status, database tables, version, resource usage, logs, and debugging processes for troubleshooting.

The **Support Information** page lets you perform the following actions:

- View system information (Basic)
- View system information (Advanced)
- Show logs
- Download all logs

- Start and stop debug logging
- Start and stop API logging

Viewing System Information

Cisco UCS Director allows you to access system information from the user interface. You can access the following types of system information:

- Basic system information
- Advanced system information

Basic system information includes the following:

- Software version
- Uptime
- Service status
- System license status
- System usage
- Compute accounts status
- Compute server status
- Storage account status
- System catalogs
- Network device status and
- Cloud status

The advanced system information includes the following:

- Basic system information
- Database tables summary
- Product configuration
- Top process information
- Information on processors, memory, disks, log files, network, and login
- System task status
- Cloud inventory
- Monitoring status

Procedure

Step 1 Choose **Administration** > **Support Information**.

Step 2 From the **System Information** drop-down list, choose the type of system information you want to view.

Step 3 Click **Submit**.

The **System Information** page opens in a new tab and displays information about the Cisco UCS Director appliance.

Showing Logs

Cisco UCS Director collates the following logs in the system:

- Infra Manager
- Web Context Cloud Manger
- Tomcat Log
- Authenticator Log
- Mail Delivery Log
- Patch Log

Procedure

Step 1 Choose **Administration** > **Support Information**.

Step 2 From the **System Information** drop-down list, choose **Show Log**.

Step 3 From the **Show Log** drop-down list, choose the log file that you want to view.

Step 4 Click **Show Logs**.

The log file opens in a new tab or browser window and displays any available information, warning, and error logs.

Downloading Logs

You can download all the log files as a zipped file.

Procedure

Step 1 Choose **Administration** > **Support Information**.

Step 2 From the **Support Information** drop-down list, choose **Download All Logs**.

Step 3 Click **Download**.
A zipped file containing log files is downloaded in the default download location.

Starting the Debug Log

Debug logging enables you to record a maximum of 30 minutes debug logging to a log file.

Procedure

Step 1 Choose **Administration** > **Support Information**.

Step 2 From the **System Information** drop-down list, choose **Debug Logging**.

Step 3 Click **Start Debug Logging**.

Step 4 Click **Stop Debug Logging** to stop the recording.

The recording will automatically stop once it reaches the 30 minute limit.

Step 5 Click **Download Debug Logs from *HH.MM.SS*** (time) to download the zipped log file.

Note
To view the log details and SQL information in debug mode for reports, log into the Cisco UCS Director using shelladmin or ucsdadmin credentials and do one of the following:

- As a shelladmin user, choose **`Tail Inframgr Logs`** option and press Enter
- As a ucsdadmin user, execute **tail -f /opt/infra/inframgr/logfile.txt**.
- As a root user, execute **tail -f /opt/infra/inframgr/logfile.txt**.

Generating API Logs

Procedure

Step 1 Choose **Administration** > **Support Information**.

Step 2 From the **System Information** drop-down list, choose **API Logging**.

Step 3 Click **Start API Logging**.

Step 4 Perform any tests that you want to run.

Step 5 Click **Stop API Logging** to stop the recording.

Step 6 Click **Download API Debug Logs from *HH.MM.SS*** (time) to download the zipped file.

A compressed (zip) file is generated and downloaded on to your desktop. This zipped file contains a text file that lists all the REST APIs that invoked on the appliance, along with the timestamp.

Database Audit Logging

Database audit logging lets the system record information on login events and query events. These events are logged in the `/var/lib/mariadb/data/audit.log` file. By default, database audit logging is disabled. To enable database audit logging, use the **dbAuditLog.sh** command. For more information, see Enabling Audit Logging, on page 162.



Note You can disable database audit logging if the system encounters performance issues due to a heavy audit log output.

Enabling Audit Logging

Procedure

Step 1 Log in to Cisco UCS Director SSH client as ucsdadmin user.

Step 2 Run the following commands to stop all services running on the system.

```
[root@localhost infra]# pwd
/opt/infra
[root@localhost infra]# ./stopInfraAll.sh
[root@localhost infra]# ./statusInfra.sh
```

Step 3 Run the following command to enable audit logging.

```
[root@localhost infra]# cd bin
[root@localhost bin]# pwd
/opt/infra/bin
[root@localhost bin]# ./dbAuditLog.sh ON
```

Step 4 Run the following commands to restart the services:

```
[root@localhost infra]# pwd
/opt/infra/bin
[root@localhost infra]#./startInfraAll.sh
```

Step 5 Run the following command to check the status of audit logging.

```
[root@localhost bin]# ./dbAuditLog.sh STATUS
audit-log= ON
```

If you see a message that states that there is an issue with the database startup, you must remove or rename the `audit.log` file and restart the Cisco UCS Director database server.

Device Connector

The device connector connects Cisco UCS Director to Cisco Intersight, the cloud-hosted server management system. It enables Cisco UCS Director to be managed and monitored through Cisco Intersight.

To register a device with Cisco Intersight in the cloud, you must do the following:

1. Configure the device connector proxy settings to connect Cisco UCS Director with Cisco Intersight.

   This is required only if you have proxy configuration enabled.

2. Validate your access to the device from Cisco Intersight using the device serial number and the security code and claim the device.



Note After a system running Cisco UCS Director is claimed in Cisco Intersight, you must refresh the information displayed on the **Device Connector** screen. Choose **Administration** > **Device Connector** to view the updated information.

Configuring Device Connector

Procedure

Step 1 Choose **Administration** > **Device Connector**.

Step 2 Click **Settings**.

Step 3 In the **Settings** dialog box, choose **Proxy Configuration**.

Step 4 For the **HTTPS Proxy** field, move the slider to **Enabled**.

Step 5 Enter the proxy hostname or IP address in the **Proxy Hostname/IP** field.

Step 6 Enter the proxy port number in the **Proxy Port** field.

Step 7 To authenticate access to the proxy server, turn the **Authentication** mode on and enter the **Username** and **Password**.

Step 8 Click **Ok**.

Based on the connectivity to Cisco Intersight, the **Status** field displays one of the following messages:

- When the connection to Cisco Intersight is successful, the status messages could be one of the following:
  - **Unclaimed**—Implies that the connection is successful but the device is not claimed. You can claim an unclaimed connection through Cisco Intersight.

    For information on claming a device, see the integrated guided walkthrough titled *Learn How to Claim a Device* available within the **Online Help** menu in the Cisco Intersight user interface.

  - **Claimed**—Implies that the connection to Cisco Intersight is successful and you have claimed the device.

Note

The header pane of the user interface now includes an icon to indicate the status of the device in Cisco Intersight. This icon is visible only to administrator users and the status change is reflected only when the browser is refreshed or when a new login session is initiated.

Icon	Description
	Indicates that the device is not claimed in Cisco Intersight.
	Indicates that the device is claimed in Cisco Intersight.

- When the connection to Cisco Intersight is unsuccessful, the status messages could be one of the following:
  - **Administratively disabled**—Implies that the administrator has disabled managing the device from Cisco Intersight.
  - **Certification Validation Error**—Implies that an invalid certificate exists on the system.
  - **Not Claimed**—Indicates that the device is registered, but not claimed in Cisco Intersight.
  - **DNS is not configured** or **DNS is mis-configured**.
  - **Unable to resolve DNS name of the service**—Indicates that although DNS is configured, the DNS name of the Cisco Intersight platform cannot be resolved.
  - **NTP is not configured**
  - **Unable to establish a network connection**—Indicates that Cisco UCS Director cannot connect to Cisco Intersight.

If you have enabled HTTP using option 28 from the Shell Admin console, then the status messages displayed on this screen may not be accurate.

Launching Cisco UCS Director from Cisco Intersight

After the device connector is configured and the device is claimed, you can launch the Cisco UCS Director user interface from Cisco Intersight.



Important If any of the Cisco UCS Director services are down, you cannot launch Cisco UCS Director from Cisco Intersight.

A message stating that there is no service is displayed.

Although you can launch Cisco UCS Director from Cisco Intersight, following are some of the restrictions that you need to be aware of:

- You cannot edit a user profile.
- You cannot perform any import and export actions.

- The main menu and the Dashboard are disabled.
- The **Device Connector** tab is not visible.
- You cannot perform any launch actions.
- You cannot upgrade connector packs.
- You cannot generate any summary reports.
- The user name is displayed as Cisco Intersight user when you launch Cisco UCS Director.
- All service requests and audit log details are logged as Admin user.

Procedure

Step 1 Log into the Cisco Intersight user interface.

Step 2 Choose **Devices**.
The **Devices** screen appears that displays a list of available Cisco UCS Director systems.

Step 3 Select a Cisco UCS Director device from the list, and click **....**.

You must scroll to the far right of the list of devices to see the **....** option.

Note
The IP address displayed for the Cisco UCS Director device in Cisco Intersight is determined by the IP address you entered for the **Server IP address** field while configuring the outgoing mail server for Cisco UCS Director.

If you modify the server IP address after the Device Connector process is up, you must restart the Device Connector process. To do so, login to the Cisco UCS Director device, and run the following commands:

```
/opt/infra/bin/stopdc.sh
/opt/infra/bin/startdc.sh
```

Refresh the **Devices** screen in Cisco Intersight to view the updated server IP address.

Step 4 Choose **Launch UCSD**.

Cisco Intersight is connected to the Cisco UCS Director system and the Cisco UCS Director user interface opens in a new tab.

Note
Users with read-only permissions created in Cisco Intersight cannot perform any actions. These users can only view reports.

Connector Pack Management

Connector packs help you perform connector level upgrade in Cisco UCS Director without impacting other connectors. After a system running Cisco UCS Director is claimed in Cisco Intersight, as a system administrator, you can view information on new versions of connector packs that are available for upgrade. The top header pane of the user interface displays a notification indicating that new connector pack versions are available.

You can select and upgrade the connector packs on the system. For more information, see Upgrading Connector Packs, on page 167.

Connector packs help you perform connector level upgrade in Cisco UCS Director without impacting other connectors. As a system administrator, you can view information on new versions of connector packs that are available for upgrade.

Following are the connectors that are available in this release:

- Cisco UCS which includes Cisco UCS Central and Cisco UCS Manager
- ACI APIC
- ACI Multi-Site Controller
- F5 Load Balancer
- Network Devices
- EMC Isilon
- EMC RecoverPoint
- EMC VMAX
- EMC VNX
- EMC VNXe
- EMC VPLEX
- EMC Unity
- EMC XtremIO
- IBM
- NetApp ONTAP
- VCE VisionIO
- Microsoft Hyper-V
- RedHat KVM
- Vmware
- Bare Metal Agent
- Cisco IMC
- Cisco HyperFlex

As a system administrator, you can upgrade connector packs from:

- Cisco UCS Director. For more information on upgrading the connector packs using Cisco UCS Director user interface, see Upgrading Connector Packs, on page 167.
- Cisco Intersight user interface in which Cisco UCS Director is claimed. For more information on upgrading the connector packs from Cisco Intersight UI, see Upgrading Connector Packs on UCS Director Instances.

The top header pane of the user interface displays a notification indicating that new connector pack versions are available.



Important Latest versions of these connectors are made available to Cisco UCS Director only through Cisco Intersight. So Cisco UCS Director must be claimed in Cisco Intersight.

Upgrading Connector Packs

As a system administrator, you can upgrade connector packs using the Cisco UCS Director graphical user interface. When new connector pack versions are available, the system notifies you in the following ways:

- Pop-up message when you log in to Cisco UCS Director user interface.

  When you log in to the user interface of Cisco UCS Director, and if there are new connector pack versions available for upgrade, a pop-up message prompting you to upgrade these versions is displayed. Click **Yes** to upgrade these connector pack versions immediately or click **No** to upgrade at a later time.



Note This pop-up notification message is displayed once every 3 days. It is not displayed every time you log in to the user interface.

- An alert with a downward facing arrow image and a number in the header pane of the user interface.

  This number indicates the number of connector packs that are available for upgrade.

The pop-up message and the alert on the header pane are displayed only when Cisco UCS Director has been claimed in Cisco Intersight. For information on establishing a connection with Cisco Intersight, see Configuring Device Connector, on page 163.



Note You can upgrade system packs (System Update Manager, Base Platform Pack and Connector Pack versions) in a standalone setup and in a multi-node setup. In a multi-node setup, you must upgrade the versions only on the primary node.

Before you begin

- You must have system administrator privileges in Cisco UCS Director.
- Cisco UCS Director has been claimed in Cisco Intersight.
- Cisco UCS Director is successfully connected to Cisco Intersight.
- The latest version of the Base Platform connector pack is installed.

Procedure

Step 1 On the header, click **New Upgrades Available**.

The **Available System Upgrades** screen appears and will display all available connector packs for upgrade along with version information. Upon login, if you clicked **Yes** to the pop-up message, then the very same upgrade screen appears.

Note
The **New Upgrades Available** icon is visible on the header only when new versions of the current running connector packs are available for upgrade.

Step 2 Check the check box of a connector pack from the list.

You can check the check boxes of multiple connector packs.

Step 3 Click **Upgrade**.

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

After you confirm that the connector version must be upgraded, the validation process is initiated. If the validation process completes successfully, the upgrade process is initiated and the **System Upgrade Status** screen displays the upgrade status. After the upgrade process is successful, the **Logout** option is enabled.

For more information on possible outcomes of the validation and upgrade process, see Upgrade Process Validation and Failure Scenarios, on page 171.

Step 5 Click **Logout**.

While upgrading a base platform pack that includes changes to all infrastructure components, all Cisco UCS Director services are restarted. As a result, after clicking **Logout**, the screen could appear to be unresponsive for a few minutes. After all the services are restarted, and the upgrade process is complete, you can login to Cisco UCS Director .

What to do next

You can view the upgrade reports by choosing **Administration** > **System** > **System Updates**. From this screen, you can double-click on a report, and view additional details on the upgrade process. For more information, see Viewing Connector Pack Upgrade Information, on page 168.

Viewing Connector Pack Upgrade Information

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **Connector Pack Upgrades**.
Information such as upgrade request ID, user that initiated the upgrade, upgrade start time and end time, and the upgrade status are displayed.

Step 3 Select a connector pack and choose **View Details** to view details such as connector pack name, upgraded version, and prior version.

Step 4 Click **State History** to view the various states of the connector pack upgrade process. For example, upgrade request received, upgrade process initiated or upgrade process completed.

Step 5 Click **Stages** to view the entire lifecycle of the connector pack upgrade request.

Base Platform Pack and System Update Manager

Cisco UCS Director includes the capability to update the following components of the software:

- Base Platform Pack—Includes basic infrastructure components such as the user interface, Shell admin console changes, and critical defect fixes.
- System Update Manager—Includes the framework that helps you upgrade all connector packs and the base platform pack.
- Connector Packs—Includes connector-specific updates and critical defect fixes, which you can upgrade in your environment without affecting other connectors. See Connector Pack Management, on page 165.

Prior to upgrading any of these packs, ensure that the following prerequisites are met:

- You must have system administrator privileges in Cisco UCS Director.
- Cisco UCS Director has been claimed in Cisco Intersight.
- Cisco UCS Director is successfully connected to Cisco Intersight.
- The latest version of the Base Platform connector pack is installed.

When you login to the user interface, the header pane will indicate the number of updates that are available for your system. Clicking that number will display the **Available System Upgrades** screen. This screen displays information on base packs and the connector packs that are available for upgrade. From this screen, you can perform the following actions:

- Upgrade connector packs that you need for your environment.

  See Upgrading Connector Packs, on page 167.

- Upgrade the Base Platform pack—Selecting this base pack will also automatically select the System Update Manager Pack, and the connector packs that are available for upgrade.
- Upgrade only the System Update Manager

  See Upgrading the System Update Manager, on page 170.

- Upgrade the connector packs, Base Platform pack and System Update Manager together

  If you select all three options, the System Update Manager is upgraded first, followed by the connector packs, and then finally the Base Platform pack. After the System Update Manager upgrade is complete, the System Update Manager service is restarted, following which the upgrade process for the connector packs and the Base Platform pack is initiated. If the upgrade process for the connector packs fail, then the versions on the system are reverted to the previously installed versions, and the upgrade of the Base Platform pack is also terminated.

Upgrading Base Platform Pack

Before you begin

- You must have system administrator privileges in Cisco UCS Director.

- Cisco UCS Director has been claimed in Cisco Intersight.
- Cisco UCS Director is successfully connected to Cisco Intersight.
- The latest version of the Base Platform connector pack is installed.

Procedure

Step 1 On the header, click **New Upgrades Available**.

The **Available System Upgrades** screen appears that displays a list of available connector packs for upgrade along with the version information.

Note
The **New Upgrades Available** icon is visible on the header only when new versions of the current running connector packs are available for upgrade.

Step 2 Check the **Base Platform** check box.

Checking this check box will also automatically select the System Update Manager and connector packs, if available.

Step 3 Click **Upgrade**.

To complete the upgrade, the required Cisco UCS Director services will restart.

Step 4 In the **Confirm Upgrade** dialog box, click **Yes** to proceed with the upgrade.

After you click **Yes**, the validation process is initiated. If the validation process completes successfully, the upgrade process is initiated and the **System Upgrade Status** screen displays the upgrade status.

For more information on possible outcomes of the validation and upgrade process, see Upgrade Process Validation and Failure Scenarios, on page 171.

Step 5 Review the status messages on the **System Upgrade Status** screen.

Step 6 After the upgrade process completes successfully, click **Logout**.

While upgrading a base platform pack that includes changes to all infrastructure components, all Cisco UCS Director services are restarted. As a result, after clicking Logout, the screen could appear to be unresponsive for a few minutes. After all the services are restarted, and the upgrade process is complete, you can login to Cisco UCS Director.

Step 7 Login to the user interface.

Upgrading the System Update Manager

Before you begin

- You must have system administrator privileges in Cisco UCS Director.
- Cisco UCS Director has been claimed in Cisco Intersight.
- Cisco UCS Director is successfully connected to Cisco Intersight.

- The latest version of the Base Platform connector pack is installed.

Procedure

Step 1 On the header, click **New Upgrades Available**.

The **Available System Upgrades** screen appears that displays a list of available connector packs for upgrade along with the version information.

Note
The **New Upgrades Available** icon is visible on the header only when new versions of the current running connector packs are available for upgrade.

Step 2 Check the **System Update Manager** check box.

Step 3 Click **Upgrade**.

To complete the upgrade, the required Cisco UCS Director services will restart.

Step 4 In the **Confirm Upgrade** dialog box, click **Yes** to proceed with the upgrade.

After you click **Yes**, the validation process is initiated. If the validation process completes successfully, the upgrade process is initiated and the **System Upgrade Status** screen displays the upgrade status.

For more information on possible outcomes of the validation and upgrade process, see Upgrade Process Validation and Failure Scenarios, on page 171.

Step 5 Review the status messages on the **System Upgrade Status** screen.

Step 6 After the System Update Manager upgrade process completes successfully, click **Logout**.

After the upgrade process is complete, the System Update Manager service is restarted.

Step 7 Login to the user interface.

Upgrade Process Validation and Failure Scenarios

After you initiate a system pack upgrade, a validation process is initiated in the system. The following table describes the possible outcomes of the validation for system packs:

Scenario	Validation Process Outcome	Information in the User Interface	Recommended Action
No problems with any system pack versions No workflows in progress No users logged into the system	Succeeds	The **System Upgrade Validation** screen displays the status	None. The upgrade process is initiated.

Scenario	Validation Process Outcome	Information in the User Interface	Recommended Action
Problems with one or more system packs	Fails	The **System Upgrade Validation** screen displays an error message and corrective action.	Review the information and perform the corrective action suggested.
Other users are logged into the system or Workflows are in progress	Fails	The **System Upgrade Validation** screen displays an error message and corrective action.	Review the corrective action, and click **Force Upgrade** to proceed with the upgrade. **Note** The **Force Upgrade** option is available only for Base Platform pack and connector packs. It is not displayed for the System Update Manager. The **System Upgrade Status** screen is displayed with current status for the upgrade request. Users are automatically logged out of the system with a system broadcast message about the upgrade.

After validation process completes successfully, the upgrade process is initiated and the **System Upgrade Status** screen displays the status. On successful completion of the upgrade process, the **Logout** option is enabled on the user interface. The following table describes the possible issues that you could encounter during an upgrade process:

Scenario	Information in the User Interface	Impact to Upgrade Process
System pack upgrade is in progress and other users with administrator privileges logs in to the user interface.	The **System Upgrade Status** screen is displayed to the user with current status for the upgrade request.	The upgrade process completes successfully.
System pack upgrade is in progress and an end user logs in to the user interface.	The system startup page is displayed to the user.	The upgrade process completes successfully.
You selected multiple packs for upgrade, and the upgrade for one system pack fails.	The **System Upgrade Status** screen displays the status of the upgrade. The overall upgrade status is indicated as partially completed. The status for each system pack will help you determine the system pack that was not upgraded.	When the upgrade process for any system pack fails, then the version of that system pack is reverted to the previously installed version.

Scenario	Information in the User Interface	Impact to Upgrade Process
You selected the base platform pack for upgrade and you are logged out of the user interface before the **System Upgrade Status** screen displays the complete workflow of the upgrade process.	If the base platform pack that you selected for upgrade includes an update to the Tomcat service, then the **System Upgrade Status** screen does not display the complete workflow of the upgrade process. This is because the Tomcat service restarts in the system which results in terminating your session in the user interface. Also, you are automatically directed to the system start-up screen. You can login to the user interface only after all Cisco UCS Director services are restarted.	Although the **System Upgrade Status** screen does not display the complete workflow, the upgrade process completes successfully.

Alert About Insecure Protocols

From the Cisco UCS Director Release 6.9(4.0), an alert about the usage of insecure protocols is displayed in the **Diagnostic System Messages** area. Support for insecure protocols such as HTTP, Telnet, and FTP is planned to be deprecated. These protocols will be restricted from the future release, and removed from the subsequent release. To ensure data protection and enhance security, you must use the secure protocols such as HTTPS, SSH, SFTP, and SCP.

Viewing Details About Insecure Protocols

Procedure

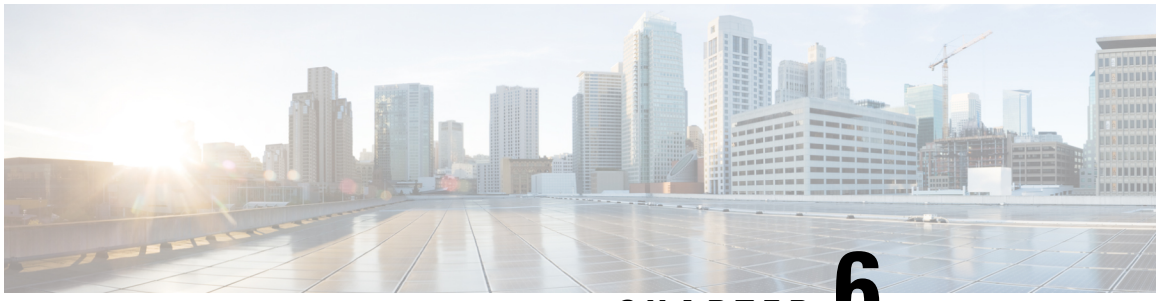
Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, choose **Insecure Protocol Usage**.

The following information related to the insecure protocol is displayed:

- Insecure protocol used—Name of insecure protocol currently used
- Impacted Area—Physical account, credential policy, or workflow component associated with the insecure protocol
- Report/Workflow task—Report or workflow task where the insecure protocol is used
- Menu—Top-level GUI element in which the insecure protocol is used
- Count—Number of times the insecure protocol is used in a particular form or workflow task
- Supported protocol—Alternative secure protocol that can be used

- Remarks—Short description about the usage of insecure protocol



CHAPTER 6

Managing Integration Settings

This chapter contains the following sections:

- About Integration Settings, on page 175
- Configuration Management Database Integration, on page 176
- Metering Data Export, on page 177
- Change Records, on page 178
- System Logs, on page 179
- Storage and OVF Upload, on page 179
- Multiple Language Support, on page 180
- Adding a Repository, on page 181

About Integration Settings

Using this menu, you can perform the following actions in Cisco UCS Director:

- View the license status
- Manage appliance storage
- Manage user OVF
- CMDB Integration setup
- Metering data export setup
- View change records
- Manage repositories
- Syslog server configuration



Important Starting with Cisco UCS Director Release 6.9(4.0), support for the insecure FTP protocol is planned to be deprecated. When you setup CMDB integration and metering data export, you must select secure protocols such as SFTP or SCP to ensure secure data communication.

Configuration Management Database Integration

The Configuration Management Database (CMDB) is used to track and manage changes in the system. CMDB typically displays ADD, DELETE, or MODIFY event types on resources such as virtual machines (VMs), service requests, groups, and so on.

Setting Up CMDB Integration

Procedure

Step 1 Choose **Administration** > **Integration**.

Step 2 On the **Integration** page, click **CMDB Integration Setup**.

Step 3 On the **CMDB Integration Setup** screen, complete the following fields:

Name	Description
Export to Server check box	When selected, the change records are sent to the target server.
Transport Protocol drop-down list	Choose the type of protocol for transferring the data: • FTP • SFTP • SCP
Export Format drop-down list	Choose the file export format: • CSV • XML
Server field	IP address of the server associated with the selected transport protocol.
Port field	Port number of the target server.
User field	User name used to authenticate and connect to the target server.
Password field	Password associated with the user name.
Export Frequency drop-down list	Choose how often the change records must be exported to the target server. Default is 5 mins.

Name	Description
File Name field	The file name for the exported change records. The following variables can be used to generate a new filename each time a file is exported to the target server: MONTH, WEEK, DAY, YEAR, HOUR, MIN, SEC, MLLIS. Example: XYZ-$DAY-$HOUR-$MIN-$SEC
Test Connectivity check box	When selected, the system verifies the connection to the configured target server using the provided settings.

Step 4 Click **Save**.

Metering Data Export

You can export trend data, such as VM resource usage and resource accounting details, by setting up a metering data export to a target server.

Setting Up Metering Data Export

Procedure

Step 1 Choose **Administration** > **Integration**.

Step 2 On the **Integration** page, click **Metering Data Export Setup**.

Step 3 On the **Metering Data Export Setup** screen, complete the following fields:

Name	Description
Export to Server check box	When selected, the change records are sent to the target server.
Export Format drop-down list	Choose the file export format: • CSV • XML
Transport Protocol drop-down list	Choose the type of protocol for transferring the data: • FTP • SFTP • SCP

Name	Description
Server field	IP address of the server associated with the selected transport protocol.
Port field	The target server port number.
User field	User name used to authenticate and connect to the target server.
Password field	Password associated with the user name.
Export Frequency drop-down list	Choose how often the change records must be exported to the target server. Default is 1 hr.
File Name field	The file name for the exported change records. The following variables can be used to generate a new filename each time a file is exported to the target server: MONTH, WEEK, DAY, YEAR, HOUR, MIN, SEC, MLLIS. Example: XYZ-$DAY-$HOUR-$MIN-$SEC
Test Connectivity check box	When selected, the system verifies the connection to the configured target server using the provided settings.

Step 4 Click **Save**.

Change Records

Viewing Change Records

You can view a maximum of 1000 records. The reports are listed in descending order, wherein the recent reports are displayed in the top row.

Procedure

Step 1 Choose **Administration** > **Integration**.

Step 2 On the **Integration** page, click **Change Records**.

System Logs

You can forward system log (syslog) information to configured servers. Each system message is associated with a severity level. You can determine the severity level of the system logs that you want forwarded to the target server.

Setting up System Logs

Procedure

Step 1 Choose **Administration** > **Integration**.

Step 2 On the **Integration** page, click **Syslogs**.

Step 3 Check the **Enable Syslog Forward** check box and complete the required fields, including the following:

Field	Description
Minimum Severity drop-down list	Choose a threshold below which any severity messages are not forwarded to the syslog server.
Primary Syslog Server	
Server Address field	The primary server address.
Protocol drop-down list	Choose the protocol: UDP or TCP.
Port field	The port number.
Syslog Message Format drop-down list	Choose the message format: XML or plain text.
Secondary Syslog Server	
Server Address field	The secondary server address.
Protocol drop-down list	Choose the protocol: UDP or TCP.
Port field	The port number.
Syslog Message Format drop-down list	Choose the message format: XML or plain text.

Step 4 Click **Save**.

Storage and OVF Upload

You can configure the storage location for files that are uploaded by the administrator, group administrator, or the end user. The uploaded files can either be stored locally or configured to go to an external NFS share mount point. As an administrator in the system, you can configure the Network File System (NFS) location.

The Upload files feature provides an option for administrators, group administrators, or the end-user (service end-user portal) to upload Open Virtualization Format (OVF) files to the local storage or to an external NFS share mount point. For more details, see the *Cisco UCS Director OVF File Upload Guide*.

Multiple Language Support

Cisco UCS Director supports the following languages for concurrent display and input:

- English (United States)
- Japanese (Japan)
- Spanish (Latin America)
- French (France)
- Korean (Korea)
- Chinese (China)
- Russian (Russia)

All input fields support entering text in the user's language of choice.

As an administrator, you can set a language preference for specific users while you are adding them to the system. For more information, see Adding Users, on page 105. In addition, each user in the system can select a language for the user interface. For more information, see Setting a Locale for the User Interface, on page 180

Choosing a Language for Cisco UCS Director

You can choose a language for the Cisco UCS Director user interface.

Procedure

Step 1 Choose **Administration** > **User Interface Settings**.

Step 2 On the **User Interface Settings** page, click **Language**.

Step 3 From the **Language** drop-down list, choose a language.

Step 4 Click **Save**.

Important
You must restart the system for the language change to take effect.

Setting a Locale for the User Interface

As a user in the system, you can select a specific language for the user interface. This language preference is set only for your login session, and does not impact the language selected for other users.

Procedure

Step 1 Click your user name that is displayed on the top right corner of the screen, and choose **Edit My Profile**.

Step 2 In the **Edit My Profile** screen, choose a language from the **Language** drop-down list.

Step 3 Click **Save**.

The language in the user interface is changed immediately.

Note
If the **Language** drop-down list and **Save** option is not visible, then you must clear browser cache and launch Cisco UCS Director again.

Adding a Repository

Procedure

Step 1 Choose **Administration** > **Integration**.

Step 2 On the **Integration** page, click **Manage Repositories**.

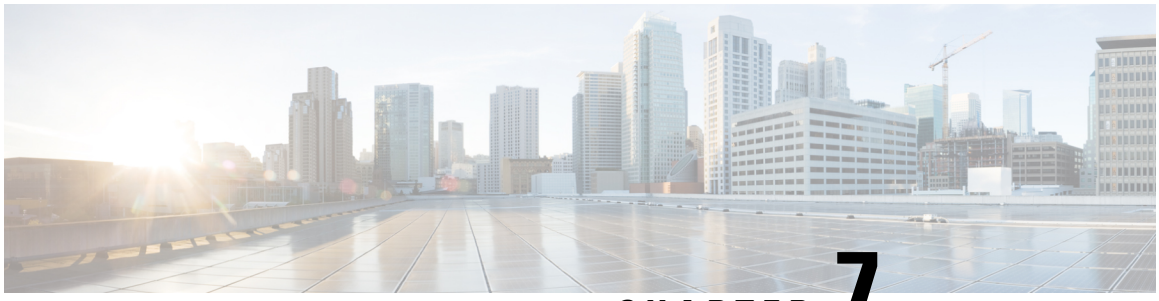
Step 3 Click **Add**.

Step 4 In the **Add Repository** page, complete the required fields, including the following:

Name	Description
Repository Nickname	A nickname to identify the repository. It must be a unique value.
Repository URL	The URL to access the repository.
Repository Name	The name of the repository to identify it within Cisco UCS Director.
Branch Name	The branch that contains the files. By default, it is set to master.
Repository User	The user name of the GitHub account.
Repository Password	The password of your GitHub account.
Make this my default repository	Check this check box to use this repository for all script files.

Step 5 Click **Test Connectivity** to check connectivity to the repository.

Step 6 Click **Submit**.



CHAPTER 7

Managing a Physical Infrastructure

This chapter contains the following sections:

- About Managing a Physical Infrastructure, on page 183
- Testing Connectivity, on page 192
- Enabling Device Discovery, on page 193

About Managing a Physical Infrastructure

Cisco UCS Director enables you to manage both physical and virtual infrastructures. While managing a physical account, you would need to first create a site, and add a pod to the site. After you create this account, Cisco UCS Director discovers all components within the newly created physical account. Typically, the discovery process takes about 5 minutes. In the system, you can either add a new pod or you can use the default pod that is available. A physical account can be associated with the default pod or with one that you add.

Note As an administrator, you can create either a physical account or a virtual account first in the system. A physical account in Cisco UCS Director has no dependency on a virtual (cloud) account.

Using the Converged View

The **Converged** view provides you with a graphical representation of the sites, and pods that you have configured in Cisco UCS Director. To access this view, choose **Converged** from the side navigation bar. If you have configured a site or multiple sites in the system, then this **Converged** view page displays a drop-down list from where you can select a site and view the pods that are associated with the site. However, you cannot add a site from this page. For information on adding a site, see Adding a Site, on page 184. After you have added a site in the system, you can either add a pod from the **Converged** page, or you can add a pod from the **Administration** > **Physical Accounts** > **Pods** screen.

The **Converged** page, in addition to letting you view the pods associated with each site, also provides the following options:

- Search—If your site has several pods, then you can use the search feature to locate a specific pod using the name as the search criteria.
- Add, Edit and Delete—Use these options to add, modify or delete pods.

- Collapse and expand the row of pods displayed for a site.
- View specific account information of each pod:
  - If you select a pod, and mouse over an account, then all account details are displayed. Alternatively, you can click an account to view the detailed information.
  - Power status of the account - the power icon on the account indicates if the account is powered on or powered off. Green color indicates that it is powered on, and red color indicates that it is powered off.

Adding a Site

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Site Management**.

Step 3 Click **Add**.

Step 4 On the **Add Site** screen, complete the following fields:

Name	Description
Site Name field	A descriptive name for the site.
Description field	The description of the site, such as the location, significance, and so on.
Contact Name field	The name of the person responsible for this site.

Step 5 Click **Submit**.

Adding a Pod

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Pods**.

Step 3 Click **Add**.

Step 4 On the **Add Pod** screen, complete the following fields:

Name	Description
Name field	A descriptive name for the pod.

Name	Description
Type drop-down list	Choose the type of pod that you want to add. This can be one of the following: • **Flexpod** • **VersaStack** • **Generic** • **ExpressPod Medium** • **VSPEX** • **ExpressPod Small** • **Vblock** • **HyperFlex** • **Virtual SAN Pod** The nongeneric pod types accommodate only specific physical and virtual components. A generic pod does not require a specific pod license. You can add any type of physical or virtual component to a generic pod. For more information about bundled pod licenses (FlexPod, Vblock, and VSPEX), which include the necessary individual device licenses to run a pod, see the Cisco UCS Director Installation and Upgrade Guides. **Note** Only VersaStack and Generic pods are supported in the IBM accounts in Cisco UCS Director.
Site drop-down list	Choose the site where you want to add the pod. If your environment does not include sites, you can omit this step.
Description field	(Optional) A description of the pod.
Address field	The physical location of the pod. For example, this field could include the city or other internal identification used for the pod.
Hide Pod check box	Check to hide the pod if you do not want it to show in the Converged Check View. You can continue to add or delete accounts from the pod. For example, you can use this check box to ensure that a pod that does not have any physical or virtual elements is not displayed in the Converged View.

Step 5 Click **Add**.

What to do next

Add one or more accounts to the pod.

Adding a Physical Account

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Physical Accounts**.

Step 3 Click **Add**.

Step 4 On the **Add Account** screen, complete the following fields:

Name	Description
Pod drop-down list	Choose the pod to which this physical account belongs.
Category drop-down list	Choose the category type (Computing or Storage). If you chose Storage, continue to Step 6.
Account Type drop-down list	Choose from the following account types for this physical account: • **UCSM** • **HP ILO** • **Cisco Rack Server (CIMC)** • **IPMI**

Step 5 Click **Submit**.

Step 6 On the **Add Account** screen, complete the following fields:

Name	Description
Authentication Type drop-down list	Choose from the following authentication types to be used for this account: • **Locally Authenticated**—A locally authenticated user account is authenticated directly through the fabric interconnect and can be enabled or disabled by anyone with admin or AAA privileges. • **Remotely Authenticated**—A remotely authenticated user account is any user account that is authenticated through LDAP, RADIUS, or TACACS+.

Name	Description
Server Management drop-down list	Choose how servers are managed by this account by selecting one of the following options: • **All Servers** • **Selected Servers**
Account Name field	A unique name for the physical account that you want to add.
Server Address field	The IP address of the server.
Use Credential Policy check box	Check this check box if you want to use a credential policy for this account rather than enter the information manually.
Credential Policy drop-down list	If you checked **Use Credential Policy**, choose the credential policy that you want to use from this drop-down list. This field is only displayed if you choose to use a credential policy.
User ID field	The username for accessing this account. This field is not displayed if you choose to use a credential policy.
Password field	The password associated with the username. This field is not displayed if you choose to use a credential policy.
Transport Type drop-down list	Choose the transport type that you want to use for the account. This can be one of the following: • **HTTP** • **HTTPS** This field is not displayed if you choose to use a credential policy.
Port field	The server port number. This field is not displayed if you choose to use a credential policy.
Description field	The description of the account.
Contact Email field	The contact email address for the account.
Location field	The location.

Name	Description
Service Provider field	The service provider's name, if any.

Step 7 If this account is Storage, choose the appropriate account type: **NetApp ONTAP**, **NetApp OnCommand**, **EMC VNX**, **EMC VMAX Solutions Enabler** or **WHIPTAIL**.

Step 8 Click **Add**.

Adding a Multi-Domain Manager Account

You can add the following types of multi-domain manager accounts:

- PNSC—Cisco Prime Network Services Controller account
- DCNM—Cisco Prime Data Center Network Manager account
- UCS Central—Cisco UCS Central account
- APIC—Cisco Application Policy Infrastructure Controller account
- EMC RecoverPoint account
- EMC VPLEX account

Before you begin

You must be logged in to the appliance to complete this task.

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Multi-Domain Managers**.

Step 3 Click **Add**.

Step 4 On the **Add Account** screen, choose the account type from the drop-down list.

Step 5 Click **Submit**.

Step 6 On the **Multi-Domain Manager Account** screen, complete the following fields:

Name	Description
Account Name field	Choose the account name to which this multi-domain manager account belongs.
Description field	(Optional) The description of the account.
Server Address field	Enter the IP address of the server managing the multi-domain manager account.
Account Name field	A unique name for the physical account that you want to add.

Name	Description
Server Address field	The IP address of the server.
User ID field	The username for accessing this account.
Password field	The password associated with the username.
Transport Type drop-down list	Choose the transport type that you want to use for the account. This can be one of the following: • http • https
Port field	The server port number. The default port is 443.
Contact Email field	(Optional) The contact email address for the account.
Location field	(Optional) The location.

Step 7 Click **Submit**.

Adding a Network Element

In order to create a virtual server that supports load balancing, first add a network element in Cisco UCS Director. After a Load Balancer is added as a network element in Cisco UCS Director, it appears on the **Managed Network Element** screen.

Before you begin

You must be logged in to the appliance to complete this task.

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Managed Network Elements**.

Step 3 Click **Add Network Element**.

Step 4 On the **Add Network Element** screen, complete the following fields:

Name	Description
Pod drop-down list	Choose the pod to which the network element belongs.
Device Category drop-down list	Choose the device category for this network element. For example: **F5 Load Balancer**.
Device IP field	The IP address for this device.

Name	Description
Protocol drop-down list	Choose the protocol to be used. The list may include the following: • Telnet • SSH • HTTP • HTTPS **Note** When working with an F5 load balancer device, HTTP and HTTPS are the only valid selections.
Port field	The port to use.
Login field	The login name.
Password field	The password associated with the login name.

Step 5 Click **Submit**.

Adding the F5 Load Balancer triggers the system task inventory collection. The polling interval configured on the **System Tasks** screen specifies the frequency of inventory collection.

What to do next

To modify or edit a virtual server, choose the server, and then click **Modify**. To remove a virtual server, choose the server, and then click **Delete**.

Enabling DHCP Logging

Before you begin

You must be logged in to the appliance to complete this task.

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.
Step 2 On the **Physical Accounts** page, choose the **Network Service Agents**.
Step 3 Click **Embedded Network Services**.
Step 4 On the **Embedded Network Services** screen, check the **Enable DHCP Logging**.

Configuring Inventory Data Collection Schedule for Physical Accounts

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Physical Accounts**.

Step 3 Click **Inventory Scheduler**.

Step 4 On the **Inventory Scheduler** screen, complete the required fields, including the following:

Name	Description
Task Type drop-down list	Displays the available task types. Choose**UCS Inventory Collector**, **UCS Monitoring DataCollector Task**, or **Virtual SAN Ready Node Qualification Task**.
System tasks field	Choose the system tasks.

Step 5 Click **Next** and complete the required fields, including the following:

Name	Description
Task Execution drop-down list	Choose**Enable**.
Schedule Type drop-down list	Specify the schedule type. It can be one of the following options: • **Fixed Delay**—Implies the time period between the completion of one task execution and the initiation of the next task execution. • **Fixed Rate**—Implies the time period between successive tasks executions. If there is a delay in the execution of one task or if one task takes longer to execute than its scheduled time, it results in delays in subsequent task executions. These tasks will not run concurrently.
Hours	Choose a number from the dropdown list. If you chose **Fixed Delay** as the schedule type, then this number indicates the time gap, in hours, between the completion of one task exection and the initiation of the next task execution. If you chose **Fixed Rate**, then this number indicates time period, in hours, between successive task executions.
Enable Custom Frequency check box	Check this check box to enable a custom frequency for the system task.

Name	Description
Recurrence Type drop-down list	Specify the recurrence schedule. It can be one of the following: • **No End** • **Only Once** This field is displayed only when you check the **Enable Custom Frequency** check box.
Start Time field	Specify the date and time for the recurrence schedule. This field is displayed only when you check the **Enable Custom Frequency** check box.
Frequency drop-down list	Choose a frequency. It can be one of the following: • **Hourly** • **Daily** • **Weekly** • **Monthly** **Note** This field is displayed only when you select **No End** in the **Recurrence Type** drop-down list.
Frequency Interval drop-down list	Choose a frequency interval from the drop-down list. The values in this list vary depending on the frequency you have specified. This field is displayed only when you check the **Enable Custom Frequency** check box.

Step 6 Click **Submit**.

Testing Connectivity

You can test connectivity for managed network elements, virtual accounts, and physical accounts.

Testing Connectivity of Managed Network Elements

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Managed Network Elements**.

Step 3 Click the row with the pod for which you want to test connectivity.

Step 4 Click **Test Connection**.

Testing the Connection to a Physical Account

You can test the connection at any time after you add an account to a pod.

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Multi-Domain Managers**.

Step 3 On the **Multi-Domain Managers** screen, click the row of the account for which you want to test the connection.

Step 4 Click **Test Connection**.

Step 5 When the connection test has completed, click **Close**.

What to do next

If the connection fails, verify the configuration of the account, including the username and password. If the username and password are correct, determine whether there is a network connectivity problem.

Enabling Device Discovery

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Discovered Devices**.

Step 3 Click **Setup Discovery**.

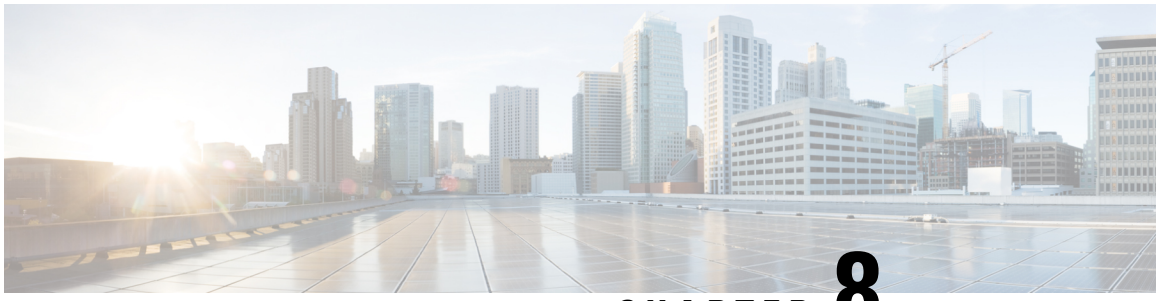
Step 4 On the **Setup Discovery** screen, check **Enable Discovery**.

Step 5 On the **Setup Discovery** screen, complete the IP address range field and determine if the default values for the following fields are adequate for your environment:

Name	Description
Enable Discovery check box	The check box is checked by default to enable device discovery for this account.
IP Range field	The IP address range for device discovery. (For example, 10.1.1.1-10.1.1.12)
TCP Timeout (ms) field	The TCP timeout (ms) (default value is 2000 ms).

Name	Description
SNMP Timeout (ms) field	The SNMP timeout (ms) (default is 1500 ms).
SNMP Community Strings field	The SNMP community string (default is public).

Step 6 Click **Submit**.



CHAPTER 8

Managing a Virtual Infrastructure

This chapter contains the following sections:

- About Managing VMware Clouds, on page 195
- Verifying Cloud Discovery and Connectivity, on page 202
- Viewing vCenter Plug-ins, on page 203
- Provisioning Virtual Machines in Cisco UCS Director, on page 203

About Managing VMware Clouds

Cisco UCS Director supports VMware through vCenter (ESX 3.5, ESX/ESXi 4.x, 5.x, 6.0 and 6.5). Cisco UCS Director automatically discovers all existing virtual machines (VMs) and images in the newly added cloud account. Typically, the discovery process takes about 5 minutes. You can also add VMware clouds

Note The term “cloud” refers to one vCenter installation.

Cisco UCS Director supports inventory collection and VM provisioning using multiple datacenters and clusters. When creating a VMware cloud, you can choose the option to discover and select multiple datacenters and clusters. Once you add a discovered datacenter and cluster to a cloud, you cannot de-select them from the cloud by editing it. However, you can edit the cloud to add extra datacenters and clusters.

Note Cisco UCS Director does not support the creation of clouds that use the same vCenter account. If there are duplicate accounts, you cannot create a VMware Cloud. In addition, if there are duplicate accounts, VM provisioning fails and an error appears in the status for the virtual account. The **Test Connectivity** function also fails with the error message. This error also occurs if the same server with the same combination of clusters is used in different clouds.

To disable this functionality, you can manually modify the `vmware.properties` file in the `cd /opt/infra/inframgr` directory to allow duplicate account IDs by setting the `allowDuplicateClouds` field to true. By default the field is set to false.

When upgrading from a previous release, all duplicate accounts display a failed connection status. Though an error message displays, all the actions can still be executed on the VMs.

Creating a VMware Cloud

When creating a VMware cloud, you can specify a datacenter and clusters in one of the following ways:

- Within the credential policy
- In the **VMware Datacenter** and **VMware Cluster** fields
- From the **Discover Datacenters / Clusters** check box

Note Either a datacenter within the credential policy or the VMware datacenter and VMware cluster can be selected. Specifying the datacenter in the **Add Cloud** screen and in the credential policy form results in an error.

Procedure

Step 1 Choose **Administration** > **Virtual Accounts**.

Step 2 On the **Virtual Accounts** page, click **Virtual Accounts**.

Step 3 Click **Add**.

Step 4 On the **Add Cloud** screen, complete the required fields, including the following:

Name	Description
Cloud Type drop-down list	Displays the available cloud types. Choose VMware. **Note** The following fields are displayed when VMware is chosen. Other cloud types display fields that are specific to that cloud type.
Cloud Name field	The cloud name. The name cannot include single quotes. **Note** Each cloud requires a unique name in Cisco UCS Director. Once a cloud has been added, all reports refer to the cloud using the Cloud Name.
Server Address field	The vCenter server address
Use Credential Policy check box	Check this check box if you want to use a credential policy for this account rather than enter the information manually.
Use Credential Policy drop-down list	If you checked **Use Credential Policy**, choose the crednetial policy that you want to use from this drop-down list. This field is only displayed if you choose to use a credential policy.

Name	Description
Server User ID field	The vCenter server username.
Server Password field	The vCenter server password.
Server Access Port field	The server port number.
Server Access URL field	The server access URL.
VMware Datacenter field	The data center name on the vCenter account.
Discover Datacenters / Clusters check box	Check this check box to discover and use any VMware datacenters and associated VMware clusters.
VMware Cluster field	The name of the VMware cluster in the vCenter account. This name allows you to discover, monitor, and manage the specified pod's resources. Leave the field blank if the entire vCenter account is managed by Cisco UCS Director.
Select Datacenters / Clusters field	Check the associated datacenters and clusters you want to use. **Note** This field is visible only when you check the **Discover Datacenters / Clusters** check box.
Enable SRM check box	Check this check box to enable Site Recovery Manager (SRM) for the account.
Primary SRM Server Address field	The IP address of the primary SRM server. **Note** This field is visible only when you check the **Enable SRM** check box.
Primary SRM Server User ID field	The user ID for the primary SRM server. **Note** This field is visible only when you check the **Enable SRM** check box.
Primary SRM Server Password field	The password of the user for the primary SRM server. **Note** This field is visible only when you check the **Enable SRM** check box.

Name	Description
Primary SRM Server Access Port field	The port number for the primary SRM server. For SRM version 6.0, enter 9086 as the port number. **Note** This field is visible only when you check the **Enable SRM** check box.
Remote SRM Server User ID field	The user ID for the remote SRM server. **Note** This field is visible only when you check the **Enable SRM** check box.
Remote SRM Server Password field	The password of the user ID for the remote SRM server. **Note** This field is visible only when you check the **Enable SRM** check box.
Use SSO check box	Check this check box to use Single Sign-On (SSO) for authentication. The SSO option is only available for Virtual SAN (VSAN). SSO credentials are required for VM provisioning using storage profiles on the Virtual SAN cluster.
SSO Server Address field	The IP address of the Single-Sign On server. **Note** This field is visible only when you check the **Use SSO** check box.
SSO Server User ID field	The user ID for the SSO server. **Note** This field is visible only when you check the **Use SSO** check box.
SSO Server Password field	The password of the user ID for the SSO server. **Note** This field is visible only when you check the **Use SSO** check box.
SSO Server Access URL field	The URL for SSO server access. **Note** This field is visible only when you check the **Use SSO** check box.

Name	Description
SSO Server Access Port field	The port number. For vCenter version 5.x, enter 7444 as the port number. **Note** This field is visible only when you check the **Use SSO** check box.
Server Access URL field	The URL for server access.
Description field	The description of the cloud.
Contact Email field	The contact email address for the cloud.
Location field	The location.
Pod drop-down list	Choose the converged infrastructure pod. When you choose a pod name, the VMware cloud account is made available in the converged infrastructure stack. **Note** You cannot add more than one virtual account to a virtual SAN pod.
Service Provider field	The service provider's name.

Step 5 Click **Add**.

Configuring Inventory Data Collection Schedule for Virtual Accounts

Procedure

Step 1 Choose **Administration** > **Virtual Accounts**.

Step 2 On the **Virtual Accounts** page, click **Virtual Accounts**.

Step 3 Click **Inventory Scheduler**.

Step 4 On the **Inventory Scheduler** screen, complete the required fields, including the following:

Name	Description
Task Type drop-down list	Displays the available task types. Choose **Inventory Collector** or **Event Collector**.
System tasks field	Choose the system tasks.

Step 5 Click **Next** and complete the required fields, including the following:

Name	Description
Task Execution drop-down list	Choose**Enable**.
Schedule Type drop-down list	Specify the schedule type. It can be one of the following options: • **Fixed Delay**—Implies the time period between the completion of one task execution and the initiation of the next task execution. • **Fixed Rate**—Implies the time period between successive tasks executions. If there is a delay in the execution of one task or if one task takes longer to execute than its scheduled time, it results in delays in subsequent task executions. These tasks will not run concurrently.
Hours	Choose a number from the dropdown list. If you chose **Fixed Delay** as the schedule type, then this number indicates the time gap, in hours, between the completion of one task exection and the initiation of the next task execution. If you chose **Fixed Rate**, then this number indicates time period, in hours, between successive task executions.
Enable Custom Frequency check box	Check this check box to enable a custom frequency for the system task.
Recurrence Type drop-down list	Specify the recurrence schedule. It can be one of the following: • **No End** • **Only Once** This field is displayed only when you check the **Enable Custom Frequency** check box.
Start Time field	Specify the date and time for the recurrence schedule. This field is displayed only when you check the **Enable Custom Frequency** check box.

Name	Description
Frequency drop-down list	Choose a frequency. It can be one of the following: • **Hourly** • **Daily** • **Weekly** • **Monthly** **Note** This field is displayed only when you select **No End** in the **Recurrence Type** drop-down list.
Frequency Interval drop-down list	Choose a frequency interval from the drop-down list. The values in this list vary depending on the frequency you have specified. This field is displayed only when you check the **Enable Custom Frequency** check box.

Step 6 Click **Submit**.

Downloading the PowerShell Agent Installer

The PowerShell Agent is installed on Windows Server 2008 R2 or Windows Server 2012 64-bit virtual machines.

Procedure

Step 1 Choose **Administration** > **Virtual Accounts**.

Step 2 On the **Virtual Accounts** page, click **PowerShell Agents**.

Step 3 Click **Download Installer**.

Step 4 In the **Download Agent Installer** screen, check if your system meets the listed installation requirements.

Step 5 If the requirements are met, click **Submit**.

The **Opening PSASetup. exe** dialog box prompts you to save the executable file.

Step 6 Click **Save File**.

The file is saved to your system's download location.

Step 7 Install the **PSASetup. exe file** on your Windows Server 2008 R2 or Windows Server 2012 64-bit virtual machine (VM).

Creating a PowerShell Agent

Procedure

Step 1 Choose **Administration** > **Virtual Accounts**.

Step 2 On the **Virtual Accounts** page, click **PowerShell Agents**.

Step 3 Click **Add**.

Step 4 In the **Add Agent** screen, complete the required fields, including the following:

Name	Description
Agent Name field	The agent name.
Agent Address field	The agent address.
Agent Access Port field	The agent access port number.
Access Key field	The access key.
Description field	The description of the agent.

Step 5 Click **Submit**.

Verifying Cloud Discovery and Connectivity

Testing the Connection

Procedure

Step 1 Choose **Administration** > **Virtual Accounts**.

Step 2 On the **Virtual Accounts** page, click **Virtual Accounts**.

Step 3 Choose the VMware account that you want to test.

Step 4 Click **Test Connectivity**.

There is no progress bar that displays the results of the connectivity test. Use the **Summary** tab to verify that the cloud account is added and its data is collected.

Step 5 Choose **Virtual** > **Compute**.

Step 6 Click **Summary**.

It can take a few minutes to complete autodiscovery and populate the data.

Step 7 Choose the cloud name to view its status details.

Viewing vCenter Plug-ins

Procedure

Step 1 Choose **Administration** > **Virtual Accounts**.

Step 2 On the **Virtual Accounts** page, click **Plugins**.

Provisioning Virtual Machines in Cisco UCS Director

Provisioning virtual machines in Cisco UCS Director is a multi-step process. It involves steps such as creating a virtual account, creating policies, and creating catalogs and service requests. Prior to starting this task, as an administrator, determine the following:

- The cluster in which the VM must be deployed
- The datastores within the cluster that are available for VM provisioning
- The available network within the cluster in which the VM must be deployed



Attention In the absence of this information, if you select invalid datastores or an incorrect network for a cluster, VM provisioning in Cisco UCS Director fails.

The process of provisioning a VM in Cisco UCS Director can be summarized as:

1. Create a user group.

   For more information, see Creating a User Group, on page 55.

2. Create a virtual account.

   A VM is provisioned within a virtual account in Cisco UCS Director. For more information, see Creating a VMware Cloud, on page 196.

3. Create a VMware system policy.

   This policy defines the system-specific information for the VM. You must specify the VM naming template to use, the OS to be configured, and the domain in which the VM must be provisioned. For more information, see Configuring a System Policy, on page 235.

4. Create a VMware computing policy.

   Computing policies determine the compute resources that can be used during provisioning to satisfy group or workload requirements. The cluster that you specify in this policy determines the choices you make in subsequent policies. For more information, see Creating a Computing Policy, on page 208.

5. Create a storage policy.

   A storage policy defines resources such as the datastore scope, type of storage to use, minimum conditions for capacity, latency, and so on. For more information, see Adding and Configuring a Storage Policy, on page 219.

6. Create a network policy.

   The network policy defines resources such as network settings, DHCP or static IP, and the option to add multiple vNICs for provisioning VMs. For more information, see Configuring a Network Provisioning Policy, on page 233.

7. Create a virtual data center.

   A Virtual Data Center (VDC) is an environment that combines virtual resources, operational details, rules, and policies. While creating a VDC, select the user group that you created for VM provisioning, and select the cloud that you specified while creating the policies. Based on the cloud account that you select, all the subsequent policy-related fields are populated. For more information, see Adding a Virtual Data Center, on page 248.

8. Create a catalog to select a template.

   You can self-provision virtual machines (VMs) using predefined catalog items. A catalog defines parameters such as the cloud name and the group name to which the VM is bound. For more information, see Publishing a Catalog, on page 300.

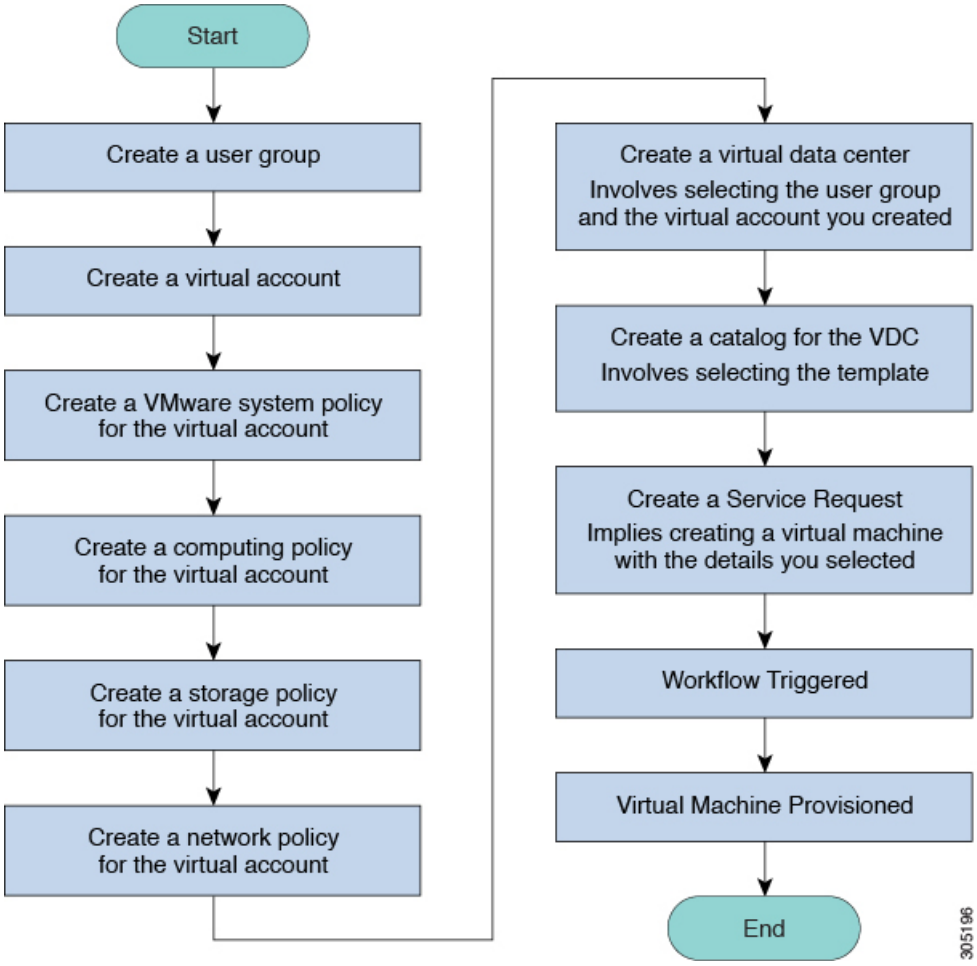
9. Create and submit a service request.

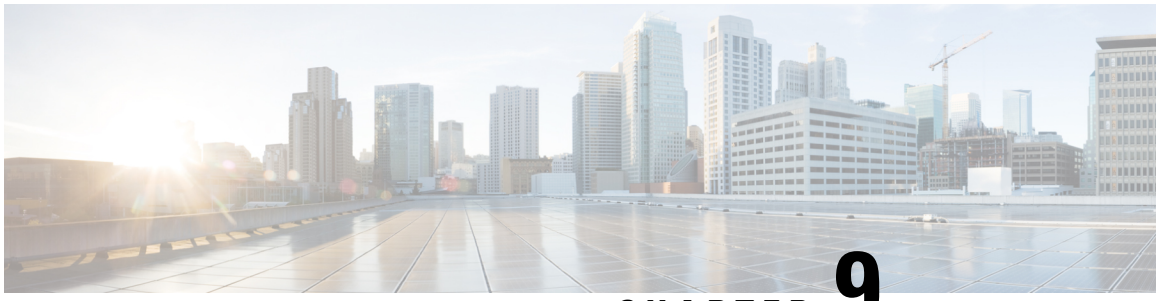
   You can use the self-service provisioning feature to create a service request to provision virtual machines (VMs), services, or applications. The service request process produces a provisioning workflow for VM creation. For more information, see Creating a Service Request with Catalog Type—Standard, on page 316.

   After you submit a service request, a workflow is triggered, and the VM is provisioned.

The following image illustrates the workflow to provision a VM in Cisco UCS Director.

Figure 2: Workflow for Provisioning a Virtual Machine in Cisco UCS Director





CHAPTER 9

Managing Policies

This chapter contains the following sections:

- Policies, on page 207
- Computing Policies, on page 208
- Configuring a Bare Metal Server Provisioning Policy, on page 211
- Data Collection Policy, on page 215
- About Group Share Policy, on page 218
- Storage Policies, on page 219
- Credential Policies, on page 226
- Network Policies, on page 227
- System Policies, on page 235
- End User Self-Service Policy, on page 242
- Configuring a VM Management Policy, on page 243

Policies

Cisco UCS Director provides an End User Portal in which resources, such as virtual machines (VMs) or bare metal servers, are provisioned from a pool of assigned resources using predefined policies set by administrators.

A policy is a group of rules that determine where and how a new resource, be it a virtual machine or a bare metal server, is provisioned within the infrastructure, based on available system resources.

Cisco UCS Director requires that you set up the following policies to provision resources:

- Computing
- Storage
- Network
- System
- Bare Metal



Important Create a cloud account prior to setting up policies to provision VMs.

Computing Policies

Computing policies determine the compute resources that can be used during provisioning to satisfy group or workload requirements.

As an administrator, you can define advanced policies by mixing and matching various conditions in the computing policy.

Note We recommend that you thoroughly understand all the fields in the computing policy. Some combinations of conditions can result in no host machines being available during self-service provisioning.

Creating a Computing Policy

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Computing**.

Step 2 On the **Computing** page, click **VMware Computing Policy**.

Step 3 Click **Add**.

Step 4 On the **Add Computing Policy** screen, complete the following fields:

Name	Description
Policy Name field	The name of the policy. **Note** This name is used during catalog definition.
Policy Description field	The description of the policy.
Cloud Name drop-down list	Choose the cloud where resource allocation occurs.
Host Node/Cluster Scope drop-down list	Choose the scope of deployment. **Note** You can narrow the scope of deployment by specifying whether to use all, include chosen, or exclude chosen options. Depending on the choices, a new field appears where the required hosts or clusters can be chosen.
Resource Pool drop-down list	Choose the resource pool.
ESX Type drop-down list	Choose the ESX installation type: **ESX**, **ESXi**, or **both**.
ESX Version drop-down list	Choose the version of ESX.

Name	Description
Filter Conditions check boxes	Check one or more conditions that should match. Any hosts that do not meet these criteria are excluded from consideration. If more than one condition is chosen, all of the chosen conditions must match.
Deployment Options	
Override Template check box	Check to override the template properties. You are provided with options to enter custom settings for CPU and memory.
Number of vCPUs field	A custom number of vCPUs. The specified number of vCPUs for a VM should not exceed the total cores for the chosen scope of host nodes or clusters. **Note** This option appears if you checked **Override Template**.
CPU Reservation (MHz) field	The CPU reservation for the VM. The reservation depends upon the number of vCPUs specified. **Note** This option appears if you checked **Override Template**.
CPU Limit (MHz) field	The CPU limit for the VM. The CPU limit is based on the chosen scope of host nodes or clusters.
CPU Shares drop-down list	Choose the CPU shares: low, normal, or high. The CPU shares determine which VM gets CPU resources when there is competition among VMs. **Note** This option appears if you checked **Override Template**.
Memory field	The custom memory for the VM. **Note** This option appears if you checked **Override Template**.
Memory Reservation (MB) field	The memory reservation for the VM. The reservation depends upon the memory specified. **Note** This option appears if you checked **Override Template**.

Name	Description
Memory Limit (MB) field	The memory limit for the VM. The memory limit is based on the chosen scope of host nodes or clusters. **Note** This option appears if you checked **Override Template**.
Memory Shares drop-down list	Choose the memory shares: low, normal, or high.1 Memory shares determine which VM gets memory resources when there is competition among VMs. **Note** This option appears if you checked **Override Template**.
Resizing Options	
Allow Resizing of VM check box	Check to allow VM resizing before provisioning or to resize an existing VM.
Permitted Values for vCPUs field	The range of vCPUs to use while provisioning a VM or resizing an existing VM. A range of more than 8 is visible during VM provisioning or resizing only if the chosen cloud (vCenter) is 5 or above and has VM version 8. Only the values specified in the box are visible. **Note** This option appears if you checked **Allow Resizing of VM**.
Permitted Values for cores per socket	The number of permitted cores per socket. The number of cores per socket can be configured when creating a service request, deploying a VM, cloning a VM, or provisioning a VM using an orchestration workflow. If this field is empty, you will not have the option to specify the cores per socket while provisioning a VM and other actions.
Permitted Values for Memory in MB field	The range of memory to use while provisioning a VM or resizing an existing VM. For example: 512, 768, 1024, 1536, 2048, 3072, 4096, and so on. Only the values specified in the box are visible. **Note** This option appears if you checked **Allow Resizing of VM**.

Step 5 Click **Submit**.

Configuring a Bare Metal Server Provisioning Policy

Before you begin

- A Bare Metal Agent (BMA) account must be added and configured with Bare Metal OS images.
- A Cisco UCS Manager account must be added.
- A Cisco UCS Central account must be added.
- If you need a specific cost associated with the bare metal server, then you must create a bare metal server cost model prior to creating this policy.

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **Bare Metal Servers**.

Step 2 On the **Bare Metal Servers** page, click **Bare Metal Server Provisioning Policy**.

Step 3 Click **Add**.

Step 4 On the **Add Bare Metal Server Provisioning Policy** screen, complete the required fields, including the following:

Name	Description
Policy Name field	Enter a unique name for the policy.
Policy Description field	Enter a description for the policy.
Account Type drop-down list	Choose an account type from the drop-down list. It can be one of the following: • UCS Central • UCS Manager
UCS Central Account Name drop-down list	Choose a Cisco UCS Central account name. **Note** This field is displayed only if you selected **UCS Central** in the **Account Type** drop-down list.
Account Name drop-down list	Choose an account name from the drop-down list.
Server Selection Scope drop-down list	Choose the scope for the policy. It can be one of the following: • **Include Servers** • **Include Server Pools**

Name	Description
Domain Group(s) list	Expand the list to check the UCS domain groups to be included in this policy. After checking the domain groups, click **Validate**. **Note** This field is displayed only if you selected **UCS Central** in the **Account Type** drop-down list.
Include Ungrouped Domains check box	Check this check box to populate the **Domain Name(s)** list with ungrouped domains along with the domain names included in the selected domain groups. **Note** This field is displayed only if you selected **UCS Central** in the **Account Type** drop-down list and if you have selected a domain group from the **Domain Group(s)** list.
Domain Name(s) list	Expand the list to check the UCS domain names to be included in this policy. After checking the domain name, click **Validate**. **Note** This field is displayed only if you selected **UCS Central** in the **Account Type** drop-down list.
Servers field	Check the servers for this policy. This field is visible only if you selected **Include Servers** in the **Server Selection Scope** drop-down list.
Server Pools field	Check the server pools for this policy. This field is visible only if you selected **Include Server Pools** in the **Server Selection Scope** drop-down list.
Service Profile Template drop-down list	Choose a service profile template.
Use for SAN Boot check box	Check to include servers that contain at least one FCoE capable interface card.
Minimum Number of CPUs field	Specify the minimum number of CPUs that the server must contain.
Minimum Amount of Memory (MB) field	Specify the minimum amount of memory that must be available on the server.
Minimum Number of Cores Enabled field	Specify the number of cores that must be enabled on the server.

Name	Description
Allow User to Choose Servers check box	Check to allow users to select servers while using this policy to provision bare metal servers. If you do not check this check box, a bare metal server is provisioned based on the parameters you specify in this policy.
Show Server Resources to User check box	Check to have the system resources displayed when provisioning bare metal servers. You can choose any of the following resources: • **CPU** • **Memory** • **Storage**
Target BMA drop-down list	Select a bare metal agent for the PXE setup.
Use Windows Images check box	Check this check box to view a list of Windows images that you can select.
OS Image Selection	Check the check boxes of the OS images. If you checked **Use Windows Images**, then a list of Windows images are displayed. If you did not check **Use Windows Images**, then a list of Windows and CentOS images are displayed. While creating a service request for provisioning bare metal servers, you are prompted to select a Windows image.
Network Boot Manager drop-down list	Choose a boot manager from the drop-down list. It can be one of the following: • PXE • iPXE-BIOS • iPXE-EUFI
IP Configuration Type drop-down list	Choose the type of IP configuration from the drop-down list. It can be one of the following: • DHCP • Static

Name	Description
Domain Mapping list	Expand this list to map a domain to a specific BMA, or OS image. Click + to add a domain mapping. You will need to specify information for the following fields: • Domain Name—check the names of the domains that you want to map. • Target BMA—Choose a target BMA from the drop-down list. • OS Image—Check an OS image. **Note** This field is displayed only if you selected **UCS Central** in the **Account Type** drop-down list.
Network Management	
Use Static IP Pool Policy check box	Check to select a static IP pool policy for provisioning a bare metal server. If you check this check box, an IP address is automatically assigned to the bare metal server from the IP range provided in the static IP pool policy.
Server IP Address field	Specify an IP address range.
Server Netmask field	Specify the server netmask.
Server Gateway field	Specify the server gateway IP address
Name Server field	Specify the name server IP address
Management VLAN field	Specify the management VLAN. By default, it is set to 0.
System Parameters	
Server Host Name field	Specify the server host name.
Host Name Validation Policy drop-down list	Choose a policy from the drop-down list. The server host name is validated against the policy that you select in this field before it is applied on the bare metal server.
Password field	Specify the password for the server host name.
Confirm Password field	Confirm the password for the server host name.
Timezone drop-down list	Set the time zone for the servers.

Name	Description
Cost Model drop-down list	Choose a cost model for the servers.

Step 5 Click **Submit**.

What to do next

You can validate the policy.

Validating a Bare Metal Server Provisioning Policy

To ensure that the parameters specified in the bare metal server provisioning policy are accurate, you can run this validation process on the policy.

Before you begin

You should have created a bare metal server provisioning policy.

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **Bare Metal Servers**.

Step 2 On the **Bare Metal Servers** page, click **Bare Metal Server Provisioning Policy**.

Step 3 Choose a policy from the list of policies.

Step 4 From the **More Actions** drop-down list, choose **Validate**.

The validation process is initiated, and the results are displayed in the **Status** column on the **Bare Metal Server Provisioning Policy** screen.

Data Collection Policy

A data collection policy can be created to control the parameters that can be retrieved from the vCenter server for each VMware account. Each of the parameters mentioned in a data collection policy is collected and used in specific trend reports in Cisco UCS Director.



Note VMware is the only supported virtual account type. When a VMware account is added, it is automatically associated with the **default-data-collection-policy**.

Configuring a Data Collection Policy for a Virtual Account

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Service Delivery**.

Step 2 On the **Service Delivery** page, click **Data Collection Policy**.

Step 3 Click **Add**.

Step 4 On the **Add** screen, complete the following fields:

Name	Description
Name field	The name of the data collection policy. **Note** This name is used during catalog definition.
Description field	The description of the policy.
Account Type drop-down list	The VMware virtual account is selected.

Name	Description
Resource window	Choose a data collection group containing vCenter parameters. For example: CPU. Click the pencil icon to edit the data collection group. On the **Edit Resource Entry** screen, you can enable or disable data collection by checking or unchecking **Enable Collection**. To view the datastore-specific performance data in the Cisco UCS Director GUI, select the following resources: • Datastore throughput in kilobytes per second • Datastore number of read average • Datastore number of write average • Disk total latency in milliseconds For a Disk Latency report, in addition to selecting the resources listed above, set the vCenter Server performance data statistics collection level to 3. For a Throughput report, in addition to selecting the resources listed above, set the vCenter Server performance data statistics collection level to 4. **Important** Increasing the statistics collection to level 2 and above in the vCenter server could have an impact on the performance of the vCenter server and of Cisco UCS Director. For more information, see https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2003885.

Step 5 Click **Submit**.

Associating the Data Collection Policy for a Virtual Account

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Service Delivery**.

Step 2 On the **Service Delivery** page, click **Data Collection Policy Association**.

Step 3 Choose the **Data Collection Policy Association** tab.

Step 4 Click the row with the virtual (VMware) account for which you want to associate the data collection policy, and click **Edit**.

Step 5 In the **Edit** dialog box, choose the data collection policy from the **Policy** drop-down list that you configured.

Step 6 Click **Submit**.

The VMware account is now associated with the data collection policy.

About Group Share Policy

A group share policy provides more control to the users on resources and on what they can share with other users. With this policy, users can view resources that are currently assigned only to them or can view resources that are assigned to all groups that the users are part of.

While you are creating a group, you can define a group share policy and determine which groups have read/write permissions. Later, when users are added to this group, their access to resources is defined by the group share policy.

Creating a Group Share Policy

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **Group Share Policy**.

Step 3 Click **Add**.

Step 4 On the **Add Group Share Policy** screen, complete the following fields:

Name	Description
Policy Name field	The name of the group share policy.
Policy Description field	The description of the policy.
MSP Group Share Policy check box	Check to apply this policy to one or more MSP organizations.
MSP Organizations field	Click **Select** to choose the MSP organizations that have read/write permissions for the resources defined with this policy. This file is only available if you check **MSP Group Share Policy**.
Customer Organizations field	Click **Select** to choose the organizations that have read/write permissions for the resources defined with this policy.

Step 5 Click **Submit**.

What to do next

You can associate this group share policy with user groups in the system. Based on the permissions, users within those groups inherit read/write permissions to resources.

Storage Policies

A storage policy defines resources such as the datastore scope, type of storage to use, minimum conditions for capacity, latency, and so on.

The storage policy also provides options to configure additional disk policies for multiple disks, and to provide datastore choices for use during a service request creation.

Note Cisco UCS Director supports datastore choice during a service request creation for VM provisioning. You can enable or disable datastore choices for the end user during service request creation. The datastores listed depend upon the scope conditions specified in the storage policy that is associated with the VDC during the service request creation.

To use the datastore selection feature while creating a service request, the template for VM provisioning must have the disk type assigned as **System**. This is applicable for templates with single or multiple disks.

Storage Policies for Multiple VM Disks

Cisco UCS Director supports VM provisioning with multiple disks on multiple datastores.

Disks are classified into five types: system, data, database, swap, and log. The system disk policy is configured first, and the other disks can be configured depending on requirements. You can configure the disk policy individually for each disk type or choose the default system disk policy for each disk.

Note For information on creating a storage policy for a template with multiple disks, see Multiple Disk VM Provisioning, on page 343.

Adding and Configuring a Storage Policy

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Storage**.

Step 2 On the **Storage** page, click **VMware Storage Policy**.

Step 3 Click **Add**.

Step 4 On the **Add Storage Resource Allocation Policy** screen, complete the following fields:

Name	Description
Storage Policy - System Disk Policy	
Policy Name field	Enter the cloud in which resource allocation occurs.
Policy Description field	Enter the description of the policy. If you want to narrow the scope of deployment, choose whether to use all data stores, include selected data stores, or exclude selected data stores.
Cloud Name drop-down list	Choose the cloud account for this resource allocation. If you choose an SRM account, the **Enable Protection** check box is displayed. For more information about how to enable protection groups for Site Recovery Manager, see the Cisco UCS Director VMware Management Guide.
Use ReadyClone check box	Check to ensure that VMs are deployed using ReadyClones. This option is available only if the cloud account you chose is an HyperFlex (HX) cloud.
Enable HX Protection check box	Check if you want to protect the VMs using HyperFlex cloud. This field is displayed only when the VM is enabled with Hyperflex Dataprotection.
Select Protection Group field	Choose the protection group to protect the VM. Click **Select** to choose the protection group. This field is displayed only when you check the **Enable HX Protection** check box.
System Disk Scope	
Use Linked Clone check box	Check if you want to use a linked clone. If you do not check this box, the configuration uses a full clone.
Storage Profile drop-down list	Choose a storage profile if you want to provision one or more VMs with the associated storage profile.

Name	Description
Data Stores/Datastore Clusters Scope drop-down list	To define the scope of deployment, choose one of the following options: • **All** • **Include Selected Datastores** • **Exclude Selected Datastores** • **Include Selected Datastore Clusters** • **Exclude Selected Datastore Clusters** Depending on which option you choose, additional fields may display. **Note** The option that you choose determines which datastores or datastore clusters are available when you create a VM disk.
Selected Data Stores field	If you chose **Include Selected Datastores** or **Exclude Selected Datastores**, expand **Selected Data Stores** to choose the appropriate datastores.
Use Shared Data Store only check box	Check to use only shared datastores. This option is available only if you chose to include or exclude selected datastores.
Selected Datastore Clusters field	If you chose **Include Selected Datastore Clusters** or **Exclude Selected Datastore Clusters**, expand **Selected Datastore Clusters** to choose the appropriate datastore clusters.
Select SDRS Rule Type drop-down list	If you chose to include or exclude selected datastore clusters, choose one of the following SDRS rule types: • **Keep VMDKs Together**—You need to select an existing rule on the filtered clusters. The newly provisioned VM is added to the VM anti-affinity rule. • **Separate VMDKs**—If the newly provisioned VM contains more than one disk, a new VM affinity rule is created on the datastore cluster.
Select SDRS Rule field	If you chose **Keep VMDKs Together**, you must choose the VMs to which you want to apply the rule.
Storage Options	
Use Local Storage check box	By default, the option is checked. Uncheck if you do not want to use local storage.

Name	Description
Use NFS check box	By default, the option is checked. Uncheck if you do not want to use NFS storage.
Use SAN check box	By default, the option is checked. Uncheck if you do not want to use SAN storage.
Filter Conditions check boxes	To add one more conditions to filter the datastores, do the following for each desired condition: • Check the appropriate box. • Choose the desired option from the drop-down list. • Enter the criteria by which you want to filter the datastores. Any datastores that do not meet these criteria are excluded from consideration. If more than one condition is chosen, all conditions must match.
Override Template check box	Check to override the template properties. You are provided with options to enter custom settings, such as using thin provisioning or setting a custom disk size.
Use Thin Provisioning check box	Check to use thin provisioning during VM storage provisioning. Thin provisioning enables dynamic allocation of physical storage capacity to increase VM storage utilization. This option is available only if you choose **Override Template**.
Manual Disk Size check box	Check to use a custom disk size that overrides the disk size of the template used for VM provisioning. This option is available only if you choose **Override Template**.
Resizing Options for VM Lifecycle	
Allow Resizing of Disk check box	Check to provide the end user with an option to choose the VM disk size before provisioning.

Name	Description
Permitted Values for Disk in GB field	Specify the disk size values that can be chosen while provisioning a VM. You can specify these values in one of the following formats: • Range such as 10-1000 • Comma separated values such as 1, 5, 10, 50, 100, 500, 1024, 5120, 10240. • Combination of range and comma separated values such as 1,5,10, 10-1000. This option is available only if you choose **Allow Resizing of Disk**.
Allow user to select datastores from scope check box	Check to provide the end user with an option to choose the datastore during the service request creation.

Note
If you use this storage policy for OVF deployment, then the deployed OVF VM is created without thin provisioning.

Step 5 Click **Next**.

Step 6 On the **Additional Disk Policies** screen, do one of the following:

- Expand **Disk Policies** to choose a disk type to configure if you do not want to use the same disk policy for that disk type as you configured in the System Disk Policy.
- Click **Next** if you want to use the System Disk Policy options for all disk types.

Note
By default, the disk policy for the disk is the same as in the System Disk Policy that you configured on the **Add Storage Resource Allocation Policy** screen.

Step 7 If you chose to configure a custom system disk policy for a specific disk type, do the following:

a) Click **Edit** to edit the disk type.
b) On the **Edit Disk Policies Entry** screen, uncheck **Same As System Disk Policy**.
c) On the**Edit Entry** screen, complete the fields.

All the fields displayed here are the same as the fields displayed on the **Add Storage Resource Allocation Policy** screen.

Note
This configuration determines which datastores are available for the disk type when you create a VM disk.

d) Click **Submit**.
e) Repeat these steps to configure the other disk types, if desired.

Note

To use the storage policy created with additional disk policies, you must associate the policy with the VDC that is used for the VM provisioning

Step 8 Click **Next**.

Step 9 On the **Hard Disk Policy** screen, specify the number of physical disks that you want to create during VM provisioning.

a) Expand **Disks** to add a disk by completing the following fields:

Field	Description
Disk Label field	Enter a descriptive label for the disk you are adding.
Disk Size (GB) field	Enter the size of the disk.
Disk Type drop-down list	Choose the disk type. The options that you see in this drop-down list depends on whether you checked **Same as System Policy** earlier in this procedure.
Controller Options	
Controller Type drop-down list	Choose a controller type from the drop-down list. Based on the availability of ports, a controller is mapped to the VM disks.
Create Disk on new Controller check box	Check this box to create a new controller. The type of controller that is created is based on the selection you made in the **Controller Type** drop-down list.
Disk Provisioning Options	
Disk Provisioning Options radio buttons	Click the radio button of the type of provisioning you want to specify. You can specify one of the following: • **Thin Provision** • **Thick Provision lazy zeroed** • **Thick Provision eager zeroed**
Resizing Options for VM Lifecycle	
Allow Resizing of Disk check box	Check to enable editing of the VM disk size before provisioning.

Field	Description
Permitted Values for Disk in GB field	Specify the disk size values that can be chosen while provisioning a VM. You can specify these values in one of the following formats: • Range such as 10-1000 • Comma separated values such as 1, 5, 10, 50, 100, 500, 1024, 5120, 10240. • Combination of range and comma separated values such as 1,5,10, 10-1000. This option appears if **Allow Resizing of Disk** is checked.
Allow user to select datastores from scope check box	Check to provide the user with an option to choose the datastore during the service request creation.

Step 10 Click **Submit**.

Note

- If you use a storage policy for OVF deployment, then the deployed OVF VM is created without thin provisioning.
- To use the storage policy created with additional disk policies, you need to associate the policy with the VDC that is used for the VM provisioning.
- When using the Additional Disks Policies configured in a policy, make sure to uncheck **Provision all disks in a single database** during catalog creation for the multiple disk template. For more information about catalog creation, see Managing Catalogs, on page 299.

Virtual Storage Catalogs

You can use a virtual storage catalog to customize storage policies. Using the virtual storage catalog, you can choose more than one storage policy and give it a custom storage entry name.

You map a storage catalog to a catalog by enabling it during catalog creation. When you raise a service request using the catalog, you are provided with the **Storage Tier** choice.

Configuring a Virtual Storage Catalog

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Storage**.

Step 2 On the **Storage** page, click **Virtual Storage Catalog**.

Step 3 Click **Add**.

Step 4 On the **Add Catalog** screen, complete the following fields:

Name	Description
Catalog Name field	The name of the catalog. This name is used during catalog custom actions definition.
Catalog Description field	The description of the catalog.
Cloud Name drop-down list	Select the cloud account.
Choose No of Entries drop-down list	Choose the number of entries. The range is from 1 to 10. Depending on the choice, storage entry options are provided in the subsequent dialog box.

Step 5 Click **Next**.

Step 6 On the **Add Entries** screen, complete the following fields:

Name	Description
Storage Entry #1	
Storage Entry Name field	The name of the storage entry.
Storage Policy drop-down list	Choose the storage policy.
Storage Entry # 2	
Storage Entry Name field	The storage entry name of the second policy.
Storage Policy drop-down list	Choose the storage policy.

Step 7 Click **Submit**.

What to do next

- You can map the virtual storage catalog during catalog creation.

  See Managing Catalogs.

- You can view the storage tier options during the Service request creation.

  See Using Self-Service Provisioning.

Credential Policies

A policy comprises a set of rules that controls access to a system or network resource. A credential policy defines password requirements and account lockouts for user accounts. Credential policies that are assigned

to user accounts control the authentication process in Cisco UCS Director. After you add a credential policy, you can assign the new policy as the default policy for a credential type or to an individual application.

Configuring a Credential Policy

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **Credential Policies**.

Step 2 On the **Credential Policies** page, click **Credential Policies**.

Step 3 Click **Add**.

Step 4 On the **Add Credential Policy** screen, check the check the account type.

Step 5 Click **Select**.

Step 6 On the **Add Credential Policy** screen, complete the required fields, including the following:

Name	Description
Policy Name field	A unique name for the policy.
Description field	A description for the policy.
Username field	The user name for the account.
Password field	The password for the user account.
Protocol drop-down list	Select the protocol.
Port field	The port number.

The fields displayed in this screen vary depending on the type of account that you are creating the policy for.

Step 7 Click **Submit**.

At a later point in time, if you modify the credentials in this policy, the changes are automatically applied to accounts configured with the policy. These changes are applied when Cisco UCS Director attempts to connect with these accounts.

Network Policies

The network policy includes resources such as network settings, DHCP or static IP, and the option to add multiple vNICs for VMs provisioned using this policy.

Adding a Static IP Pool Policy

You can optionally configure a static IP pool policy that can be used with a network policy.

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Network**.

Step 2 On the **Network** page, click **Static IP Pool Policy**.

Step 3 Click **Add**.

Step 4 On the **Static IP Pool Policy Information** screen, complete the following fields:

Name	Description
Policy Name field	Name of the IP pool policy.
Policy Description field	Description of the IP pool policy.
Allow IP Overlap drop-down list	Indicate whether IP overlap is allowed or not. By default, overlapping IP is not enabled. Enabling overlapping of IP implies the following: • You can create an IP pool and have IP addresses overlap within that pool. • You can create two static IP pools and have the IP addresses overlap between the pools.
Scope drop-down list	The scope of the IP pool overlap. The options are: • MSP Organization This option is visible only if you have enabled MSP. • Group/Customer Organization • Container **Note** This option is visible only if you select Yes in the **Allow IP Overlap** drop-down list.
User Group ID field	Choose **Select** to check the user group for the policy. All the user groups created in the system are displayed.
Container ID field	Choose **Select** to check the container.

Step 5 Expand the **Static IP Pools** section section and click **(+)** to add and configure multiple static IP pools.

Step 6 On the **Add Entry to Static IP Pools** screen, complete the following fields:

Name	Description
Static IP Pool field	The static IP pool. For example: 10.5.0.1 - 10.5.0.50, 10.5.0.100, 10.5.1.20 -10.5.1.70.
Subnet Mask field	The subnetwork mask for the pool. For example: 255.255.255.0.
Gateway IP Address field	The IP address of the default gateway for this network.
VLAN ID field	The VLAN ID to be used for the network. Enter a valid VLAN ID range.

Step 7 Click **Submit**.

Step 8 Click **Submit** on the **Static IP Pool Policy Information**screen.

Configuring a IP Subnet Pool Policy

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Network**.

Step 2 On the **Network** page, click **IP Subnet Pool Policy**.

Step 3 Click **Add**.

Step 4 On the **IP Subnet Pool Policy Information** screen, complete the following fields:

Field	Description
Policy Name field	The name of the policy.
Policy Description field	The description of the policy.
Network Supernet Address field	The network supernet address.
Network Supernet Mask field	The network supernet mask.
Number of Subnets Required drop-down list	Choose the number of subnets required for your configuration.
Gateway Address drop-down list	Choose a gateway address index:

Field	Description
Allow IP Overlap drop-down list	Indicate whether IP overlap is allowed or not. By default, overlapping IP is not enabled. Enabling overlapping of IP implies the following: • You can create an IP pool and have IP addresses overlap within that pool. • You can create two IP subnet pools and have the IP addresses overlap between the pools.
Scope drop-down list	The scope of the IP subnet pool overlap. The options are: • MSP Organization This option is visible only if you have enabled MSP. • Group/Customer Organization • Container **Note** This option is visible only if you select Yes in the **Allow IP Overlap** drop-down list.

Important
While creating a policy with overlapping IP enabled, you must first determine if there are any other IP subnet pool policies created with the same IP range. If those other policies also have overlapping IP enabled, then you can create an additional policy with no errors. However, if a previously created IP subnet pool policy, which uses the same IP range that you want to specify for the policy you are creating, does not have overlapping IP enabled, then you cannot proceed. The same behavior holds true in the case of creating a policy without enabling overlapping IP.

While creating this policy without enabling overlapping IP, you must first determine if there are any other policies that are created with the same IP range. If previously created pool policies have overlapping IP enabled, then you cannot specify the same IP range to create another policy with overlapping IP disabled.

Step 5 Click **Submit**.

Adding a Network Policy

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Network**.
Step 2 On the **Network** page, click **VMware Network Policy**.

Step 3 Click **Add**.

Step 4 On the **Network Policy Information** screen, complete the following fields:

Name	Description
Policy Name field	The name of the network policy.
Policy Description field	The description of the network policy.
Cloud Name drop-down list	Choose the cloud account to which the policy applies.
Allow end user to select optional NICs check box	Check if you want to provide vNICs selection during the creation of a service request-deployment configuration.
VM Networks field	Expand the **VM Networks** table to add a new entry to the VM network.

Step 5 Click **Add** in the VM Networks section to add and configure multiple vNICs. These vNICs are applicable to the VM that is provisioned using this policy.

Note
To add or replace vNICs for provisioned or discovered VMs using VM actions, you must configure the vNICs.

Step 6 On the **Add Entry to VM Networks** screen, complete the following fields:

Name	Description
NIC Alias field	The name for the new NIC
Mandatory check box	If **Allow end user to select optional NICs** is checked on the **Network Policy Information** screen, this box is pre-selected. If the **Allow end user to select optional NICs** box was not checked, and this check box is not selected, then the **NIC Alias** field is optional. **Note** At least one of the NICs should have the **Mandatory** option selected. The NICs that have the **Mandatory** option selected are used in VM provisioning and there will be no option for the user during VM service request creation.
Allow end user to choose portgroups check box	Check to allow the end user to choose port groups during provisioning.
Show policy level portgroups check box	Checking this check box along with the **Allow end user to choose portgroups** check box lists all the selected portgroups of NICs in the policy.

Name	Description
Copy Adapter from Template check box	Check if you do not need custom settings. Clear this check box for custom settings. The **Adapter Type** drop-down list is not visible when you check this check box.
Allow the end user to override IP Address check box	Check to allow users to override the IP address.
Adapter Type drop-down list	Choose the adapter type. Select this option if the user wants to have the same Adapter Type that is available in the template. **Note** This option is not visible if the **Copy Adapter from Template** option is chosen.

Step 7 Click **Add (+)** in the **Port Groups** section. The **Add Entry to Port Groups** screen appears.

Step 8 Click **Select** to choose the port group name.

Step 9 From the **Select IP Address Type** drop-down field, choose **DHCP** (default) or **Static**.

a) If you choose **Static**, you must choose **IP Pool Policy** (default) or **Inline IP Pool**.

If you choose **IP Pool Policy**, click **Select to choose a static IP pool**. On the **Select** screen, choose from the list of preconfigured static IP pool(s). If no preconfigured static IP pools exist, see Adding a Static IP Policy for more information.

b) If you choose **Inline IP Pool**, complete the following fields:

Name	Description
Static IP Pool field	The static IP pool. For example: 10.5.0.1 - 10.5.0.50, 10.5.0.100, 10.5.1.20-10.5.1.70
Subnet Mask field	The subnetwork mask for the pool. For example: 255.255.255.0
Gateway IP Address field	The IP address of the default gateway for this network.
Allow IP Overlap drop-down list	Indicate whether IP overlap is allowed or not. By default, overlapping IP is not enabled. Enabling overlapping of IP implies the following: • You can create an IP pool and have IP addresses overlap within that pool. • You can create two static IP pools and have the IP addresses overlap between the pools

Name	Description
Scope drop-down list	The scope of the IP pool overlap. The options are: • MSP Organization This option is visible only if you have enabled MSP. • Group/Customer Organization • Container **Note** This option is visible only if you select Yes in the **Allow IP Overlap** drop-down list.
User Group ID field	Choose **Select** to check the user group. All the user groups created in the system are displayed.
Container ID field	Choose **Select** to check the container.

Step 10 Check **IPv6** to configure IPv6.

You must configure the identical fields that you specified for IPv4 configuration.

Step 11 Click **Submit**.

Step 12 Click **Submit** on the **Add Entry to VM Networks** screen.

Step 13 Click **Submit** on the **Network Policy Information** screen.

Networking Provisioning Policies

A network provisioning policy is used during orchestration workflow tasks. This policy defines Layer 2 network configuration and access control lists (ACLs) for switches in the network.

Configuring a Network Provisioning Policy

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Network**.

Step 2 On the **Network** page, click **Network Provisioning Policy**.

Step 3 Click **Add**.

Step 4 On the **Add Policy** screen, complete the following fields:

Name	Description
General Information	
Policy Name field	The name of the policy.

Name	Description
Policy Description field	The description of the policy.
L2 Network Configuration VLAN	
Use Private VLAN check box	If checked, the following fields are automatically populated: • Private VLAN Type: community • Primary VLAN ID: 0 • Secondary VLAN Range—Starting ID 500 • Secondary VLAN Range—Ending ID 1000
VLAN Range - Starting ID field	A starting ID for the VLAN range. 500 is the default ID start range.
VLAN Range - Ending ID field	An ending ID for the VLAN range. 1000 is the default ID end range.
Base Profile Name field	The VLAN base profile name. This is the profile that contains one or more nested profile assignments.
Access Control List	
ACL Type drop-down list	By default, it is set to **Simple**. This is the only option available currently.
Allow ICMP check box	Check to allow ICMP on the VLAN.
Permit Incoming Traffic to TCP Ports field	The following options are available: • FTP • SSH • Telnet • SMTP • POP3 • HTTP • HTTPS • MariaDB
Permit Incoming Traffic to UDP Ports field	The following options are available: • SNMP • Syslog

Step 5 Click **Submit**.

VLAN Pool Policies

A VLAN pool policy defines the VLAN range for a pod. This policy is used in the orchestration workflow for generating a free VLAN ID from the defined range specified in the policy.

Configuring a VLAN Pool Policy

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Network**.

Step 2 On the **Network** page, click **VLAN Pool Policy**.

Step 3 Click **Add**.

Step 4 On the **Add Policy** screen, complete the following fields:

Name	Description
Pod drop-down list	Allows you to choose the pod.
Policy Name field	The policy name. This policy name is used in orchestration workflows.
Policy Description field	The description of the policy.
VLAN Range field	The VLAN range. For example: 1,3, 5—15.

Step 5 Click **Submit**.

System Policies

A system policy defines system-specific information, such as the template to use, time zone, OS-specific information, and so on.

Configuring a System Policy



Note When you use the system policy to provision virtual machines by deploying an OVF, enter only the **VM Name Template** and the **Host Name Template** fields. The remaining fields in the system policy are not applicable.

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Service Delivery**.

Step 2 On the **Service Delivery** page, click **VMware System Policy**.

Step 3 Click **Add**.

Step 4 On the **System Policy Information** screen, complete the following fields:

Name	Description
Policy Name field	The name of the policy. This name is used during catalog definition.
Policy Description field	The description of the policy.
VM Name Template field	The VM name template to use. Cisco UCS Director allows automatic creation of VM names. VM names can be automatically created using a set of variable names. Each variable must be enclosed in ${VARIABLE_NAME}. For example: vm-${GROUP_NAME}-SR${SR_ID}.
Disable VM Name Uniqueness Check check box	Check to disable the VM name uniqueness check when the VM is provisioned. Disabling the VM name uniqueness check allows you to disable the VM name validation across Cisco UCS Director and use the same VM name in a multi-tenant and multi-domain environment. If this field is unchecked, the VM name uniqueness check runs and only allows the same VM name if it is provisioned in a different folder or datacenter.
VM Name Validation Policy drop-down list	Allows you to choose a VM name validation policy. This list is populated with the policies that you created previously.

Step 5 Choose from the following optional **VM Name Template** features:

Name	Description
End User VM Name or VM Prefix check box	Check to allow the user to add a VM name or VM prefix during a service request creation for VM provisioning.
Power On after deploy check box	Check to automatically power on all VMs deployed using this policy.
Host Name Template field	The VM hostnames that can be automatically created using set of variable names. Each variable must be enclosed in **${VARIABLE}**.

Name	Description
Disable Host Name Uniqueness Check check box	Check to disable the host name uniqueness check when the VM is provisioned with guest OS customizations. Disabling the host name uniqueness check allows you to disable the host name validation across Cisco UCS Director and use the same host name in a multi-tenant and multi-domain environment. If this field is unchecked, the host name uniqueness check runs and only allows the same host name if the VM is going to be provisioned in a different tenant, domain, or workgroup.
Host Name Validation Policy drop-down list	Choose a host name validation policy. This list is populated with the policies that you created earlier on.

Step 6 Complete the following fields:

Name	Description
Linux Time Zone drop-down list	Choose the time zone.
Linux VM Max Boot Wait Time drop-down list	Choose the maximum waiting period for the Linux VM to boot.
DNS Domain field	The IP domain to use for the VM.
DNS Suffix List field	The DNS suffixes to configure for the DNS lookup. Use commas to separate multiple entries.
DNS Server List field	The list of DNS server IP addresses. Use commas to separate multiple entries.
VM Image Type drop-down list	Choose the OS of the image that is installed on the VM. You can choose between: • Windows and Linux • Linux Only
Windows	
Product ID field	The Windows product ID or license key. The product ID or license key can be provided here or at the OS license pool. The key entered in the OS license pool overrides the key provided here.
License Owner Name field	The Windows license owner name.
Organization field	The organization name to configure in the VM.
License Mode drop-down list	Choose per-seat or per-server.

Name	Description
Number of License Users	The number of license users or connections.
WINS Server List field	The WINS server IP addresses. Use commas to separate multiple entries.
Windows VM Max Boot Wait Time drop-down list	Choose the maximum waiting period for the Windows VM to boot.
Create a unique SID check box	Check to create a unique SID for the system.
Auto Logon check box	Check to enable auto logon.
Auto Logon Count field	The number of times to perform auto logon.
Administrator Password field	The password for the administrator's account.
Windows Time Zone drop-down list	Choose the time zone that must be set for the Windows VM.
Domain/Workgroup drop-down list	Choose either **Domain** or **Workgroup**.
Workgroup field	The name for the workgroup. This option appears if **Workgroup** is chosen as the value in the **Domain/Workgroup** drop-down list.
Domain field	The name of the Windows domain. **Note** This option appears if **Domain** is chosen as the value in the **Domain/Workgroup** drop-down list.
Domain Username field	The Windows domain administrator’s username. **Note** This option appears if **Domain** is chosen as the value in the **Domain/Workgroup** drop-down list.
Domain Password field	The Windows domain administrator’s password. **Note** This option appears if **Domain** is chosen as the value in the **Domain/Workgroup** drop-down list.

Name	Description
Define VM Annotation check box	

Name	Description
	Check to specify annotations to the VM. You can specify a note and custom attributes as part of the annotation. After you select this check box, complete the following fields: • **VM Annotation** field Enter a description for the VM. • **Custom Attributes** Click **Add (+)** to specify the **Name**, **Type**, and **Value**. Following are some of the **Custom Attributes** that you can add: • ${VM_HOSTNAME} • ${VM_HOSTNAME_SHORT} • ${VM_HOSTNAME_DOMAIN} • ${VM_IPADDRESS} • ${VM_ID} • ${VM_NAME} • ${VM_STATE} • ${VM_STATE_DETAILS} • ${VM_PARENT} • ${VM_CLOUD} • ${VM_GROUP_NAME} • ${VM_GROUP_ID} • ${VM_VDC_NAME} • ${VM_VDC_ID} • ${VM_SR_ID} • ${VM_SCHED_TERM} • ${VM_TYPE} • ${VM_COMMENTS} • ${VM_CATALOG_ID} • ${ INITIATING_USER} • ${SUBMITTER_EMAIL}

Name	Description

	• ${SUBMITTER_FIRSTNAME}
	• ${SUBMITTER_LASTNAME}
	• ${SUBMITTER_GROUPNAME}
	• Variables for VM creation:
	  • ${SR_ID}
	  • ${GROUP_NAME}
	  • ${USER}
	  • ${APPCODE}
	  • ${COST_CENTER}
	  • ${UNIQUE_ID}
	  • ${LOCATION}
	  • ${PROFILE_NAME}
	  • ${COMMENTS}
	  • ${CATALOG_NAME}
	  • ${CLOUD_NAME}
	
	Note
	The information that you add as part of the VM Annotation is displayed for the VM in the **VM Details** page.

Step 7 Click **Submit**.

OS Licenses

Cisco UCS Director provides an option for users to add Windows OS licenses. These licenses are mapped to Windows images during the creation of a catalog. You have an option to provide the Windows OS license for a Windows image in VMware System Policy or choose the key from the OS version field during catalog creation.

Adding an OS License

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Service Delivery**.

Step 2 On the **Service Delivery** page, click **OS License**.

Step 3 Click **Add**.

Step 4 On the **Add License Details** screen, complete the following fields:

Name	Description
Windows Version Name field	The Windows version name.
License field	The Windows product ID or license key. This field accepts KMS client set-up keys.
License Owner Name field	The Windows license owner name.
Organization field	The organization name to configure in the VM.
License Mode drop-down list	Allows you to choose per-seat or per-server.
Number of Licensed Users field	The number of license users or connections.

Step 5 Click **Submit**.

End User Self-Service Policy

An End User Self-Service Policy controls the actions or tasks that a user can perform on a VDC. The starting point for creating this policy is to specify an account type (for example, VMware). After you specify an account type, you can continue with creating the policy. After you create the policy, you must assign the policy to a vDC that is created with the same account type. For example, if you have created an end user policy for VMware, then you can specify this policy when you create a VMware vDC. You cannot view or assign policies that have been created for other account types.

In addition to creating an end user self-service policy, Cisco UCS Director allows you to perform the following tasks:

- View—Displays a summary of the policy.
- Edit—Opens the **End User Policy** screen from which you can modify the description or the end user self-service options.
- Clone—Opens the **End User Policy** screen through which you can create an additional policy using the parameters defined in an existing end user self-service policy.
- Delete—Deletes the policy from the system. You cannot delete a policy that has a VDC assigned to it.



Important The tasks that a user can perform on a VDC are defined by the role that the user is mapped to and by the end user self-service policy assigned to the VDC. If you have upgraded to the current release, then the permissions to perform VM management tasks are retained in any pre-existing end user self-service policy. However, the permissions defined in the user role to which the user belongs takes precedence.

Creating an End User Policy

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Service Delivery**.

Step 2 On the **Service Delivery** page, click **End User Self-Service Policy**.

Step 3 Click **Add**.

Step 4 On the **Add End User Policy** screen, select an account type from the drop-down list.

Step 5 Click **Submit**.

Step 6 On the **End User Policy** screen, complete the following fields:

Name	Description
Policy Name field	The name of the policy.
Policy Description field	The description for the policy.
End User Self-Service Options field	A list of tasks that a user can perform on a VDC that is assigned with this policy. The list of tasks varies according to the **Account Type**.

Step 7 Click **Submit**.

What to do next

Assign this end-user policy to a VDC. For more information, see Adding a Virtual Data Center, on page 248.

Configuring a VM Management Policy

This policy defines how VMs are managed in the VDC.

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Service Delivery**.

Step 2 On the **Service Delivery** page, click **VM Management Policy**.

Step 3 Click **Add**.

Step 4 On the **Add VM Management Policy** screen, complete the following fields:

Field	Description
Policy Name field	A unique name for the policy.

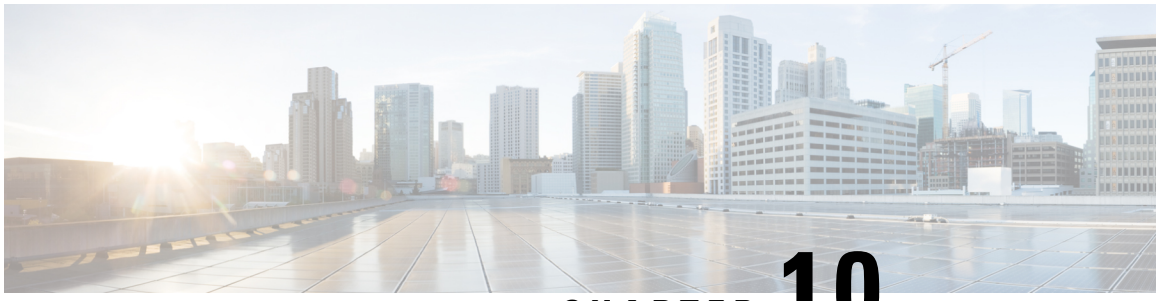
Field	Description
Policy Description field	A description for the policy.
VM Lease Expiry Notification Settings	
Configure VM Lease Notification check box	Check to set notification parameters for VMs configured with lease time.
How many days before VM Lease expiry should notifications be sent field	Enter a number. This number indicates the number of days prior to VM lease expiry that an email notification is sent to the VM owner.
How many notifications should be sent field	Enter a number. This number indicates the number of email notifications that will be sent informing the user of the VM lease expiration.
Interval between notifications drop-down list	Choose a number from the drop-down list. This number defines the time gap or interval between the notification emails that are sent.
Inactive VM Management Settings	
Delete after inactive VM days field	Enter a number. This number indicates the number of days after which an inactive VM is deleted from the system. **Note** Inactive VMs are deleted only if the **Delete Inactive VMs Based on vDC Policy** option is selected in the Properties pane. This option is displayed when you select **Administration** > **System** > **Advanced Controls**. See Enabling Advanced Controls, on page 143
Additional grace period for deleting expired VMs field	Enter a number. This number indicates the number of days that the system waits before deleting an inactive VM from the system. **Note** When the time period specified in the **Delete after inactive VM days** and **Additional grace period for deleting expired VMs** fields elapse, VMs discovered through Cisco UCS Director are deleted, and service requests for VMs provisioned through Cisco UCS Director are rolled back. A new email template for rolled back Service Requests (SR) for these system—provisioned VMs has been introduced.

Field	Description
Action to be taken when a service request (SR) roll back task fails for VMs provisioned through Cisco UCS Director drop-down list	Select an action to be taken when a service request (SR) roll back task fails for VMs provisioned through Cisco UCS Director. You can choose one of the following options: • Send notification and delete the VM • Send notification and do not delete the VM **Note** In the VM Automatic Deletion email template, a new field titled **Rollback SR ID** has been introduced. This field is populated for VMs provisioned through Cisco UCS Director and is blank for VMs discovered through Cisco UCS Director.
Configure VM Delete Notification check box	Check to set notification parameters for VMs that are to be deleted.
How many days before VM deletion should notifications be sent field	Enter a number. This number indicates the number of days prior to VM deletion that an email notification is sent to the user.
How many notifications should be sent field	Enter a number. This number indicates the number of notification emails that are sent to the user.
Interval between notifications drop-down list	Choose a number from the drop-down list. This number defines the time gap or interval between the notification emails that are sent.

Step 5 Click **Submit**.

What to do next

You can map this policy to a virtual data center.



CHAPTER 10

Managing Virtual Data Centers

This chapter contains the following sections:

- Virtual Data Centers, on page 247
- VDC Actions, on page 248
- Virtual Data Center Service Profiles, on page 253

Virtual Data Centers

A Virtual Data Center (VDC) is a logical grouping that combines virtual resources, operational details, rules, and policies to manage specific group requirements.

A group or organization can manage multiple VDCs, images, templates, and policies. Organizations can allocate quotas and assign resource limits for individual groups at the VDC level.

You can also define approvers specific to a VDC. The approvers assigned to a particular VDC must approve all service requests from users for VM provisioning.

Note There is a default VDC in Cisco UCS Director, and all discovered VMs are part of this default VDC. Discovered VMs are VMs that are created outside of Cisco UCS Director or were already created on VMware vCenter before Cisco UCS Director was installed. Cisco UCS Director automatically discovers such VMs and adds them to the default VDC.

A VM that is provisioned using a service request can be associated with a specific VDC. When you create a service request, you can choose the VDC on which this VM is provisioned. You can view a list of the VDCs that are available for a particular group and choose the required VDC when provisioning VMs.

VDC Actions

Adding a Virtual Data Center

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Virtual Data Centers**.

Step 2 On the **Virtual Data Centers** page, click **vDC**.

Step 3 Click **Add**.

Step 4 On the **VDC Add** screen, select an account type from the drop-down list.

The account type that you select determines the list of cloud names that are displayed on the **Add VDC** screen.

Step 5 Click **Submit**.

Step 6 On the **Add VDC** screen, complete the following fields:

Name	Description
VDC Name field	The name of the VDC. You can include special characters such as ( ). & - _ `~ $% ^ {}! ' @ **Note** A name cannot be edited after it is entered.
VDC Locked check box	Check the check box to deny the use of the VDC for any further deployments. Uncheck the check box to allow the use of the VDC for further deployments.
VDC Description field	The VDC-specific description.
Group drop-down list	Click **Select** to check the check box of the group for which the VDC is being set up.
Cloud Name drop-down list	Choose the cloud on which the VDC is being set up. The options available in this drop-down list are determined by the account type you specified.
Approvers and Contacts	
First Level Approver(s)	
Approval required from Groups check box	Check this check box to select the groups of users that need to approve the service request at the first level.

Name	Description
User Group	Click **Select** to check the check boxes of the user groups. You can select multiple groups. **Note** This field is displayed only when you have checked the **Approval required from Groups** check box.
User field	The users who must approve the service request at the first level. Click **Select** and check the check boxes of the users. You can select multiple users. **Note** This field is displayed when you have not checked the **Approval required from Groups** check box.
Second Level Approver(s) field	
Approval Required from Groups	Check this check box to select the groups of users that need to approve the service request at the second level.
User Group	Click **Select** to check the check boxes of the user groups. You can select multiple groups. **Note** This field is displayed only when you have checked the **Approval required from Groups** check box.
User field	The users who must approve the service request at the second level. Click **Select** and check the check boxes of the users. You can select multiple users. **Note** This field is displayed when you have not checked the **Approval required from Groups** check box.
Approval Required from all users check box	Check this check box to indicate that approval is required from all users who have been selected as first-level and second-level approvers.
Number of Approval Requests Reminders field	The number of times the reminder email to approve the service request is sent to the approvers. By default, the system sends a reminder email once in every 24 hours until the service request is approved or rejected.

Name	Description
Reminder Interval (Hours) field	The time interval between the reminder emails that are sent to the approvers. By default, the system sends a reminder email every 24 hours.
Provider Support Email Address field	The contact or user's email address. The person who is notified about VM provisioning using this VDC.
Copy Notifications to Email Address field	The second contact's email address for copying notifications about this VDC.
Policies	
System Policy drop-down list	Choose the system policy applicable to the VDC.
Computing Policy drop-down list	Choose the computing policy applicable to the VDC.
Network Policy drop-down list	Choose the network policy applicable to the VDC.
Storage Policy drop-down list	Choose the storage policy applicable to the VDC.
ISO Image Mapping Policy drop-down list	Choose the ISO image mapping policy applicable to the VDC.
Cost Model drop-down list	Choose the cost model applicable to the VDC.
Disable displaying cost details check box	Check the check box to disable displaying cost details in the following pages for this VDC: • Create Service Request wizard The cost information is not displayed in the **Deployment Configuration** pane, **Custom Specification** pane and the **Summary** pane. • Specific VM action pages - VM resize, Resize VM disk, and Create VM disk. • Email notifications
User Action Policy drop-down list	Choose the policy that is used for execution of orchestration workflow post provisioning of the VMs. The chosen workflow appears as an action button for VMs within the VDC.
VM Management Policy drop-down list	Choose the VM management policy for the VDC. This policy defines how VMs are managed in the VDC.
Enable Storage Efficiency check box	Check the check box to clone the VM using RCU. This option is only available for some VDC types.

Name	Description
End User Self-Service Policy	Select a self-service policy for the VDC. The policy defines the tasks or actions that can be performed on the VDC. **Note** This drop-down list is populated with policies that are relevant to the account type that you are creating the VDC for. The tasks that a user can perform on a VDC are defined by the role that the user is mapped to and by the end user self-service policy assigned to the VDC. If you have upgraded to the current release, then the permissions to perform VM management tasks are retained in any pre-existing end user self-service policy. However, the permissions defined in the user role to which the user belongs takes precedence.

Step 7 Click **Add**.

Note
The following tasks can no longer be performed by users on a VM:

- Migrate a VM
- Use Stack View
- Assign a VM

What to do next

After adding a VDC, you can edit, clone, or delete it by selecting the respective option in the user interface.

Viewing a Virtual Data Center

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Virtual Data Centers**.
Step 2 On the **Virtual Data Centers** page, choose the VDC group.
Step 3 On the **Virtual Data Centers** page, click **vDC**.
Step 4 Click the row with the VDC that you want to view.
Step 5 Click **View** to open the **VDC Details** screen.

Managing Application Categories in a Virtual Data Centers

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Virtual Data Centers**.

Step 2 On the **Virtual Data Centers** page, choose the VDC group.

Step 3 On the **Virtual Data Centers** page, click **vDC**.

Step 4 Click the row with the VDC that you want to edit.

Step 5 Click **Manage Categories**.

Step 6 On the **Edit App Category** screen, edit the appropriate fields that apply to modify the system policy, computing policy, network policy, or storage policy. You can also change the cost model and the smart allocation policy.

Step 7 Click **Save**.

Assigning an Application Category to Multiple VDCs

You can assign application categories to multiple VDCs.

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, choose the cloud.

Step 3 On the **Compute** page, click **Application Categories**.

Step 4 Click the row with the application category that you want to assign to one or more VDCs.

Step 5 Click **Assign App Category**.

Step 6 On the **Assign Application Category** screen, click **+** to map policies to multiple VDCs.

The **Assign Application Category** screen lists all the application categories that have been previously assigned to VDCs. You can select an assigned application category, and either edit it or delete it from the VDC.

Step 7 On the **Add Entry to Map Policies to Multiple VDCs** screen, complete the following fields:

Name	Description
Policies	
System Policy drop-down list	Choose a system policy from the drop-down list.
Computing Policy drop-down list	Choose a computing policy from the drop-down list.
Storage Policy drop-down list	Choose a storage policy from the drop-down list.
Smart Allocation Policy drop-down list	Choose a smart allocation policy from the drop-down list.

Name	Description
Network Policy drop-down list	Choose a network policy from the drop-down list.
Cost Model drop-down list	Choose a cost model from the drop-down list. All cost models for the cloud are displayed in this drop-down list.
VDC	
Select VDCs field	Click **Select** to check the check boxes of the VDCs that you want to map the policies to. **Note** The system displays VDCs that are part of the cloud you selected. If the VDC you selected has policies mapped to it previously, a warning message is displayed.
Overwrite policies for mapped VDCs check box	Check this check box to overwrite policies that have been previously mapped to the VDC you selected.

Step 8 Click **Submit**.

Step 9 On the **Assign Application Category** screen, click **Submit**.

Virtual Data Center Service Profiles

A Virtual Data Center Service Profile is similar to a VDC. However, you only need to create a VDC service profile if you plan to create VDCs from workflow tasks, such as Gold, Silver, and Bronze VDCs.

Adding a Virtual Data Center Service Profile

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Virtual Data Centers**.

Step 2 On the **Virtual Data Centers** page, click **vDC Service Profiles**.

Step 3 Click **Add**.

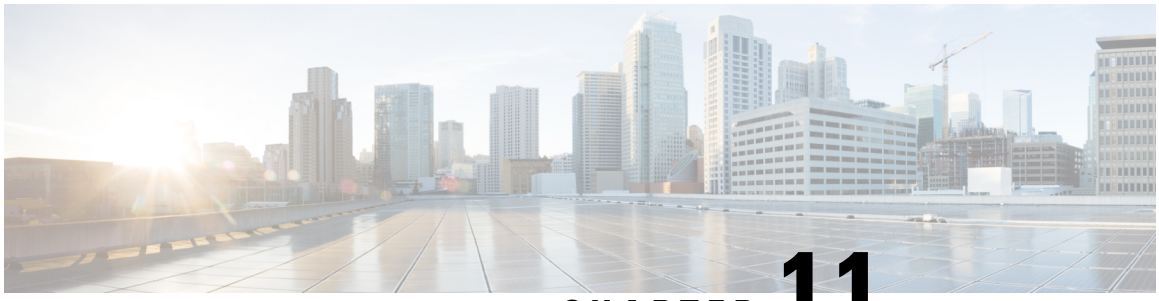
Step 4 On the **Add VDC Service Profile** screen, complete the following fields:

Name	Description
VDC Profile Name field	The name of the VDC profile. A name cannot be edited after it is entered.

Name	Description
VDC Locked check box	Check the check box to deny the use of the VDC for any further deployments. Actions on existing VMs, within this VDC, are disabled. Uncheck the check box to allow the use of the VDC for further deployments.
VDC Description field	The VDC-specific description.
Group drop-down list	Choose the group for which the VDC is being set up.
Cloud Name drop-down list	Choose the cloud on which the VDC is being set up.
Approvers and Contacts	
First Approver User Name field	The users who must approve the service request at the first level. Click **Select** and check the check boxes of the users. You can select multiple users.
Second Approver User Name field	The users who must approve the service request at the second level. Click **Select** and check the check boxes of the users. You can select multiple users.
Approval Required from all users check box	Check this check box to indicate that approval is required from all users who have been selected as first-level and second-level approvers.
Number of Approval Requests Reminders field	The number of times the reminder email to approve the service request is sent to the approvers. By default, the system sends a reminder email once in every 24 hours until the service request is approved or rejected.
Reminder Interval (Hours) field	The time interval between the reminder emails that is sent to the approvers. By default, the system sends a reminder email every 24 hours.
Provider Support Email Address field	The contact or user's email address. The person who is notified about VM provisioning using this VDC.
Copy Notifications to Email Address field	The second contact's email for copying notifications about this VDC.
Policies	
System Policy drop-down list	Choose the system policy applicable to the VDC service profile.

Name	Description
Computing Policy drop-down list	Choose the computing policy applicable to the VDC service profile.
Network Policy drop-down list	Choose the network policy applicable to the VDC service profile.
Storage Policy drop-down list	Choose the storage policy applicable to the VDC service profile.
Cost Model drop-down list	Choose the cost model applicable to the VDC service profile.
Disable displaying cost in the SR summary and email page check box	Check the check box to disable displaying cost in the SR summary and email page for this VDC service profile.
User Action Policy drop-down list	Choose the policy that is used for execution of orchestration workflow after provisioning of the VMs. The chosen workflow appears as an action button for VMs within the VDC.
End User Self-Service Options	
VM Power Management check box	Check the check box to enable all VM power management actions for VMs that belong to this VDC.
VM Resize check box	Check the check box to enable the VM resize action for VMs that belong to this VDC.
VM Snapshot Management check box	Check the check box to enable all storage snapshot actions for VMs in this VDC.
VM Deletion check box	Check the check box to enable the VM delete action for VMs in this VDC.
VM Disk Management check box	Check the check box to enable the VM disk management for VMs in this VDC.
VM Network Management check box	Check the check box to enable network management for the VM that belongs to this VDC.
Delete after Inactive VM days drop-down list	Choose the number of days to wait before deleting an inactive VM. The VM in the inactive state is when it is not in the power-on state.

Step 5 Click **Add**.



CHAPTER 11

Managing Resource Groups

This chapter contains the following sections:

- Resource Groups, on page 257
- Tenant, on page 280
- Service Offerings, on page 281
- Tenant Profiles, on page 293

Resource Groups

You can use a resource group to select the appropriate resources for a tenant based on the requirements of an application. Additional concepts, such as a service offering, tenant profile, application profile, and resource group, are all required. Using these resource group concepts, you can onboard tenants and deploy applications based on a dynamic selection of resources. You can share resources in a resource group across tenants or you can dedicate them to a specific tenant.

A resource group is a pool of resources. Each group can contain physical infrastructure resources, virtual infrastructure resources, or a combination of physical and virtual infrastructure resources. Resource groups enable you to onboard tenants into Cisco UCS Director with minimum intervention.

As an infrastructure administrator or system administrator, you can add physical or virtual accounts to a resource group one at a time. Also, you can assign a pod to a resource group where all the accounts in the pod are added to the resource group. For more information about assigning a pod to a resource group, see Adding a Pod to a Resource Group, on page 277.

When an account is added to a resource group, the resource group by default announces all the capabilities and capacities for objects for that account as resource group entity capacities and capabilities. With Cisco UCS Director, you can selectively disable certain capacities or capabilities from the resource group.

Environment Variables

You can configure the environment variable for each resource. These environment variables are used during provisioning of the tenant onboarding and application deployment.

You can set the following default environment variables for both virtual and physical accounts. Also, you can add an environment variable in Cisco UCS Director and use the environment variable in the resource group. For more information on how to add an environment variable, see Adding a Custom Environment Variable, on page 266.

Note The listed environment variables are not required for every workflow. The subset of required environment variables depends on the use case and the specific workflow(s) being executed.

Virtual Compute Environment Variables

Environment Variable	Description	Sample Value
Container Parent Folder	The folder to which you want to add the newly created container.	*APIC*
IP Subnet Pool Policy	The APIC container uses an IP subnet pool policy that is defined in Cisco UCS Director. Each tier inside the container gets a unique subnet address from the IP subnet pool policy. This environment variable is used for container provisioning.	*IP-Pool*

Virtual Storage Environment Variables

No environment variables are required for virtual storage.

Virtual Network Environment Variables

Environment Variable	Description	Sample Value
VMM Domain for VMware	VMware vCenter is configured ACI-vCenter with the Virtual Machine Manager (VMM) domain. When VMware vCenter is associated with Cisco APIC, a distributed virtual switch (DVS) with the same name is created in VMware vCenter. This environment variable is used for tenant onboarding. Choose VMM domain with Cisco AV switch to support AVS in VXLAN mode. Cisco UCS Director offers AVS support in both VLAN and VXLAN mode. The VM gets the VLAN ID or VXLAN ID from the pool assigned to the VMM domain.	*ACI-Bldg4-1-vCenter*

Environment Variable	Description	Sample Value
DV Switch	Choose either DV switch or Cisco AV switch according to the requirement. The DV switch is available on the vCenter account and is used to connect the selected host during onboarding. The Cisco AV switch is used to support AVS in VXLAN mode. This environment variable is used for tenant onboarding.	*virt_switch*

Physical Compute Environment Variables

Environment Variable	Description	Sample Value
Physical Domain for UCS	The physical domain for Cisco UCS. This environment variable is used for bare metal provisioning.	*Phys*
VLAN Pool	The VLAN pool from which you want to assign a VLAN ID for the account.	*ACI3-Eng-VLAN-Pool*
iSCSI PXE Boot Service Profile Template	The template used for creating the host service profile on which you want to provision bare metal. This environment variable is used for bare metal provisioning on a NetApp storage system.	*DR_UCSM;org-root;org-root/ls-ACI-DR-Hosts*
Service Profile Template for Full Width Blade	The service profile template is used to create a service profile. When a service profile is created, the software identifies and selects free servers from the server pool that is associated with the service profile template. This environment variable is used for the VNX tenant onboarding.	*VNX_UCSM;org-root/ls-PSC-FullBlade-Template*

Environment Variable	Description	Sample Value
Service Profile Template for Half Width Blade	The service profile template is used to create a service profile. When a service profile is created, the software identifies and selects free servers from the server pool that is associated with the service profile template. This environment variable is used for the VNX tenant onboarding.	*VNX_UCSM;org-root/ls-PSC-HalfBlade-Template*
IQN Pool	The IQN pool that contains the iSCSI Qualified Names (IQNs) used as initiator identifiers by iSCSI vNICs in a Cisco UCS domain. The IQN pool is used to create a service profile iSCSI boot policy. This environment variable is used for bare metal provisioning on a NetApp storage system.	*IQN_Pool*
Boot Policy	Boot policy for the physical compute account. This environment variable is used for a VNX-type account.	*VNX_UCSM;org-root;org-root//boot-policy-SAN_NEW*
VLAN	VLAN for the physical compute account. This environment variable is used for a VNX-type account.	*VNX_UCSM;fabric/lan/net-MGT-ACI-POOL*

Physical Storage Environment Variables

Environment Variable	Description	Sample Value
Physical Domain for NetApp	The physical domain that is used to connect the NetApp account to the APIC. This environment variable is used for tenant onboarding.	topology/pod-1/paths-201/pathep-[eth1/36] • Pod-1—The pod ID of the APIC account. • Paths-201—The node ID of the leaf to which the NetApp controller is connected. • Pathep-[eth1/36]—The port on which the NetApp controller is connected.

Environment Variable	Description	Sample Value
NetApp Static Path	The static path defines the port on the APIC where the NetApp cluster node is connected. This environment variable is used to add the static path to the endpoint group (EPG) during tenant onboarding.	*topology/pod-1/node-302/sys /cdp/inst/if-[eth1/47]adj-1*
Vlan pool	The VLAN pool that is used to create the cluster vServer. This environment variable is used for tenant onboarding.	*Vlan_pool*
SP Port	The storage processor (SP) port for the physical storage account. This environment variable is used for VNX type account.	*VNX-POD;VNX_BLOCK;A-0;50:06:01:60:88:60:1B:6A:50:06:01:60:08:60:1B:6A ,VNX-POD;VNX_BLOCK;A-1;50:06:01:60:88:60:1B:6A:50:06:01:61:08:60:1B:6A*
Replication Storage Group	The replication storage group for the physical storage account. This environment variable is used for VNX type account.	
NFS Vlan Pool	This environment variable is used to define a VLAN pool. Individual VLANs are then assigned to a physical storage account dynamically from the pool.	*NetApp-vlan-pool*
SVM mgmt Vlan Pool	The VLAN pool for management of Storage Virtual Machine (SVM).	*NetApp-vlan-pool*
iSCSI_A VLAN Pool	The VLAN pool from which a VLAN is chosen as iSCSI_A VLAN.	*NetApp-vlan-pool*
iSCSI_B VLAN Pool	The VLAN pool from which a VLAN is chosen as iSCSI_B VLAN.	*NetApp-vlan-pool*
APIC vPC Static Path for Node 1	The static path of virtual port channel (vPC) for node 1.	*topology/pod-1/path-101/pathep-[PGr-FAS-A]*
APIC vPC Static Path for Node 2	The static path of virtual port channel (vPC) for node 2.	*topology/pod-1/path-101/pathep-[PGr-FAS-B]*
NFS IP Subnet Pool Policy	The subnet IP pool policy for NFS.	*ip_nfs_subnet_pool*
iSCSI_A IP Subnet Pool Policy	The IP subnet pool policy to be used for the first iSCSI VLAN.	*NetApp_ISCSI_A_Subnet_pool*

Environment Variable	Description	Sample Value
iSCSI_B IP Subnet Pool Policy	The IP subnet pool policy to be used for the second iSCSI VLAN.	*NetApp_ISCSI_B_Subnet_pool*
SVM mgmt IP Subnet Pool Policy	The subnet IP pool policy for SVM management.	*netapp_svm_subnet_pool*
VMNet IP Subnet Pool Policy	The subnet IP pool policy for VM network.	*VMNet_IP_Subnet_pool_policy*
APIC Vlan Pool for Node 1	The APIC VLAN pool from which the VLAN ID needs to be assigned for node 1.	*NetApp-Pool*
APIC Vlan Pool for Node 2	The APIC VLAN pool from which the VLAN ID needs to be assigned for node 2.	*NetApp-Pool*
Cluster Node 1 Identity	The identity of the first Netapp C-mode account node.	*ACI2-CMODE-01*
Cluster Node 2 Identity	The identity of the second Netapp C-mode account node.	*ACI2-CMODE-02*
Default Recovery Point	The recovery point attached to the VNX account.	*RP*
Recovery Point Cluster Identity	The identity of the recovery point attached to the VNX account.	*RP@1649417791*

Physical Network Environment Variables

Environment Variable	Description	Sample Value
IP Pool	The IP pool that is used to assign the IP addresses between the NetApp datastore and host vmkernel. This environment variable is used for tenant onboarding.	*IP_pool*
PXE Server IP Pool	The IP pool of the Preboot eXecution Environment (PXE) server. This environment variable is used for bare metal provisioning.	*pxe_ip_new11*
BMA EPG Entity	The Cisco UCS Director Bare Metal Agent endpoint group (EPG) entity. This environment variable is used for bare metal provisioning.	*VNX_APIC185@common@BMA-AP@PSC_BMA*

Environment Variable	Description	Sample Value
Connected to FI A	When configuring the physical setup for FlexPod, VSAN is created for the Fabric Interconnect (FI) A - NXOS switch 1 connection and FI B - NXOS switch 2 connection. In BMA provisioning, zoning is configured for FI A - NXOS controller. Choose this environment variable to specify whether a Cisco Nexus switch is connected to Cisco UCS FI A. This environment variable appears for the MDS switch.	*Yes*
Physical domain for LB	The physical domain that you need to use for the load balancer service.	*Phy_LB_Domain*
Physical LB Path	The physical path of the load balancer service.	*topology/pod-1/node-101/sys/cdp /inst/if-[eth1/12]/adj-1*
DPC Static path 1	The static path of the first Direct Port Channel (DPC).	*topology/pod-1/paths-302/ pathep-[PC_Policy_1Gb]*
DPC Static path 2	The static path of the second DPC.	*topology/pod-1/paths-303/ pathep-[PC_Policy_1Gb]*
Path 1 to L3Out	The first transit path from the ACI leaf to an external router.	*topology/pod-1/protpaths-103-104/pathep-[ifs-n3k-b_PolGrp]*
Path 2 to L3Out	The second transit path from the ACI leaf to an external router.	*topology/pod-1/protpaths-103-104/pathep-[ifs-n3k-a_PolGrp]*
L2 Physical Domain	The physical domain for Layer 2. This environment variable is used for configuring EPG transit.	*L2-2960*
IP Subnet Pool Policy	The pool policy to be used to get the IP addresses for sub-interfaces.	*Ipsubnetpoolpolicy*
L3 Vlan Pool	The pool to be used to get the VLAN ID that is used to communicate between the external router and ACI fabric. This environment variable is used to configure the external routed network.	*L3out_Pool*
L2 Transit Vlan Pool	The pool to be used to get the VLAN ID for the transit EPG. This environment variable is used for creating a transit EPG.	*L2out_Pool*

Environment Variable	Description	Sample Value
Node	The leaf nodes of the APIC account. This environment variable is used for creating a transit EPG.	*topology/pod-1/node-302*
Routed Sub-Interface Path	The sub-interface routed path based on the leaf node selection.	*topology/pod-1/paths-303/pathep-[eth1/47], topology/pod-1/paths-303/pathep-[eth1/48], topology/pod-1/paths-302/pathep-[eth1/47] topology/pod-1/paths-302/pathep-[eth1/48]*
Nexus Switches	The Nexus switches for the APIC account.	*192.0.232.166, 192.0.232.167*
Loop Back IP Subnet Pool Policy	The pool policy to be used to get the IP address for Loop Back.	*loop_back_ip_pool_policy*
L3 Domain	The Layer 3 domain of the APIC account. This environment variable is used to configure the external routed network.	*Phy_L3out_domain*
Router IP Pool	The IP pool to configure router ID for routers on an external Layer 3 network. This environment variable is used to configure the external routed network.	*IP_pool*
LB Cluster IP Pool	The IP pool to provide the cluster management IP address for the load balancer device cluster.	*IP_pool*
SVI Path	The interface connecting APIC to a router on an external Layer 3 network. This environment variable is used to configure the external routed network.	*topology/pod-1/protpaths-101-102 /pathep-[vpcPG_ec1acifwi001-2_DATA*
SVI IP Pool	The subnet for configuring a switch virtual interface (SVI) on APIC leaves. This environment variable is used to configure the external routed network.	*IP_pool*



Note The following environment variable are not supported in Cisco UCS Director Release 5.4: IP Subnet Pool Policy, iSCSI PXE Boot Service Profile Template, IQN Pool, Replication Storage Group, PXE Server IP Pool, BMA EPG Entity, Physical domain for LB, and Physical LB Path.

The environment variable that need to be defined for VNX tenant onboarding are:

- Physical Compute—Cisco UCS Manager
  - Service Profile Template for Full Width Blade
  - Service Profile Template for Half Width Blade
- EMC VNX Unified
  - SP Port
- VMware Account
  - DV Switch-Virtual Network
  - VMM Domain for VMware-Virtual Network
- APIC (Physical Network)
  - DPC Static Path 1 (for L2 configuration)
  - DPC Static Path 2 (for L2 configuration)
  - L2 Physical Domain (for L2 configuration)
  - IP Subnet Pool Policy (for L3 configuration)
  - L3 VLAN Pool (for L3 configuration)
  - Routed Sub-Interface Path (for L3 configuration)
  - Node (for L3 configuration)
  - Nexus Switches (for L3 configuration)
  - Loop Back IP Subnet Pool Policy (for L3 configuration)

The environment variable that need to be defined for FlexPod tenant onboarding as per the Cisco UCS Director and FlexPod Cisco validated design (CVD) are:

- APIC Account
  - IP Pool
- NetApp
  - Vlan Pool
  - Physical Domain for NetApp
  - NFS Vlan Pool

- SVM mgmt Vlan Pool
- APIC vPC Static Path for Node 1
- APIC vPC Static Path for Node 2
- NFS IP Subnet Pool Policy
- SVM mgmt IP Subnet Pool Policy
- VMNet IP Subnet Pool Policy
- APIC Vlan Pool for Node 1
- APIC Vlan Pool for Node 2
- Cluster Node 1 Identity
- Cluster Node 2 Identity
- iSCSI_A VLAN Pool
- iSCSI_B VLAN Pool
- iSCSI_A IP Subnet Pool Policy
- iSCSI_B IP Subnet Pool Policy

- VMware Account
  - DV Switch
  - VMM Domain for VMware-Virtual Network

The environment variable that need to be defined for NetApp tenant onboarding (obsolete) are:

- APIC Account
  - IP Pool
- NetApp
  - Vlan Pool
  - NetApp Static Path
  - Physical Domain for NetApp
- Virtual Network
  - DV Switch
  - VMM Domain for VMware

Adding a Custom Environment Variable

You can define an environment variable that you want to use in the resource group and workflow. The type of the user-defined environment variable is custom.

Procedure

Step 1 Choose **Policies** > **Resource Groups**.

Step 2 On the **Resource Groups** page, click **Environment Variables**.

Step 3 Click the row with anenvironment variable and click **View** to view the name, variable type, and identity type of the environment variable.

Step 4 Click the row with the environmental variable and click **Delete** to delete the environment variable.

You can delete only the user-defined environment variable that is categorized as custom.

Step 5 Click **Add**.

Step 6 On the **Resource Group Environment Variable** screen, complete the following fields:

Name	Description
Custom Environment Name field	The name of the environment variable.
Description field	The description of the environment variable.
Resource Type drop-down list	Choose one of the following as the resource type for the environment variable: • VIRTUAL_COMPUTE • VIRTUAL_NETWORK • VIRTUAL_STORAGE • PHYSICAL_COMPUTE • PHYSICAL_STORAGE • PHYSICAL_NETWORK The environment variable is categorized under the chosen resource type.
Input Type field	Expand **Input Type** and check the variable type that you want to use for the environment variable. The variable type can be text, list of variable (LoV), multiple selection, table, and popup table.

Step 7 Click **Submit**.

The added custom environment variable is listed on the **Environment Variables** page. You can add this custom environment variable in the Resource Group.

Adding a Resource Group

Before you begin

Ensure that the IP subnet pool policy and VLAN pool policy are defined to use the policy in the environment. Also, you can add a policy on the **Add Entry to Environment Variables** screen when adding a resource group.

Procedure

Step 1 Choose **Policies** > **Resource Groups**.

Step 2 On the **Resource Groups** page, click **Resource Groups**.

Step 3 Click the row with a resource group and click **View** to view the name and description of the resource group.

Step 4 Click the row with a resource group and click **View Details** to view the resources that are associated with a resource group.

The ID, pod, account name, category, account type, resource type, and resource name of the resources in the resource group are displayed.

Step 5 Click the row with a resource and click **View Details** to view the capacities and capabilities of a resource.

Step 6 Click **Add**.

Step 7 On the **Create Resource Group** screen, complete the following fields:

Name	Description
Name field	The name of the resource group.
Description field	The description of the resource group.
Enable DR check box	Check to enable the disaster recovery service support for the resource group. **Note** The disaster recovery service support is enabled based on the use case and the workflow being executed.
Accounts Priority drop-down list	This field appears only when **Enable DR** is checked. By default, **Primary** is selected to set the resource group as primary. If you want to set the resource group as secondary, choose **Secondary**.
DRS Resource Group drop-down list	Choose a resource group as a disaster recovery service resource group for handling failover and recovering data during disaster.

Note
The primary and secondary resource groups must each have an equal number of accounts in order to support the disaster recovery service.

Step 8 Click **Next**.

Step 9 (Optional) On the **Virtual Compute** screen, choose the virtual compute account and the interested capabilities and capacities:

a) Expand **Virtual Accounts** and click the + icon to add a virtual account.

b) On the **Add Entry to Virtual Accounts** screen, expand **Accounts**, check the virtual account that you want to use, and then click **Validate**.

Note
You can choose either a VMware account or a Hyper-V account from the account list. According to the chosen virtual account, you need to choose environment variable, capabilities, and capacities. If the required environment variable is not available in the drop-down list, you can create a new environment variable. For more information on how to create an environment variable, see Adding a Custom Environment Variable, on page 266.

c) Expand **Environment Variables** and click the + icon.

1. On the **Add Entry to Environment Variables** screen, choose an environment variable from the **Name** drop-down list.
2. In the **Required Value** field, choose the value according to the selected environment variable. When you choose **IP Subnet Pool Policy** from the **Name** drop-down list, expand **Required Value** and check the policy that you want to use. You can also add a policy by clicking the + icon.
3. Click **Submit**.

d) In the **Selected Capabilities** field, the capabilities of the chosen virtual account appear by default.

You can opt to disable the capabilities by unchecking the capability in the edit window that appears on clicking the Edit icon. You can remove the capability from the list by clicking the Delete icon.

e) In the **Selected Capacities** field, the capacities of the chosen virtual account appear by default.

You can opt to disable the capacities by unchecking the capacity in the edit window that appears on clicking the Edit icon. You can remove the capacity from the list by clicking the Delete icon.

f) Click **Submit** on the **Add Entry to Virtual Accounts** screen.

Note
An account that is added to a resource group cannot be added to another resource group and cannot be deleted from Cisco UCS Director.

Step 10 Click **Next**.

Step 11 On the **Virtual Storage** screen, expand **Virtual Accounts** click the row with the virtual compute account and the interested capabilities and capacities.

a) Click the + icon to add a virtual account.

b) On the **Add Entry to Virtual Accounts** screen, expand **Accounts**, check the virtual account you want to use, and click **Validate**.

Note
You can choose either a VMware account or a Hyper-V account from the account list. According to the chosen virtual account, you need to choose environment variable, capabilities, and capacities. If the required environment variable is not available in the drop-down list, you can create a new environment variable. For more information on how to create an environment variable, see Adding a Custom Environment Variable, on page 266.

c) Expand **Environment Variables** and click the + icon.

1. On the **Add Entry to Environment Variables** screen, choose an environment variablefrom the **Name** drop-down list.
2. In the **Required Value** field, choose the value according to the selected environment variable.
3. Click **Submit**.

d) In the **Selected Capabilities** field, the capabilities of the chosen virtual account appear by default.

You can opt to disable the capabilities by unchecking the capability in the edit window that appears on clicking the Edit icon. You can remove the capability from the list by clicking the Delete icon.

e) In the **Selected Capacities** field, the capacities of the chosen virtual account appear by default.

You can opt to disable the capacities by unchecking the capacity in the edit window that appears on clicking the Edit icon. You can remove the capacity from the list by clicking the Delete icon.

f) Click **Submit** on the **Add Entry to Virtual Accounts** screen.

Note
An account that is added to a resource group cannot be added to another resource group and cannot be deleted from Cisco UCS Director.

Step 12 Click **Next**.

Step 13 On the **Virtual Network** screen, expand **Virtual Accounts** and click the row with the virtual network account and the interested capabilities and capacities:

a) Click the + icon to add a virtual account.

b) On the **Add Entry to Virtual Accounts** screen, expand **Accounts**, check the virtual account that you want to use, and click **Validate**.

Note
You can choose either a VMware account or a Hyper-V account from the account list. According to the chosen virtual account, you need to choose environment variable, capabilities, and capacities. If the required environment variable is not available in the drop-down list, you can create a new environment variable. For more information on how to create an environment variable, see Adding a Custom Environment Variable, on page 266.

c) Expand **Environment Variables** and click the + icon.

1. On the **Add Entry to Environment Variables** screen, choose an environment variable from the **Name** drop-down list.
2. Expand **Required Value** field and check the value according to the selected environment variable that you want to use in the environment.
3. Click **Submit**.

d) In the **Selected Capabilities** field, the capabilities of the chosen virtual account appear by default.

You can opt to disable the capabilities by unchecking the capability in the edit window that appears on clicking the Edit icon. You can remove the capability from the list by clicking the Delete icon.

e) In the **Selected Capacities** field, the capacities of the chosen virtual account appear by default.

You can opt to disable the capacities by unchecking the capacity in the edit window that appears on clicking the Edit icon. You can remove the capacity from the list by clicking the Delete icon.

f) Click **Submit** on the **Add Entry to Virtual Accounts** screen.

Note
An account that is added to a resource group cannot be added to another resource group and cannot be deleted from Cisco UCS Director.

Step 14 Click **Next**.

Step 15 (Optional) On the **Physical Compute** screen, expand **Compute Accounts** and click the row with the physical compute account and the interested capabilities and capacities:

a) Click the + icon to add a compute account.
b) On the **Add Entry to Compute Accounts** screen, check the compute account that you want to use, and click **Validate**.
c) Expand **Environment Variables** and click the + icon.

1. On the **Add Entry to Environment Variables** screen, choose an environment variable from the **Name** drop-down list.
2. Expand **Required Value** field, and check the value according to the selected environment variable. When you choose **Vlan pool** from the **Name** drop-down list, expand **Required Value** and check the policy that you want to use. You can also add a policy by clicking the + icon.
3. Click **Submit**.

d) Expand **Selected Capabilities** and click on the row with the resource and resource capability that you want to use.
e) Expand **Selected Capacities** and click on the row with the resource and resource capacities that you want to use.
f) Click **Submit** on the **Add Entry to Compute Accounts** screen.

Note
An account that is added to a resource group cannot be added to another resource group and cannot be deleted from Cisco UCS Director.

Step 16 Click **Next**.

Step 17 (Optional) On the **Physical Storage** screen, expand **Storage Accounts** and click the row with the physical storage account and the interested capabilities and capacities:

a) Click the + icon to add a storage account.
b) On the **Add Entry to Storage Accounts** screen, check the storage account that you want to use, and click **Validate**.
c) Expand **Environment Variables** and click the + icon.

1. In the **Add Entry to Environment Variables** dialog box, choose an environment variable from the **Name** drop-down list.
2. Expand **Required Value** and check the value according to the selected environment variable. When you choose **Vlan pool** from the **Name** drop-down list, expand **Required Value** and check the policy that you want to use. You can also add a policy by clicking the + icon.
3. Click **Submit**.

   The IP address and subnet mask of the storage device must be within the IP address range specified based on the policy.

d) Expand **Selected Capabilities** and click on the row with the resource and resource capability that you want to use.
e) Expand **Selected Capacities** and click on the row with the resource and resource capacities that you want to use.
f) Click **Submit** on the **Add Entry to Storage Accounts** screen.

Note
An account that is added to a resource group cannot be added to another resource group and cannot be deleted from Cisco UCS Director.

Step 18 Click **Next**.

Step 19 (Optional) On the **Physical Network** screen, expand **Network Accounts** and click the row with the physical network account and the interested capabilities and capacities:

a) Click the + icon to add a network account.
b) On the **Add Entry to Network Accounts** screen, choose the storage account.
c) Expand **Environment Variables** and click the + icon.

1. On the **Add Entry to Environment Variables** screen, choose an environment variable from the **Name** drop-down list.
2. Expand **Required Value** and check the value according to the selected environment variable. When you choose **IP Pool** from the **Name** drop-down list, expand **Required Value** and check the policy that you want to use.
3. Click **Submit**.

d) Expand **Selected Capabilities** and click the + icon.

1. On the **Add Entry to Selected Capabilities** screen, choose **FC Capability on MDS** or **Zone Support** from the **Select Resource** drop-down list.
2. In the **Resource Capability** field, choose a value from the list of values that are displayed according to the selected resource.
3. Click **Submit**.

e) Expand **Selected Capacities** and click on the row with the resource and resource capacities that you want to use.
f) Click **Submit** on the **Add Entry to Network Accounts** screen.

Note
An account that is added to a resource group cannot be added to another resource group and cannot be deleted from Cisco UCS Director.

Step 20 Click **Next**.

Step 21 On the **L4L7 Devices** screen, choose the firewall specification and load balancer specification:

a) Expand **Firewall Specification** and click the + icon.
On the **Add Entry to Firewall Specification** screen, complete the following fields:

Name	Description
Firewall Type drop-down list	Choose **VIRTUAL** or **PHYSICAL** as the firewall type.
The following fields appear when you choose **VIRTUAL** as the firewall type:	
Virtual Accounts field	Expand **Virtual Accounts** and check the virtual account you want to use.
VM Deployment Policy drop-down list	Choose a VM deployment policy. Click the + icon to add a VM deployment policy. For more information about how to add a VM deployment policy, see the Adding an ASAv VM Deployment Policy section in the Cisco UCS Director Application Container Guide.
Firewall Management Port Group field	Expand **Firewall Management Port Group** and check the port group of vCenter that you want to use. The management interface will be placed in the chosen port group during ASAv deployment.
Management IP Pool field	Expand **Management IP Pool** and check the IP pool that you want to use for assigning management IP address.
Regular HA IP Pool field	Expand **Regular HA IP Pool** and check the IP pool (private IP range) to allocate IP address from the pool. This pool is used as failover link between primary and secondary ASA devices. This pool is used when the firewall HA is enabled in the Layer 4 through Layer 7 service policy.
Stateful HA IP Pool field	Expand **Stateful HA IP Pool** and check the IP pool (private IP range) to allocate IP address from the pool. This pool is used as state link between primary and secondary Cisco ASA devices. This pool is used when the stateful failover is enabled in the Layer 4 through Layer 7 service policy. The stateful HA IP pool and regular HA IP pool must be in different subnets to avoid network IP conflict.
The following fields appear when you choose **PHYSICAL** as the firewall type.	
APIC Accounts field	Expand **APIC Accounts** and check the APIC account that you want to use.
Multi Context Enabled check box	Check **Multi Context Enabled** if the multiple context configuration is enabled on the Cisco ASA device.

Name	Description
Firewall Cluster IP field	This field appears only when **Multi Context Enabled** is checked. The IP address of the physical Cisco ASA device. This IP address is configured as the Admin Context IP address.
Cluster Username field	This field appears only when **Multi Context Enabled** is checked. The username of the cluster that is used by APIC to access ASA.
Cluster Password field	This field appears only when **Multi Context Enabled** is checked. The password of the cluster that is used by APIC to access ASA.
Firewall/Context IP field	The IP address that is used to reach the firewall device. If **Multi Context Enabled** is checked, this field collects the User Context IP address of the virtual ASA device that is configured on Day 0.
Port field	The port number of the firewall device.
Username field	The username that is used to access the firewall device. If **Multi Context Enabled** is checked, this field collects the username of the user context.
Password field	The password that is used to access the firewall device. If **Multi Context Enabled** is checked, this field collects the password of the user context.
Physical Domain field	Expand **Physical Domain** and check the physical domain that you want to use. Click the + icon to add a physical domain.
Static Path field	Expand **Static Path** and check the static path that you want to use. Cisco UCS Director displays the path types, such as VPC and leaf, in the table.
Port Channel Name field	The port channel interface of the Cisco ASA device which is connected to leaf (for example, Po1, Port-channel1).
Channel Group Id field	The unique ID of the channel group. This field appears only when **Multi Context Enabled** is unchecked.
Port Channel Member Interfaces field	The interface name(s) of the port channel member. This field appears only when **Multi Context Enabled** is unchecked. **Note** Enter the interface name without space. If there are more than one interfaces, enter the interface names separated by comma.

b) Click **Submit**.

Note
If the multiple context is enabled on the Cisco ASA device, repeat the firewall specification to add the details for each context.

c) Expand **Load Balancer Specification**, click the + icon.

On the **Add Entry to Load Balancer Specification** screen, complete the following fields:

Name	Description
Load Balancer Type drop-down list	Choose **Virtual** or **Physical** as the load balancer type.
Virtual Accounts field	This field appears when you choose the load balancer type as **Virtual**. Expand **Virtual Accounts** and check the virtual account that you want to use.
APIC Accounts field	This field appears when you choose the load balancer type as **Physical**. Expand **APIC Accounts** and check the APIC account that you want to use.
Load Balancer IP field	The IP address that is used to reach the NetScalar device.
Port field	The port number of the NetScalar device.
Load Balancer Gateway field	The gateway IP address of the NetScalar device.
Username field	The username that is used to access the NetScalar device.
Password field	The password that is used to access the NetScalar device.
Function Profile field	Optional. Expand **Function Profile** and check the function profile that you want to use.
VMs field	This field appears when you choose the load balancer type as **Virtual**. Expand **VMs** and check the VM that you want to use.
Physical Domain field	This field appears when you choose the load balancer type as **Physical**. Expand **Physical Domain** and check the physical domain that you want to use. Click the + icon to add a physical domain.
Interface field	This field appears when you choose the load balancer type as **Physical**. The interface that is used for the device cluster configuration (for example, LA_1).

Name	Description
Static Path field	This field appears when you choose the load balancer type as **Physical**. Expand **Static Path** and check the static path that you want to use.

d) Click **Submit**.

Step 22 Click **Submit**.

Editing a Resource Group

When editing a resource group, you can add accounts to the resource group, edit the accounts that are added to the resource group, and delete accounts from the resource group.

You can delete an account from a resource group only when the account is not associated with other resource group objects, such as a tenant profile.

Procedure

Step 1 Choose **Policies** > **Resource Groups**.

Step 2 On the **Resource Groups** page, click **Resource Groups**.

Step 3 Click the row with the resource group that you want to edit.

Step 4 Click **Edit**.

Step 5 On the **Edit Resource Group** screen, complete the following fields for the resource group:

Name	Description
Name field	The name of the resource group.
Description field	The description of the resource group.
Enable DR check box	Check to enable the disaster recovery service support for the resource group. **Note** The disaster recovery service support is enabled based on the use case and the workflow being executed.
Accounts Priority drop-down list	This field appears only when **Enable DR** is checked. By default, **Primary** is selected to set the resource group as primary. If you want to set the resource group as secondary, choose **Secondary**.
DRS Resource Group drop-down list	Choose a resource group as a disaster recovery service resource group for handling failover and recovering data during disaster.

Step 6 Click **Next**.

Step 7 (Optional) The **Virtual Compute** screen displays the virtual compute accounts added to the resource group. Expand **Virtual Accounts**, click the row of an account, and click the **edit** icon to edit the environment variable, capabilities, and capacities of the account. You can also add an account using the **add** icon and delete the account using the **delete** icon.

Step 8 Click **Next**.

Step 9 The **Virtual Storage** screen displays the virtual storage accounts added to the resource group. Expand **Virtual Accounts**, click the row of an account, and click the **edit** icon to edit the environment variable, capabilities, and capacities of the account. You can also add an account using the **add** icon and delete the account using the **delete** icon.

Step 10 Click **Next**.

Step 11 The **Virtual Network** screen displays the virtual network accounts added to the resource group. Expand **Virtual Accounts**, click the row of an account, and click the **edit** icon to edit the environment variable, capabilities, and capacities of the account. You can also add an account using the **add** icon and delete the account using the **delete** icon.

Step 12 Click **Next**.

Step 13 The **Physical Compute** screen displays the physical compute accounts added to the resource group. Expand **Compute Accounts**, click the row of an account, and click the **edit** icon to edit the environment variable, capabilities, and capacities of the account. You can also add an account using the **add** icon and delete the account using the **delete** icon.

Step 14 Click **Next**.

Step 15 The **Physical Storage** screen displays the physical storage accounts added to the resource group. Expand **Storage Accounts**, click the row of an account, and click the **edit** icon to edit the environment variable, capabilities, and capacities of the account. You can also add an account using the **add** icon and delete the account using the **delete** icon.

Step 16 Click **Next**.

Step 17 The **Physical Network** screen displays the physical network accounts added to the resource group. Expand **Network Accounts**, click the row of an account, and click the **edit** icon to edit the environment variable, capabilities, and capacities of the account. You can also add an account using the **add** icon and delete the account using the **delete** icon.

Step 18 Click **Next**.

Step 19 On the **L4L7 Devices** screen, edit the firewall specification and load balancer specification as required.

Step 20 Click **Submit**.

Adding a Pod to a Resource Group

To add all accounts in a pod to a resource group, add the pod itself to the resource group.



Note You can also add a multi-domain manager account to a resource group using the **Add Pod to Resource Group** option, provided that the multi-domain manager account is associated with a pod.

Procedure

Step 1 Choose **Policies** > **Resource Groups**.

Step 2 On the **Resource Groups** page, click **Resource Groups**.

Step 3 Click **Add Pod to Resource Group**.

Step 4 On the **Resource Group** screen, complete the following fields:

Name	Description

Select drop-down list	Choose one of the following:
	• **Existing Resource Group**—To add a pod to the existing resource group.
	  • **Name** drop-down list—Choose the resource group.
	• **Add New Resource Group**—To create a new resource group and add a pod to the newly added resource group.
	  • **Name** field—The name of the resource group.
	  • **Description** field—The description of the resource group.

Pod field	Expand **Pod** and check the pod that you want to add to the resource group.

Step 5 Click **Submit**.

Managing Tags of a Resource Group

You can add a tag to a resource group, edit the assigned tag, and delete the tag from the resource group.

Note The Manage Tag dialog box displays tags according to the Taggable Entities that are assigned during creation. For more information on how to create a tag, see the Cisco UCS Director Administration Guide.

The resources need to be grouped based on the resource capabilities. Use a tag to group the resources. You can create the tag library based on the resource type, capacity, quality, and capability of each resource, so as to group the resources in a proper pattern.

Procedure

Step 1 Choose **Policies** > **Resource Groups**.

Step 2 On the **Resource Groups** page, click **Resource Groups**.

Step 3 Click the row with the resource group for which you want to manage the associated tags.

Step 4 From the **More Actions** drop-down list, choose **Manage Tags**.

Step 5 On the **Manage Tags** screen, expand **Tag** and click the + icon to add a tag.

Alternatively, you can click **Add Tags** on the **Resource Groups** page.

a) On the **Add Entry to Tag** screen, complete the following fields:

Name	Description
Tag Name drop-down list	Choose the name of the tag.
Tag Value drop-down list	Choose the value of the tag.

b) Click **Submit**.

Step 6 On the **Manage Tags** screen, click the row with the tag you want to edit and click the pencil icon.

a) On the **Edit Tag Entry** screen, complete the following fields:

Name	Description
Tag Name drop-down list	Choose the name of the tag.
Tag Value drop-down list	Choose the value of the tag.

b) Click **Submit**.

Step 7 On the **Manage Tags** screen, click the row with the tag you want to delete and click the delete icon.

Alternatively, you can click **Delete Tags** on the **Resource Groups** page.

a) On the **Delete Tag Entry** screen, expand **Tag Name**, check the tag you want to delete, and click **Submit**.

Step 8 Click **Submit**.

Deleting a Resource Group



Note You cannot delete a resource group that is in use.

Procedure

Step 1 Choose **Policies** > **Resource Groups**.

Step 2 On the **Resource Groups** page, click **Resource Groups**.

Step 3 Click the row with the resource group that you want to delete.

Step 4 Click **Delete**.

The **Delete Resource Group** screen appears.

Step 5 Click **Submit**.

Tenant

A tenant is a customer who uses resources in Cisco UCS Director to deploy and manage their application.

When a customer wants to deploy an application in Cisco UCS Director, the customer is onboarded as a tenant and the infrastructure is provided to deploy the application, using the APIC use case workflows.

To view the list of tenants that are onboarded in Cisco UCS Director choose **Policies** > **Resource Groups**. Click the row with a tenant and click **View Details** to view the service offerings of the tenant. Click the row with a service offering and click **View Details** to view the resource groups of a tenant.

Note If the disaster recovery support is enabled for the tenant, the resource groups of the primary site and the disaster recovery site are displayed.

To view the resource entity, reserved resources, and resources available for use in tenant and container, click the row with the resource group and click **View Details**. The following information appears:

- **Resource Entity**—Displays the details of the entity in the resource group. The details include name, type, component, resource group, tenant resource allocation type, application resource allocation type, container, and state of the resource entity.
- **Tenant Resource Limits**—Displays availability of both virtual and physical resources in a tenant. The resources reserved during tenant onboarding are displayed along with the used and available resource values. The VDCs Limit column specifies the maximum number of containers that are reserved for the tenant. The Available Number of VDCs column represents the number of containers that are available for provisioning. The physical resource limits display the blades that are reserved as part of tenant onboarding, along with the number of blades used for bare metal provisioning.
- **Container Resource Limits**—Displays availability of both virtual and physical resources in a container. The resource limits that are set during container creation are displayed along with the used and available resources.

Note If a container is created without a resource limit, the value of the virtual resources is displayed as Not Set.

- **Private Network**—Displays the private networks created for the tenant. Click the row of a private network and click **View Details** to view the supernet and subnet pools of the private network. The **Supernets** screen lists the supernets available for the tiers. The **Subnets** screen displays the sub-network pool that is used for load balancer configuration during the container deployment.

The tenant-specific and container-specific resource limits assist in provisioning VMs and BMs.

Service Offerings

A service offering defines the resources required to provision an application. Each service offering must include one or more service classes that represents the capacity and capability needed for the following resource layers:

- Virtual Compute
- Virtual Storage
- Virtual Network
- Physical Compute
- Physical Storage
- Physical Network
- Layer 4 to Layer 7 Services

When you define a service offering, you can specify the usage of resource groups as one of the following:

- Shared—The resources are shared among the applications or tenants.
- Dedicated —The resources are dedicated to a single application or tenant.

Based on the capacity, capability, and resource tags defined in the service offering, the resource groups are filtered and the matching resource groups are selected for further processing in the tenant onboarding and application deployment.

Adding a Service Offering

Before you begin

If tag-based resource selection is required for any of the resources, ensure that the tags are created in the tag library and are associated with the respective object. So that, the tags are listed when you define resource tag for service class. For more information on how to create a tag, see the Cisco UCS Director Administration Guide.

Procedure

Step 1 Choose **Policies** > **Resource Groups**.

Step 2 On the **Resource Groups** page, click **Service Offering**.

Step 3 Click the row of a service offering and click **View** to view the name, description, and service classes of the service offering.

Step 4 Click the row of a service offering and click **View Details** to view the service classes of the service offering.

Step 5 Click the row of a service class and click **View Details** to view the capabilities, capacity, and resource-group tag of the service class.

Step 6 Click **Add**.

Step 7 On the **Add Service Offering** screen, complete the following fields:

Name	Description
Name field	The name of the service offering.
Description field	The description of the service offering.
Override Mandatory Service Class Requirement check box	If checked, the user can define any number of resource types (minimum of one resource type to maximum of six resource types) for the service class according to the topology. If unchecked, the user has to define all the six resource types (physical compute, physical storage, physical network, virtual compute, virtual storage, and virtual network) for the service class. Even if the user does not define all the virtual and physical infrastructure resource types, Cisco UCS Director looks for resources for the missing resource types along with the defined resource types. **Note** To create a service offering that is used for onboarding a tenant using APIC account and VMware account, check this check box and create a service offering with service class for four resource types (physical network, virtual compute, virtual storage, and virtual network). This service offering needs to be chosen during creation of a tenant profile. The tenant profile will be used for onboarding a tenant using APIC account and VMware account (for example, tenant onboarding with private networks).

Step 8 Click **Next**.

Step 9 On the **Service Class** screen, expand **Service Class** and click the + icon to define the service class that the service offering has to provide.

Step 10 On the **Add Entry to Service Class** screen, complete the following fields:

Name	Description
Name field	The name of the service class.
Description field	The description of the service class.

Name	Description
Resource Allocation type for Tenant drop-down list	Choose the type of resource allocation for the tenant. It can be one of the following: • **Dedicated**—To dedicate the resources for a tenant. • **Shared**—To share the resources among the tenants.
Resource Allocation type for Application drop-down list	Choose the type of resource allocation for the application. It can be one of the following: • **Dedicated**—To dedicate the resources for an application. • **Shared**—To share the resources among the applications.
Resource Type drop-down list	Choose the type of resource that you are adding to the service class. It can be one of the following: • **Virtual_Compute** • **Virtual_Storage** • **Virtual_Network** • **Physical_Compute** • **Physical_Storage** • **Physical_Network** The user can define a minimum of two resource types (physical or virtual compute, and physical or virtual network) and a maximum of six resource types (virtual compute, virtual storage, virtual network, physical compute, physical storage, and physical network) during the addition of the service class, only when **Override Mandatory Service Class Requirement** is unchecked.

Name	Description
Resource Tag field	Expand **Resource Tag** and click the row with the resource tag that you want to use. For more information about the tag library, see the Cisco UCS Director Administration Guide. **Note** You can add the data store tags with multiple tag values (for example, gold, silver, bronze) in the virtual storage service class level. **Note** You can add the ESXi cluster tag with multiple tag values in the virtual compute service class level. **Important** You can modify only the required values of the tags defined in this table. You cannot add new tags to this table. For information on how to create a tag, see the Tag Library section in the Cisco UCS Director Administration Guide.
Resource Capability field	By default, the capabilities that are applicable for the VMware and Hyper-V account are displayed according to the chosen resource type. You can edit the value of the resource capability using the Edit icon. You can remove a resource capability from the service offering using the Delete icon. **Important** All the resource capabilities related to the resource type are prepopulated with the default value as **false**. You can modify the capability value.
Resource Capacity field	The available resource capacity for the service offering. To add a resource capacity, expand **Resource Capacity** and click the Add icon and choose the capacity type from the list of capacities that are applicable for the VMware and Hyper-V account. The capacities are displayed based on the chosen resource type. Choose the capacity matching criteria and set the required capacity value. To remove the resource capacity, click the Delete icon. To modify the values of the capacity, click the Edit icon.

Note
The tag is used along with resource capability and capacity for filtering the resources in the resource group.

Step 11 Click **Submit**.

The service class information is added to the table. You can define multiple service classes for the service offering.

Step 12 Click **Submit**.

Cloning a Service Offering

Before you begin

Ensure that the tags are created in the tag library and the tags are associated with the respective object. So that, the tags are listed when you define resource tag for service class. For more information on how to create a tag, see the Cisco UCS Director Administration Guide.

Procedure

Step 1 Choose **Policies** > **Resource Groups**.

Step 2 On the **Resource Groups** page, click **Service Offering**.

Step 3 Click the row with the service offering that you want to clone.

Step 4 Click **Clone Service Offering**.

Step 5 On the **Clone Service Offering** screen, complete the following fields:

Name	Description
Name field	The name of the service offering.
Description field	The description of the service offering.

Name	Description
Override Mandatory Service Class Requirement check box	If checked, the user can define any number of resource types (minimum of one resource type to maximum of six resource types) for the service class according to the topology. If unchecked, the user has to define all the six resource types (physical compute, physical storage, physical network, virtual compute, virtual storage, and virtual network) for the service class. Even if the user does not define all the virtual and physical infrastructure resource types, Cisco UCS Director looks for resources for the missing resource types along with the defined resource types. **Note** To create a service offering that is used for onboarding a tenant using APIC account and VMware account, check this check box and create a service offering with service class for four resource types (physical network, virtual compute, virtual storage, and virtual network). This service offering needs to be chosen during creation of a tenant profile. The tenant profile will be used for onboarding a tenant using APIC account and VMware account (for example, tenant onboarding with private networks).

Step 6 Click **Next**.

Step 7 On the **Service Class** screen, expand **Service Class** and click the + icon to define the service class that the service offering has to provide.

Step 8 On the **Add Entry to Service Class** screen, complete the following fields:

Name	Description
Name field	The name of the service class.
Description field	The description of the service class.
Resource Allocation type for Tenant drop-down list	Choose the type of resource allocation for the tenant. It can be one of the following: • **Dedicated**—To dedicate the resources for a tenant. • **Shared**—To share the resources among the tenants.

Name	Description
Resource Allocation type for Application drop-down list	Choose the type of resource allocation for the application. It can be one of the following: • **Dedicated**—To dedicate the resources for an application. • **Shared**—To share the resources among the applications.
Resource Type drop-down list	Choose the type of resource that you are adding to the service class. It can be one of the following: • **Virtual_Compute** • **Virtual_Storage** • **Virtual_Network** • **Physical_Compute** • **Physical_Storage** • **Physical_Network** The user can define a minimum of two resource types (physical or virtual compute, and physical or virtual network) and a maximum of six resource types (virtual compute, virtual storage, virtual network, physical compute, physical storage, and physical network) during the addition of the service class, only when **Override Mandatory Service Class Requirement** is unchecked.

Name	Description
Resource Tag field	Expand **Resource Tag** and click the row with the resource tag that you want to use. For more information about the tag library, see the Cisco UCS Director Administration Guide. **Note** You can add the data store tags with multiple tag values (for example, gold, silver, bronze) in the virtual storage service class level. **Note** You can add the ESXi cluster tag with multiple tag values in the virtual compute service class level. **Important** You can modify only the required values of the tags defined in this table. You cannot add new tags to this table. For information on how to create a tag, see the Tag Library section in the Cisco UCS Director Administration Guide.
Resource Capability field	By default, the capabilities that are applicable for the VMware and Hyper-V account are displayed according to the chosen resource type. You can edit the value of the resource capability using the Edit icon. You can remove a resource capability from the service offering using the Delete icon. **Important** All the resource capabilities related to the resource type are prepopulated with the default value as **false**. You can modify the capability value.
Resource Capacity field	The available resource capacity for the service offering. To add a resource capacity, expand **Resource Capacity** and click the Add icon and choose the capacity type from the list of capacities that are applicable for the VMware and Hyper-V account. The capacities are displayed based on the chosen resource type. Choose the capacity matching criteria and set the required capacity value. To remove the resource capacity, click the Delete icon. To modify the values of the capacity, click the Edit icon.

Step 9 (Optional) Click the **pencil** icon to edit the values of an already configured service class.

Step 10 (Optional) Click the **trash** icon to delete an already configured service class from the service offering.

Step 11 Click **Submit**.

Editing a Service Offering



Note Do not edit the service offering that is mapped to a resource group and tenant profile. If you edit the service offering that is mapped to a resource group and tenant profile, the tenant that is onboarded using the service offering will be affected.

Before you begin

Ensure that the tags are created in the tag library and the tags are associated with the respective object. So that, the tags are listed when you define resource tag for service class. For more information on how to create a tag, see the Cisco UCS Director Administration Guide.

Procedure

Step 1 Choose **Policies** > **Resource Groups**.

Step 2 On the **Resource Groups** page, click **Service Offering**.

Step 3 Click the row with the service offering that you want to edit.

Step 4 Click **Edit**.

Step 5 On the **Modify Service Offering** screen, complete the following fields:

Name	Description
Name field	The name of the service offering.
Description field	The description of the service offering.

Name	Description
Override Mandatory Service Class Requirement check box	If checked, the user can define any number of resource types (minimum of one resource type to maximum of six resource types) for the service class according to the topology. If unchecked, the user has to define all the six resource types (physical compute, physical storage, physical network, virtual compute, virtual storage, and virtual network) for the service class. Even if the user does not define all the virtual and physical infrastructure resource types, Cisco UCS Director looks for resources for the missing resource types along with the defined resource types. **Note** To create a service offering that is used for onboarding a tenant using APIC account and VMware account, check this check box and create a service offering with service class for four resource types (physical network, virtual compute, virtual storage, and virtual network). This service offering needs to be chosen during creation of a tenant profile. The tenant profile will be used for onboarding a tenant using APIC account and VMware account (for example, tenant onboarding with private networks).

Step 6 Click **Next**.

Step 7 On the **Service Class** screen, expand **Service Class** and click the + icon to define the service class that the service offering has to provide.

Step 8 On the **Add Entry to Service Class** screen, complete the following fields:

Name	Description
Name field	The name of the service class.
Description field	The description of the service class.
Resource Allocation type for Tenant drop-down list	Choose the type of resource allocation for the tenant. It can be one of the following: • **Dedicated**—To dedicate the resources for a tenant. • **Shared**—To share the resources among the tenants.

Name	Description
Resource Allocation type for Application drop-down list	Choose the type of resource allocation for the application. It can be one of the following: • **Dedicated**—To dedicate the resources for an application. • **Shared**—To share the resources among the applications.
Resource Type drop-down list	Choose the type of resource that you are adding to the service class. It can be one of the following: • **Virtual_Compute** • **Virtual_Storage** • **Virtual_Network** • **Physical_Compute** • **Physical_Storage** • **Physical_Network** The user can define a minimum of two resource types (physical or virtual compute, and physical or virtual network) and a maximum of six resource types (virtual compute, virtual storage, virtual network, physical compute, physical storage, and physical network) during the addition of the service class, only when **Override Mandatory Service Class Requirement** is unchecked.

Name	Description
Resource Tag field	Expand **Resource Tag** and click the row with the resource tag that you want to use. For more information about the tag library, see the Cisco UCS Director Administration Guide. **Note** You can add the data store tags with multiple tag values (for example, gold, silver, bronze) in the virtual storage service class level. **Note** You can add the ESXi cluster tag with multiple tag values in the virtual compute service class level. **Important** You can modify only the required values of the tags defined in this table. You cannot add new tags to this table. For information on how to create a tag, see the Tag Library section in the Cisco UCS Director Administration Guide.
Resource Capability field	By default, the capabilities that are applicable for the VMware and Hyper-V account are displayed according to the chosen resource type. You can edit the value of the resource capability using the Edit icon. You can remove a resource capability from the service offering using the Delete icon. **Important** All the resource capabilities related to the resource type are prepopulated with the default value as **false**. You can modify the capability value.
Resource Capacity field	The available resource capacity for the service offering. To add a resource capacity, expand **Resource Capacity** and click the Add icon and choose the capacity type from the list of capacities that are applicable for the VMware and Hyper-V account. The capacities are displayed based on the chosen resource type. Choose the capacity matching criteria and set the required capacity value. To remove the resource capacity, click the Delete icon. To modify the values of the capacity, click the Edit icon.

Step 9 Click **Submit**.

Deleting a Service Offering



Note You cannot delete a service offering that is in use.

Procedure

Step 1 Choose **Policies** > **Resource Groups**.
Step 2 On the **Resource Groups** page, click **Service Offering**.
Step 3 Click the row with the service offering that you want to delete.
Step 4 Click **Delete**.
Step 5 On the **Service Offering** screen, click **Delete**.

Tenant Profiles

Tenant profiles represent the pairing of one or more service offerings with one or more resource groups. Each tenant profile defines the characteristic of infrastructure requirements and application requirements.

You can create a tenant profile to meet each possible combination of customer and application. You can associate a tenant profile with multiple service offerings and choose a resource group for each service offering. A tenant profile can be shared by more than one tenant.

Adding a Tenant Profile

Before you begin

If the DR service support is enabled for the tenant profile, the resources that satisfy the following are displayed for choosing a resource group for a specific service offering:

- The DR service is enabled.
- The resource group is configured as primary.
- The primary resource group is mapped with the secondary resource group.
- The primary and secondary resource groups have same number of accounts.
- The resources required for the tenant are available in both the primary and secondary resource groups.

For more information on how to enable DR service and set the resource group as primary or secondary, see Adding a Resource Group, on page 268.

Procedure

Step 1 Choose **Policies** > **Resource Groups**.

Step 2 On the **Resource Groups** page, click **Tenant Profile**.

Step 3 Click the row with a tenant profile and click **View** to view the name, description, and service offering of the tenant profile with the resource limit added to the tag.

Step 4 Click the row with a tenant profile and click **View Details** to view the tenants that are associated with a tenant profile.

The name, resource group, service offering, APIC account, service request ID, and customer assigned for the tenants in the tenant profile are displayed.

Step 5 Click the row with a tenant and click **View Details** to view the service offering.

Step 6 Click the row with a service offering and click **View Details** to view the resource entity of a tenant.

Step 7 Click **Add**.

Step 8 On the **Add Tenant Profile** screen, complete the following fields:

Name	Description
Name field	The name of the tenant profile. Once specified, you cannot edit the name of the profile.
Description field	The description of the tenant profile.
Enable DR check box	Check to enable the disaster recovery service support for the tenant profile. If checked, the tenant is allocated with resources from both the primary resource group and the secondary resource group.
Service Offering field	The service offerings to be associated with the tenant profile. Expand **Service Offering** , check the service offering that you want to use, and then click **Validate**. The service offerings are displayed based on the matching resource group availability. To create a new service offering, click the + icon. For more information about how to create a service offering, see Adding a Service Offering, on page 281. **Note** If you receive an error message instead of the service offerings list, take action according to the error message. For more details, see Troubleshooting a Service Offering List, on page 295.

Name	Description
Resource Group Selection drop-down list	Choose how the resource group selection will be made for the tenant profile: • **Admin Selection**—The resource group is selected by the administrator. • **Resource Group Tag based selection**—The resource group is selected based on the tag.

Step 9 Click **Next**.

Step 10 Expand **Resrouce Group** and click the **Add (+)** icon to choose a resource group for a specific service offering. For each service offering selected for the tenant profile, you can select the resource group.

The resource groups that match the specified requirement of the tenant profile are displayed.

Note
If there is no matching resource group for the resource requirements defined in a service offering, Cisco UCS Director will not list any resource group.

Step 11 Click **Submit**.

Troubleshooting a Service Offering List

While creating a tenant profile, you associate a tenant profile with multiple service offerings. The service offerings list is displayed based on the matching resource group availability. If you receive an error message instead of the service offerings list, take action according to the error message.

For example, on receiving the error message: *Host is not mounted on UCS servers*, check for the following:

Procedure

	Command or Action	Purpose
Step 1	Verify that the Cisco UCS server is managed by Cisco UCS Director. To check the status of the Cisco UCS servers, choose **Physical** > **Compute**, choose the Cisco UCS Manager account, and click the **UCS Discovered Servers**.	
Step 2	Verify that the vCenter account and Cisco UCS Manager account are in the same resource group, and host in the vCenter account is mounted on the Cisco UCS Manager account.	
Step 3	Verify that the Cisco UCS Manager accounts that are available in Cisco UCS Director each have a unique IP address. If more than one account exists with the same IP address, remove	

	Command or Action	Purpose
	one of the accounts that is not part of the resource group.	

Cloning a Tenant Profile

Procedure

Step 1 Choose **Policies** > **Resource Groups**.

Step 2 On the **Resource Groups** page, click **Tenant Profile**.

Step 3 Click the row with the tenant profile that you want to clone.

Step 4 Click **Clone**.

Step 5 On the **Clone Tenant Profile** screen, complete the following fields:

Name	Description
Name field	The name of the tenant profile.
Description field	The description of the tenant profile.
Service Offering field	The service offerings to be associated with the tenant profile. Expand **Service Offering**, check the service offering you want to use, and then click **Validate**. The service offerings are displayed based on the matching resource group availability. To create a new service offering, click the + icon. For more information about how to create a service offering, see Adding a Service Offering, on page 281. **Note** If you receive an error message instead of the service offerings list, take action according to the error message. For more details, see Troubleshooting a Service Offering List, on page 295.
Resource Group Selection drop-down list	Choose how the resource group selection will be made for the tenant profile: • **Admin Selection**—The resource group is selected by the administrator. • **Resource Group Tag based selection**—The resource group is selected based on the tag.

Step 6 Click **Next**.

Step 7 Expand **Resource Group** and click the **Add (+)** icon to choose a resource group for a specific service offering. For each service offering selected for the tenant profile, you can select the resource group.

The resource groups that match the specified requirement of the tenant profile are displayed.

Note
If there is no matching resource group for the resource requirements defined in the service offering, Cisco UCS Director will not list any resource group.

Step 8 Click **Submit**.

Editing a Tenant Profile

Procedure

Step 1 Choose **Policies** > **Resource Groups**.

Step 2 On the **Resource Groups** page, click **Tenant Profile**.

Step 3 Click the row with the tenant profile that you want to edit.

Step 4 Click **Edit**.

Step 5 On the **Modify Tenant Profile** screen, complete the following fields:

Name	Description
Name field	The name of the tenant profile. Once specified, you cannot edit the name of the profile.
Description field	The description of the tenant profile.
Service Offering field	The service offerings to be associated with the tenant profile. Expand **Service Offering**, check the service offering you want to use, and then click **Validate**. The service offerings are displayed based on the matching resource group availability. To create a new service offering, click the + icon. For more information about how to create a service offering, see Adding a Service Offering, on page 281. **Note** If you receive an error message instead of the service offerings list, take action according to the error message. For more details, see Troubleshooting a Service Offering List, on page 295.

Name	Description
Resource Group Selection drop-down list	Choose how the resource group selection will be made for the tenant profile: • **Admin Selection**—The resource group is selected by the administrator. • **Resource Group Tag based selection**—The resource group is selected based on the tag.

Step 6 Click **Next**.

Step 7 Expand **Resource Group** click the **Add (+)** icon to choose a resource group for a specific service offering. For each service offering selected for the tenant profile, you can select the resource group.

The resource groups that match the specified requirement of the tenant profile are displayed.

Note
If there is no matching resource group for the resource requirements defined in the service offering, Cisco UCS Director will not list any resource group.

Step 8 Click **Submit**.

Deleting a Tenant Profile



Note You cannot delete a tenant profile that is in use.

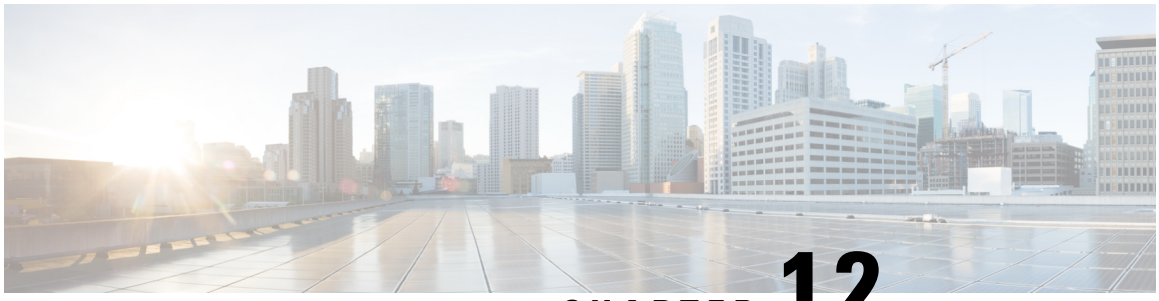
Procedure

Step 1 Choose **Policies** > **Resource Groups**.

Step 2 On the **Resource Groups** page, click **Tenant Profile**.

Step 3 Click the row with the tenant profile that you want to delete.

Step 4 Click **Delete**.
The tenant profile is deleted after confirmation.



CHAPTER 12

Managing Catalogs

This chapter contains the following sections:

- About Managing Catalogs, on page 299
- Publishing a Catalog, on page 300
- About Publishing Advanced Catalogs, on page 308
- Publishing Advanced Catalogs, on page 308
- Creating a Bare Metal Server Catalog, on page 310
- Reordering Catalogs Within a Folder, on page 312
- Accessing Hosts for Deployment, on page 312
- Reordering Catalog Folders, on page 313

About Managing Catalogs

You can self-provision virtual machines (VMs) and bare metal (BM) servers using predefined catalog items. Only a system administrator can create a catalog. A catalog defines parameters, such as the cloud name and the group name to which the VM is bound.

The following folders are available by default. You cannot edit or delete them.

- Standard
- Advanced
- Service Container
- Bare Metal

To aid in managing catalogs, Cisco UCS Director allows you to group similar catalogs within a folder. While creating a catalog, you can choose to add it in a previously created folder, or create a new folder. A folder is visible in the system only when it contains a catalog.

The **Manage Folder** option on the **Catalog** page allows you to perform the following tasks:

- Edit a folder—Modify the name of a user-created folder or the folder icon for all folders. You cannot modify the name of a default folder.
- Delete a folder—Delete a folder from Cisco UCS Director. If this folder contains catalogs, then these catalogs are automatically moved into the folders that are available by default, based on the catalog type.

  Default folders cannot be deleted.

- Re-order the list of folder—Change the order in which the folders are listed in the **Catalog** page. By default, folders are listed alphabetically.

Important If you have upgraded Cisco UCS Director to the latest version, then all catalogs created in prior versions are grouped into folders available by default, based on their catalog types.

By default, catalogs are displayed in a tile view format. You can choose to have the catalogs displayed in a table view format as well. Use the options on the far right of the screen to switch between the table view and the tile view format. In the table view format, you can use the options to expand or collapse all folders.

From the **Catalog** page, you can create a Service Request. Click **Create Service Request**, and complete the procedure documented in Creating a Service Request with Catalog Type—Standard, on page 316.

Publishing a Catalog

Procedure

Step 1 Choose **Policies** > **Catalogs**.

Step 2 On the **Catalogs** page, click **Add**.

Step 3 On the **Add Catalog** screen, choose the **Catalog Type** that you want to add.

It can be one of the following:

- **Standard**—Used to create catalogs for VM provisioning, using images from a list of clouds.
- **Advanced**—Used to publish orchestration workflows, such as catalog items.
- **Service Container**—Used to publish application containers as catalog items.
- **Bare Metal**—Used to create catalogs for bare metal server provisioning.

  For information on how to create a bare metal catalog, see Creating a Bare Metal Server Catalog, on page 310.

Step 4 Click **Submit**.

Step 5 On the **Add Catalog: Basic Information** screen, complete the required fields, including the following:

Name	Description
Catalog Name field	Enter a name for the catalog. **Note** After created, a catalog name cannot be modified.
Catalog Description field	Enter a description of the catalog.

Name	Description
Catalog Type drop-down list	Displays the type of catalog you previously chose. To change the catalog type, you need to cancel and restart this procedure.
Catalog Icon drop-down list	Choose from a list of icons to associate this catalog with an image. This icon is seen when you are creating a service request using this catalog.
Applied to all groups check box	Check the box to enable all groups to use this catalog. Leave it unchecked to deny its use to other groups.
Support Contact Email Address field	Enter the email address of the support contact who is notified when a service request is created using this catalog item.
Selected Groups list	Click **Select** to the check the checkboxes of specific user groups. The checked groups use this catalog to provision new VMs. After checking the checkboxes of user groups, click **Select** to return to the **Add Catalog** screen.
Publish to end users check box	By default, this box is checked. Uncheck this box if you do not want this catalog to be visible to users. If you do not uncheck this box, then this catalog is visible to the users of the system.
Cloud Name drop-down list	Choose the cloud with the image for VM provisioning.
Provision new VM for ISO mounting check box	Check this box to clone a new VM from a selected image. If you do not check this check box, a blank VM is created.
Image list	Click **Select** to the check the checkboxes of the type of image (any existing templates such as Windows, Linux, and other files that make up the image) to use when VMs are provisioned using this catalog. After checking the checkboxes of the required images, click **Select** to return to the **Add Catalog** screen. If you are a group administrator, or a user in a group with permissions to create catalogs, this field displays images that are assigned to the group to which you belong. If you are an MSP administrator, then this field displays images that are assigned to your MSP organization, and to the groups within the MSP organization.
Provision new VM using Content Library VM Template check box	Check this box to ensure that the new VM is provisioned using the Content Library VM Template. If you choose this option, the **Image** list is hidden.

Name	Description
Content Library VM Template list	Choose the content library VM template.
Windows License Pool field	Enter the Windows License. **Note** This field appears only when a Windows image is chosen. This option is not supported in the RHEV KVM Connector.
Use ReadyClone check box	Check the box to ensure that VMs are deployed using ReadyClones. When this box is checked, the **Use Linked Clone** and **Provision all disks in single datastore** check boxes are not available for editing. **Note** This checkbox is not visible if: 1. The selected image is not on the HX datastore. 2. The VM has multiple disks.
Use Linked Clone check box	Check the box if you want to use a linked clone. Linked Clone or Full Clone depends on the Linked Clone selection in the Storage Policy. **Note** This field appears only when a Snapshot image is chosen.
Provision all disks in single datastore check box	Check the box to provision all disks in a single datastore. You can also choose to use the datastores configured for each disk in the storage policy. For more information on multiple disk storage policy creation, see Managing Policies, on page 207. **Note** This field appears only if the chosen template has multiple disks. This option is not supported in the RHEV KVM Connector.
Service Container Template Name drop-down list	Choose the template from the list. **Note** This field appears only when the chosen Catalog Type is **Service Container**.

Name	Description
Select Folder drop-down list	Choose the folder within which this catalog must be created. **Note** The drop-down list includes names of folders that are available by default. You can either choose a folder that is available, or click **Create New Folder**. On the **Add New Folder** screen, enter a **Folder Name**, choose a **Folder Icon**, and click **Add**.
Bare Metal Server Provisioning Policy drop-down list	**Note** This field appears only when the chosen Catalog Type is **Bare Metal**.
Configure Service Request Support Email check box	Check this box to enable the user to set the support email for sending service request status.

Step 6 Click **Next**.

Step 7 On the **Add Catalog: Application Details** screen, complete the required fields, including the following:

Name	Description
Category list	Expand the list to choose a VDC category and click **Select**.
Override check box	Check the box to enable the user to override the selected category while provisioning a VM using a service request.
Support Contact Email Address field	Enter the email address of the contact who is notified when a service request is created using this catalog item.
Specify OS drop-down list	Choose the type of OS installed on the VM when it is provisioned. **Note** This option is not supported in the RHEV KVM Connector.
Specify Other OS field	Enter an OS that is not available in the **Specify OS** drop-down list. **Note** This option is not supported in the RHEV KVM Connector.

Name	Description
Specify Applications check boxes	Check the appropriate boxes to specify applications that are installed on the VM during provisioning. **Note** This option is not supported in the RHEV KVM Connector.
Specify Other Applications field	Enter other applications that are not available from the **Specify Applications** check boxes. **Note** This option is not supported in the RHEV KVM Connector.
Application Code field	Enter an application code that is used in the VM name. The application code can be between 1 to 4 characters (for example: W2K3, DB, WS). The application code can be used in a system policy for the VM name by using the variable ${APPCODE}. For example, if the VM Name Template is vm-${GROUP_NAME}-${APPCODE}, the VM provisioned with the system policy has the name vm-groupname-W2K3. **Note** This option is not supported in the RHEV KVM Connector.

Step 8 Click **Next**.

Step 9 On the **Add Catalog: User credentials** screen, complete the required fields, including the following:

Note
These options are not supported in the RHEV KVM Connector.

Name	Description
Credential Options drop-down list	Choose to allow or disallow users to retrieve VM access credentials (shared). The following options are available: • **Do not share** • **Share after password reset** • **Share template credentials** The **Do not share** option is chosen if the administrator wants to send the credentials privately to another user outside Cisco UCS Director.

Name	Description
User ID field	Enter the user ID. **Note** This field is available only if a choice is made to share under **Credential Options**.
Password field	Enter the password. **Note** This field is available only if a choice is made to share under **Credential Options**.

Step 10 Click **Next**.

Step 11 On the **Add Catalog: Customization** screen, complete the required fields, including the following:

Name	Description
Automatic Guest Customization Enable check box	Check the box to enable automatic guest customization. If you do not check this check box, then Cisco UCS Director does not configure the DNS, Network, and Guest OS properties.
Service Request Options Lock check box	Check the **Lock** check box to lock a service request. Selecting the **Lock** check box prevents archiving of the service request. This is applicable only when you choose the catalog type as **Standard**.
Pre Provisioning Custom Actions Enable	Check the **Enable** check box to enable execution of an orchestration workflow before VM provisioning.
Workflow field	Click **Select** to check the compound workflow that should be used in the orchestration workflow before VM provisioning. Check the check boxes of the required workflows, and click **Select** to return to the **Add Catalog** screen. **Note** This field appears when **Pre Provisioning Custom Actions Enable** is checked.
Post Provisioning Custom Actions Enable check box	Check the box to enable execution of an orchestration workflow after VM provisioning.

Name	Description
Workflow drop-down list	Click **Select** to check the check boxes of the workflows that need to be used in the orchestration workflow after VM provisioning. Check the check boxes of the required workflows, and click **Select** to return to the **Add Catalog** screen. **Note** This field appears when **Post Provisioning Custom Actions Enable** is checked.
Virtual Storage Catalog Enable check box	Check the box to choose storage entries from the Virtual Storage catalog.
Virtual Storage Catalog drop-down list	Chose a storage entry from the catalog. **Note** This field appears when **Virtual Storage Catalog Enable** is checked.
Cost Computation	
Charge Duration drop-down list	Choose **Hourly** or **Monthly**.
Active VM Application Cost USD field	Enter the cost for the application that is included in the template. **Note** This option is not supported in the RHEV KVM Connector.
Inactive VM Application Cost USD field	Enter the cost to this catalog of a VM in inactive state, per hour or month. **Note** This option is not supported in the RHEV KVM Connector.
VM Life Cycle Configuration	
Lease Time check box	Check the box to define a lease time (in days and hours).
Days field	Enter the number of days. **Note** This field appears when **Lease Time** is checked.
Hours field	Enter the number of hours. **Note** This field appears when **Lease Time** is checked.

Name	Description
Hide end user lease configuration check box	Check the box to prevent service users from configuring a lease time for VMs.
Hide end user VM provision later check box	Check the box to prevent service users from provisioning VMs at a later time.

Step 12 Click **Next**.

Step 13 On the **Add Catalog: VM Access** screen, complete the required fields, including the following:

Name	Description
Web Access Configuration Enable check box	Check the box to enable web access to the VM. By default, this check box is unchecked which means that web access to the VM is disabled.
URL field	Enter the URL of the VM. **Note** This field appears when **Web Access Configuration Enable** is checked.
Label field	Enter the label that is defined for this URL. **Note** This field appears when **Web Access Configuration Enable** is checked.
Remote Desktop Access Configuration Enable check box	Check the box to enable remote desktop access to the VM. By default, this check box is unchecked, which means that remote desktop access to the VM is disabled.
Server field	Enter the IP address of the server for remote access. **Note** This field appears when **Remote Desktop Access Configuration Enable** is checked.
Port field	Enter the port number on the server for remote access. **Note** This field appears when **Remote Desktop Access Configuration Enable** is checked.
Label field	Enter the label that is defined for this remote access. **Note** This field appears when **Remote Desktop Access Configuration Enable** is checked.

Name	Description
VMRC Console Configuration Enable check box	Check the box to enable VMRC console access to the VM. By default, this check box is unchecked, which means that the VMRC console access to the VM is disabled.

Step 14 Click **Next**.

Step 15 Review the catalog information on the **Add Catalog: Summary** screen.

Step 16 Click **Submit**.

About Publishing Advanced Catalogs

When you choose the Advanced catalog type, you can provision workflow catalogs. End users can execute workflows with these catalogs during a Service Request. You create an Advanced Catalog Item by defining parameters such as Group Name and Workflow.

Publishing Advanced Catalogs

Procedure

Step 1 Choose **Policies** > **Catalogs**.

Step 2 On the **Catalog** page, click **Add**.

Step 3 In the **Catalog Add** screen, from the **Catalog Type** drop-down list, select **Advanced**.

Step 4 Click **Submit**.

Step 5 In the **Add Catalog** screen, complete the required fields, including the following:

Name	Description
Basic Information Pane	
Catalog Name field	The name of the catalog.
Catalog Description field	The description of the catalog.
Catalog Type	Choose **Advanced**.
Catalog Icon drop-down list	Choose the icon to associate this catalog with an image. The icon is seen when creating a service request using this catalog.
Applied to all groups check box	Check the check box to enable all groups to use this catalog. By default, this check box is not checked, which means that all groups cannot use this catalog.

Name	Description
Support Contact Email Address field	The email address of the support contact person.
Selected Groups	Click **Select** and complete the following: **a.** (Optional) Click **Check All** to choose all of the categories or click **Check None** to deselect all categories. **b.** From the **Select Items** dialog box, check the appropriate groups to include. The checked groups can use this catalog to provision new VMs. **c.** Click **Select** to finish your selection of categories.
Publish to end users check box	By default, this check box is checked, which means that the catalog is available to end users. Uncheck this check box if you do not want this catalog to be visible to end users.
Select Folder drop-down list	Choose the folder within which this catalog must be created in. **Note** The drop-down list includes names of folders that are already available. You can either select a folder that is available, or click the + icon to create a new folder. To create a new folder in the **Add New Folder** dialog box, specify a folder name, and select an icon for the folder.
Configure Service Request Support Email field	Check this check box to specify the email address to which the service request status email must be sent to.

Step 6 Click **Next**.

Step 7 In the **vApp Workflow** pane, click **Workflow Select**.

Step 8 In the **Select** pane, check the check box next to the appropriate workflow.

Step 9 Click **Select**.

Step 10 Review the catalog information on the **Summary** page.

Step 11 Click **Submit**.

Creating a Bare Metal Server Catalog

Before you begin

You should have created a bare metal provisioning policy.

Procedure

Step 1 Choose **Policies** > **Catalogs**.

Step 2 On the **Catalog** page, click **Add**.

Step 3 In the **Add Catalog** screen, choose **Bare Metal** as the Catalog Type.

Step 4 Click **Submit**.

Step 5 In the **Add Catalog** screen, complete the required fields, including the following:

Name	Description
Basic Information pane	
Catalog Name field	Enter a name of the catalog. **Note** Once created, a catalog name cannot be modified.
Catalog Description field	Enter a description of the catalog.
Catalog Type drop-down list	This field cannot be edited. It displays Bare Metal.
Catalog Icon drop-down list	Choose from a list of icons to associate this catalog with an image. This icon is seen when you are creating a service request using this catalog.
Applied to all groups check box	Check the check box to enable all groups to use this catalog. Leave it unchecked to deny its use to other groups.
Support Contact Email Addresses field	Specify the email address of the support contacts. These users will receive email notifications on the status of the bare metal server provisioning using the catalog. **Note** This notification email is also sent to the user who initiates the bare metal server provisioning.
Selected Groups check box list	Check the check boxes for included groups that are from the **Select Items** dialog box. The checked groups use this catalog to provision new bare metal servers.

Name	Description
Publish to end users check box	By default, this check box is checked. Uncheck this check box if you do not want this catalog to be visible to end users. If you do not uncheck this check box, then this catalog is visible to the end users of the system.
Select Folder drop-down list	Choose the folder within which this catalog must be created. **Note** The drop-down list includes names of folders that are available by default. You can either select a folder that is available, or click the + icon to create a new folder. To create a new folder in the **Add New Folder** dialog box, specify a folder name, and select an icon for the folder.
Bare Metal Server Provisioning Policy drop-down list	Choose a bare metal provisioning policy.
Configure Service Request Support Email check box	By default, this check box is unchecked. Check this check box to specify an email address to which the status of the service request must be emailed to.

Step 6 Click **Next**.

Step 7 In the **Bare Metal Workflow** pane, click **Select** to choose a bare metal server provisioning workflow.

To create a bare metal workflow, you will need to include the following set of tasks at a minimum:

- The Bare Metal Provisioning wrapper
- Select UCS Server
- Create UCS Service Profile from Template
- Associate UCS Service Profile
- Setup PXE Boot With BMA Selection
- Power On UCS Server
- Monitor PXE Boot
- Modify UCS Service Profile Boot Policy
- Power On UCS Server
- Assign UCS Server to Group

Step 8 Click **Next**.

Step 9 Review the catalog information in the **Summary** pane.

Step 10 Click **Submit**.

What to do next

Using this catalog, you can create a service request for bare metal servers.

Reordering Catalogs Within a Folder

By default the catalogs within a folder are listed alphabetically, but you can customize the order.

Procedure

Step 1 Choose **Policies** > **Catalogs**.
Step 2 On the **Catalog** page, expand a folder to view the catalogs within it.
Step 3 Select a catalog from the list.
Step 4 Click the **Move Up** or **Move Down** options to reorder the catalogs.

Accessing Hosts for Deployment

You can choose a catalog item to assess deployable hosts and provide a reason for hosts that are excluded. You can determine if you want to run this assessment on all configured VDCs, or on certain specific VDCs.

Procedure

Step 1 Choose **Policies** > **Catalogs**.
Step 2 On the **Catalog** page, choose a **Catalog Entry** to assess.
Step 3 Click **Deployability Assessment**.
Step 4 In the **Select vDC** screen, complete the required fields, including the following:

Field	Description
Run Assessment Across all VDCs check box	By default, this check box is checked, which indicates that this catalog item will be assessed with all VDCs. Uncheck this check box to select specific VDCs.
Select VDC field	Click **Select** to check the check boxes of the VDCs against which you want the catalog item assessed. The list displays all the vDCs associated with the user group for the selected catalog.

Step 5 Click **Submit**.

Step 6 View the **Deployability Assessment** report and the click **Close**.

Reordering Catalog Folders

By default the catalog folders are listed alphabetically, but you can customize the order.

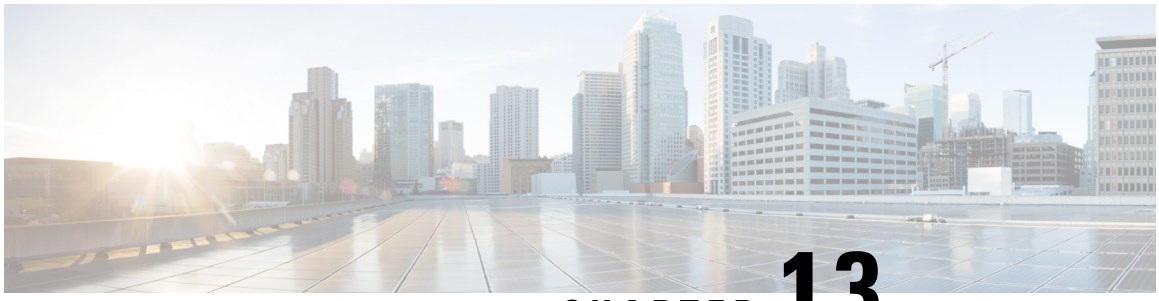
Procedure

Step 1 Choose **Policies** > **Catalogs**.

Step 2 Click **Manage Folder**.

Step 3 In the **Manager Folder** screen, select a catalog folder and use the arrows to reorder the folders.

Step 4 Click **Submit**.



CHAPTER 13

Using Self-Service Provisioning

This chapter contains the following sections:

- Self-Service Provisioning, on page 315
- Service Requests, on page 315
- Service Request Workflow and Details, on page 327
- About Scheduling a Service Request, on page 331
- About Resubmitting a Service Request, on page 331
- Other Service Request Functions, on page 332
- Service Request Approval Process, on page 339
- Service Request Budgeting, on page 341

Self-Service Provisioning

You can provision virtual machines (VMs) or applications through self-service provisioning. To provision a VM or an application using self-service provisioning, you must first create a service request. This action initiates a VM-creation workflow that includes the following:

- Budget validation
- Dynamic resource allocation
- Approval
- Provisioning
- Lifecycle setup
- Notification about the status of service requests

Service Requests

You can use the self-service provisioning feature to create a service request to provision virtual machines (VMs), services, or applications. The service request process produces a provisioning workflow for VM creation that includes the following actions:

- Budget validation

- Dynamic resource allocation
- Approvals
- Provisioning
- Lifecycle setup and notification

Note If you change the number of CPU Cores or memory allocation while in the **Deployment Configuration** screen, the total cost is automatically updated and displayed.

To provision a VM or execute an orchestration workflow, you must first create a service request. If desired, you can require approval from one or two administrators or designated users before the VM is provisioned or the workflow executed. VMs can be immediately approved or scheduled to be approved within a maximum of 90 days from the original request.

Creating a Service Request with Catalog Type—Standard

Procedure

Step 1 Choose **Organizations** > **Service Requests**.

Step 2 On the **Service Requests** page, click **Service Requests**.

Step 3 Click **Create Request**.

Step 4 On the **Create Request** screen, choose **Standard** as the catalog type.

Step 5 Click **Submit**.

Step 6 On the **Create Service Request** screen, complete the following fields:

Name	Description
Catalog Selection Request Screen	
VM Ownership	
Customer Organization radio button	Select this radio button to choose the customer organization for which a VM is provisioned.

Name	Description
Customer Organizations field	Click **Select** to choose the customer organizations for which you want to provision the VM. Customer organizations that have valid vDCs are displayed. **Note** This field is visible only when you select the **Customer Organizations** radio button. If you chose **Create Service Request** from the **Catalog** screen, then the group list that is displayed is dependent on the user groups you select in the left pane
User radio button	Select this radio button to choose the users to whom you want a VM is provisioned.
User field	Click **Select** to choose the users to whom you want to provision the VM. This list is populated with users from groups which allow resource assignment to users. **Note** Currently, only VMs that are in a VMware cloud can be assigned to a specific end user. If you chose **Create Service Request** from the **Catalog** screen, then the user list that is displayed is dependent on the user groups you select in the left pane.
VM Access Sharing	
Users with Access Privilege field	Click **Select** to choose users who can only access VM information. The selected users can only access the VM. They cannot perform any administrative tasks.
Users with Manage Privilege field	Click **Select** to choose users who can only manage the VM. The selected users can perform administrative tasks on the VM.

Name	Description
Catalog Type drop-down list	Displays the catalog type. It can be one of the following: • **Standard** • **Advanced** • **Service Container** • **VDI** **Note** **Advanced** is used for Orchestration Workflow.
Select Catalog drop-down list	Choose the catalog that is used for VM provisioning. If you chose **Create Service Request** from the **Catalog** screen, then you cannot select a catalog.
Perform deployment assessment check box	Check this check box to perform an assessment of the budget allocation, resource limits and resource availability prior to submitting a service request. After you check this check box, the summary of the assessment is displayed in the **Deployment Assessment** pane. **Important** This option is visible only for VMware catalogs, and for catalogs that are not ISO-based.

Step 7 Click **Next**.

Step 8 On the **Provisioning Configuration** screen, complete the following fields:

Name	Description
Select vDC drop-down list	Choose a vDC for the service request.
VM Name field	Specify a name for the VM. If you do not specify a name, the system will automatically generate a VM name.
Guest OS field	Click **Select** to choose a Guest OS for the service request.
Number of vCPUs drop-down list	Choose the number of vCPUs from the drop-down list. This field is populated and editable only if you checked **Allow Resizing of VM** while creating the VMware computing policy.

Name	Description
Memory drop-down list	Choose the memory capacity from the drop-down list. This field is populated and editable only if you checked **Allow Resizing of VM** while creating the VMware computing policy.
Category field	Click **Select** to choose an application category that is different from the one specified while creating the catalog.

Step 9 Click **Next**.

Step 10 On the **Deployment Configuration** screen, complete the following fields:

Name	Description
Select VDC drop-down list	The VDC on which the VM is provisioned. VDCs are defined by the administrator.
VM Name or VM Prefix field	The VM name or prefix.
Comment field	Any comments relating to the deployment configuration.
Provision drop-down list	Choose either **Now** or **Later**. Choose **Now** to set provisioning for any time within the next 90 days. When you choose **Later**, a calendar for the Day, drop-down lists for the Hour and Minute, and radio buttons for AM or PM appear.
Days calendar	The number of days after which the VM is terminated. **Note** This option appears when **Power OFF the VM After** is checked.
Hours drop-down list	Choose the number of hours after which the VM is terminated. **Note** This option appears when **Power OFF the VM After** is checked.
Minutes drop-down list	Choose the number of minutes after which the VM is terminated. **Note** This option appears when **Power OFF the VM After** is checked.

Name	Description
Lease Time check box	Check to indicate that a lease time is configured for the VM.
Default Cost Computation Period Settings **Important** If you checked the **Disable displaying cost details** check box while adding or modifying the VDC, then this information is not displayed.	
Charge Duration drop-down list	Choose a duration for which the cost is calculated. By default, this duration is set to **Monthly**.
Month field	Specify the number of months to be included in the cost computation **Note** This field is displayed only when you select **Monthly** in the **Charge Duration** drop-down list.
Day field	Specify the number of days to be included in the cost computation **Note** This field is displayed only when you select **Daily** in the **Charge Duration** drop-down list.
Hours field	Specify the number of hours to be included in the cost computation **Note** This field is displayed only when you select **Hourly** in the **Charge Duration** drop-down list.

Step 11 Click **Next**.

Step 12 On the **Custom Specification** screen, complete the following fields:

Name	Description
CPU Cores drop-down list	Choose the CPU cores for the VM being provisioned. **Note** This list opens if the resizing option is chosen on the **Computing Policy** screen.

Name	Description
Cores Per Socket drop-down list	Choose the cores per socket for the VM being provisioned. The number of cores per socket available is specified in the VM computing policy. The values displayed are based on the VM computing policy and the CPU count selected. The values in the **Cores Per Socket** drop-down list are divisors of the CPU count. For example, if the CPU count is 4, and the allowed sockets per core specified in the VM computing policy are 1, 2, 3, and 4, the **Cores Per Socket** drop-down list displays 1, 2, and 4 as available options.
Memory drop-down list	Choose the amount of memory for the VM being provisioned. **Note** This list opens if the resizing option is chosen on the **Computing Policy** sreen.
Approximate SR Cost Estimate field	Displays an approximate SR cost based on the values you provided in the **Default Cost Computation Period Settings** fields. **Important** If you checked **Disable displaying cost details** while adding or modifying the VDC, then this information is not displayed.
Storage Tier drop-down list	Choose an option to customize storage entries for the VM being provisioned. **Note** This custom list opens if the Virtual Storage Catalog was enabled when the chosen catalog was created. See more information about the creation of a virtual storage catalog in Policies, on page 207. See more information about enabling this option during catalog creation in About Managing Catalogs, on page 299.

Name	Description
Disk Datastores table	Choose the preferred hard disk size for VM provisioning. The list of available datastores depends upon the scope conditions specified in the storage policy. You can enable or disable this option in the storage policy. Choose a disk from the table, and click the pencil icon to select a datastore. **Note** You can edit the size of the disk if you have enabled the **Allow Resizing of Disk** option in the storage policy.

Step 13 To choose a datastore for a disk, choose a disk from the list and click the Pencil icon.

Step 14 Click **Select** to view available datastores.

Step 15 Choose a datastore from the list and click **Select**.

Step 16 Click **Submit**.

Step 17 (Optional) For templates with multiple disks, you must choose a datastore for each disk.

Step 18 On the **Custom Specification** screen, click **Select** to view available VM Networks.

Note
This option is available only if **Allow end user to select optional NICs** or **Allow end user to choose portgroups** are checked in the network policy associated with the VDC selected for this VM provisioning service request. For more information, see Adding a Network Policy, on page 230.

Step 19 Choose a VM Network from the list and click **Select**.

Step 20 Click **Next**.

Step 21 Complete the details on the **Custom Workflow** screen.

Note
Custom workflow inputs apply if the catalog chosen for VM provisioning has Post Provisioning Custom Actions enabled. In this procedure, the post-provisioning workflow allows users to specify custom inputs.

Step 22 Click **Next**.

Note
The list of available datastores depends upon the scope conditions specified in the storage policy. You can choose only one datastore for each disk category (System, Data, Database, Swap, and Log).

Step 23 Required: If you checked **Perform deployment assessment**, then review the report of the assessment displayed on the **Deployment Assessment** screen.

If this assessment report identifies errors, then you must return to the previous panes and rectify the errors before submitting the request. If the assessment report shows no errors, then click **Next**.

Step 24 Review the summary for the service request.

Step 25 Click **Submit**.

Creating a Service Request with Catalog Type—Advanced

By choosing the advanced catalog type during the creation of a service request, you can execute orchestration workflows. The steps for creating an advanced catalog are much the same as those for creating a standard catalog.

Procedure

Step 1 Choose **Organizations** > **Service Requests**.

Step 2 On the **Service Requests** page, click **Service Requests**.

Step 3 Click **Create Request**.

Step 4 In the **Create Request** screen, choose **Advanced** as the catalog type.

Step 5 Click **Submit**.

Step 6 On the **Catalog Selection** screen, choose the **Group**, **Catalog Type** (Advanced), and the **Catalog** (workflow).

Step 7 Click **Next**.

Step 8 On the **Custom Workflow** screen, provide the custom workflow input values.

If you want to provision a VM using this service request, then you must select a standard catalog in this screen. If you select an advanced catalog, then VM provisioning will fail.

Step 9 Click **Next**.

Step 10 Review the summary of the service request.

All information that you entered in the previous screens is displayed in this summary screen.

Note
While provisioning a VM with a service request using an advanced catalog, be sure to have included the following information while creating the service request:

- Include the following workflow tasks in the VM provisioning workflow:
  - VMware VM Provision Inputs
  - Resource Allocation Configuration
  - VM Provision Engine
- Include the following custom workflow inputs of respective input types:
  - vDC
  - Catalog or image
- The **Disable displaying cost details** check box is not checked.

If all of these conditions are met, the summary screen of the service request will display the approximate service request cost.

Step 11 Click **Submit**.

Creating a Service Request with Catalog Type—Bare Metal

Before you begin

You should have created a bare metal catalog, and a provisioning policy.

Procedure

Step 1 Choose **Organizations** > **Service Requests**.

Step 2 On the **Service Requests** page, click **Service Requests**.

Step 3 Click **Create Request**.

Step 4 On the **Create Request** screen, choose **Bare Metal** as the catalog type.

Step 5 Click **Submit**.

Step 6 On the **Create Service Request** screen, complete the required fields, including the following:

Name	Description
Catalog Selection pane	
Select Group drop-down list	Select a user group from the list of groups that already exist in the system.
Catalog Type drop-down list	You cannot edit this field. It displays Bare Metal.
Select Catalog drop-down list	Select a catalog from the drop-down list. It displays the list of bare metal catalogs you created.
Perform Deployment Assessment check box	Check to run a deployment assessment with the specified information.

Step 7 Click **Next**.

Step 8 On the **Bare Metal Deployment Configuration** screen, complete the required fields, including the following:

The following table lists the fields displayed for Cisco UCS Manager accounts.

Name	Description
Server drop-down list	While creating the bare metal provisioning policy, if you checked **Allow Users to Select Servers**, then you can use this drop-down list to choose the servers on which you want the server provisioned. After you select a server, resource information such as CPU, memory and Storage details displayed. This information is displayed only if you checked **Show Server Resources to User** while creating the bare metal server provisioning policy. **Note** If you did not check **Allow Users to Select Servers**, then this field is not editable. It is populated with the server name that matches the criteria specified in the provisioning policy.
Charge Duration drop-down list	Choose a duration for which the cost is calculated. By default, this duration is set to **Monthly**.
Month field	Specify the number of months to be included in the cost computation. **Note** This field is displayed only when you select **Monthly** in the **Charge Duration** drop-down list.
Day field	Specify the number of days to be included in the cost computation. **Note** This field is displayed only when you select **Daily** in the **Charge Duration** drop-down list.
Hours field	Specify the number of hours to be included in the cost computation. **Note** This field is displayed only when you select **Hourly** in the **Charge Duration** drop-down list.
Approximate SR Cost Estimate field	Click the **Compute SR Cost Estimate** option to view the cost estimate. This cost estimate calculated based on the information that you have entered on this screen.

Attention
If a cost model is not associated with the provisioning policy, then all cost-related fields such as **Charge Duration**, and the **Approximate SR Cost Estimate** fields are not displayed. If a cost model is associated with the policy, then these fields are displayed.

If you are creating a service request for Cisco UCS Central accounts, complete the required fields, including the following:

Name	Description
Domain Group drop-down list	You can choose a domain group. The available groups are determined by the domain groups selected in the bare metal server provisioning policy.
Domain Name drop-down list	This list displays the domain names that were selected in the bare metal server provisioning policy.
Server drop-down list	This list displays the servers that are available in the chosen domain name.
CPU field	Displays the CPU details.
Memory field	Displays memory information.
Storage field	Displays storage-related information. This field is not editable.
OS image drop-down list	Choose an OS image from the drop-down list. This field is populated based on the domain mapping parameters specified in the bare metal server provisioning policy. By default, Target BMA and OS Image selected in the policy are used for provisioning. However, if you have specified any domain mapping parameters in the policy, then the OS image selected in the mapped domains takes preference over the default images.

Step 9 On the **Custom Workflow** screen, specify a Service Profile name.

Step 10 Click **Next**.

Step 11 Review the deployment assessment summary for the service request.

This information is displayed only if you checked **Perform deployment assessment** on the **Catalog Selection** screen.

Step 12 Review the summary for the service request.

Step 13 Click **Submit**.

What to do next

After you click **Submit**, the workflow is triggered, and the bare metal servers are provisioned. After the workflow is completed, the bare metal server is displayed in the selected group. In addition, the chargeback cycles are initiated for the servers.

If you want to change the cost model for the server, then you must edit the cost model selection in the bare metal provisioning policy.

Service Request Workflow and Details

After you create a service request, you can check its status and workflow, cancel the request, resubmit the request, and so on. These actions are controlled by the toolbar buttons at the top of the service request lists.

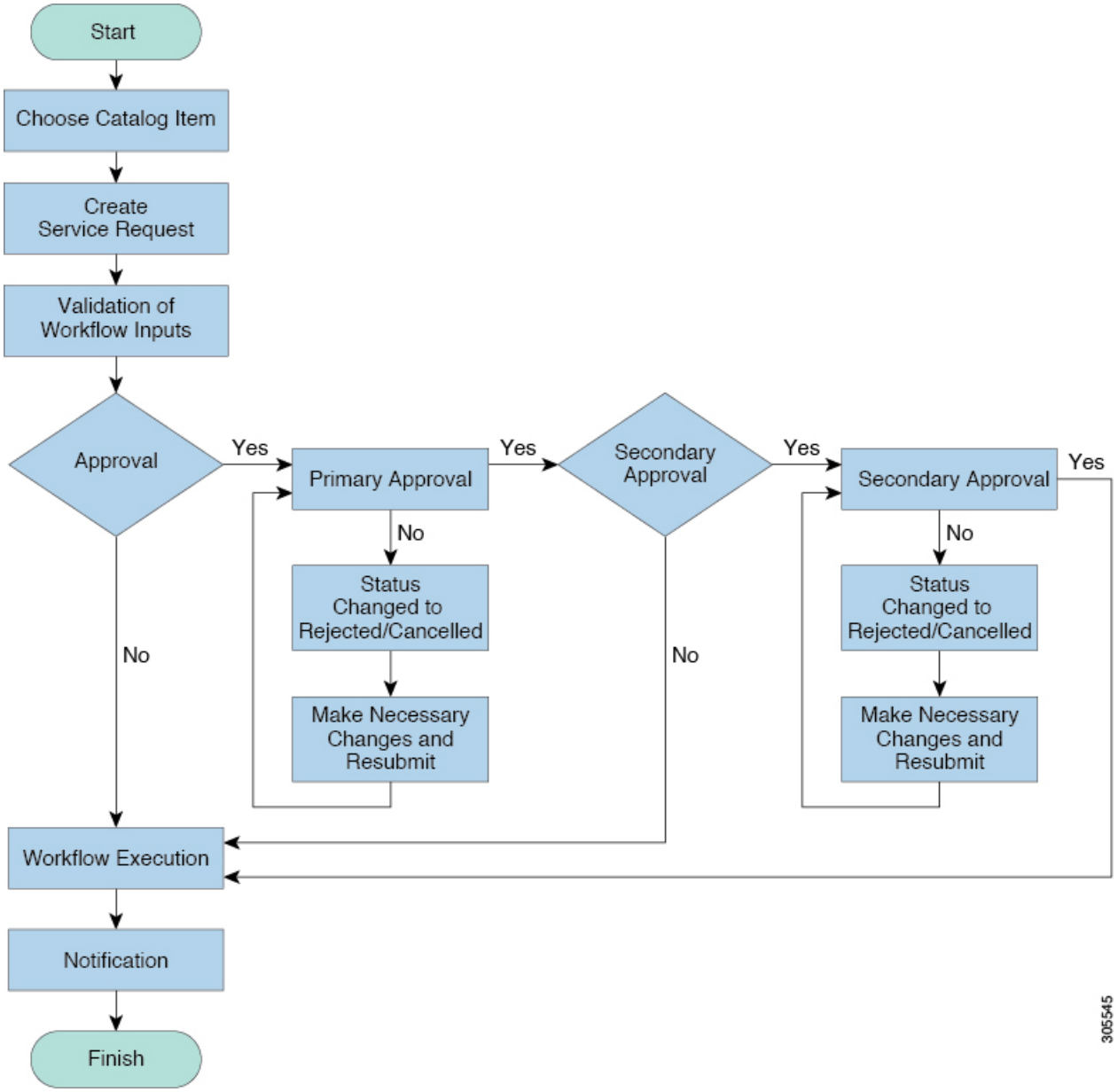
Service Request Workflow

The **Workflow Status** box displays details about the service request and the workflow steps. A typical service request workflow to provision a VM includes the following steps:

1. Initiation—Service request is initiated by the user.
2. Resource Allocation—Required resources, such as virtual compute, are allocated to the VM.
3. Approval—VM provisioning is approved, if required. During this step, an email is sent to the approvers defined in the catalog chosen for VM provisioning. If you selected user groups for approval, then an email is sent to all users in the selected groups.
4. Provision—VM is created and provisioned.
5. Set Up Lifecycle Schedule—Lifecycle scheduling is configured with the setup, scheduled times, and termination times.
6. Notify—User is notified by email that the VM has been created and provisioned.

Following is a graphical representation of the workflow.

Figure 3: Catalog Service Request Workflow



Optional service request workflow steps include Budget Watch and Check Resource Limits:

- Budget Watch—An administrator has to enable budgeting for a group. This step determines if a sufficient budget is available for provisioning a new VM in that group.
- Check Resource Limits—Resource limits for a group must be enabled by an administrator. This step determines if sufficient resources are available for provisioning a new VM in that group.

Any user who has been assigned the **Read-Group Service Request** permission can view the progress of a service request.

Service Request Details

Service Request details include items under Overview, Ownership, Catalog Information, and the Current Status of the service request, as follows:

Name	Description
Overview	
Request ID	The service request ID number.
Request Type	The type of request (in this case, creating a VM).
VDC	The VDC where the VM is provisioned.
Image	The image from which the VM is provisioned.
Request Time	The time of the service request creation.
Request Status	The status of the service request as Complete, Canceled, Failed, and so on.
Comments	Any comments.
Ownership	
Group	The group to which the service request initiating user belongs.
Initiating User	The user who has initiated the service request.
Duration Hours	The amount of time that the VM is active. If this time is defined, the VM is deleted after the specified time.
Scheduled Time	The time at which the VM is provisioned. If defined, the VM is provisioned at 6 a.m. on the scheduled date. If not defined, the VM is provisioned when the workflow steps for the service request are complete.
Catalog Information	
VDC Owner Email	The email ID provided by the administrator when creating a VDC.
Approving Users	The user (if defined) who must approve the service request for VM provisioning.
Catalog Name	The catalog item name from which the VM is provisioned.
Catalog Description	The catalog item description.
Service Request Cost	The cost (projected) of provisioning the VM. This cost is determined based on the Cost Model that is defined for the catalog item.

You can view the status of each workflow step. Details such as warning or error messages and the time of the request are also displayed. The workflow steps are color-coded to indicate their status:

Color Code	Description
Gray	The step is incomplete.
Green	The step completed successfully.
Red	The step failed. The reason for failure is also described.
Blue	More input is required for the step to complete. For example, an approver was defined for a service request, and until the request is approved, this step is incomplete.



Note Approvers may look under the **Approvals** tab to see their assigned service requests.

Viewing the Workflow Status of a Service Request

Procedure

Step 1 Choose **Organizations** > **Service Requests**.

Step 2 Choose a user group.

The default is **All User Groups**, which lists all service requests.

Step 3 On the **Service Requests** page, click **Service Requests**.

Step 4 Click the row with the service request for which you want to view the workflow status.

Step 5 Click **View Details** and click **Workflow Status** to see the details and status of the service request.

Viewing Log Details for a Service Request

Procedure

Step 1 Choose **Organizations** > **Service Requests**.

Step 2 Choose a user group.

The default is **All User Groups**, which lists all service requests.

Step 3 On the **Service Requests** page, click **Service Requests**.

Step 4 Click the row with the service request for which you want to view the service request log.

Step 5 Click **View Details**, and click **Log**.

About Scheduling a Service Request

You can schedule VM provisioning for a later date using Deferred Provisioning. The default provisioning is at 8.30 a.m. on the date of scheduling. Once a new date is set, the VM provisioning status in the workflow displays the change.

Scheduling Service Requests

Procedure

Step 1 Choose **Organizations** > **Service Requests**.

Step 2 On the **Service Requests** page, click **Service Requests**.

Step 3 Click **Create Request**.

Step 4 Choose the group, catalog type, and catalog. See Creating a Service Request with Catalog Type—Standard, on page 316.

Step 5 Click **Next**.

Step 6 Choose the **Later** option for the **Provision** field, and the provisioning date on the **Service Request** screen.

Step 7 Click **Next** until the **Summary** screen appears.

Step 8 Click **Submit**.

About Resubmitting a Service Request

You can resubmit a failed service request. A service request could fail for the following reasons:

- Budget limit (if defined by administrator) is exceeded for the group under which the VM is being provisioned.
- Resource limits (if defined by administrator) are exceeded for the group under which the VM is being provisioned.
- Provisioning could fail if a service request lacks relevant information.

When a service request is resubmitted, the process starts again from the workflow step that failed in the earlier submissions. For example, if a service request fails in the Resource Allocation workflow (Step 2), when this service request is resubmitted, the process is re-initiated from that step.

Resubmitting a Service Request

Procedure

Step 1 Choose **Organizations** > **Service Requests**.

Step 2 Choose a user group.

The default is **All User Groups**, which lists all service requests.

Step 3 On the **Service Requests** page, click **Service Requests**.

Step 4 Click the row with the service request to that you want to resubmit.

Step 5 Click **Resubmit Request**.

Other Service Request Functions

Canceling a Service Request

As an administrator in the system, you can cancel any service request that has been created. If you are an MSP admin, or a group admin, you can cancel service requests that you have created, and those created by users in member groups that you manage.

Procedure

Step 1 Choose **Organizations** > **Service Requests**.

Step 2 Choose a user group.

The default is **All User Groups**, which lists all service requests.

Step 3 On the **Service Requests** page, click **Service Requests**.

Step 4 Click the row with the service request that you want to cancel.

Step 5 Click **Cancel Request**.

Step 6 Click **Submit** to cancel the service request.

Rolling Back a Service Request

You can roll back a service request when a service request is created using orchestration workflow or fenced container deployment.

Procedure

Step 1 Choose **Organizations** > **Service Requests**.

Step 2 Choose a user group.

The default is **All User Groups**, which lists all service requests.

Step 3 On the **Service Requests** page, click **Service Requests**.

Step 4 Click the row with the service request that you want to roll back.

Step 5 From the **More Actions** drop-down list, choose **Rollback Request**.

Step 6 On the **Rollback Service Request** screen, select the tasks in the service requests that must be rolled back.

By default, all of the tasks in the service request are checked.

Step 7 (Optional) Check **Abort rollback, if any rollback task fails**.

Step 8 Click **Submit**.

Archiving a Service Request

Procedure

Step 1 Choose **Organizations** > **Service Requests**.

Step 2 Choose a user group.

The default is **All User Groups**, which lists all service requests.

Step 3 On the **Service Requests** page, click **Service Requests**.

Step 4 Click the row with the service request that you want to archive.

Step 5 Click **Archive**.

Step 6 On the **Archive Request** screen, click **Archive**.

On the **Service Requests** page, you can click **Archived Service Requests** to view all the archived requests.

What to do next

If you need to use this archived service request at a later time, you can re-instate it. For more information, see Reinstating an Archived Service Request, on page 338.

Bulk Archiving Service Requests

Procedure

Step 1 Choose **Organizations** > **Service Requests**.

Step 2 Choose a user group.

The default is **All User Groups**, which lists all service requests.

Step 3 On the **Service Requests** page, click **Service Requests**.

Step 4 Click **Bulk Archive**.

Important
Service requests with locked and in-progress state cannot be archived.

Step 5 On the **Bulk Archive** page, select the required option from the **Bulk Archive** drop-down list. The options include:

- Service Request Range: Specify the service request IDs separated by a comma, in one of the following:
  - Individual SR IDs, for example, 8, 9, 15, 77
  - Range of SR IDs, for example, 44-68, 108-332
  - Combination of a range and individual SR IDs, for example, 23-44, 55-90, 66, 8
- Date: All the services requests which have been triggered before the selected date are archived.
- Status: Service requests are archived based on the status selected. You can select any of the following status:
  - Completed Service Requests
  - Failed Service Requests
  - Canceled Service Requests
- Status with Range: Service requests are archived based on the status selected and the service request IDs specified.

  You can select any of the following status:
  - Completed Service Requests
  - Failed Service Requests
  - Canceled Service Requests

  You can specify the service request IDs separated by a comma, in one of the following:
  - Individual SR IDs, for example, 8, 9, 15, 77
  - Range of SR IDs, for example, 44-68, 108-332
  - Combination of a range and individual SR IDs, for example, 23-44, 55-90, 66, 8

- Date with Range: Service requests are archived based on the date selected and the service request IDs specified. All the services requests which have been triggered before the selected date are archived.

  You can specify the service request IDs separated by a comma, in one of the following:

  - Individual SR IDs, for example, 8, 9, 15, 77
  - Range of SR IDs, for example, 44-68, 108-332
  - Combination of a range and individual SR IDs, for example, 23-44, 55-90, 66, 8

Based on the option selected, the input field is displayed.

Step 6 Specify the field.

A message screen, that shows the total number of service requests to be archived, appears.

Step 7 Click **Archive**.

A confirmation message that the service requests archived successfully appears on top of the screen.

What to do next

You can view archived service requests in the **Archived Service Request** page. You can use the **Unarchive** option if you want to reinstate a service request back to the **Service Request** screen.

Deleting Service Requests

You can delete archived service requests from Cisco UCS Director. The deleted service requests are removed permanently from Cisco UCS Director.

You can enter archived service requests to delete in one of two ways:

- By selecting the service requests on the **Archived Service Requests** screen and clicking **Delete Requests**.
- By clicking **Purge Requests** and entering the IDs of the archived service requests.

Both methods result in the permanent removal of the specified service requests. The only difference is the method of data entry.

You can delete only archived service requests. For information about archiving service requests, see the current release of the Cisco UCS Director Administration Guide. Because active service requests cannot be archived, you cannot delete service requests that are in progress, or that contain child service requests that are in progress.

You also cannot delete a service request that has a rollback that is in progress or that has failed. For example, say that you submit a rollback for service request (SR) 100 that generates a rollback service request SR 101. You cannot delete SR 100 while SR 101 is in progress. Furthermore, you cannot delete SR 100 if SR 101 fails.

To delete service requests, do the following:

Procedure

Step 1 Choose **Organizations** > **Service Requests**.

Step 2 On the **Service Requests** page, click **Archived Service Requests**.

Step 3 You can either enter service request IDs using the keyboard or choose service requests from the **Archived Service Requests** report.

To enter service request IDs, skip to the next step. To choose service requests instead, do the following:

a) Choose all the service requests that you want to delete.

Note
Select multiple items as you would in any other application on your system. For example, in Windows, hold down the **Ctrl** key to choose more items or **Shift** to choose a range of items.

When you choose one or more service requests, the **Delete Request** icon appears.

b) Click **Delete Request**.

c) On the **Delete Request** screen, click **Delete**.

Step 4 To enter service requests, do the following:

a) Click **Purge Requests**.

b) In **SR IDs** on the **Delete Request** screen, enter the IDs of the service requests that you want to delete . Use hyphens to indicate ranges of IDs and commas to separate ranges or individual IDs; for example: `101-111, 113, 116-118`.

c) Click **Delete**.

Viewing Service Requests for a Particular Group

Procedure

Step 1 Choose **Organizations** > **Service Requests**.

Step 2 Choose a user group.

The default is **All User Groups**, which lists all service requests.

Step 3 On the **Service Requests** page, click **Service Requests**.

All of the service requests for the selected user group are displayed.

Searching the Records of Service Requests for a Group

Procedure

Step 1 Choose **Organizations** > **Service Requests**.

Step 2 On the **Service Requests** page, click **Service Requests**.

Step 3 Click **Search and Replace**.

Step 4 On the **Search and Replace** screen, enter the search terms in the search fields. You must enter the following information:

- Asset Identity
- Asset Type
- New Asset Identity
- Selected SRs

Step 5 Click **Submit**.

Exporting a Report of Service Requests for a Group

Procedure

Step 1 Choose **Organizations** > **Service Requests**.

Step 2 On the **Service Requests** page, choose the user group.

Step 3 On the **Service Requests** page, click **Service Requests**.

Step 4 Click **Export Report**.

Step 5 On the **Export Report** screen, choose the report format.

The report format can be PDF, CSV, or XLS.

Step 6 Click **Generate Report**.

After the report is generated, the **Download** option appears.

Step 7 Click **Download** to open the report and to save it on your system.

Reinstating an Archived Service Request

Procedure

Step 1 Choose **Organizations** > **Service Requests**.

Step 2 On the **Service Requests** page, click **Archived Service Requests**.

Step 3 Click the row with the service request that you want to reinstate.

Step 4 Click **Unarchive**.

Launching the Service Request Quick View

The header pane of the Cisco UCS Director graphical user interface displays an icon that launches the Quick View panel for service requests. This **Service Request Quick View** panel includes sections which display 25 of the most recent service requests that are in the following states:

- In-Progress
- Completed Successfully
- Failed

If there are no service requests for a particular status in the system, then that section is not displayed in the **Service Request Quick View** panel. For example, if there are no failed service requests in the system, then the **Service Request Quick View** panel does not display the **Failed Service Requests** section. Also, if there are no service requests that are either in the running, completed, or failed state, then the icon to launch the **Service Request Quick View** panel is not displayed on the header pane.

Note This feature is not available in Cisco UCS Director instances that have been cross-launched from Cisco Intersight.

Procedure

Step 1 On the header pane, click the icon to launch the **Service Request Quick View** panel.

The **Service Request Quick View** panel is displayed on the far right of the screen.

Step 2 Click on any of the following panels to view details of the service requests:

- Recent In-Progress Service Requests
- Recent Completed Service Requests
- Recent Failed Service Requests

Step 3 (Optional) Click on any service request within a panel to view additional details.

Step 4 Click the icon again or on any other area of the screen to close the **Service Request Quick View** panel.

Service Request Approval Process

Before the VM is provisioned, a service request must be approved by a specified approver or approvers named in the VDC. You have an option to define one or two approvers for a group.

- Once created, the service request workflow has a step requiring VM approval that displays the name of the approver.
- A service request notification email is sent to the approvers. Approvers may view all pending requests under the **Approvals** tab.
- Once approved is granted, VM provisioning is initiated.

Note For more information about defining approvers, see Virtual Data Centers, on page 247.

Approving a Service Request

Procedure

Step 1 Choose **Organizations** > **My Approvals**.
Step 2 Click the row with the service request that you want to approve.
Step 3 (Optional) To verify the details, click **View Details**.

You can view the Workflow and Input/Output information and click **Close**.

Step 4 Click **Approve**.
Step 5 Add comments on the **Service Request** screen if necessary.
Step 6 Click **Approve**.

Rejecting a Service Request

Procedure

Step 1 Choose **Organizations** > **My Approvals**.
Step 2 Click the row with the service request that you want to reject.
Step 3 (Optional) Verify the details by clicking **View Details** and then click **Close**.

Step 4 Click **Reject**.

Step 5 Add comments on the **Service Request** screen if necessary.

Step 6 Click **Reject**.

Viewing Approval Information on Service Requests

Procedure

Step 1 Choose **Organizations** > **My Approvals**.

Step 2 Click **My Approvals**.

All approvals that are either already approved or pending approval are listed.

Searching the Records of Service Request Approvals

Procedure

Step 1 Choose **Organizations** > **My Approvals**.

Step 2 Click **My Approvals**.

All approvals that are either already approved or pending approval are listed.

Step 3 In the **Search** field, enter your search term.

The service requests that match the search criteria are displayed.

Exporting a Report of Service Request Approvals

Procedure

Step 1 Choose **Organizations** > **My Approvals**.

Step 2 Click the row with the service request for which you want to export a report..

Step 3 Click **Export Report**.

Step 4 On the **Export Report** screen, choose the report format.

The report format can be PDF, CSV, or XLS.

Step 5 Click **Generate Report**.

After the report is generated, the **Download** option appears.

Step 6 Click **Download** to open the report and to save it on your system.

Service Request Budgeting

Viewing the Current Month Budget Availability

Procedure

Step 1 Choose **Organizations** > **Service Requests**.
Step 2 On the **Service Requests** page, choose the user group.
Step 3 On the **Service Requests** page, click **Current Month Budget Availability**.

Viewing Budget Entries

Procedure

Step 1 Choose **Organizations** > **Summary**.
Step 2 On the **Summary** page, choose the user group.
Step 3 On the **Summary** page, click **Budget Entries**.

Adding a Budget Entry

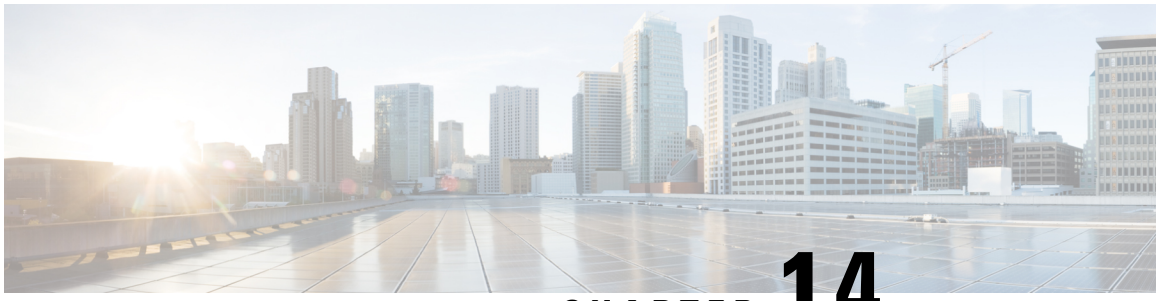
Procedure

Step 1 Choose **Organizations** > **Summary**.
Step 2 On the **Summary** page, choose the user group.
Step 3 On the **Summary** page, click **Budget Entries**.
Step 4 Click **Add**.
Step 5 On the **Add Budget Entry** screen, complete the following fields:

Name	Description
Entry Name field	The name of the budget entry.

Name	Description
Budget Amount field	The amount of the budget per month.
Year drop-down list	Choose the year.
Month drop-down list	Choose the month.
Repeat Entries drop-down list	Choose the number of months for the same amount of budget to repeat.

Step 6 Click **Add**.



CHAPTER 14

Multiple Disk VM Provisioning

This chapter contains the following sections:

- About Multiple Disk VM Provisioning, on page 343
- Overview of the Procedure for Multiple Disk VM Provisioning, on page 344
- About Templates with Multiple Disks, on page 344
- Assigning Disk Categories, on page 344
- Defining Storage Policies, on page 345
- Creating a Catalog, on page 351
- Creating a VM Disk, on page 359

About Multiple Disk VM Provisioning

Cisco UCS Director supports virtual machine (VM) provisioning of multiple disks from a template. You can configure VM disk provisioning on a preferred single datastore or on multiple datastores. You can also configure individual disk policies for each additional disk in a template.

Cisco UCS Director classifies the disks into the following categories:

- System
- Data
- Database
- Swap
- Log

Note The disk categories that are defined by Cisco UCS Director are for disk labeling only.

Overview of the Procedure for Multiple Disk VM Provisioning

Procedure

Step 1 Check for the availability of a template with multiple disks.
Step 2 Assign disk categories.
Step 3 Define the storage policy.
Step 4 Create the template catalog.

About Templates with Multiple Disks

To provision a multiple disk virtual machine (VM), a template (image) with multiple disks, must be available. Before using a template with multiple disks for VM provisioning, you must assign the disk categories for individual disks.

Assigning Disk Categories

Procedure

Step 1 Choose **Virtual** > **Compute**.
Step 2 On the **Compute** page, choose the cloud.
Step 3 On the **Compute** page, click **Images**.
Step 4 Click the row with a template with multiple disks and click **View Details**.
Step 5 Click **Disks**.
Step 6 Choose a disk.
Step 7 Click the row with the disk for which you want to assign a disk type and click **Assign Disk Type**.
Step 8 On the **Assign Disk Type** screen, choose the disk type from the drop-down list.

It can be one of the following:

- **System**
- **Data**
- **Database**
- **Swap**
- **Log**

Step 9 Click **Submit**.

Defining Storage Policies

A storage policy defines resources such as datastore scope, type of storage to use, minimum conditions for capacity, and latency. This policy also provides an option to configure additional disk policies for multiple disks, and an option to provide datastore choices for end users during a service request creation.

Cisco UCS Director supports VM provisioning with multiple disks on multiple datastores. There are five types of disks: System, Data, Database, Swap, and Log. The System disk policy is configured first, and the other disks are configured later depending on the requirements. You can configure the disk policy individually for each disk type, or choose the default system disk policy.

When using additional disk policies, be sure to uncheck the **Provision all disks in a single datastore** option during catalog creation for the multiple disk template. For more information about catalog creation, see Adding a Catalog, on page 351.

In addition, Cisco UCS Director supports datastore selection during the creation of a service request for VM provisioning. It gives you an option to enable or disable datastore selection for the end user. When a VDC is specified at creation of a service request, the scope conditions defined in its storage policy determine which datastores appear for selection here.

Note VMware VM provisioning fails when the datastore capacity specified in a storage policy uses the **equals** condition for decimal values with two values after the decimal (hundreths place). If specifying a capacity that includes decimal values, round the value up to one value after the decimal (tenths place).

See the Cisco UCS Director Troubleshooting Guide.

Creating a Storage Policy

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Storage**.

Step 2 On the **Storage** page, click **VMware Storage Policy**.

Step 3 Click **Add**.

Step 4 On the **Add Storage Resource Allocation Policy- System Disk Policy** screen, complete the following fields

Name	Description
Policy Name field	Choose the cloud in which resource allocation occurs.

Name	Description
Policy Description field	The description of the policy. If you want to narrow the scope of deployment, choose whether to use all, include selected data stores, or exclude selected data stores.
Cloud Name drop-down list	Choose the cloud account for this resource allocation. If you choose an SRM account, the **Enable Protection** check box is displayed. For more information about how to enable protection groups for Site Recovery Manager, see the Cisco UCS Director VMware Management Guide.
System Disk Scope	
Use Linked Clone check box	If you want to use a linked clone, click the check box. If you do not click this check box, the configuration uses a full clone.
Storage Profile drop-down list	Choose a storage profile if you want to provision one or more VMs with the associated storage profile.
Data Stores/Data Store Clusters Scope drop-down list	To define the scope of deployment, choose one of the following options: • **All** • **Include Selected Datastores** • **Exclude Selected Datastores** • **Include Selected Datastore Clusters** • **Exclude Selected Datastore Clusters** Depending upon which option you choose, additional fields may display. **Note** The option that you choose determines which datastores or datastore clusters are available when you create a VM disk.
Selected Data Stores field	If you chose **Include Selected Datastores** or **Exclude Selected Datastores**, click **Select** to choose the appropriate datastores.
Use Shared Data Store Only check box	Click the check box to use shared datastores only. This option is only available if you chose to include or exclude selected datastores.

Name	Description
Selected Datastore Clusters field	If you chose **Include Selected Datastore Clusters** or **Exclude Selected Datastore Clusters**, click **Select** to choose the appropriate datastore clusters.
Select SDRS Rule Type drop-down list	If you chose to include or exclude selected datastore clusters, choose one of the following SDRS rule types: • **Keep VMDKs Together**—You need to select an existing rule on the filtered clusters. The newly provisioned VM is added to the VM anti-affinity rule. • **Separate VMDKs**—If the newly provisioned VM contains more than one disk, a new VM affinity rule is created on the datastore cluster.
Select SDRS Rule field	If you chose **Keep VMDKs Together**, you must choose the VMs that you want to apply the rule to.
Storage Options	
Use Local Storage check box	By default, the field is checked. Uncheck the check box if you do not want to use local storage.
Use NFS check box	By default, the field is checked. Uncheck the check box if you do not want to use NFS storage.
Use VMFS check box	By default, the field is checked. Uncheck the check box if you do not want to use VMFS storage.
Use SAN check box	By default, the field is checked. Uncheck the check box if you do not want to use SAN storage.

Name	Description
Filter Conditions check boxes	To add one more conditions to filter the datastores, do the following for each desired condition: • Click the appropriate check box. • Choose the desired option from the drop-down list. • Enter the criteria by which you want to filter the datastores. Any datastores that do not meet these criteria are excluded from consideration. If more than one condition is chosen, all conditions must match. **Note** VMware VM provisioning fails when the datastore capacity specified in a storage policy uses the **equals** condition for decimal values with two values after the decimal (hundreths place). If specifying a capacity that includes decimal values, round the value up to one value after the decimal (tenths place). For example if the value is 10.25 GB, it displays as 10.3 GB in the datastore report. For all options, you must specify any value less than 10.3 but rounded to one value after the decimal, such as 10.2 GB, 10.1 GB, or 10 GB.
Override Template check box	Check the check box to override the template properties. You are provided with options to enter custom settings, such as using thin provisioning or setting a custom disk size.
Use Thin Provisioning check box	Check the check box to use thin provisioning during VM storage provisioning. Thin provisioning enables dynamic allocation of physical storage capacity to increase VM storage utilization. This option is only available if you choose **Override Template**.
Manual Disk Size	A custom disk size that overrides the disk size of the template used for VM provisioning. This option is only available if you choose **Override Template**.
Resizing Options for VM Lifecycle	
Allow Resizing of Disk check box	Check the check box to provide the end user with an option to choose the VM disk size before provisioning.

Name	Description
Permitted Values for Disk in GB field	Specify the disk size values that can be chosen while provisioning a VM. You can specify these values in one of the following formats: • Range such as 10-1000 • Comma separated values such as 1, 5, 10, 50, 100, 500, 1024, 5120, 10240. • Combination of range and comma separated values such as 1,5,10, 10-1000. This option is only available if you choose **Allow Resizing of Disk**.
Allow user to select datastores from scope check box	Check the check box to provide the end user with an option to choose the datastore during the service request creation.

Step 5 Click **Next**.

Step 6 On the **Additional Disk Policies** screen, do one of the following:

- Choose a disk type to configure if you do not want to use the same disk policy for that disk type as you configured in the System Disk Policy.
- Click **Next** if you want to use the System Disk Policy options for all disk types.

Note
By default, the disk policy for the disk is the same as in the System Disk Policy that you configured on the **Add Storage Resource Allocation Policy** screen.

Step 7 If you chose to configure a custom system disk policy for a specific disk type, do the following:

a) Click the row with the policy you want to edit, and click **Edit** to edit the disk type.
b) On the **Edit Policies Entry** screen, uncheck **Same as System Disk Policy**.
c) On the **Edit Entry** screen, complete the fields.

All the fields displayed here are the same as the fields displayed in the **Add Storage Resource Allocation Policy** screen.

Note
This configuration determines which datastores are available for the disk type when you create a VM disk.

d) Click **Submit**.
e) Repeat these steps to configure the other disk types, if desired.

Note
To use the storage policy created with additional disk policies, you must associate the policy with the VDC that is used for the VM provisioning

Step 8 Click **Next**.

Step 9 On the **Hard Disk Policy** screen, you can specify the number of physical disks that you want to create during VM provisioning.

a) Click **Add** to add a disk and complete the following fields:

Field	Description
Disk Label field	A descriptive label for the disk you are adding.
Disk Size (GB) field	The size of the disk.
Disk Type drop-down list	Choose the disk type. The options that you see in this drop-down list depends on whether you selected the **Same as System Policy** check box earlier in this procedure.
Controller Options	
Controller Type drop-down list	Choose a controller type from the drop-down list. Based on the availability of ports, a controller is mapped to the VM disks.
Create Disk on new Controller check box	Check this check box to create a new controller. The type of controller that is created is based on the selection you made in the **Controller Type** drop-down list.
Disk Provisioning Options	
Disk Provisioning Options radio buttons	Check the radio button of the type of provisioning you want to specify. You can specify one of the following: • **Thin Provision** • **Thick Provision lazy zeroed** • **Thick Provision eager zeroed**
Resizing Options for VM Life cycle	
Allow Resizing of Disk check box	Check the check box to enable editing of the VM disk size before provisioning.

Field	Description
Permitted Values for Disk in GB field	This option appears if **Allow Resizing of Disk** is checked. Specify the custom range of disk size values that are chosen while provisioning a VM. You can specify these values in one of the following formats: • Range such as 10-1000 • Comma separated values such as 1, 5, 10, 50, 100, 500, 1024, 5120, 10240. • Combination of range and comma separated values such as 1,5,10, 10-1000.
Allow user to select datastore from scope check box	Check the check box to provide the user with an option to choose the datastore during the service request creation.

Step 10 Click **Submit**.

Note
To use the storage policy created with additional disk policies, you need to associate the policy with the VDC that is used for the VM provisioning.

When using the Additional disks policies configured in a policy, make sure to uncheck **Provision all disks in a single database** during catalog creation for the multiple disk template. For more information about catalog creation, see Managing Catalogs, on page 299.

Creating a Catalog

Adding a Catalog

Procedure

Step 1 Choose **Policies** > **Catalogs**.

Step 2 On the **Catalogs** page, click **Add**.

Step 3 On the **Add Catalog** screen, choose the **Catalog Type** that you want to add.

It can be one of the following:

- **Standard**—Used to create catalogs for VM provisioning, using images from a list of clouds.

- **Advanced**—Used to publish orchestration workflows, such as catalog items.
- **Service Container**—Used to publish application containers as catalog items.
- **Bare Metal**—Used to create catalogs for bare metal server provisioning.

  For information on how to create a bare metal catalog, see Creating a Bare Metal Server Catalog, on page 310.

Step 4 Click **Submit**.

Step 5 On the **Add Catalog: Basic Information** screen, complete the required fields, including the following:

Name	Description
Catalog Name field	Enter a name for the catalog. **Note** After created, a catalog name cannot be modified.
Catalog Description field	Enter a description of the catalog.
Catalog Type drop-down list	Displays the type of catalog you previously chose. To change the catalog type, you need to cancel and restart this procedure.
Catalog Icon drop-down list	Choose from a list of icons to associate this catalog with an image. This icon is seen when you are creating a service request using this catalog.
Applied to all groups check box	Check the box to enable all groups to use this catalog. Leave it unchecked to deny its use to other groups.
Support Contact Email Address field	Enter the email address of the support contact who is notified when a service request is created using this catalog item.
Selected Groups list	Click **Select** to the check the checkboxes of specific user groups. The checked groups use this catalog to provision new VMs. After checking the checkboxes of user groups, click **Select** to return to the **Add Catalog** screen.
Publish to end users check box	By default, this box is checked. Uncheck this box if you do not want this catalog to be visible to users. If you do not uncheck this box, then this catalog is visible to the users of the system.
Cloud Name drop-down list	Choose the cloud with the image for VM provisioning.
Provision new VM for ISO mounting check box	Check this box to clone a new VM from a selected image. If you do not check this check box, a blank VM is created.

Name	Description
Image list	Click **Select** to the check the checkboxes of the type of image (any existing templates such as Windows, Linux, and other files that make up the image) to use when VMs are provisioned using this catalog. After checking the checkboxes of the required images, click **Select** to return to the **Add Catalog** screen. If you are a group administrator, or a user in a group with permissions to create catalogs, this field displays images that are assigned to the group to which you belong. If you are an MSP administrator, then this field displays images that are assigned to your MSP organization, and to the groups within the MSP organization.
Provision new VM using Content Library VM Template check box	Check this box to ensure that the new VM is provisioned using the Content Library VM Template. If you choose this option, the **Image** list is hidden.
Content Library VM Template list	Choose the content library VM template.
Windows License Pool field	Enter the Windows License. **Note** This field appears only when a Windows image is chosen. This option is not supported in the RHEV KVM Connector.
Use ReadyClone check box	Check the box to ensure that VMs are deployed using ReadyClones. When this box is checked, the **Use Linked Clone** and **Provision all disks in single datastore** check boxes are not available for editing. **Note** This checkbox is not visible if: 1. The selected image is not on the HX datastore. 2. The VM has multiple disks.
Use Linked Clone check box	Check the box if you want to use a linked clone. Linked Clone or Full Clone depends on the Linked Clone selection in the Storage Policy. **Note** This field appears only when a Snapshot image is chosen.

Name	Description
Provision all disks in single datastore check box	Check the box to provision all disks in a single datastore. You can also choose to use the datastores configured for each disk in the storage policy. For more information on multiple disk storage policy creation, see Managing Policies, on page 207. **Note** This field appears only if the chosen template has multiple disks. This option is not supported in the RHEV KVM Connector.
Service Container Template Name drop-down list	Choose the template from the list. **Note** This field appears only when the chosen Catalog Type is **Service Container**.
Select Folder drop-down list	Choose the folder within which this catalog must be created. **Note** The drop-down list includes names of folders that are available by default. You can either choose a folder that is available, or click **Create New Folder**. On the **Add New Folder** screen, enter a **Folder Name**, choose a **Folder Icon**, and click **Add**.
Bare Metal Server Provisioning Policy drop-down list	**Note** This field appears only when the chosen Catalog Type is **Bare Metal**.
Configure Service Request Support Email check box	Check this box to enable the user to set the support email for sending service request status.

Step 6 Click **Next**.

Step 7 On the **Add Catalog: Application Details** screen, complete the required fields, including the following:

Name	Description
Category list	Expand the list to choose a VDC category and click **Select**.
Override check box	Check the box to enable the user to override the selected category while provisioning a VM using a service request.
Support Contact Email Address field	Enter the email address of the contact who is notified when a service request is created using this catalog item.

Name	Description
Specify OS drop-down list	Choose the type of OS installed on the VM when it is provisioned. **Note** This option is not supported in the RHEV KVM Connector.
Specify Other OS field	Enter an OS that is not available in the **Specify OS** drop-down list. **Note** This option is not supported in the RHEV KVM Connector.
Specify Applications check boxes	Check the appropriate boxes to specify applications that are installed on the VM during provisioning. **Note** This option is not supported in the RHEV KVM Connector.
Specify Other Applications field	Enter other applications that are not available from the **Specify Applications** check boxes. **Note** This option is not supported in the RHEV KVM Connector.
Application Code field	Enter an application code that is used in the VM name. The application code can be between 1 to 4 characters (for example: W2K3, DB, WS). The application code can be used in a system policy for the VM name by using the variable ${APPCODE}. For example, if the VM Name Template is vm-${GROUP_NAME}-${APPCODE}, the VM provisioned with the system policy has the name vm-groupname-W2K3. **Note** This option is not supported in the RHEV KVM Connector.

Step 8 Click **Next**.

Step 9 On the **Add Catalog: User credentials** screen, complete the required fields, including the following:

Note
These options are not supported in the RHEV KVM Connector.

Name	Description
Credential Options drop-down list	Choose to allow or disallow users to retrieve VM access credentials (shared). The following options are available: • **Do not share** • **Share after password reset** • **Share template credentials** The **Do not share** option is chosen if the administrator wants to send the credentials privately to another user outside Cisco UCS Director.
User ID field	Enter the user ID. **Note** This field is available only if a choice is made to share under **Credential Options**.
Password field	Enter the password. **Note** This field is available only if a choice is made to share under **Credential Options**.

Step 10 Click **Next**.

Step 11 On the **Add Catalog: Customization** screen, complete the required fields, including the following:

Name	Description
Automatic Guest Customization Enable check box	Check the box to enable automatic guest customization. If you do not check this check box, then Cisco UCS Director does not configure the DNS, Network, and Guest OS properties.
Service Request Options Lock check box	Check the **Lock** check box to lock a service request. Selecting the **Lock** check box prevents archiving of the service request. This is applicable only when you choose the catalog type as **Standard**.
Pre Provisioning Custom Actions Enable	Check the **Enable** check box to enable execution of an orchestration workflow before VM provisioning.

Name	Description
Workflow field	Click **Select** to check the compound workflow that should be used in the orchestration workflow before VM provisioning. Check the check boxes of the required workflows, and click **Select** to return to the **Add Catalog** screen. **Note** This field appears when **Pre Provisioning Custom Actions Enable** is checked.
Post Provisioning Custom Actions Enable check box	Check the box to enable execution of an orchestration workflow after VM provisioning.
Workflow drop-down list	Click **Select** to check the check boxes of the workflows that need to be used in the orchestration workflow after VM provisioning. Check the check boxes of the required workflows, and click **Select** to return to the **Add Catalog** screen. **Note** This field appears when **Post Provisioning Custom Actions Enable** is checked.
Virtual Storage Catalog Enable check box	Check the box to choose storage entries from the Virtual Storage catalog.
Virtual Storage Catalog drop-down list	Chose a storage entry from the catalog. **Note** This field appears when **Virtual Storage Catalog Enable** is checked.
Cost Computation	
Charge Duration drop-down list	Choose **Hourly** or **Monthly**.
Active VM Application Cost USD field	Enter the cost for the application that is included in the template. **Note** This option is not supported in the RHEV KVM Connector.
Inactive VM Application Cost USD field	Enter the cost to this catalog of a VM in inactive state, per hour or month. **Note** This option is not supported in the RHEV KVM Connector.

Name	Description
VM Life Cycle Configuration	
Lease Time check box	Check the box to define a lease time (in days and hours).
Days field	Enter the number of days. **Note** This field appears when **Lease Time** is checked.
Hours field	Enter the number of hours. **Note** This field appears when **Lease Time** is checked.
Hide end user lease configuration check box	Check the box to prevent service users from configuring a lease time for VMs.
Hide end user VM provision later check box	Check the box to prevent service users from provisioning VMs at a later time.

Step 12 Click **Next**.

Step 13 On the **Add Catalog: VM Access** screen, complete the required fields, including the following:

Name	Description
Web Access Configuration Enable check box	Check the box to enable web access to the VM. By default, this check box is unchecked which means that web access to the VM is disabled.
URL field	Enter the URL of the VM. **Note** This field appears when **Web Access Configuration Enable** is checked.
Label field	Enter the label that is defined for this URL. **Note** This field appears when **Web Access Configuration Enable** is checked.
Remote Desktop Access Configuration Enable check box	Check the box to enable remote desktop access to the VM. By default, this check box is unchecked, which means that remote desktop access to the VM is disabled.
Server field	Enter the IP address of the server for remote access. **Note** This field appears when **Remote Desktop Access Configuration Enable** is checked.

Name	Description
Port field	Enter the port number on the server for remote access. **Note** This field appears when **Remote Desktop Access Configuration Enable** is checked.
Label field	Enter the label that is defined for this remote access. **Note** This field appears when **Remote Desktop Access Configuration Enable** is checked.
VMRC Console Configuration Enable check box	Check the box to enable VMRC console access to the VM. By default, this check box is unchecked, which means that the VMRC console access to the VM is disabled.

Step 14 Click **Next**.

Step 15 Review the catalog information on the **Add Catalog: Summary** screen.

Step 16 Click **Submit**.

Creating a VM Disk

You can add an additional disk with a custom size to provisioned or discovered VMs using the **Create VM disk** option.

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, choose the cloud.

Step 3 On the **Compute** page, click **VMs**.

Step 4 Click the row with the VM for which you want to create a VM disk.

Step 5 From the **More Actions** drop-down list, choose **Create VM Disk**.

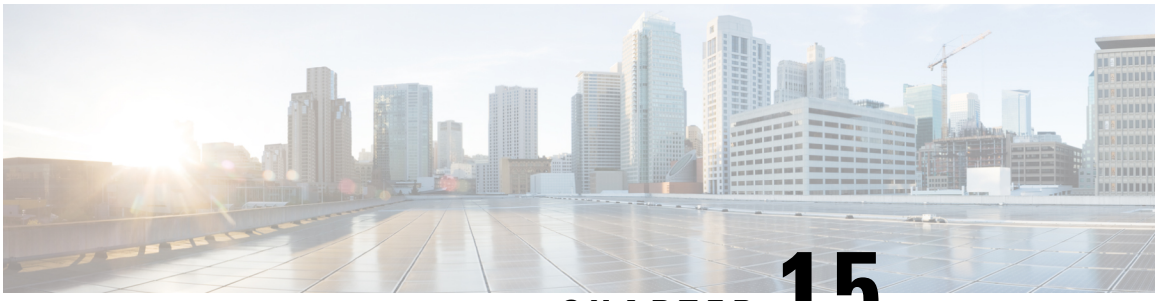
Step 6 On the **Create VM Disk** screen, complete the following fields:

Name	Description
VM Name field	The name of the VM. Once entered, the VM name cannot be edited.

Name	Description
New Disk Size (GB) field	The disk size for the VM, in GB. Enter an integer in this field. This integer should be within the range or among the comma separated values specified in the storage policy associated with this VM.
Select Disk Type drop-down list	Choose the disk type. It can be one of the following: • **System** • **Swap** • **Data** • **Database** • **Log**
Select Datastore/Datastore Cluster drop-down list	Specify if the VM disk should be created from a datastore or a datastore cluster.
Select Datastore field	Click **Select** and choose which datastore you want to use to create the VM disk. **Note** The available datastores depend upon the storage policy associated with the VDC. Only datastores that meet the criteria specified in the storage policy are available for the VM disk. This field is only available if you specify that the VM disk should be created from a datastore.
Select Datastore Cluster field	Click **Select** and choose which datastore cluster you want to use to create the VM disk. **Note** The available datastore clusters depend upon the storage policy associated with the VDC. Only datastore clusters that meet the criteria specified in the storage policy are available for the VM disk. This field is only available if you specify that the VM disk should be created from a datastore cluster.
Thin Provision check box	Check the check box to add a thin provisioned disk to the VM. **Note** Thin provisioning enables dynamic allocation of physical storage capacity to increase VM storage utilization.

Name	Description
Compute New Disk Cost option	This option calculates the cost of the new disk based on the input you specified, and displays it in the dialog box.

Step 7 Click **Create**.



CHAPTER 15

Using the Chargeback Module

This chapter contains the following sections:

- About Chargeback Features, on page 363
- Budget Policies, on page 364
- Cost Models, on page 365
- Modifying a VDC to Include a Cost Model, on page 370
- Package-Based Cost Models, on page 372
- Storage Tier Cost Models, on page 374
- About Assigning a Datastore to Tiers, on page 375
- Chargeback Reports, on page 375
- About Change Records, on page 380
- Chargeback Calculations, on page 380

About Chargeback Features

The chargeback module in Cisco UCS Director offers in-depth visibility into the costs of the virtual infrastructure. It allows the definition of cost models and their assignment to policies within departments and organizations. Virtual machine (VM) metering data is collected at frequent intervals to ensure accurate calculation of resource costs.

Attention The chargeback module is supported only for physical servers that are within an application container.

Following are the features of the chargeback module:

- Flexibility—Provides fixed costs, one-time costs, allocation costs, usage costs, and a combination of these costs, based on the organizational requirements.
- Reusable Cost Models—Assigns cost models to VMs using standardized cost models or templates. These templates apply cost models to new environments quickly.
- Reporting—Generates various summary and comparison reports of costs and resource usage for the virtual infrastructure. These reports are exported to PDF, CSV, and XLS formats and allow you to view them with a web browser.
- Top Five Reports—Monitors the top five reports for organizations or groups with the highest VM cost, CPU, memory, storage, and network costs.

- Dashboard—Monitors and analyzes VM metering information and chargeback in real time with the built-in dashboard and an extensive set of graphical widgets.

Budget Policies

Overall resources are accounted for by the chargeback module. In addition to chargeback, individual groups or organizations must be associated with a budget policy where you can enable or disable the budget watch and over budget.

Configuring a Budget Policy

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **User Groups**.

Step 3 Choose a group and click **Budget Policy**.

Step 4 In the **Budget Policy** screen, complete the required fields, including the following:

Name	Description
Enable Budget Watch check box	If checked, the group's budget usage is monitored. If unchecked, all budget entries for this group are ignored.
Allow Over Budget check box	If checked, the group members are allowed to go over the provisioned budget. If unchecked, once the budget is exhausted, all requests are rejected until a new budget is added.

Step 5 Click **Save**.

Creating a Tag-Based Cost Model

The tag-based cost model capability is supported on all VMs that have been provisioned through a container.

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Service Delivery**.

Step 2 On the **Service Delivery** page, click **Tag Based Cost Model**.

Step 3 Click **Add** to create a new cost model.

Step 4 In the **Add Tag Based Cost Model** screen, complete the required fields, including the following:

Field	Description
Cost Model Name field	The name of the cost model.
Cost Model Description	The description of the cost model.
Tag Name drop-down list	Select a VM tag from the drop-down list. The tag costs that you specify are restricted to the VM tag that you select in this drop-down list. The tag-based cost model is restricted to the VM tag that you selected.

Step 5 Click + sign to add tag costs to the cost model.

Step 6 In the **Add Entry to Tag Costs** screen, complete the required fields, including the following:

Field	Description
VM Tag drop-down list	Choose a tag value from the drop-down list. This drop-down list displays the possible values for the tag name that you selected.
Fixed Cost field	The per-hour fixed cost for the tag.
One Time Cost field	The fixed one-time cost for the tag.
Include VM in Regular Chargeback check box	Check the check box to include the tag-based cost model along with the regular cost model for the VM.

Step 7 Click **Submit**.

Step 8 In the **Add Tag Based Cost Model** screen, click **Submit**.

Step 9 Click **OK**.

Cost Models

A cost model is used to define the unit-level costs of virtual resources, and physical resources. These costs are used for chargeback calculations of VMs within the virtual infrastructure as well as physical resources. Cost models offer a definition of costs in a linear model.

The cost of a particular resource is calculated on how many units are assigned to that resource in the VM or physical resource. For example, the cost of 1 GB of RAM is defined within the cost model. This unit cost is used to determine the cost of RAM for a particular VM.

You can define one-time provisioning costs, active or inactive VM costs, and provisioned, reserved, or used costs for resources, such as CPU, and memory. These values are used to calculate VM costs based on usage.

In addition, you can also create a cost model for bare metal servers within the physical infrastructure.

Note You can map a cost model to a VDC or to an application container. For more information on mapping a cost model to an application container, see the *Cisco UCS Director Application Container Guide* available at the following link:

http://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-director/products-installation-and-configuration-guides-list.html

Creating a Cost Model

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Service Delivery**.

Step 2 On the **Service Delivery** page, click **Cost Model**.

Step 3 Click **Add**.

Step 4 In the **Add Cost Model** screen, complete the required fields, including the following:

Name	Description
Cost Model Name field	The name of the cost model.
Cost Model Description field	The description of the cost model.
Cost Model Type drop-down list	Choose the type of cost model. **Standard** indicates a linear cost model. **Advanced** indicates a package or script-based cost model. See the Package-Based Cost Models for the Advanced cost model description and usage. You can also choose **HyperV**, if appropriate.
Charge Duration drop-down list	Choose the interval at which costs for the VM's resources are defined. It can be one of the following options: • **Hourly**—If you want to quantify the costs of resources on an hourly basis. • **Daily**—If you want to quantify the costs of resources on a daily basis. • **Weekly**—If you want to quantify the costs of resources on a weekly basis. • **Monthly**—If you want to quantify the costs of resources on a monthly basis. • **Yearly**—If you want to quantify the costs of resources on a yearly basis.

Name	Description
Virtual Machine Cost Parameters	
Fixed Costs (Currency: USD)	
One Time Cost field	The fixed one-time cost for provisioning the VM.
VM Costs (Currency: USD)	
Active VM Cost field	The per-hour cost of a VM in the active state.
Inactive VM Cost field	The per-hour cost of a VM in the inactive state.
CPU Charge Unit drop-down list	Choose the charge unit for CPU: GHz or cores.
Provisioned CPU Cost field	The provisioned CPU cost per CPU charge unit per-hour. The system calculates the percentage of CPU that was provisioned for the VM. **Note** The cost of the CPU charge unit is GHz. If you enter a value for the **Used CPU Cost** field, you must leave this field blank.
Reserved CPU Cost field	The reserved CPU cost per GHz per hour. The amount of CPU that has been actually reserved to the VM is taken into consideration, including the provisioned CPU cost calculation. Any extra cost for the reserved CPU (apart from the provisioning cost) is entered here. For example, if the provisioning cost is $1 and the reserved cost is $1.4, the extra amount to reserve must be mentioned. In this example, it is $1.4 – $1 = $0.4. **Note** The cost if the CPU charge unit is GHz. If you enter a value for the **Used CPU Cost** field, you must leave this field blank.
Used CPU Cost field	The used CPU cost per GHz per hour. The cost is based on the actual CPU usage. This cost does not take into consideration the provisioned and reserved costs. If you enter a value for the **Used CPU Cost** field, the provisioned cost and reserved cost fields must be left blank. **Note** The cost if the CPU charge unit is GHz.
Provisioned Memory Cost field	The provisioned memory cost per GB per hour.

Name	Description
Reserved Memory Cost field	The reserved memory cost per GB per hour.
Used Memory Cost field	The used memory cost per GB per hour.
Received Network Data Cost field	The received data cost per GB per hour.
Transmitted Network Data Cost field	The transmitted data cost per GB per hour.
Committed Storage Cost field	The committed storage cost per GB per hour.
Uncommitted Storage Cost field	The uncommitted storage cost per GB per hour. The unused but provisioned storage is defined as uncommitted storage.
Tag Based Cost Model drop-down list	Select a tag-based cost model. This list displays all the tag-based cost models that you have created.
Physical Server Cost Parameters	
Fixed Costs (Currency: USD)	
One Time Cost field	The fixed one-time cost for provisioning the server.
CPU Charge Unit drop-down list	Choose the charge unit for CPU: GHz or cores.
Provisioned CPU Cost field	The provisioned CPU cost per CPU charge unit per hour. The CPU percentage that was provisioned to the server is taken into consideration. **Note** The cost if the CPU charge unit is GHz. If you enter a value for the **Used CPU Cost** field, you must leave this field blank.
Provisioned Memory Cost field	The provisioned memory cost per GB, per-hour.
Used Memory Cost field	The used memory cost per GB, per-hour.
Committed Storage Cost field	The committed storage cost per GB, per-hour.
Full Length Blade Cost field	The cost of full-length blade servers, per-hour. **Note** This field does not appear when **HyperV** is selected as the cost model type.
Half Length Blade Cost field	The cost of half-length blade servers, per-hour. **Note** This field does not appear when **HyperV** is selected as the cost model type.

Step 5 Click **Add**.

Creating a Bare Metal Cost Model

Procedure

Step 1 Choose **Policies** > **Physical Infrastructure Policies** > **Bare Metal Servers**.

Step 2 On the **Bare Metal Servers** page, click **Bare Metal Cost Model**.

Step 3 Click **Add**.

Step 4 In the **Add Bare Metal Cost Model** screen, complete the required fields, including the following:

Name	Description
Cost Model Name field	The name of the cost model.
Cost Model Description field	The description of the cost model.
Charge Duration drop-down list	Choose the charge duration from the drop-down list. It can be Hourly, Daily, Weekly, Monthly, and Yearly.
One Time Cost field	The fixed one-time cost for provisioning a bare metal server.
CPU Charge Unit drop-down list	Choose the charge unit for the CPU. It can be GHz or Cores.
CPU Cost field	The CPU cost per CPU charge unit per hour.
Memory Cost field	The memory cost per GB per hour.
Used Memory Cost field	The used memory cost per GB per hour.
Storage Cost field	The storage cost per GB per hour.
Full Width Blade Cost field	The cost of the full width blade servers per hour.
Half Width Blade Cost field	The cost of the half width blade servers per hour.

Step 5 Click **Submit**.

What to do next

You can choose this cost model when you create a Bare Metal Server provisioning policy.

Modifying a VDC to Include a Cost Model

You can add or edit an existing VDC to assign a newly created cost model. You can edit an existing VDC, or create a new VDC and assign a cost model to it.

After the cost model is assigned to a VDC, all VMs within the VDC are charged based on the advanced cost model. Any VMs within VDCs that have the standard type of cost model are still charged according to the standard cost model.

Adding a Cost Model to a VDC

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Virtual Data Centers**.

Step 2 On the **Virtual Data Centers** page, click **vDC**.

Step 3 Choose the VDC to which you want to add the cost model.

Step 4 Click **Add**.

Step 5 In the **Add vDC** screen, select the account type, and click **Submit**.

Step 6 In the **Add VDC** screen, complete the required fields, including the following:

Name	Description
VDC Name field	The name of the VDC.
VDC Locked check box	By default, this check box is not checked, which means that the VDC is available for further deployments. Check the check box to deny the use of the VDC for any further deployments. Actions on existing VMs, within this VDC, are disabled. Uncheck the check box to allow the use of the VDC for further deployments.
VDC Description field	The VDC-specific description.
Group drop-down list	Choose the group for which the VDC is being set up.
Cloud Name drop-down list	Choose the cloud on which the VDC is being set up.
Enable Protection check box	Check the check box to enable SRM.
Approvers and Contacts	
First Level Approvers list	The users who must approve the service request at the first-level. Expand the list to check the check boxes of the users. You can select multiple users.

Name	Description
Second Level Approvers list	The users who must approve the service request at the second-level. Expand the list to check the check boxes of the users. You can select multiple users.
Approval Required from all users check box	Check this check box to indicate that approval is required from all users who have been selected as first-level and second-level approvers.
Number of Approval Requests Reminders field	The number of times the reminder email to approve the service request is sent to the approvers. By default, the system sends a reminder email once every 24 hours until the service request is approved or rejected.
Reminder Interval (Hours) field	The time interval between the reminder emails that are sent to the approvers. By default, the system sends a reminder email every 24 hours.
Provider Support Email Address field	The contact or user's email address. The person who is notified about VM provisioning using this VDC.
Copy Notifications to Email Address field	The second contact's email for receiving copies of notifications about this VDC.
Policies	
System Policy drop-down list	Choose the system policy applicable to the VDC.
Computing Policy drop-down list	Choose the computing policy applicable to the VDC.
Network Policy drop-down list	Choose the network policy applicable to the VDC.
Storage Policy drop-down list	Choose the storage policy applicable to the VDC.
Cost Model drop-down list	Choose the cost model applicable to the VDC.
Disable displaying cost in the SR summary and email page check box	Check the check box to disable displaying cost in the SR summary and email page for this VDC.
User Action Policy drop-down list	Choose the policy that is used for execution of orchestration workflows after provisioning of the VMs. The chosen workflow appears as an action button for VMs within the VDC.
End User Self-Service Policies	
VM Power Management check box	Check the box to enable all VM power management actions for VMs that belong to this VDC.

Note
End user self-service policies also include VM Resizing, VM Snapshot Mangement, VM deletion, VM Disk Management, and VM Network Management. For more information, see Adding a Virtual Data Center, on page 248.

Step 7 Click **Add**.

Editing a VDC to Include a Cost Model

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Virtual Data Centers**.
Step 2 On the **Virtual Data Centers** page, click **vDC**.
Step 3 Choose the VDC to add to the cost model.
Step 4 Click **Manage Categories**.
Step 5 Choose the category to edit.
Step 6 Click **Edit**.
Step 7 In the **Edit App Category** screen, in the drop-down list, choose a **Cost Model** and a **Deploy Policy**.
Step 8 Click **Save**.

Package-Based Cost Models

A package-based cost model enables you to define the costs for the system resources as packages instead of as individual definitions. There are different packages to choose from based on your requirements. This type of cost model is suitable for nonlinear models.

Note Cisco UCS Director supports definitions of CPU memory (server) packages.

In this type of cost model, the definition is based on the available resource packages. The model is in the following format:

C – M:X.

C is the number of CPU cores.

M is the memory in GB.

X is the combined monthly cost of C and M.

For example, a package with an entry of 2-4:200 implies CPU cores = 2, memory = 4 GB, and the cost of this package is $200 per month.

You can define multiple packages using the following format: C1-M1:X1,C2-M2:X2,.....,CN-MN:XN.

For example, 1-1:50,1-2:70,1-4:90,2-4:150,2-6:170,2-8:190,4-8:350,4-12:380,4-16:400. The first entry 1-1:50 is a package of 1 core CPU and 1 GB memory that costs $50 per month.



Note These entries can be edited at any time to suit the cost package requirements.

Creating a Package-Based Cost Model

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Service Delivery**.

Step 2 On the **Service Delivery** page, click **Cost Model**.

Step 3 Click **Add**.

Step 4 In the Add Cost Model screen, enter a cost model name and description.

Step 5 For the **Cost Model Type** field, choose **Advanced**.

Step 6 Paste the script provided in the **Advanced Cost Model** field.

```
/*********************************/
var CPU_MEMORY_COST =
"1-2:81,1-4:95,1-8:109,2-4:162,2-6:176,2-8:189,2-16:378,4-12:352,4-16:378";
var oneTimeCost = 150;
/*********************************/
/* define cost packages as shown above.
The cost packages can be defined in the following format:
C-M:X.
C is the number of CPU cores.
M is the memory in GB.
X is the combined monthly cost of C and M.
For example, 2-4:162 means CPU cores = 2, memory = 4 GB and the cost of this package is $162 per month.
*/
/* When defining multiple packages, define it in the following format: C1-M1:X1,C2-M2:X2,
.....,CN-MN:XN
The standard packages are defined at the top of the script using the variable CPU_MEMORY_COST.
This variable can be edited to suit the cost package requirement. */
/* For reference, the storage cost to use is based on the storage tier cost model definition. */
/* do not edit any script below */
computeChargeback(data);
function computeChargeback(data)
```

```
{
var map = chargeBackAPI.getCPUMemCostModelMap(CPU_MEMORY_COST);
var cpuCores = data.getVmMeter().getCpuCores();
var memory = data.getVmMeter().getAllocMemGB();
var serverCost = chargeBackAPI.getCostForItem(map,cpuCores, memory);
serverCost = serverCost / (24 * 30);
var storageTierCost = chargeBackAPI.getStorageCostForItem(data.getVmMeter().getVmId());
var storageGB = (data.getVmMeter().getCommittedDiskGB()) +
(data.getVmMeter().getUncommittedDiskGB());
var committedDiskGBCost = (data.getVmMeter().getCommittedDiskGB()) * storageTierCost;
var unCommittedDiskGBCost = (data.getVmMeter().getUncommittedDiskGB()) * storageTierCost;
var storageCost = (storageGB * storageTierCost) / (24 * 30);
var totalVMCost = serverCost + storageCost;
var cb = data.getCbSummary();
cb.setCpuCores(cpuCores);
cb.setMemory(memory);
cb.setServerCost(serverCost);
cb.setCommittedDiskGB(data.getVmMeter().getCommittedDiskGB());
cb.setCommittedDiskGBCost(committedDiskGBCost);
cb.setUncommittedDiskGB(data.getVmMeter().getUncommittedDiskGB());
cb.setUncommittedDiskGBCost(unCommittedDiskGBCost);
cb.setTotalCost(totalVMCost);
}

/*******************************/
```

Step 7 Click **Add**.

Note
Once the cost model has been defined, assign it to a VDC in order to start the chargeback of VMs based on this cost model.

Storage Tier Cost Models

You can use a storage tier cost model to define multiple costs for storage using the tier format. Current storage types include but not limited to local storage, NFS, SAN, and NAS. Each storage cost could vary. You can incorporate this variation while calculating costs for storage usage.

You can use this model to define different costs for different tiers and then assign existing datastores to these tiers. You can group similar datastore types by cost wise using the tier cost model.

Each tier must be assigned a cost, at a per-GB, per-month value. For example, when assigning $0.50 to a tier, all datastores within this tier are charged at $0.50 per GB per month. By default, four tiers are already created, so you must assign the costs to them.

Assigning a Cost to a Tier

Procedure

Step 1 Choose **Policies** > **Virtual/Hypervisor Policies** > **Service Delivery**.

Step 2 On the **Service Delivery** page, click **Storage Tier Cost Model**.

Step 3 Choose the tier to edit.
Step 4 Click **Edit**.
Step 5 Edit the **Disk Cost (GB)/Month** field.
Step 6 Click **Submit**.

About Assigning a Datastore to Tiers

You can assign a datastore to a tier so that the cost defined in the tier is used to calculate the cost of storage within that particular datastore.

When calculating the chargeback for VMs within a datastore, the cost is determined by which tier the datastore was assigned to. If no tier is assigned to a datastore, the storage cost for that datastore is not considered when using the advanced (script-based) cost model.

With a regular cost model, you define resource costs in a form. Storage tier costs are taken into consideration if tier costs are assigned and datastores are assigned to those tiers. However, if no tier is assigned to a datastore, the storage cost for VMs under that datastore is removed from the storage cost entry of the cost model form.



Note Assigning a datastore to a tier applies only to the regular cost model.

Assigning a Datastore to a Tier

Procedure

Step 1 Choose **Virtual** > **Storage**.
Step 2 On the **Storage** page, choose the cloud.
Step 3 On the **Storage** page, click **Datastore Capacity Report**.
Step 4 Choose the datastore to assign to a tier.
Step 5 Click **Assign Tier** and the **Storage Tier** screen appears.

Currently, the tier-based cost is supported only on VMware cloud accounts.

Step 6 From the drop-down list, choose a tier.
Step 7 Click **Submit**.

Chargeback Reports

Chargeback provides information about how much your organization may be paying for resources, even unused resources. This feature allows you to optimize resource consumption and costs. System resources

accounting can be based on monthly usage. Resources, such as CPU and memory usage, are monitored and measured.

Chargeback reports are based on the cost model type. Chargeback is calculated and shown in the user interface in the form of tabular reports, summaries, graphical reports, and widgets.

Chargeback summary data is stored only at a daily and monthly interval. So, you cannot generate daily and hourly trend cost reports using the **Chargeback** menu option. You can generate trend reports only for weekly and monthly duration. You can generate these trend reports, in addition to several other trend reports, using the **Report Builder** menu available under **CloudSense**. For more information on using the **Report Builder** option, see Report Builder for Custom Report Templates, on page 428.



Important While generating trend reports for a month, the data is caculated from the first day of the month till the current date. For example, if you are generating a trend report on 5th March, this report includes data from March 1st, to March 5th.



Note For VMs that are provisioned through a container, you can associate a tag-based cost model and include those costs in the regular chargeback calculations and subsequent reports.

Following are the report types that are available:

- Viewing
  - Current month summary—The current month summary cost report (VM, CPU, storage costs, and so on).
  - Previous month summary—The previous month summary cost report (VM, CPU, storage costs, and so on).
  - Monthly resource accounting details—The resource accounting details (CPU and memory usage statistics) on a monthly basis.
  - VM level resource accounting details—The resource accounting details at the VM level.
  - VM level chargeback details—The charges that are applicable for VM usage calculated with the chargeback feature.
- Export
  - Export monthly resource accounting details—These reports can be exported as tables.
  - Export VM level resource Accounting details—These reports can be exported as tables.
  - Export VM level chargeback details—Chargeback reports can be exported as tables.



Important You can generate these reports for a group, or for a specific virtual data center (VDC). These reports include information on virtual resources as well as on physical servers.

Viewing the Current Month Summary

Using the **Current Month Summary** tab, you can view the month's chargeback details for all VMs and physical servers that belong to the group.

Procedure

Step 1 Choose **Organizations** > **Chargeback**.
Step 2 On the **Chargeback** page, choose the user group.
Step 3 On the **Chargeback** page, click **Current Month Summary**.

Viewing the Previous Month's Summary

Using the **Previous Month Summary** tab, you can view the previous month's chargeback details for all VMs and physical servers that belong to the group.

Procedure

Step 1 Choose **Organizations** > **Chargeback**.
Step 2 On the **Chargeback** page, choose the user group.
Step 3 On the **Chargeback** page, click **Previous Month Summary**.

Viewing Monthly Resource Accounting Information

Procedure

Step 1 Choose **Organizations** > **Chargeback**.
Step 2 Choose a group or a virtual data center (VDC).
Step 3 On the **Chargeback** page, click **Resource Accounting**.

Viewing the VM Level Resource Accounting Details

Using the **Resource Accounting Details** tab, you can view the individual VM's resource usage details.

Procedure

Step 1 Choose **Organizations** > **Chargeback**.

Step 2 Choose a group or a virtual data center (VDC).

Step 3 On the **Chargeback** page, click **Resource Accounting Details**.

Viewing the VM Level Chargeback Details

Using the **Chargeback** tab, you can view the chargeback report for the selected group or VDC.

If you indicated that the tag-based cost model must be included in the regular VM chargeback calculations, then you will see the **Fixed Costs** column in the report. This column retrieves the cost that you indicated in the tag-based cost model.

Procedure

Step 1 Choose **Organizations** > **Chargeback**.

Step 2 Choose a group or a virtual data center (VDC).

Step 3 On the **Chargeback** page, click **Chargeback**.

Exporting the Monthly Resource Accounting Details

Procedure

Step 1 Choose **Organizations** > **Chargeback**.

Step 2 On the **Chargeback** page, click **Resource Accounting**.

Step 3 Click the **Export Report** icon.

Step 4 In the **Export Report** screen, choose a format.

It can be one of the following options:

- **PDF**
- **CSV**
- **XLS**

Step 5 Click **Generate Report**.

After the report is generated, the **Download** option appears.

Step 6 Click **Download** to open the report in another browser.

After the report opens in another browser, you can save it on your system.

Exporting VM Level Resource Accounting Details

Procedure

Step 1 Choose **Organizations** > **Chargeback**.

Step 2 On the **Chargeback** page, click **Resource Accounting Details**.

Step 3 Click the **Export Report** icon.

Step 4 In the **Export Report** screen, choose a format.

It can be one of the following options:

- **PDF**
- **CSV**
- **XLS**

Step 5 Click **Generate Report**.

After the report is generated, the **Download** option appears.

Step 6 Click **Download** to open the report in another browser.

After the report opens in another browser, you can save it on your system.

Exporting VM Level Chargeback Details

Procedure

Step 1 Choose **Organizations** > **Chargeback**.

Step 2 On the **Chargeback** page, click **Chargeback**.

Step 3 On the right side of the toolbar, click the **Export Report** icon.

Step 4 In the **Export Report** screen, choose a format.

It can be one of the following options:

- **PDF**
- **CSV**
- **XLS**

Step 5 Click **Generate Report**.

After the report is generated, the **Download** option appears.

Step 6 Click **Download** to open the report in another browser.

After the report opens in another browser, you can save it on your system.

About Change Records

You can use change records within the Change Management Database (CMDB) to track and manage changes in the system. These records typically display ADD, DELETE, and MODIFY types of events on any resource, such as a VM, service request, or group.

Change records display information about the resource type (VM), including the resource name, change type, change time, and description. When a VM is resized, the change records display information on the resources that were resized. This includes information on the original resource size and the resized values. You can view this information from the **Change Records** tab.

Accessing Change Records

Procedure

Step 1 Choose **Administration** > **Integration**.

Step 2 On the **Integration** page, click **Change Records**.

Chargeback Calculations

The total cost calculated for a VM includes the following:

Total cost = active VM cost or inactive VM cost + one-time cost + CPU cost + memory cost + disk cost + CPU reserved cost + memory reserved cost + CPU used cost + CPU core cost + memory used cost + network received used cost + network transmitted used cost + application cost.

If a VM is associated with a tag, and has a cost model and a tag-based cost model associated with the vDCs, then the chargeback calculation is derived as follows:

- When the **Include VM in Regular Chargeback** check box is not checked, only the tag-based cost is calculated.

  Total Cost - Fixed Cost + One-Time Cost

- When the **Include VM in Regular Chargeback** check box is checked, the total cost is calculated including the tag-based cost and the regular chargeback computation.

Total Cost = active VM cost or inactive VM cost + one-time cost + CPU cost + memory cost + disk cost + CPU reserved cost + memory reserved cost + CPU used cost + CPU core cost + memory used cost + network received used cost + network transmitted used cost + application cost + Fixed Cost



Note The one-time cost for the VM is determined from the cost specified in the tag-based cost model. If you have not specified a one time cost in the tag-based cost model, then this cost is derived from the regular cost model.

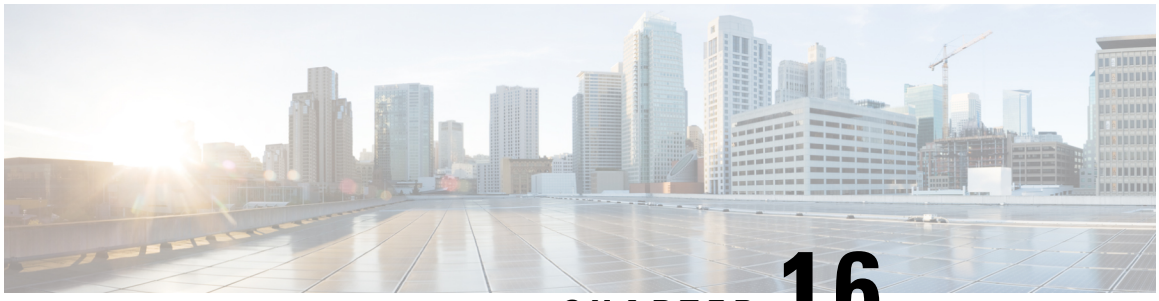
The total cost calculated for a physical server includes the following:

Total cost = one time cost + CPU cost + memory cost + memory used cost + committed disk cost + CPU core cost + full blade cost + half blade cost.

The VM cost calculation is done only on an hourly basis. There is no other option available to calculate the VM cost. The cost for each resource is calculated based on the values that are defined in the cost model. The cost calculations are based as follows:

Cost	Cost Description
Active VM Cost	The value defined in the cost model for the active VM cost.
Inactive VM Cost	The value defined in the cost model for the inactive VM cost.
One Time Cost	The value defined in the cost model for the one-time cost.
CPU Cost	CPU usage (provisioned) × cost that is defined in the cost model for the provisioned CPU cost. The CPU charge unit is GHz.
Memory Cost	Memory usage (provisioned) × cost that is defined in the cost model for the provisioned memory cost. The memory charge unit is GB.
Disk Cost	The committed storage × committed storage cost that is defined in the cost model + uncommitted storage × uncommitted storage cost that is defined in the cost model. The storage charge unit is GB.
CPU Reserved Cost	The reserved CPU × cost that is defined in the cost model for the reserved CPU cost.1.
Memory Reserved Cost	The reserved memory × cost that is defined in the cost model for the reserved memory cost.2.
CPU Used Cost	The used CPU × cost that is defined in the cost model for the used CPU cost.1.
CPU Core Cost	The used CPU core × cost that is defined in the cost model for the CPU core cost. The CPU charge unit is per core.

Cost	Cost Description
Memory Used Cost	The used memory × cost that is defined in the cost model for the used memory cost.2.
Network Received Used Cost	The network received usage in KB / (1024.0 × 1024.0) × cost that is defined in the cost model for the received network data cost. The network charge unit is GB.
Network Transferred Used Cost	The network transmitted usage in KB / (1024.0 × 1024.0) × cost that is defined in the cost model for the transmitted network data cost.5.
Application Cost	The active VM hours × cost that is defined in a catalog for active VM application cost + inactive VM hours × cost that is defined in a catalog for the inactive VM application cost.
Full-length Blade Cost	The cost of full-length blade servers per-hour. This cost is applicable only for physical servers. This is applicable only for physical servers that are part of an application container.
Half-Length Blade Cost	The cost of half-length blade servers per-hour. This cost is applicable only for physical servers. This is applicable only for physical servers that are part of an application container.
Fixed Cost USD	The fixed cost, per-hour, determined for the VM. This is applicable only if you have indicated that the tag-based cost model should be included with the regular cost model for the VM.



CHAPTER 16

System Monitoring and Reporting

This chapter contains the following sections:

- Dashboard, on page 383
- Summary, on page 385
- Inventory Management, on page 386
- Resource Pools, on page 387
- Clusters, on page 387
- Images, on page 388
- Host Nodes, on page 389
- Virtual Machines (VMs), on page 389
- Topology, on page 390
- Assessment, on page 391
- Reports, on page 391
- Diagnostic System Messages, on page 392
- Compatibility Matrix Information, on page 393

Dashboard

In Cisco UCS Director, you can enable the **Dashboard** option in the user interface. On the **Dashboard** screen, you can add important, or frequently accessed report widgets. If you have enabled the **Dashboard** option, then this is the first window that you see when you log in to the user interface. After enabling the **Dashboard**, you can create additional dashboards, and delete them when you no longer need them. For more information, see Creating Additional Dashboards, on page 384 and Deleting a Dashboard, on page 384.

Enabling the Dashboard

Procedure

Step 1 On the header, click the user icon, and choose **Edit My Profile**.

Step 2 On the **Edit My Profile** screen, scroll down to the **Dashboard** section.

Step 3 Check **Enable Dashboard**.

Step 4 Click **Save**.

When you log out and log in, the first screen that you see is the Dashboard.

Step 5 Click **Close** to view the Dashboard immediately.

What to do next

If there are no widgets on the Dashboard, you can access any summary report in the user interface, and select **Add to Dashboard**.

Creating Additional Dashboards

Before you begin

You should have enabled the **Dashboard** in the user interface.

Procedure

Step 1 Log into Cisco UCS Director user interface.

The default **Dashboard** screen is displayed.

Step 2 Click the down arrow displayed next to the default dashboard name and choose **Create Dashboard**.

Step 3 Enter the name of the dashboard.

Step 4 Click **Submit**.

Deleting a Dashboard

You cannot delete the default dashboard.

Procedure

Step 1 Log into Cisco UCS Director user interface.

The default **Dashboard** screen is displayed.

Step 2 Click the drop-down list to view the list of dashboards that you have created.

Step 3 Click the **X** mark displayed next to the dashboard name.

Step 4 Confirm that you want to delete the dashboard.

Adding Report Widgets

Before you begin

You must be logged in to the appliance to complete this task.

Procedure

Step 1 Choose the desired option and navigate to the summary report you want to add to your dashboard.

For example, if you want to add a VM-related summary report, choose **Virtual** > **Compute** and then click **Summary**.

Step 2 On the **Summary** screen, scroll down to the report that you want to add to your dashboard.

Step 3 In the upper right corner of the report, click **Settings** and then choose **Add to Dashboard**.

Refreshing Widget Data

After enabling the **Dashboard** option, you can set a refresh interval to the widgets on this page. Automatic refresh can occur at intervals from a minimum of 5 minutes to a maximum of 60 minutes.

The **Automatic Refresh** button on the dashboard should be set to **ON** to configure the interval.

Summary

The **Summary** screen allows you to manage system inventory. It gives you access to a wide array of tabular, graphical, and map reports, and also helps in managing inventory lifecycle actions.

Each report is displayed as a widget. Reports can be hidden through customization.

Viewing Virtual Machine, Cloud, and System Summary Information

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, click **Summary**.

All information is displayed in the form of tables, graphs, and charts.

Customizing Summary Report Widgets

Procedure

Step 1 Choose **Virtual** > **Compute**.
Step 2 On the **Compute** page, click **Summary**.
Step 3 Click the reports drop-down icon to display the available reports.
Step 4 Click and drag a widget onto the **Dashboard**.
Step 5 From the **Show more reports** drop-down list, check the name of the report that you want to add.

Inventory Management

You can monitor the system inventory using the **Dashboard**. The **Dashboard** displays the entire system level infrastructure information for administrative management.

Accessing System Inventory Details

Procedure

Step 1 Choose **Virtual** > **Compute**.
Step 2 On the **Compute** page, choose the cloud.
Step 3 Choose any of the options to view detailed information.

Following is a list of some of the report options visible for each cloud:

- Summary
- Polling
- VDCs
- Clusters
- Host Nodes
- Resource Pools
- VMs
- VM Action Requests
- Events
- Assessment
- Application Categories

- Data Centers
- SRM Sites

Resource Pools

The **Resource Pools** screen shows resource details at the host node level. These details include the CPU configured reservation, CPU limit, CPU used, and memory used.

Accessing Resource Details

Procedure

Step 1 Choose **Virtual** > **Compute**.
Step 2 On the **Compute** page, choose the cloud.
Step 3 On the **Compute** page, click **Resource Pools**.

All the resource pools for the selected cloud are displayed. You can select a resource pool and click **View Details** to view detailed information of each resource pool.

Clusters

If a pod includes clusters, then the **Clusters** screen displays all the cluster-related information.

Accessing Clusters

Procedure

Step 1 Choose **Virtual** > **Compute**.
Step 2 On the **Compute** page, choose the cloud.
Step 3 On the **Compute** page, click **Clusters**.

All clusters available in the selected cloud accounts are displayed. You can select a specific cluster, and click **View Details**.

Images

The **Images** screen displays all available image IDs and their details. These images include guest OS, CPU, memory, and storage provisioned. You can use these image IDs to provision new virtual machines (VMs). If you are a group administrator, or an MSP administrator, then the **Images** screen displays images that have been assigned to your group.

If you select a specific VMware cloud account, and click **Images**, you can assign images to groups or to individual users. Images assigned to a particular group or user are displayed when administrators of the relevant group log in to the system.

Accessing Images

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, choose the cloud.

Step 3 On the **Compute** page, click **Images**.

A list of images associated with the selected clouds is displayed. You can select a specific image and click **View Details**.

Assigning VM Images to Users or Groups

As an administrator, you can assign specific VM images to users or groups. The assignments filter the images that are displayed when you perform VM provisioning tasks, such as creating catalogs.

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, choose the cloud.

Step 3 On the **Compute** page, click **Images**.

Step 4 Click the row with the image that you want to assign to a group.

Step 5 Click **Assign Image to Group**.

Step 6 On the **Assign Image to Group** screen, expand the **Group ID** field, and check the names of the groups to which you want to assign the image.

Step 7 To assign an image to individual users, complete the following fields:

Name	Description
Assign to Users check box	Check to assign the image to specific users.

Name	Description
User field	Expand this field to check the names of users to whom you want to assign the image.

Step 8 Click **Submit**.

Host Nodes

The **Host Nodes** screen displays all physical host nodes that are available in the infrastructure. The screen lists details such as the ESX/ESXi version installed, active VMs, and power status.

Accessing Host Nodes

Before you begin

You must be logged in to the appliance to complete this task.

Procedure

Step 1 Choose **Virtual** > **Compute**.
Step 2 On the **Compute** page, click **Host Nodes**.
Step 3 Click the row with the host node that you want view, and click **View Details**.

Virtual Machines (VMs)

The **VMs** screen displays all the VMs and VM-specific details for the chosen cloud.

Accessing VMs

Procedure

Step 1 On the menu bar, choose **Virtual** > **Compute**.
Step 2 On the **Compute** page, click **VMs**.

All virtual machines for all cloud accounts are displayed. You can perform additional tasks on these VMs such as launching VM client or powering off VMs. For more information, see Managing VM Actions, on page 400.

Accessing Group Level VMs

Procedure

Step 1 Choose **Organizations** > **Virtual Resources**.

Step 2 On the **Virtual Resources** page, choose the user group.

Step 3 On the **Virtual Resources** page, click **VMs**.

All virtual machines for the selected group are displayed. You can perform additional tasks on these VMs such as launching VM client or powering off VMs. For more information, see Managing VM Actions, on page 400.

Topology

The **Topology** screen displays VMware cloud topology. There are four view mode types: Hierarchical, Concentric, Circular, and Force Directed. Depending on the mode, you can adjust the item spacing, distance, radius, rigidity, and force distance.

Accessing Topology Types

Before you begin

You must be logged in to the appliance to complete this task.

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, choose the cloud.

Step 3 On the **Compute** page, click **Topology**.

Step 4 Choose **Hostnode-Datastore Topology** or **Hostnode-VM Topology**.

Step 5 Click **View Connectivity**.
The topology appears in a new window.

Note
Not all of the topology types are displayed.

Assessment

The **Assessment** screen displays assessment reports such as cloud readiness, and virtualization best practices for a cloud account.

Accessing Assessments

Before you begin

You must be logged in to the appliance to complete this task.

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, choose the cloud.

Step 3 On the **Compute** page, click **Assessment**.

Step 4 From the drop-down list, choose a report type to filter the report.

Reports

Cisco UCS Director can help you monitor virtual infrastructure and system resources. It displays a wide variety of reports that provide insight into how the system is performing

Following are the types of reports:

- Tabular reports for system information, including overview, host nodes, new VMs, and deleted VMs.
- Bar and pie graph comparisons, including VMs active versus inactive, and CPU provisioned versus capacity.
- Trend graphs about system resources, including CPU trends, memory trends, and VM additions and deletions.
- Other reports include Top 5 reports at the group, VDC, host node, and VM levels. The Top 5 reports focus on groups with the highest number of VMs, groups with the greatest CPU usage, VDCs with the highest number of VMs, and host nodes with the greatest CPU usage.
- Map reports, displaying the system resource information in the form of heat maps or color-coded maps.

Additional trend reports are available for certain accounts (for example: KVM accounts). Trend reports display data over a selected time frame.

Accessing Reports

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, choose the cloud.

Step 3 Click the name of the report that you want to view (**Map**, **Top 5**, or **More Reports**).

Diagnostic System Messages

The Cisco UCS Director performs system audits and displays diagnostic system messages to help you quickly assess issues and take necessary actions to prevent potential outages and ensure system stability. For example, when the VM count on a standalone setup is about to reach its maximum allowed limit, the system shows the severity level as 'WARNING' and provides a recommendation to switch to a multinode setup.

Viewing Diagnostic System Messages

Procedure

Click **System Messages** icon.

The **Diagnostic System Messages** window opens, displaying the following details:

- **Severity**: Level of importance or impact of an issue. This can be one of the following:
  - OK
  - CRITICAL
  - WARNING
  - NOTICE
  - ERROR
- **Category**: Classification of the item.
- **Item**: Part of the Cisco UCS Director system for which the audit was performed.
- **Description**: Provides information about the audit result.
- **Recommendation**: Provides actions to resolve or mitigate the reported issue.
- **Audit Time**: The time when the audit was performed.

Compatibility Matrix Information

You can view detailed information about various hardware and software components, including operating systems, compatible with Cisco UCS Director.

Viewing Compatibility Matrix Information

Procedure

Step 1 Choose **Administration** > **Compatibility Matrix**.

The **Compatibility Matrix** window opens.

Step 2 Select the folder category for the required hardware or software components.
The related details are displayed in the following areas:

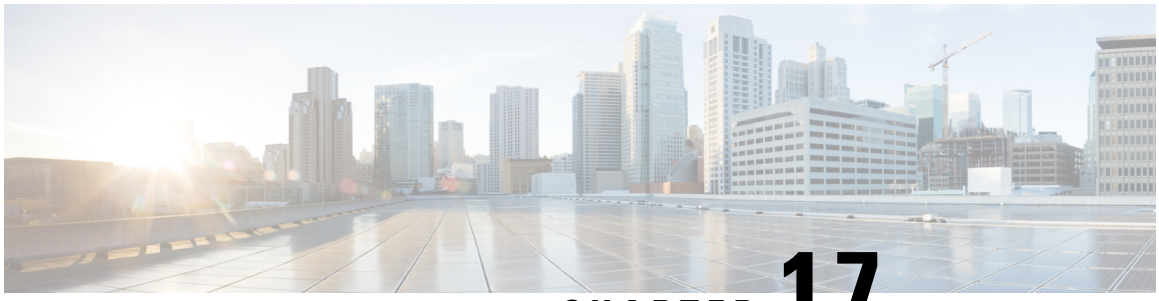
- Component
- Certified Model
- Supported Model
- Certified Software Version
- Supported Software Version

Step 3 To view the compatibility matrix details for Operating Systems, expand the **Virtualization - Operating System Support** folder, select the entry, and then click **View OS Support Information**.

Step 4 Select the folder category for the required Operating Systems.
The related details are displayed in the following areas:

- Operating System
- Versions
- Legacy-BIOS
- UEFI
- vMedia Support
- Third Party Server

Note
You can also access the latest Compatibility Matrix Guide by clicking the **Launch Compatibility Matrix Guide** icon under the **Compatibility Matrix** area.



CHAPTER 17

Managing Lifecycles

This chapter contains the following sections:

- Managing VM Power Settings, on page 395
- Managing VM Snapshots, on page 396
- Configuring the Lease Time for a Virtual Machine, on page 399
- Managing VM Actions, on page 400
- Applying a Tag to a VM, on page 423
- Mounting an ISO Image as a CD/DVD Drive, on page 423
- Unmounting an ISO Image as a CD/DVD Drive, on page 424

Managing VM Power Settings

Before you begin

You must be logged in to the appliance to complete this task.

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, choose the cloud.

Step 3 On the **Compute** page, click **VMs**.

Step 4 Click the row with the VM on which you want to perform an action.

Step 5 Choose an action and the **VM Task** screen appears.

Name	Description
VM Name display-only field	The name of the VM that is the subject of the action.
Power Off display-only field	The task to power off the VM.
Power On display-only field	The task to power on the VM.
Suspend display-only field	The task to put the VM in a suspended state.

Name	Description
Shutdown Guest display-only field	The task to shut down the guest OS on the VM.
Standby display-only field	The task to move the VM into a standby state. **Note** Not supported in the RHEV KVM Connector.
Reset display-only field	The task to perform a hard reset of the VM. **Note** Not supported in the RHEV KVM Connector.
Reboot display-only field	The task to perform a soft reboot of the VM. **Note** Not supported in the RHEV KVM Connector.
Comments field	Enter any comments that help identify the VM.
Schedule Action radio button	The task to power on a VM now or later at a specific date and time.

Step 6 Click **Proceed**.

Managing VM Snapshots

This process includes the following tasks:

- Create Snapshot—You can create a snapshot of all the VM's resources in their current state.
- Revert Snapshot—If the VM crashes or malfunctions (For example, if the OS becomes corrupt), you can revert to the most recent snapshot of the VM. Where there are multiple snapshots for a VM, you can revert to a specific snapshot.
- Mark Golden Snapshot—You can mark a specific snapshot for a VM as a Golden Snapshot. This feature protects the snapshot from accidental deletion.
- Delete a Snapshot—You can delete a snapshot, if necessary. A Golden Snapshot must be first unmarked before it can be deleted.
- Delete All Snapshots—You can delete all snapshots for a VM. However, you cannot delete all snapshots if they include Golden Snapshots. You must first unmark any Golden Snapshot and then delete all snapshots.

Creating VM Snapshots

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, choose the cloud.

Step 3 On the **Compute** page, click **VMs**.

Step 4 Click the row with the VM for which you want to create a snapshot.

Step 5 From the **More Actions** drop-down list, choose **Create Snapshot**.

Step 6 On the **Create Virtual Machine Snapshot** screen, complete the following fields:

Name	Description
Snapshot Name field	The snapshot name.
Snapshot Description field	The snapshot description.
Snapshot Memory check box	Check the check box to include the VM memory in the snapshot.
Quiesce Guest File System check box	Check the check box to take the snapshot in quiesce mode. **Note** Quiescing a file system brings the on-disk data of a physical or virtual computer into a state that is suitable for backups. This process might include operations such as flushing buffers from the operating systems in-memory cache to disk, or other higher-level application-specific tasks. To use this option, VMware Tools must be installed on the VM.

Step 7 Click **Proceed**.

Reverting to a Snapshot

Before you begin

You must be logged in to the appliance to complete this task.

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, choose the cloud.

Step 3 On the **Compute** page, click **VMs**.
Step 4 Click the row with the VM that you want to revert to a snapshot.
Step 5 From the **More Actions** drop-down list, choose **Revert Snapshot**.
Step 6 On the **Revert Snapshot Task** screen, check the name of the desired snapshot.
Step 7 Click **Proceed**.

Marking a Golden Snapshot

Procedure

Step 1 Choose **Virtual** > **Compute**.
Step 2 On the **Compute** page, choose the cloud.
Step 3 On the **Compute** page, click **VMs**.
Step 4 Click the row with the VM for which you want to mark a snapshot as golden.
Step 5 From the **More Actions** drop-down list, choose **Mark Golden Snapshot**.
Step 6 On the **Mark Golden Snapshot Task** screen, check the name of the desired snapshot.
Step 7 Check **Mark as Golden Snapshot**.
Step 8 Click **Proceed**.

Deleting a Snapshot

Procedure

Step 1 Choose **Virtual** > **Compute**.
Step 2 On the **Compute** page, choose the cloud.
Step 3 On the **Compute** page, click **VMs**.
Step 4 Click the row with the VM for which you want to delete a snapshot.
Step 5 From the **More Actions** drop-down list, choose **Delete Snapshot**.
Step 6 On the **Delete Snapshot Task** screen, check the name of the desired snapshot.
Step 7 Check **Delete Children** to delete child snapshots of the selected snapshot.
Step 8 Click **Proceed**.

Deleting All Snapshots

Procedure

Step 1 Choose **Virtual** > **Compute**.
Step 2 On the **Compute** page, choose the cloud.
Step 3 On the **Compute** page, click **VMs**.
Step 4 Click the row with the VM for which you want to delete all snapshots.
Step 5 From the **More Actions** drop-down list, choose **Delete All Snapshots**.
Step 6 On the **VM Snapshot Task** screen, enter an optional comment.
Step 7 Click **Proceed**.

Configuring the Lease Time for a Virtual Machine

A user can configure a lease expiration time for a selected virtual machine (VM). Once the lease time expires, the VM is powered down. The lease time end is a calendar selection.

Procedure

Step 1 Choose **Virtual** > **Compute**.
Step 2 On the **Compute** page, choose the cloud.
Step 3 On the **Compute** page, click **VMs**.
Step 4 Click the row with the VM for which you want to configure the lease time.
Step 5 From the **More Actions** drop-down list, choose **Configure Lease Time**.
Step 6 On the **Configure Lease Time** screen, check **Set Lease Time**. Complete the following fields:

Name	Description
VM Name field	The name specified while creating the VM. Once entered, you cannot edit the name of the VM.
Lease Date/Time calendar, drop-down lists, radio buttons	The lease date and time for the VM. There are calendars for the Date, drop-down lists for the Time (hour and minute), and radio buttons for AM or PM.

Step 7 Click **Submit**.

Managing VM Actions

After creating a VM, you can perform additional tasks on it, by using menus available in the user interface. You can access these menus in one of the following ways:

- Right clicking on a VM to view a list of limited options,
- Choosing a VM and clicking the down arrow option on the toolbar for a complete list of options.

Following are the other VM actions:

- View VM Details—You can access individual VMs to view details, such as summary reports, vNICs, disks, and snapshots.
- Stack View—You can view stacks of information about a particular VM including, OS, hypervisor, and infrastructure information.
- Delete a VM—You can delete a VM from the list. Only a powered-off VM can be deleted.
- Create a VM Disk—You can add an additional disk with a custom size to a VM.
- Delete a VM Disk—You can delete a disk.
- Add vNICs—You can add multiple vNICs to a VM. You also have the option to add or replace a vNIC in a VM. The options for vNICs depend on the network policy mapped to the VDC associated with the VM.
- Launch VM Client—You can set up and access either web access, remote desktop, or VMRC Console access for a VM.
- VMRC Console (HTML5)—You can launch a VMRC HTML5 console that is web browser and plug-in independent.
- Assign VM—You can assign a VM to a group or VDC and modify the category of the VM. You can set the provisioning time, termination time, and label for a VM.
- Access VM Credentials—You can access a VM's login credentials when it is set up for web or remote desktop access, but only if the administrator provides the privileges in the catalog from which the VM is provisioned.
- Inventory Collection Request for VM—You can choose a VM and request on-demand inventory collection.
- Test VNC—You can test VNC connectivity, for troubleshooting purposes.
- Clone—You can clone or make a copy of an existing VM to make a new VM with the same or similar qualities.
- Move a VM to VDC—You can move a VM to a VDC so that the rules of the VDC system policy are followed in the VM.
- VM Resync—You can choose to set the number of minutes to have a VM resynchronize its time periodically with Cisco UCS Director.
- Mount ISO Image as CD/DVD Drive—You can mount ISO images on the VM without using a physical drive. Once mounted in your virtual machine, you can open, extract, and use the files from a virtual CD/DVD drive without a physical disk.

- Unmount ISO Image as CD/DVD Drive—You can unmount an ISO image already attached to CD/DVD drive on the virtual machine.

Viewing VM Details

Procedure

Step 1 Choose **Virtual** > **Compute**.
Step 2 On the **Compute** page, choose the cloud.
Step 3 On the **Compute** page, click **VMs**.
Step 4 Click the row with the VM for which you want to view the details.
Step 5 Click **View Details**.

Resizing VMs

Procedure

Step 1 Choose **Virtual** > **Compute**.
Step 2 On the **Compute** page, choose the cloud.
Step 3 On the **Compute** page, click **VMs**.
Step 4 Click the row with the VM that you want to resize.
Step 5 From the **More Actions** drop-down list, choose **Resize VM**.
Step 6 On the **Resize VM** screen, complete the following fields:

Name	Description
VM Name field	The name of the selected VM.
Current Allocated CPU field	The number of allocated CPUs being used by the VM.
Current Allocated Memory (GB) field	The amount of memory allocated to the VM.
New CPU Count drop-down list	Choose the CPU required.
New Cores Per Socket drop-down list	Choose the cores per socket.

Name	Description
New Memory (GB)	Enter the new memory size in GB. Enter a numeric value in this field. This numeric value should be among the comma separated values specified in the Computing policy associated with this VM. For VM(s) that are not associated with any Computing Policy, you can provide your own numeric input based on the resource availability.
Current CPU Cost (Currency: USD) field	Displays the current CPU cost per-hour. This value is calculated based on the currently allocated CPU for the VM.
Current Memory Cost (Currency: USD) field	Displays the current memory cost per-hour. This value is calculated based on the currently allocated memory for the VM.
New CPU Cost (Currency: USD) field	Displays the CPU cost per-hour based on the CPU count specified for the VM.
New Memory Cost (Currency: USD)	Displays the memory cost per-hour based on the memory specified for the VM.

Important
If you checked the **Disable displaying cost details** check box while adding or modifying the VDC, then information on the current and new CPU cost and memory cost is not displayed.

Step 7 Click **Resize**.

Using the Stack View Option

Procedure

Step 1 Choose **Virtual** > **Compute**.
Step 2 On the **Compute** page, choose the cloud.
Step 3 On the **Compute** page, click **VMs**.
Step 4 Click the row with the VM for which you want to view the stack view.
Step 5 Click **Stack View**.

The **Stack View** screen displays information on the selected VM.

Note
- If there are multiple components in the report, such as hard drives or network adapters, you can click the arrow displayed on each component and select a different component.

- You can view additional information on each component by clicking the eye icon.

Creating a VM Disk

You can create a VM disk only if you checked **Allow Resizing of Disk** while configuring the storage policy that is mapped to the vDC.

Before you begin

The VM should be in the powered off state.

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, choose the cloud.

Step 3 On the **Compute** page, click **VMs**.

Step 4 Click the row with the VM on which you want to create a VM disk.

Step 5 From the **More Actions** drop-down list, choose **Create VM Disk**.

Step 6 On the **Create VM Disk** screen, complete the following fields:

Name	Description
VM Name field	The name of the VM. Once entered, the VM name cannot be edited.
New Disk Size (GB) field	The disk size for the VM, in GB. You must enter an integer in this field, and this integer should be within the range specified in the storage policy associated with this VM.
Select Disk Type drop-down list	Choose the disk type. It can be one of the following: • **System** • **Swap** • **Data** • **Database** • **Log**
Select Datastore/Datastore Cluster drop-down list	Specify if the VM disk should be created from a datastore or a datastore cluster.

Name	Description
Select Datastore field	Click **Select** and choose which datastore you want to use to create the VM disk. **Note** The available datastores depend upon the storage policy associated with the VDC. Only datastores that meet the criteria specified in the storage policy are available for the VM disk. This field is only available if you specify that the VM disk should be created from a datastore.
Select Datastore Cluster field	Click **Select** and choose which datastore cluster you want to use to create the VM disk. **Note** The available datastore clusters depend upon the storage policy associated with the VDC. Only datastore clusters that meet the criteria specified in the storage policy are available for the VM disk. This field is only available if you specify that the VM disk should be created from a datastore cluster.
Thin Provision check box	Check the check box to add a thin provisioned disk to the VM. **Note** Thin provisioning enables dynamic allocation of the physical storage capacity to increase VM storage utilization.
Compute New Disk Cost field	This option calculates and displays the disk cost, per hour, based on the new disk size and the datastore you have specified for the VM disk. **Important** If you checked the **Disable displaying cost details** check box while adding or modifying the VDC, then the **Compute New Disk Cost** field is not displayed.

Step 7 Click **Create**.

Resizing a VM Disk

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, choose the cloud.

Step 3 On the **Compute** page, click **VMs**.

Step 4 Click the row with the VM for which you want to resize the VM disk.

Step 5 From the **More Actions** drop-down list, choose **Resize VM Disk**.

Step 6 On the **Resize VM Disk** screen, complete the following fields:

Name	Description
VM Name field	The name of the VM. This name cannot be edited.
Select Disk drop-down list	Select the VM disk from the drop-down list.
Total Provisioned (GB) field	Displays the total provisioned space on the VM.
New Size (GB) field	The new size for the VM. Enter an integer in this field. This integer should be within the range or among the comma separated values specified in the storage policy associated with this VM and should be greater than the total provisioned size.
Current Disk Cost (Currency: USD) field	Displays the current disk cost per hour.
Compute New Disk Cost field	This option calculates the disk cost, per hour, based on the new disk size you specified.
New Disk Cost (Currency: USD) field	Displays the disk cost per hour for the new disk size specified for the VM.

Important
If you checked the **Disable displaying cost details** check box while adding or modifying the VDC, then information on the current and new disk cost is not displayed.

Step 7 Click **Resize**.

Locking VMs in Cisco UCS Director

As an administrator in Cisco UCS Director, you can create a list of VMs that you would like locked. Locking VMs implies preventing actions from running on the specified VMs. These actions could be shutting down, resetting, or powering off VMs.

Procedure

Step 1 Create an XML file titled `VMControls.xml` which is similar to the following:

```
<VMControlList>
--<VMControl>
    <ControlType>lock</ControlType>
    <MatchType>VM-IPAddress</MatchType>
    <MatchValue>19.19.19.19</MatchValue>
    <IsRegex>false</IsRegex>
    <ContactEmail>admin@admin.com</ContactEmail>
   --<Label>
      Do not shutdown or delete my machine.
   --</Label>
--</VMControl>
--<VMControl>
    <ControlType>lock</ControlType>
    <MatchType>VM-IPAddress</MatchType>
    <MatchValue>19.29.29.29*</MatchValue>
    <IsRegex>true</IsRegex>
    <ContactEmail>admin@admin.com</ContactEmail>
   --<Label>
      Do not shutdown or delete this machine.
   --</Label>
--</VMControl>
</VMControlList>
```

Step 2 Host this file on a server that is accessible from the system that is running Cisco UCS Director.

Step 3 Choose **Administration** > **System**.

Step 4 On the **System** page, click **System Parameters**.

Step 5 In the **Download VM Locking Controls From URL** field, enter the URL of the XML file.

The URL will look similar to this: `<ip_address>:8000/VMControls.xml`.

Step 6 Click **Save**.

Step 7 On the **System** page, click **System Tasks**.

Step 8 Search for and select the **VM Control List Poller Task**.

Step 9 Click **Run Now**.

This system task downloads the `VMControls.xml` file and saves it in the inventory database. After this system task is run, actions such as powering off, or shutting down are prevented from running on VMs that match the IP addresses specified in the XML file.

Adding vNICs



Note When you add a vNIC VM, the values of the **Port Group Name** and **Adapter Type** parameters are modified. The IP address of the VM is changed only if DHCP is enabled on the selected port group. However, the IP address is not modified if it is sourced from a static pool policy.

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, choose the cloud.

Step 3 On the **Compute** page, click **VMs**.

Step 4 Click the rwo with the VM to which you want to add a vNIC.

Step 5 From the **More Actions** drop-down list, choose **Add vNICs**.

Step 6 On the **Add VM vNICs** screen, choose **Add** from the **Operation** drop-down list.

This addition is not allowed if the vNIC limit configured in the network policy will be exceeded.

Step 7 Expand the **VM NETWORKS** list.

Step 8 Click **Add (+)**.

Step 9 On the **Add Entry to VM Networks** screen, complete the following fields:

Name	Description
NIC Alias drop-down list	Choose a NIC alias from the list.
Port Group Type display-only drop-down list	Choose a port group from the list.
Port Group Name drop-down list	Choose a port group name from the list.
Adapter Type display-only drop-down list	Choose the adapter type. The choice is available only if the NIC alias does not have **Copy Adapter Type from Template** chosen in the network policy.
DHCP check box	If this field is checked, then the IP is assigned using DHCP.
Static IP Pool field	The static IP address pool.
Network Mask field	The network mask.
Gateway IP Address field	The gateway IP address.

Note
The **NIC Alias**, **Port Group Name**, **Adapter Type**, **DHCP**, and **Static IP Pool** choices depend on the settings in the network policies associated with the VM (VM's VDC). For more information about multiple NIC network policies, see Managing Policies, on page 207.

The VM is powered down to perform this action. The VM will power up once the action is completed.

Step 10 Click **Submit**.

Replacing a vNIC

Note When you replace a vNIC VM, the values for the **Port Group Name** and **Adapter Type** parameters are modified. The IP address of the VM is changed only if DHCP is enabled on the selected port group. However, the IP address is not modified if it is sourced from a static pool policy.

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, choose the cloud.

Step 3 On the **Compute** page, click **VMs**.

Step 4 Click the row with the VM for which you want to replace a vNIC.

Step 5 From the **More Actions** drop-down list, choose **Add vNICs**.

Step 6 On the **Add VM vNICs** screen, choose **Replace** from the **Operation** drop-down list.

This replacement is not allowed if the additional vNIC limit configured in the network policy will be exceeded.

Step 7 Choose a vNIC.

Step 8 On the **Add vNIC** screen, complete the following fields:

Name	Description
NIC Alias drop-down list	Choose a NIC alias. Only the vNICs configured in the network policy are visible here.
Port Group Name drop-down list	Choose a port group name from the list.
Adapter Type display-only drop-down list	Choose the adapter type. The choice is available only if the choice of the NIC alias does not have **Copy Adapter Type from Template** chosen in the network policy.
DHCP check box	Check the check box if you want the IP assigned using DHCP.
Static IP Pool field	The static IP address pool.
Network Mask field	The network mask.
Gateway IP Address field	The gateway IP address.

Step 9 Click **Submit**.

Note
The VM is powered down to perform this action. The VM is powered up once the action is completed. The **Replace** task removes all existing vNICs from the VM and replaces them with the vNICs that were added.

The **NIC Alias**, **Port Group Name**, **Adapter Type**, **DHCP**, and **Static IP Pool** choices depend on the settings in the network policy associated with the VM (VM's VDC). For more information about multiple NIC network policies, see Managing Policies, on page 207.

Launching the VM Client

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, choose the cloud.

Step 3 On the **Compute** page, click **VMs**.

Step 4 Click the row with the VM for which you want to launch the VM client.

Step 5 Click **Launch VM Client**.

Step 6 On the **Launch Client** screen choose an access scheme for the VM Client.

If a VM is provisioned through Cisco UCS Director, the access schemes displayed in this dialog box are defined by the options enabled in the catalog used to provision the VM.

For a VM that is discovered, the options, **Remote Desktop**, **Web Access**, **VMRC Console (Browser Plug-in)**, and **VMRC Console (Standalone Plug-in)** are displayed.

Step 7 Click **Proceed**.

Enabling the VNC Console on a VM

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, choose the cloud.

Step 3 On the **Compute** page, click **VMs**.

Step 4 Click the row with the VM for which you want to configure VNC.

Step 5 From the **More Actions** drop-down list, choose **Configure VNC**.

Step 6 On the **Configure VNC** screen, choose a keyboard mapping language from the drop-down list.

- French (Switzerland)
- Japanese
- US English
- Italian

- Icelandic
- UK English
- French (Belgium)
- German (Switzerland)
- German
- Spanish
- Norwegian
- Finnish
- Polish

Step 7 Click **Submit**.

Step 8 Click **OK**.

The system automatically configures VNC console access to a VM when a request is submitted.

Automatically Unconfiguring the VNC Console on a VM

You can enable the VMware Monitor VNC Port Task to enable automatic unconfiguration of VNC consoles. This task runs every 30 minutes and unconfigures VNC ports that are open for more than a default of 60 minutes. VNC is unconfigured on the ports, and the ports are released for future allocation.

You can modify the frequency in which the task is run by clicking **Manage System Task** and selecting the duration from the drop-down list.

You can modify the port wait time by editing the `unConfigureVNCPortWaitTime` parameter in the `/opt/infra/inframgr/vmware.properties` file.

Procedure

Step 1 Choose **Administration** > **System**.

Step 2 On the **System** page, click **System Tasks**.

Step 3 Click the **VMware Standard Tasks** arrow to expand its tasks.

Step 4 Click the row with the **VMware Monitor VNC Port Task** system task.

Step 5 Click **Manage Task**.

Step 6 From the **Task Execution** drop-down list, choose **Enable**.

Step 7 Click **Submit**.

Accessing VM Console Using VNC Client

The VNC client is an Ajax-based application that provides access to a VM console. The console window can be launched by using any standalone web browser. It does not require a dedicated browser plug-in and it provides full VM control capabilities. However, you must disable popup blockers in the browser for the VNC console to launch.

Before you begin

- You must configure ESX/ESXi server for VNC access to VM console. For more information, see Configuring ESX/ESXi Server for VNC Access to VM Console, on page 411.
- Cisco UCS Director provides automatic configuration of the VM console access using VNC client. To configure, you must open ports 5901-5964 in the ESX/ESXi server to the Cisco UCS Director appliance.
- Import a self-signed certificate or a CA certificate using Cisco UCS Director admin shell. Importing a certificate enables secured access to the VM console using the VNC client. For more information on importing certificates, see the Cisco UCS Director Shell Guide
- Disable popup blockers in your browser.



Note VMware with ESX 4.x, ESXi 5.x, ESXi 6.0, 6.5 and 6.7 versions is supported for configuring VM console access using the VNC client.

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, choose the cloud.

Step 3 On the **Compute** page, click **VMs**.

Step 4 Click the row with the VM for which you want to launch the VNC console.

Step 5 Click **Launch VNC Console**.

Step 6 On the **Launch VNC Console** screen, choose the keyboard mapping layout, and click **Submit**.

Tip
If the screen is blank, click in the black area and press **Enter**.

Configuring ESX/ESXi Server for VNC Access to VM Console

VMware with ESX 4.x and ESXi 5.x versions is supported to configure VNC access to the VM console.

Procedure

Step 1 Log in to ESXi5.x host.

Step 2 Using the shell, disable the firewall configuration.

Step 3 Copy and paste the following XML configuration to the `vnc.xml` file.

```
 # cat /etc/vmware/firewall/vnc.xml
<!-- Firewall configuration information for VNC -->
<ConfigRoot>
  <service>
   <id>VNC</id>
    <rule id='0000'>
    <direction>inbound</direction>
     <protocol>tcp</protocol>
     <porttype>dst</porttype>
     <port>
     <begin>5901</begin>
     <end>5964</end>
     </port>
    </rule>
    <rule id='0001'>
     <direction>outbound</direction>
     <protocol>tcp</protocol>
     <porttype>dst</porttype>
     <port>
      <begin>0</begin>
      <end>65535</end>
     </port>
    </rule>
    <enabled>true</enabled>
    <required>false</required>
  </service>
</ConfigRoot>
```

Note
This `vnc.xml` file is available when VNC is enabled for the host. If this file is not available, then create a `vnc.xml` file, add the configuration lines mentioned in this procedure, and save the file.

Step 4 Refresh the firewall rules and verify that the new configuration is accurately loaded.

```
~ # esxcli network firewall refresh
~ # esxcli network firewall ruleset list | grep VNC
VNC   true #**************************************
```

Step 5 Repeat these steps on all ESXi hosts in an ESXi cluster.

Accessing VMRC Console

Before you begin

- Make sure to import a self-signed certificate or a CA certificate using Cisco UCS Director admin shell. Importing a certificate enables secured access to the VMRC console.

Note The VMRC module does not support importing of SSL certificates that use passphrase.

For more information on importing certificates, see the Cisco UCS Director Shell Guide.

- Make sure to start the VMRC tunneling service using Cisco UCS Director admin shell. For more information on starting the VMRC tunneling service, see the Cisco UCS Director Shell Guide.
- Disable popup blockers in your browser.
- Access https://<IP-Address>:VMRC_PORT and accept the certificate. For example, https://<IP-Address>:9002

Note VMRC_PORT is a configurable parameter that is available in the `/opt/infra/inframgr/tesseract.properties` file. To view the debug logs, you can add the **traceEnabled** field in the `/opt/infra/inframgr/tesseract.properties` file and set the value to **true** or **yes**.

- Make sure to open the VMRC_PORT (for example, port 9002) in the proxy server while accessing the Cisco UCS Director appliance through the proxy server.
- Make sure that the HTTPs traffic is enabled between the Cisco UCS Director and the ESXi host.
- Make sure that VNC is disabled. If VNC is enabled on a VM, disable the VNC and reboot the VM.

Procedure

Step 1 Choose **Virtual** > **Compute**.
Step 2 On the **Compute** page, choose the cloud.
Step 3 On the **Compute** page, click **VMs**.
Step 4 Click the row with the VM for which you want to launch the VMRC console.
Step 5 Click **VMRC Console (HTLM5)**. The VMRC console opens in a new tab.

Assigning a VM

You can assign a resource or a VM to a user group. If the resource or VM is in a VMWare cloud, then you can also assign it to a specific end user in Cisco UCS Director.

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, choose the cloud.

Step 3 On the **Compute** page, click **VMs**.

Step 4 Click on the row with the VM that you want to assign.

Step 5 From the **More Actions** drop-down list, choose **Assign VM**.

Step 6 On the **Assign VM** screen, complete the following fields:

Name	Description
VM Name field	The name of the VM.
VM Ownership Section	
Customer Organizations radio button	Select this radio button to assign the VM to a specific group.
Cutomer Organizations field	Click **Select** to choose the specific user group to which you want to assign the VM. This field is visible only when you select the **Customer Organizations** radio button. **Note** Only groups that have valid vDCs are displayed.
User radio button	Select this radio button to assign the VM to a specific user.
User field	Click **Select** to choose the user to whom you want to assign the VM. This list is populated with users from groups that allow resource assignment to users.
VM Access Sharing Section	
Users with Access Privilege field	Click **Select** to choose users who can only access VM information. The selected users can only access the VM. They cannot perform any administrative actions This option is only available if the **User** radio button is selected and you have selected a specific user for this VM.

Name	Description
Users with Manage Privilege field	Click **Select** to choose users who can only manage the VM. The selected users can perform administrative tasks on the VM. This option is only available if the **User** radio button is selected and you have selected a specific user for this VM.
General Assignment Information Section	
VDC drop-down list	Choose the VDC.
Category drop-down list	Choose the category for the VM.
VM User Label field	The VM label if required.
Set Provision Time check box	Check the check box to set a specific provisioning time for the VM.
Provision Date/Time calendar, drop-down lists, radio buttons	The VM's provisioning date and time. There are calendars for the Date, drop-down lists for the Time (hour and minute), and radio buttons for AM or PM. This option appears when **Set Provision Time** is checked.
Comments field	Add any comments about the task, if necessary.

Step 7 Click **Assign**.

VM Credentials

The web or remote access login credentials for a VM can only be viewed if the administrator provides the necessary privileges in the Catalog from which the VM is provisioned.

Viewing VM Credentials

Before you begin

You must be logged in to the appliance to complete this task.

Procedure

Step 1 Choose **Virtual** > **Compute**.
Step 2 On the **Compute** page, choose the cloud.
Step 3 On the **Compute** page, click **VMs**.

Step 4 Click the row with the VM for which you want to view the credentials.

Step 5 From the **More Actions** drop-down list, choose **Access VM Credentials**.

Initiating Inventory Collection for a VM

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, choose the cloud.

Step 3 On the **Compute** page, click **VMs**.

Step 4 Click the row with the VM for which you want to request an inventory collection.

Step 5 From the **More Actions** drop-down list, choose **Inventory Collection Request for VM**.

Step 6 Click **Submit**.

Testing VNC Connectivity

Testing VNC connectivity is used for troubleshooting purposes. A successful test for VNC connectivity displays the host node IP address and VNC port number. For example: `VNC connectivity intact at 172.16.0.1:5921`.

However if connectivity fails, a failure message displays. For example: `VM is not configured for VNC yet`.

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, choose the cloud.

Step 3 On the **Compute** page, click **VMs**.

Step 4 Click the row with the VM on which you want to test VNC connectivity.

Step 5 From the **More Actions** drop-down list, choose **Test VNC**.

Step 6 On the **Test VNC Connectivity** screen, click **Submit**.

Step 7 Use the result to troubleshoot VNC connectivity.

Note
If connectivity fails, then there is no VNC port assigned to the VM IP address. For more information, see Enabling the VNC Console on a VM, on page 409.

Cloning a VM

Cloning a VM allows you to create a new VM in the system by using some of the parameters defined in an existing VM. The cloning option helps you create a VM faster, especially if you want to modify only a few parameters of an existing VM. The name that you specify for the cloned VM is defined by the system policy.

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, choose the cloud.

Step 3 On the **Compute** page, click **VMs**.

Step 4 Click the row with the VM that you want to clone.

Step 5 From the **More Actions** drop-down list, choose **Clone**.

Step 6 On the **Clone VM: Select Group** screen, complete the following fields:

Name	Description
Select Group list	Expand the list to choose a predefined group to clone and click **Select**. The **Default Group** is chosen by default.
Assign To User check box	Check the box to assign the VM to a specific user. This option is visible only if resource assignment to users is enabled for the group share policy that is applied to the selected user group. For more information on creating a group share policy, see Creating a Group Share Policy, on page 218.
User drop-down list	Choose the user to whom this VM is assigned. **Note** Currently, only VMs that are in a VMware cloud can be assigned to a specific user.
Use Linked Clone check box	Check the box to clone a VM from a linked clone. **Note** A linked clone is a copy of a virtual machine that shares virtual disks with the parent VM. A linked clone is made from a snapshot of the parent VM. A linked clone must have access to the parent VM. Without access to the parent VM, a linked clone is disabled. Linked Clone or Full Clone depends on the Linked Clone selection in the Storage Policy.

Name	Description
Select Snapshot Type drop-down list	Choose the type of snapshot that is associated with the linked clone. You can choose one of the following: • **Existing Snapshot** • **New Snapshot**
Select Existing Snapshot list	Expand the list to choose an existing snapshot and click **Select**. **Note** This field appears only when you select **Existing Snapshot**.
Snapshot Name field	Enter a name for the new snapshot. **Note** This field appears only when you select **New Snapshot**.
Use ReadyClone check box	Check the box to ensure that VMs are deployed using ReadyClones. When this box is checked, the **Use Linked Clone** check box is hidden.

Step 7 Click **Next**.

Step 8 On the **Clone VM: Customization Options** screen, complete the following fields:

Name	Description
Category list	Expand the list to choose the required VM category and click **Select**.
Credential Options drop-down list	Choose to allow or disallow users to retrieve VM access credentials (shared). The following options are available: • **Do not share** • **Share after password reset** • **Share template credentials** The **Do not share** option is chosen if the administrator wants to send the credentials privately to another user outside Cisco UCS Director.
User ID field	Enter the user ID. This field is available only if a choice is made to share under **Credential Options**.

Name	Description
Password field	Enter the user password. This field is available only if a choice is made to share under **Credential Options**.
Provision all disks in a single datastore check box	Check the box to provision all VM disks in the previously configured single datastore.
Perform deployment assessment check box	Check the box to assess the budget allocation, resource limits, and resource availability prior to cloning a VM. After you check this box, the summary of the assessment is displayed on the **Deployment Assessment** screen. **Note** This option is visible only for VMware clouds.
Automatic Guest Customization Enable check box	This box is checked.
Post Provisioning Custom Actions Enable check box	Check the box to enable execution of an orchestration workflow after VM provisioning. The chosen workflow initiates when provisioning starts.
Workflow drop-down list	Choose a defined workflow for provisioning. **Note** This field appears when **Post Provisioning Custom Actions Enable** is checked. Any workflow input values are entered on the **Clone VM: Custom Workflow** screen.
VM App Charge Frequency drop-down list	Choose **Hourly** or **Monthly**.
Active VM Application Cost field	Enter the cost for the application that is included in the template.
Inactive VM Application Cost field	Enter the cost to this catalog of a VM in inactive state, per hour or month.

Step 9 Click **Next**.

Step 10 On the **Clone VM: Deployment Configuration** screen, complete the following fields:

Name	Description
Select VDC drop-down list	Choose a VDC containing the policies you want for the VM.
Comment field	Optionally, enter a description of the VDC.

Name	Description
Provision drop-down list	Choose **Now** to provision the VDC now or choose **Later** to provision the VDC later. If you choose **Later**, then fields to specify the date and time appear.
Lease Time check box	Check the box to configure a lease expiration time.
Days field	Enter the number of days for the lease time. **Note** This field appears only when **Lease Time** is checked.
Hours field	Enter the number of hours for the lease time. **Note** This field appears only when **Lease Time** is checked.

Step 11 Click **Next**.

Step 12 On the **Clone VM: Custom Specification** screen, complete the following fields:

Name	Description
CPU Cores drop-down list	Choose the CPU cores for the VM being provisioned.
Cores Per Socket drop-down list	Choose the cores per socket for the VM being provisioned. The number of cores per socket available is specified in the VM computing policy.
Memory drop-down list	Choose the amount of memory for the VM being provisioned.

Step 13 Click **Next**.

Step 14 On the **Clone VM: Custom Workflow** screen, enter any workflow input values, if applicable.

Step 15 Click **Next**.

Step 16 On the **Clone VM: Select Datastores** screen, expand **VM Disks** to assign any applicable datastores to the applicable disk.

Step 17 Click the row of the disk to which you want to assign a datastore.

Step 18 Click **Edit selected entry in the table below**.

Step 19 On the **Edit VM Disks Entry** screen, complete the following fields:

Name	Description
Disk Name	The name of the VM disk to which datastores are assigned.
Disk Type	Choose the VM disk type. For example, **System**.

Name	Description
Selected Datastores	Choose the datastores that you want for this VM disk. The available datastore choices are from the data storage policy associated with the VDC.
Do not resize check box	Check this box if you do not want the disks resized before cloning the VM. If you check this box, then the **Size** drop-down list is hidden.
Size drop-down list	Choose the new size of the disk while cloning the VM. **Note** You can edit the size of the disk only if you enabled **Allow Resizing of Disk** in the storage policy.

Step 20 Click **Submit**.

Step 21 Click **Next**.

Step 22 On the **Clone VM: Select VM Networks** screen, click the **VM Networks** pencil icon to edit a VM network.

Note
The **Clone VM: Select VM Networks** screen is empty unless **Allow end user to select optional NICs** is chosen in the network policy.

Step 23 On the **Select** screen, choose the clouds that you want associated with the VM.

Step 24 Click **Submit**.

Step 25 Click **Next**.

Step 26 Required: If you checked **Perform deployment assessment** on the **Clone VM: Customization Options** screen, then review the report of the assessment displayed on the **Deployment Assessment** screen.

If this assessment report identifies errors, return to the previous screens and rectify the errors before submitting the request. If the assessment report shows no errors, then you can continue.

Step 27 Click **Next**.

Step 28 Review the cloned VM information on the **Clone VM: Summary** screen.

Step 29 Click **Submit**.

The cloned VM gets its new name from the VDC policy.

Moving a VM to VDC

A VM is moved to a VDC so that the rules of the VDC system policy are followed in the VM. The existing VM is replaced by the one that is moved to the VDC.

Note The old VM is deleted. The new VM name is given according to the system policy.

Before you begin

You must be logged in to the appliance to complete this task.

Procedure

Step 1 On the menu bar, choose **Virtual** > **Compute**.
Step 2 On the **Compute** page, choose the cloud.
Step 3 On the **Compute** page, click **VMs**.
Step 4 Click the row with the VM that you want to move to a VDC.
Step 5 From the **More Actions** drop-down list, choose **Move VM to VDC**.
Step 6 On the **Move VM to VDC** screen, you can make modifications to the VM that you are moving in the same way you did when cloning a VDC.
See Cloning a VM, on page 417.

Resynchronizing a VM

Before you begin

You must be logged in to the appliance to complete this task.

Procedure

Step 1 Choose **Virtual** > **Compute**.
Step 2 On the **Compute** page, click **Clouds**.
Step 3 On the **Compute** page, click **VMs**.
Step 4 Click the row with the VM that you want to resynchronize.
Step 5 From the **More Actions** drop-down list, choose **Resync VM**.
Step 6 On the **Resync VM** screen, choose the number of minutes from 0 to 30 from the **Max Wait Time** drop-down list.
Step 7 Click **Submit**.

Applying a Tag to a VM

With the introduction of tagging support for a VM, you can manage tags in Cisco UCS Director to categorize and identify specific VMs as firewall VMs or as load balancer VMs.

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, choose the cloud.

Step 3 On the **Compute** page, click **VMs**.

Step 4 Click the row with the VM to which you want to add tags.

Step 5 From the **More Actions** drop-down list, choose **Add Tags**.

Step 6 On the **Add Tags** screen, complete the following fields:

Field	Description
Tag Name drop-down list	Choose the tag that you want to apply to the VM. This drop-down list displays all the tags that you have previously created. You can choose a tag from this list, or create a new tag. For information on creating a tag, see Creating a Tag, on page 157.
Tag Value drop-down list	Choose a value for the tag.

Step 7 Click **Submit**.

What to do next

You can create a tag-based cost model for the VMs. For more information, see Creating a Tag-Based Cost Model, on page 364.

Mounting an ISO Image as a CD/DVD Drive

An ISO is a disk image. You can mount ISO images on the VM without using a physical drive. Once mounted in your virtual machine, you can open, extract, and use the files from a virtual CD/DVD drive without a physical disk.

Procedure

Step 1 Choose **Virtual** > **Compute**.

Step 2 On the **Compute** page, click **VMs**.

Step 3 Click the row with the VM on which you want to mount an ISO image.

Step 4 From the **More Actions** drop-down list, choose **Mount ISO Image As CD/DVD Drive**.

Step 5 On the **CD/DVD Drive Mount ISO** screen, choose the ISO image from the list of available images.

Step 6 Choose one of the following options:

- **Create New CD/DVD Drive** and check **Power OFF VM**.
- **Use Existing CD/DVD Drive** and choose the drive from the **Select DVD/DVD Drive** drop-down list.

Step 7 Click **Submit**.
The new or existing CD/DVD drive is mapped to your VM. You can log into the VM to view the mapped drive.

Unmounting an ISO Image as a CD/DVD Drive

You can unmount an ISO image already attached to CD/DVD drive on the virtual machine.

Procedure

Step 1 Choose **Virtual** > **Compute**.

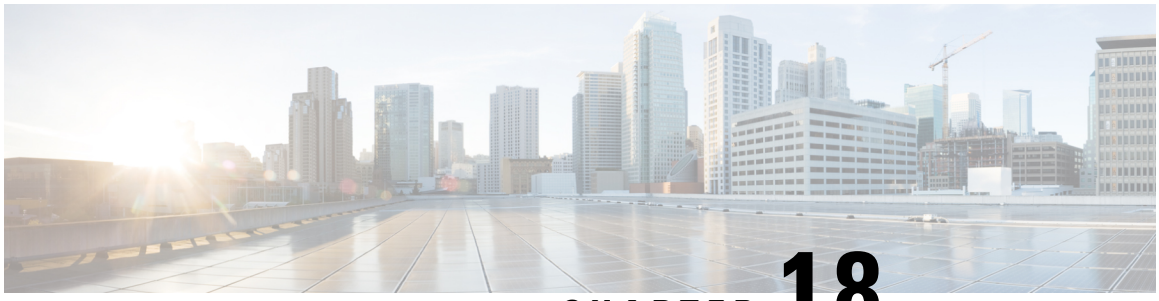
Step 2 On the **Compute** page, click **VMs**.

Step 3 Click the row with the VM on which you want to unmount an ISO image.

Step 4 From the **More Actions** drop-down list, choose **UnMount ISO Image As CD/DVD Drive**.

Step 5 On the **CD/DVD Drive UnMount ISO** screen, choose the CD/DVD drive to unmount from the **Select CD/DVD Drive** drop-down list.

Step 6 Click **Submit**.



CHAPTER 18

Managing CloudSense Analytics

This chapter contains the following sections:

- CloudSense Analytics, on page 425
- Generating a Report, on page 426
- Generating an Assessment, on page 428
- Report Builder for Custom Report Templates, on page 428
- Creating a Report Builder Template, on page 429
- Generating a Report from a Template, on page 430
- Viewing Reports Generated From a Template, on page 431
- Emailing Reports Generated From a Template, on page 432

CloudSense Analytics

CloudSense Analytics in Cisco UCS Director provide visibility into the infrastructure resources utilization, critical performance metrics across the IT infrastructure stack, and capacity in real time. CloudSense significantly improves capacity trending, forecasting, reporting, and planning of virtual and cloud infrastructures.

You can generate the following reports with CloudSense:

- Billing Report for a Customer
- EMC Storage Inventory Report
- NetApp Storage Inventory Report
- NetApp Storage Savings Per Group
- NetApp Storage Savings Report
- Network Impact Assessment Report
- Organizational Usage of Virtual Computing Infrastructure
- PNSC Account Summary Report
- Physical Infrastructure Inventory Report for a Group
- Storage Dedupe Status Report
- Storage Inventory Report For A Group

- Thin Provisioned Space Report
- UCS Data Center Inventory Report
- VM Activity Report by Group
- VMware Host Performance Summary
- Virtual Infrastructure and Assets Report



Note This is a complete list of reports available in the system. However, the number of reports available in the system for a user depends on the user role. By default, the **CloudSense** option is not visible to MSP administrators. The system administrator needs to enable this option for MSP administrators. Once this is done, then when an MSP administrator logs in, only reports relevant to customer organizations are displayed.

Generating a Report

Before you begin

You must be signed into the appliance before completing this task.

Procedure

Step 1 Choose **CloudSense** > **Reports**.

Step 2 Click a tab based on the type of report you want to generate. It can be one of the following:

- Application Container Report
- Billing Report for a Customer
- Cisco C880M4 Inventory Report
- EMC Storage Inventory Report
- Group Infrastructure Inventory Report
- Hyper V Cloud Utilization Summary Report
- IBM Storwize Inventory Report
- NetApp Storage Inventory Report
- NetApp Storage Savings Per Group Report
- NetApp Storage Savings Report
- Network Impact Assessment Report
- Organizational Usage of Virtual Computing Infrastructure Report
- PNSC Account Summary Report

- Physical Infrastructure Inventory Report for a Group
- Service Request Statistics
- Service Request Statistics Per Group
- Storage Dedupe Status Report
- Storage Inventory Report for a Group
- Thin Provisioned Space Report
- UCS Data Center Inventory Report
- VM Activity Report By Group
- VM Performance Summary Report
- VMware Cloud Utilization Summary Report
- VMware Host Performance Summary Report
- Virtual Infrastructure and Assets Report

Step 3 Click **Generate Report**.

Step 4 In the **Generate Report** screen, complete the required fields, including the following:

Name	Description
Context drop-down list	Select the group that you want to generate the report for. **Note** If you are an administrator, then this drop-down list displays all the groups for which you have administrative privileges. For example, if you are an MSP administrator, then this drop-down list displays all the customer groups that you manage. This list does not display any other groups.
Report Label field	You can provide a label for the report to distinguish it from the other reports that you generate.

Step 5 Click **Submit**.

The report is generated in the system. This generated report is accessible only to you and to users in the groups that you manage. For example, if you are an MSP administrator, then this generated report is not visible to other MSP administrators or groups.

Note
Reports are generated in HTML, PDF, and CSV formats. Starting with release 6.9, reports can be viewed and emailed in CSV format. The CSV reports include only tabular data and do not contain any graphical representations.

Generating an Assessment

Procedure

Step 1 Choose **CloudSense** > **Assessments**.

Step 2 Click **Generate Report**.

Step 3 In the **Generate Report** screen, complete the required fields, including the following:

Name	Description
Context drop-down list	Select the group that you want to generate the report for. **Note** If you are an administrator, then this drop-down list displays all the groups for which you have administrative privileges. For example, if you are an MSP administrator, then this drop-down list displays all the customer groups that you manage. This list does not display any other groups.
Report Label field	You can provide a label for the report to distinguish it from the other reports that you generate.

Step 4 Click **Submit**.

Report Builder for Custom Report Templates

Using the **Report Builder** option in Cisco UCS Director, you can create custom report templates to run reports on specific parameters. You can specify the context, the type of report to run, and the duration of the data samples for the report. You can also create multiple templates.

After you have created a report template, you can use it to generate a report in either PDF or HTML formats. You can view custom reports in Cisco UCS Director or you can email reports, either to yourself and to other users in your organization. You can review and archive these reports outside Cisco UCS Director.

In addition to creating a template, you can edit, clone, and delete custom report templates.



Note You cannot generate daily and hourly trend cost reports using the report builder. You can generate trend reports only for weekly and monthly duration. While generating trend reports for a month, the data is caculated from the first day of the month till the current date. For example, if you are generating a trend report on 5th March, this report includes data from March 1st, to March 5th.

Creating a Report Builder Template

Procedure

Step 1 Choose **CloudSense** > **Report Builder**.

Step 2 Click **Add Template**.

Step 3 In the **Add Template** screen, complete the required fields, including the following:

Name	Description
Name field	The name of the report template.
Description field	A description of the template.
Reports field	Click + to add entries to the reports.

Step 4 In the **Add Entry to Reports** screen, complete the required fields, including the following:

Name	Description
Report Context drop-down list	Choose one of the following options: • **VDC** • **Cloud** • **Physical Account** • **Multi Domain Manager** • **Global** • **Global Admin**
VDC drop-down list	Choose a VDC. This field is displayed only when the report context is set to **VDC**.
Clouds drop-down list	Choose a cloud from the drop-down list. This list displays all the clouds that have been previously configured in the system. This field is displayed only when the report context is set to **Cloud**.
Physical Accounts drop-down list	Choose a physical account from the drop-down list. This list displays all the accounts that have been previously configured in the system. This field is displayed only when the report context is set to **Physical Accounts**.

Name	Description
Multi Domain Manager	Choose a multi-domain manager from the drop-down list. This list displays all the accounts that have been previously configured in the system. This field is displayed only when the report context is set to **Multi Domain Manager**.
Reports drop-down list	Click **Select** to choose the reports that you want included in the template. This list is filtered depending on the report context that you have selected.
Duration for Trend Reports drop-down list	If you specified **VDC** as the report context, then choose one of the following durations for the template: • **Hourly** • **Daily** • **Weekly** • **Monthly** If you specified **Cloud** as the report context, then choose one of the following durations for the template: • **Daily** • **Weekly** • **Monthly**

Step 5 Click **Submit**.

Step 6 In the **Add Template** screen, click **Submit**.

What to do next

After you have created a template, you can generate a report based on the template. For more information, see Generating a Report from a Template, on page 430.

Generating a Report from a Template

Before you begin

You should have created a report template in the system. For information, see Creating a Report Builder Template, on page 429.

Procedure

Step 1 Choose **CloudSense** > **Report Builder**.

Step 2 Select a template from the table.

Step 3 From the **More Actions** drop-down menu, choose **Generate Report**.

Step 4 In the **Confirm Report Generation** screen, complete the required fields, including the following:

Name	Description
Report Title field	A title for the report.
Description field	A description of the report.

Step 5 Click **Generate**.

The report is generated and saved in the system.

What to do next

You can view the report that has been generated, and if necessary, email the report.

Viewing Reports Generated From a Template

Before you begin

You should have created a template, and generated a report using the template.

Procedure

Step 1 Choose **CloudSense** > **Report Builder**.

Step 2 Select a template from the table.

Step 3 From the **More Actions** drop-down menu, choose **View Reports**.

The **Custom Reports** screen displays the reports that have been generated using the template.

Step 4 Select a report from the table.

Step 5 Click **View Report**.

Step 6 In the **View Report** screen, choose the format in which you would like to view the report.

You can choose **HTML** or **PDF**. From Release 6.9, you can choose **CSV**.

Step 7 Click **Submit**.

The report opens in a new browser tab.

What to do next

You can email the reports to other users in the organization.

Emailing Reports Generated From a Template

You can email a report that is generated from a template to yourself or to other users within the organization.

Before you begin

- You should have created a template, and generated a report using the template.
- You should have configured your email address during the initial system set-up. Your name and email address identifies you as the sender with the report.

Procedure

Step 1 Choose **CloudSense** > **Report Builder**.

Step 2 Select a template from the table.

Step 3 Click **View Reports**.

The **Custom Reports** screen displays the reports that have been generated using the template.

Step 4 Select a report from the table.

Step 5 Click **Email Report**.

Step 6 In the **Email Report** screen, complete the required fields, including the following:

Name	Description
To field	The email address of the recipient. You can enter multiple email addresses separated by commas.
Subject field	The subject of the email message.
Format drop-down list	Choose the format of the report that will be attached to the email message. You can choose one of the following: • **HTML** • **PDF** • **CSV** (Release 6.9)

Step 7 Click **Submit**.

What to do next

If you no longer need the report, you can select it, and click **Delete** to erase the report from the system.