Cisco UCS Manager Administration Management Guide 4.1

First Published: 2020-02-20

Last Modified: 2022-01-07

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)

© 2020–2022 Cisco Systems, Inc. All rights reserved.

CONTENTS

PREFACE

Preface xi

Audience xi

Conventions xi

Related Cisco UCS Documentation xiii

Documentation Feedback xiii

CHAPTER 1

New and Changed Information for This Release 1

New and Changed Information 1

CHAPTER 2

Administration Management Overview 3

Administration Management Overview 3

CHAPTER 3

Password Management 5

Guidelines for Cisco UCS Passwords 5

Guidelines for Cisco UCS Usernames 7

Configuring the Maximum Number of Password Changes for a Change Interval 8

Configuring a No Change Interval for Passwords 8

Configuring the Password Expiration for a Locally Authenticated User 9

Configuring the Password History Count 12

Password Profile for Locally Authenticated Users 13

Clearing the Password History for a Locally Authenticated User 14

Recovering a Lost Password 14

Password Recovery for the Admin Account 14

Determining the Leadership Role of a Fabric Interconnect 15

Verifying the Firmware Versions on a Fabric Interconnect 15

Recovering the Admin Account Password in a Standalone Configuration for Cisco UCS 6200 and 6300 Series Fabric Interconnect 16
Recovering the Admin Account Password in a Standalone Configuration for Cisco UCS 6400 Series Fabric Interconnect 18
Recovering the Admin Account Password in a Cluster Configuration for Cisco UCS 6200 and 6300 Series Fabric Interconnect 19
Recovering the Admin Account Password in a Cluster Configuration for Cisco UCS 6400 Series Fabric Interconnect 21

CHAPTER 4 **Role-Based Access Configuration** 25
Role-Based Access Control Overview 25
User Accounts for Cisco UCS 25
Reserved Words: Locally Authenticated User Accounts 26
Web Session Limits for User Accounts 27
Processor Node Utility Operating System 27
User Roles 28
Default User Roles 28
Reserved Words: User Roles 29
Privileges 29
Creating a User Role 31
Adding Privileges to a User Role 32
Removing Privileges from a User Role 32
Deleting a User Role 33
Locales 33
User Locales 33
Assigning an Organization to a Locale 34
Creating a Locale 34
Deleting an Organization from a Locale 35
Deleting a Locale 35
Locally Authenticated User Accounts 36
Creating a User Account 36
Enabling the Password Strength Check for Locally Authenticated Users 39
Setting the Web Session Limits 40
Changing the Locales Assigned to a Locally Authenticated User Account 40
Changing the Roles Assigned to a Locally Authenticated User Account 41

Enabling a User Account 41
Disabling a User Account 42
Clearing the Password History for a Locally Authenticated User 42
Deleting a Locally Authenticated User Account 42
Login Profile 43
Configuring Login Profile 43
Monitoring User Sessions 44

CHAPTER 5 **Remote Authentication** 45
Authentication Services 45
Guidelines and Recommendations for Remote Authentication Providers 45
User Attributes in Remote Authentication Providers 46
Two-Factor Authentication 48
LDAP Providers and Groups 48
Nested LDAP Groups 48
LDAP Group Rule 49
Configuring Properties for LDAP Providers 49
Creating an LDAP Provider 49
Changing the LDAP Group Rule for an LDAP Provider 53
Deleting an LDAP Provider 54
LDAP Group Mapping 54
Creating an LDAP Group Map 55
Deleting an LDAP Group Map 55
RADIUS Providers 56
Configuring Properties for RADIUS Providers 56
Creating a RADIUS Provider 56
Deleting a RADIUS Provider 57
TACACS+ Providers 58
Configuring Properties for TACACS+ Providers 58
Creating a TACACS+ Provider 58
Deleting a TACACS+ Provider 59
Primary Authentication Service 59
Selecting the Console Authentication Service 59
Selecting the Default Authentication Service 61

Role Policy for Remote Users 62
Configuring the Role Policy for Remote Users 63
Multiple Authentication Services Configuration 63
Multiple Authentication Services 63
Provider Groups 63
Creating an LDAP Provider Group 64
Deleting an LDAP Provider Group 64
Creating a RADIUS Provider Group 64
Deleting a RADIUS Provider Group 65
Creating a TACACS+ Provider Group 65
Deleting a TACACS+ Provider Group 66
Authentication Domains 66
Creating an Authentication Domain 66

CHAPTER 6 **How to Enable and Disable the Call Home Feature** 69
Call Home in UCS Overview 69
Enabling Call Home 70
Disabling Call Home 71
Creating a Call Home Profile 72
Deleting a Call Home Profile 74
Configuring a Call Home Policy 74
Deleting a Call Home Policy 75

CHAPTER 7 **UCS Manager Communication Services** 77
Communication Protocols 77
Communication Services 77
Non-Secure Communication Services 79
Web Session Limits for User Accounts 79
Setting Web Session Limits 79
Setting Shell Session Limits 79
Configuring CIM-XML 80
Configuring HTTP 80
Secure Communication Services 81
Certificates, Key Rings, and Trusted Points 81

Creating a Key Ring 82
Creating a Certificate Request for a Key Ring 82
Changing the KVM Certificate 84
Clearing the KVM Certificate 85
Creating a Trusted Point 85
Importing a Certificate into a Key Ring 86
Configuring HTTPS 87
Deleting a Key Ring 88
Deleting a Trusted Point 89
Network-Related Communication Services 89
Enabling SNMP and Configuring SNMP Properties 89
Enabling the CIMC Web Service 90
Disabling Communication Services 90
Enabling Telnet 91

CHAPTER 8 **CIMC Sessions Management** 93
CIMC Session Management 93
Viewing All Open CIMC Sessions 94
Viewing the CIMC Sessions of a Server 94
Viewing the CIMC Sessions of a Service Profile 94
Viewing the CIMC Sessions Opened by a Local User 95
Viewing the CIMC Sessions Opened by a Remote User 95
Clearing All Open CIMC Sessions 95
Clearing the CIMC Sessions of a Server 96
Clearing the CIMC Sessions of a Service Profile 96
Clearing the CIMC Sessions of a Local User 96
Clearing the CIMC Sessions of a Remote User 97

CHAPTER 9 **Setting the Management IP Address** 99
Management IP Address 99
Configuring the Management IP Address on a Server 100
Configuring a Server to Use a Static IP Address 100
Configuring a Server to Use a Management IP Pool 102
Deleting the Inband Configuration from a Server 103

Setting the Management IP Address on a Service Profile Template 104
Setting the Management IP Address on a Service Profile Template 104
Management IP Pools 105
Creating an IPv6 Address Block in the Management IP Pool 105
Deleting an IP Address Block from the Management IP Pool 106
Creating an IPv4 Address Block in the Management IP Pool 106

CHAPTER 10 **Organizations in UCS Manager** 109
Organizations in a Multitenancy Environment 109
Hierarchical Name Resolution in a Multi-Tenancy Environment 110
Creating an Organization under the Root Organization 112
Creating an Organization under a Sub-Organization 112
Deleting an Organization 113

CHAPTER 11 **Backup and Restore** 115
Backup Operations in UCS 115
Considerations and Recommendations for Backup Operations 115
Required User Role for Backup and Import Operations 116
Creating a Backup Operation 116
Running a Backup Operation 121
Modifying a Backup Operation 122
Deleting One or More Backup Operations 122
Backup Types 123
Configuring the Full State Backup Policy 124
Configuring the All Configuration Export Policy 125
Import Methods 127
Import Configuration 128
Creating an Import Operation 128
Running an Import Operation 130
Modifying an Import Operation 131
Deleting One or More Import Operations 132
System Restore 132
Restoring the Configuration for a Fabric Interconnect 133

CHAPTER 12 **Scheduling Options** 137

Creating a Schedule 137

Creating a One Time Occurrence for a Schedule 142

Creating a Recurring Occurrence for a Schedule 145

Deleting a One Time Occurrence from a Schedule 147

Deleting a Recurring Occurrence from a Schedule 148

Deleting a Schedule 148

CHAPTER 13 **Deferred Deployments of Service Profile Updates** 149

Service Profile Deferred Deployments 149

Schedules for Deferred Deployments 150

Guidelines and Limitations for Deferred Deployments 150

Maintenance Policy 151

Creating a Maintenance Policy 152

Deleting a Maintenance Policy 155

Pending Activities for Deferred Deployments 155

Viewing Pending Activities 155

Deploying a Service Profile Change Waiting for User Acknowledgement 156

Deploying All Service Profile Changes Waiting for User Acknowledgement 156

Deploying a Scheduled Service Profile Change Immediately 157

Deploying All Scheduled Service Profile Changes Immediately 157

CHAPTER 14 **UCS Fault Suppression** 159

Global Fault Policy 159

Configuring the Global Fault Policy 159

CHAPTER 15 **KVM Console** 163

KVM Console 163

KVM Console for Cisco UCS B-Series M4, C-Series M4, and C-Series M5 Servers 164

KVM Direct Access 167

Starting the KVM Console from a Server 168

Starting the KVM Console from a Service Profile 168

Starting the KVM Console from the Cisco UCS KVM Direct Web Page 169

Starting the KVM Console from the KVM Launch Manager 170
KVM Folder Mapping 171
KVM Certificate 171
Changing the KVM Certificate 171
Clearing the KVM Certificate 172

CHAPTER 16 **Cisco Intersight Management** 173
Intersight Management Mode 173
Device Connector 173
Enabling or Disabling Cisco Intersight Management 174
Viewing Intersight Device Connector Properties 174
Updating Device Connector 177

Preface

- Audience, on page xi
- Conventions, on page xi
- Related Cisco UCS Documentation, on page xiii
- Documentation Feedback, on page xiii

Audience

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

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

Conventions

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

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

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

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

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

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

Warning IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS

Related Cisco UCS Documentation

Documentation Roadmaps

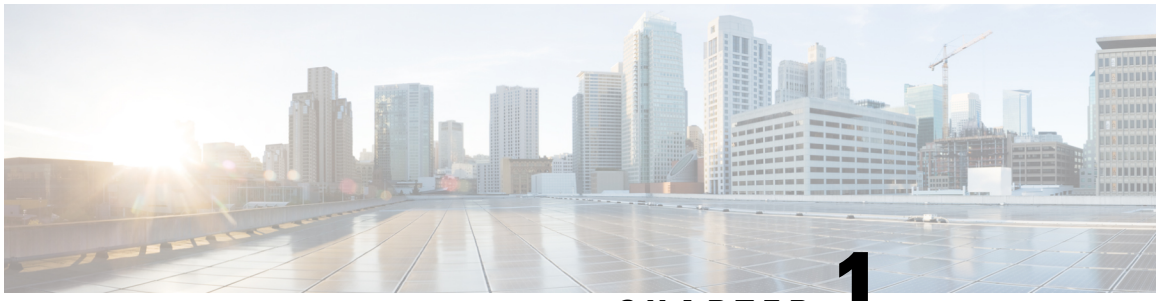
For a complete list of all B-Series documentation, see the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/UCS_roadmap.html

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

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

Documentation Feedback

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



CHAPTER 1

New and Changed Information for This Release

- New and Changed Information, on page 1

New and Changed Information

This section provides information on new features and changed behavior in Cisco UCS Manager, Release 4.1 (x).

Table 1: New Features and Changed Behavior in Cisco UCS Manager, Release 4.1(3)

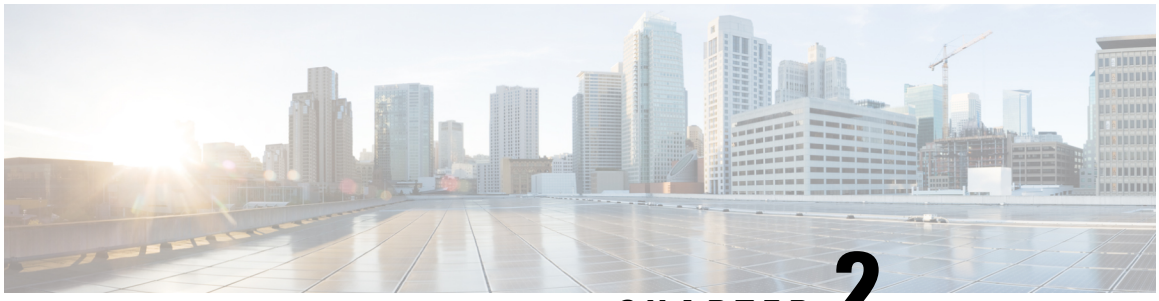
Feature	Description	Where Documented
Password expiration for locally authenticated users	Instructions on how to enable the password expiry feature, to set the password expiry duration, and to set the password expiry warning on the password profile page for locally authenticated users.	Configuring the Password Expiration for a Locally Authenticated User, on page 9

Table 2: New Features and Changed Behavior in Cisco UCS Manager, Release 4.1(2)

Feature	Description	Where Documented
Intersight Management Mode (IMM)	IMM introduces a new implementation of concepts first introduced with Cisco UCS Manager and moves ownership of the policy model into Cisco Intersight.	Intersight Management Mode, on page 173

Table 3: New Features and Changed Behavior in Cisco UCS Manager, Release 4.1(1)

Feature	Description	Where Documented
Password recovery for Cisco UCS 64108 Fabric Interconnect	Instructions on how to recover the admin password on Cisco UCS 6400 Series Fabric Interconnects.	Password Recovery for the Admin Account, on page 14



CHAPTER 2

Administration Management Overview

This chapter includes the following sections:

- Administration Management Overview, on page 3

Administration Management Overview

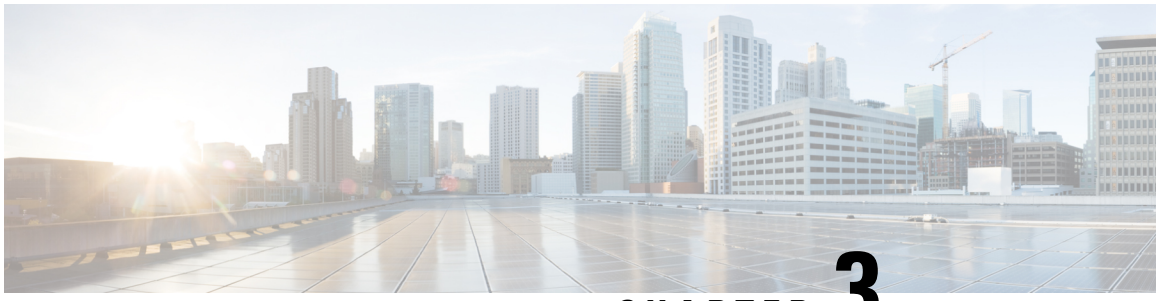
You can configure the mandatory user access features from the Cisco UCS Manager to manage the , Cisco UCS 6400 Series Fabric Interconnects,Cisco UCS 6332 40 GB Fabric Interconnects, and UCS 6200 Series 10 GB Fabric Interconnects that are in the same domain from one console.

If your environment is using a UCS 6324 40 GB Mini, you can also manage the user access features using the same Cisco UCS Manager capabilities.

You can configure the following basic administration configurations to manage user access in your environment:

- **Passwords**—Choose a password during the initial setup for the default admin user account, and create a unique username and password for each user account to access the system.
- **RBAC**—Delegate and control user access privileges according to the role and restrict user access within an organization boundary defined for the tenant, such as multi-tenancy.
- **Authentication**—Create UCS Manager local user accounts, and remote user accounts using the LDAP, RADIUS, and TACACS+ protocols.
- **Communication Services**—Configure CIM XML, HTTP, HTTPS, SMASH CLP, SNMP, SSH, and Telnet to interface third-party applications with Cisco UCS.
- **Organizations**—Create organizations for policies, pools, and service profiles. You can create multiple sub-organizations under the default Root organization, and nest sub-organization under a different sub-organization.
- **CIMC**—Close the KVM, vMedia, and SOL sessions of any user. When UCS Manager receives an event from CIMC, it updates its session table and displays the information to all users.
- **Backup and Restore** —Take a snapshot of all or part of the system configuration and export the file to a location on your network. You can configure a full state, all configuration, system configuration, and logical configuration backup.
- **Call Home**—Configure e-mail alert notifications for UCS errors and faults. You can configure the e-mail notifications for Cisco TAC (predefined) or any other recipient.

- **Deferred Deployments**—Configure deployments for a service profile to deploy immediately or during a specified maintenance window. Use this to control when disruptive configuration changes to a service profile or a service profile template are implemented.
- **Scheduling**—Schedule a one time occurrence for a schedule, a recurring occurrence for a schedule, and delete schedules.
- **Fault Suppression**—Enable fault suppression to suppress SNMP trap and Call Home notifications during a planned maintenance time.



CHAPTER 3

Password Management

- Guidelines for Cisco UCS Passwords, on page 5
- Guidelines for Cisco UCS Usernames, on page 7
- Configuring the Maximum Number of Password Changes for a Change Interval, on page 8
- Configuring a No Change Interval for Passwords, on page 8
- Configuring the Password Expiration for a Locally Authenticated User, on page 9
- Configuring the Password History Count, on page 12
- Password Profile for Locally Authenticated Users, on page 13
- Clearing the Password History for a Locally Authenticated User, on page 14
- Recovering a Lost Password, on page 14

Guidelines for Cisco UCS Passwords

Each locally authenticated user account requires a password. A user with admin or aaa privileges can configure Cisco UCS Manager to perform a password strength check on user passwords. Listed in Table 4: ASCII Table of Allowed Characters for UCS Passwords, on page 5 are the allowed ASCII characters for UCS passwords.

Table 4: ASCII Table of Allowed Characters for UCS Passwords

ASCII Printable Characters	Description
A-Z	uppercase letters A to Z
a-z	lowercase letters a to z
0-9	digits 0 to 9
!	exclamation mark
"	quotation mark
%	percent sign
&	ampersand
'	apostrophe
(	left parenthesis

ASCII Printable Characters	Description
)	right parenthesis
*	asterisk
+	plus sign
,	comma
-	hyphen
.	period
/	slash
:	colon
;	semicolon
<	less-than
>	greater-than
@	at sign
[	left square bracket
\	backslash
]	right square bracket
^	caret
_	underscore
`	grave accent
{	left curly brace
|	vertical bar
}	right curly brace
~	tilde

Cisco recommends using a strong password; otherwise, the password strength check for locally authenticated users, Cisco UCS Manager rejects any password that does not meet the following requirements:

- Must contain a minimum of eight characters and a maximum of 80 characters.
- If the password strength check is turned on, the minimum password length is variable and can be set from a minimum of 6 to a maximum of 80 characters.

Note The default is 8 characters.

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

Guidelines for Cisco UCS Usernames

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

- The login ID can contain between 1 and 32 characters, including the following:
  - Any alphabetic character
  - Any digit
  - _ (underscore)
  - - (dash)
  - . (dot)
- The login ID must be unique within Cisco UCS Manager.
- The login ID must start with an alphabetic character. It cannot start with a number or a special character, such as an underscore.
- The login ID is case-sensitive.
- You cannot create an all-numeric login ID.
- After you create a user account, you cannot change the login ID. You must delete the user account and create a new one.

Configuring the Maximum Number of Password Changes for a Change Interval

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

Procedure

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

Step 2 Expand **All** > **User Management** > **User Services**.

Step 3 Click the **Locally Authenticated Users** node.

Step 4 In the **Password Profile** area, do the following:

a) In the **Change During Interval** field, click **Enable**.

b) In the **Change Count** field, enter the maximum number of times a locally authenticated user can change his or her password during the Change Interval.

This value can be anywhere from 0 to 10.

c) In the **Change Interval** field, enter the maximum number of hours over which the number of password changes specified in the **Change Count** field are enforced.

This value can be anywhere from 1 to 745 hours.

For example, if this field is set to 48 and the **Change Count** field is set to 2, a locally authenticated user can make no more than 2 password changes within a 48 hour period.

Step 5 Click **Save Changes**.

Configuring a No Change Interval for Passwords

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

Procedure

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

Step 2 Expand **All** > **User Management** > **User Services**.

Step 3 Click the **Locally Authenticated Users** node.

Step 4 In the **Password Profile** area, do the following:

a) In the **Change During Interval** field, click **Enable**.

b) In the **No Change Interval** field, enter the minimum number of hours that a locally authenticated user must wait before changing a newly created password.

This value can be anywhere from 1 to 745 hours.

This interval is ignored if the **Change During Interval** property is set to **Disable**.

Step 5 Click **Save Changes**.

Configuring the Password Expiration for a Locally Authenticated User

The password expiration feature enables the admin or AAA privileged user to enforce the password reset for all the locally authenticated users at a defined time interval. The password reset interval is calculated based on the last password change date and time and the password expiry duration.

The following tables provide different scenarios of password expiration for a new and an existing locally authenticated user.

The following table explains how the password expiry date is calculated when the password expiry option is enabled for the first time. For instance, the password expiry is enabled on 1st Dec, the password expiry duration is set as 9 days, and the password warning notification is 4 days.

User Scenarios	Effective Last Password change date	Notification	Effective Password Expiration date
New user is created on the same day that password expiry is enabled	1st Dec	5th Dec	10th Dec
Existing user's first login happens on the same day that password expiry is enabled	1st Dec	5th Dec	10th Dec
New user is created four days after password expiry is enabled	5th Dec	10th Dec	15th Dec
Existing user's first login happens four days after password expiry is enabled	5th Dec	10th Dec	15th Dec
New user changes the password on 2nd Dec	2nd Dec	7th Dec	12th Dec
Existing user changes the password on 2nd Dec	2nd Dec	7th Dec	12th Dec

The following table explains how the password expiry date is calculated when the password expiry option is disabled. For instance, the password expiry option is disabled on 1st Dec.

User Scenarios	Effective Last Password change date	Notification	Effective Password Expiration date
New user is created on the same day that password expiry is disabled	1st Dec	NA	NA
Existing user logs in on the same day that password expiry is disabled	1st Dec	NA	NA
New user is created four days after password expiry is disabled	5th Dec	NA	NA
Existing user's first login happens four days after password expiry is disabled	5th Dec	NA	NA
New user changes the password on 2nd Dec	2nd Dec	NA	NA
Existing user changes the password on 2nd Dec	2nd Dec	NA	NA

The following table explains how the password expiry date is calculated when the password expiry option is re-enabled. For instance, the password expiry option is re-enabled on 10th Dec, the password expiry duration is set as 9 days, and the password warning notification is 4 days.

User Scenarios	Effective Last Password change date	Notification	Effective Password Expiration date	Password Status
New user is created on the same day that password expiry is re-enabled	10th Dec	15th Dec	20th Dec	Active
Existing user logs in on the same day that password expiry is re-enabled	1st Dec	5th Dec	10th Dec	Expired
New user is created four days after password expiry is re-enabled	15th Dec	20th Dec	25th Dec	Active

User Scenarios	Effective Last Password change date	Notification	Effective Password Expiration date	Password Status
Existing user logs in for the first time four days after password expiry is re-enabled	15th Dec	20th Dec	25th Dec	Active
Existing user logs in for the second time four days after password expiry is re-enabled	5th Dec	10th Dec	15th Dec	Active

The following table explains how the password expiry date is calculated when the system date is modified by the admin. For instance, the actual system date when the last password was changed is 10th Dec, the password expiry duration is set as 9 days, and the password warning notification is 4 days.

System modified date	Effective Password Expiration date	Password Status
System date modified backward		
8th Dec 2020	17th Dec 2020	Active
2nd Dec 2020	11th Dec 2020	Warning
Any date prior to 1st Dec 2020 (the date that makes the password expiry duration from actual date as zero)		Expired
System date modified forward		
14th Dec 2020	19th Dec 2020	Active
19th Dec 2020	19th Dec 2020	Warning
Any date after 19th Dec 2020		Expired

After the password expiry, the user must reset the password using the **Reset Password** link in the Cisco UCS Manager Login page.

Procedure

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

Step 2 Expand **All** > **User Management** > **User Services**

Step 3 Click the **Locally Authenticated Users** node.

Step 4 In the **Password Profile** area, do the following:

a) Check the **Password Expiry** check box to enable the password expiration feature for the locally authenticated user.

By default, the **Password Expiry** field is disabled.

b) In the **Password Expiration Period** field, enter the number of days after which the password expires for the locally authenticated user.

This value can be anywhere from 1 to 180 days. By default, the password is set to expire in 90 days.

For example, if this field is set to 60 days, the locally authenticated user's password will expire after 60 days from the last password changed date.

c) In the **Password Expiration Warning Time** field, enter the number of days by when the locally authenticated user must start to receive the password expiry notification.

This value can be anywhere from 0 to 30 days. By default, the warning is set to 15 days.

For example, if this field is set to eight, the locally authenticated user will receive a warning notification eight days before the password expiry.

Note
The **Password Expiration Period** value must be always greater than the value in the **Password Expiration Warning Time** field.

Step 5 Click **Save Changes**.

Configuring the Password History Count

You must have admin or aaa privileges to change the password profile properties.

Procedure

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

Step 2 Expand **All** > **User Management** > **User Services**.

Step 3 Click the **Locally Authenticated Users** node.

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

This value can be anywhere from 0 to 15.

By default, the **History Count** field is set to 0, which disables the history count and allows users to reuse previously used passwords at any time.

Step 5 Click **Save Changes**.

Password Profile for Locally Authenticated Users

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

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

Password History Count

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

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

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

You can clear the password history count for a locally authenticated user and enable reuse of previous passwords.

Password Change Interval

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

Interval Configuration	Description	Example
No password change allowed	Does not allow changing passwords for locally authenticated user within a specified number of hours after a password change. You can specify a no change interval between 1 and 745 hours. By default, the no change interval is 24 hours.	To prevent the user from changing passwords within 48 hours after a password change: • Set **Change during interval** to disable • Set **No change interval** to 48

Interval Configuration	Description	Example
Password changes allowed within change interval	Specifies the maximum number of times that a locally authenticated user password change can occur within a pre-defined interval. You can specify a change interval between 1 and 745 hours and a maximum number of password changes between 0 and 10. By default, a locally authenticated user is permitted a maximum of two password changes within a 48-hour interval.	To allow a password change for a maximum of one time within 24 hours after a password change: • Set **Change during interval** to enable • Set **Change count** to 1 • Set **Change interval** to 24

Clearing the Password History for a Locally Authenticated User

Procedure

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

Step 2 Expand **All** > **User Management** > **User Services** > **Locally Authenticated Users**.

Step 3 Click the user for whom you want to clear the password history.

Step 4 In the **Actions** area, click **Clear Password History**.

Step 5 If a confirmation dialog box displays, click **Yes**.

Recovering a Lost Password

Password Recovery for the Admin Account

The admin account is the system administrator or superuser account. If an administrator loses the password to this account, you can have a serious security issue. The procedure to recover the password for the admin account requires you to power cycle all fabric interconnects and will lead to a temporary data transmission outage.

When you recover the password for the admin account, you actually change the password for that account. You cannot retrieve the original password for that account.

You can reset the password for all other local accounts through Cisco UCS Manager. However, you must log in to Cisco UCS Manager with an account that includes aaa or admin privileges.

Caution For Cisco UCS Mini, this procedure requires you to pull all the fabric interconnects in a Cisco UCS domain out of their chassis slots. As a result, all data transmission in the Cisco UCS domain is stopped until you slide the fabric interconnects back into their chassis slots.

For other Cisco UCS configurations, this procedure requires you to power down all fabric interconnects. As a result, all data transmission in the Cisco UCS domain is stopped until you restart the fabric interconnects.

Note , Cisco UCS 6400 Series Fabric Interconnect does not have separate kernel and system images. It has a single unified image.

Determining the Leadership Role of a Fabric Interconnect

Important To determine the role of the fabric interconnects in a cluster when the admin password is lost, open the Cisco UCS Manager GUI from the IP addresses of both fabric interconnects. The subordinate fabric interconnect fails with the following message:

```
UCSM GUI is not available on secondary node.
```

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 In the **Equipment** tab, expand **Equipment** > **Fabric Interconnects**.

Step 3 Click the fabric interconnect for which you want to identify the role.

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

Step 5 In the **General** tab, click the down arrows on the **High Availability Details** bar to expand that area.

Step 6 View the **Leadership** field to determine whether the fabric interconnect is the primary or subordinate.

Verifying the Firmware Versions on a Fabric Interconnect

You can use the following procedure to verify the firmware versions on all fabric interconnects in a Cisco UCS domain. You can verify the firmware for a single fabric interconnect through the **Installed Firmware** tab for that fabric interconnect.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 In the **Equipment** tab, click the **Equipment** node.

Step 3 In the **Work** pane, click the **Firmware Management** tab.

Step 4 In the **Installed Firmware** tab, verify that the following firmware versions for each fabric interconnect match the version to which you updated the firmware:

- Kernel version
- System version

Recovering the Admin Account Password in a Standalone Configuration for Cisco UCS 6200 and 6300 Series Fabric Interconnect

This procedure will help you to recover the password that you set for the admin account when you performed an initial system setup on the fabric interconnect. The admin account is the system administrator or superuser account.

Before you begin

1. Physically connect the console port on the fabric interconnect to a computer terminal or console server
2. Determine the running versions of the following firmware:
   - The firmware kernel version on the fabric interconnect
   - The firmware system version

Tip To find this information, you can log in with any user account on the Cisco UCS domain.

Procedure

Step 1 Connect to the console port.

Step 2 Power cycle the fabric interconnect:

a) For Cisco UCS Mini, pull the fabric interconnect out of its chassis slot. For all other configurations, turn off the power to the fabric interconnect.

b) For Cisco UCS Mini, slide the fabric interconnect back into its chassis slot. For all other configurations, turn on the power to the fabric interconnect.

Step 3 In the console, press one of the following key combinations as it boots to get the `loader` prompt:

- **`Ctrl+l`**
- **`Ctrl+Shift+r`**

You may need to press the selected key combination multiple times before your screen displays the `loader` prompt.

Step 4 Boot the kernel firmware version on the fabric interconnect.

```
loader >
boot /installables/switch/
kernel_firmware_version
```

Example:

```
loader > boot /installables/switch/ucs-6100-k9-kickstart.4.1.3.N2.1.0.11.gbin
```

```
loader > boot /installables/switch/ucs-mini-k9-kickstart.5.0.3.N2.3.01a.bin
```

Step 5 Enter config terminal mode.

```
Fabric(boot)#
config terminal
```

Step 6 Reset the admin password.

```
Fabric(boot)(config)#
admin-password
password
```

Choose a strong password that includes at least one capital letter and one number. The password cannot be blank.

The new password displays in clear text mode.

Step 7 Exit config terminal mode and return to the boot prompt.

Step 8 Boot the system firmware version on the fabric interconnect.

```
Fabric(boot)#
load /installables/switch/
system_firmware_version
```

Example:

```
Fabric(boot)# load
/installables/switch/ucs-6100-k9-system.4.1.3.N2.1.0.211.bin
```

```
Fabric(boot)# load /installables/switch/ucs-mini-k9-system.5.0.3.N2.3.01a.bin
```

Step 9 After the system image loads, log in to Cisco UCS Manager.

Step 10 Sync the new password with Cisco UCS Manager.

```
UCS-B # scope security
UCS-B/security  # set password
Enter new password: New_password
Confirm new password: New_password
UCS-B/security* # commit-buffer
```

Recovering the Admin Account Password in a Standalone Configuration for Cisco UCS 6400 Series Fabric Interconnect

This procedure will help you to recover the password that you set for the admin account when you performed an initial system setup on the fabric interconnect. The admin account is the system administrator or superuser account.

Before you begin

1. Physically connect the console port on the fabric interconnect to a computer terminal or console server.
2. Determine the running versions of the Cisco UCS 6400 Series Fabric Interconnect image.

Note Cisco UCS 6400 Series Fabric Interconnect does not have separate kernel and system images. It has a single unified image.

Tip To find this information, you can log in with any user account on the Cisco UCS domain.

Procedure

Step 1 Connect to the console port.

Step 2 UCS-A(local-mgmt)# **reboot**

This reboots the fabric interconnect.

You can also power cycle the fabric interconnect.

Step 3 In the console, press **Ctrl+c** key combinations as it boots to get the `loader` prompt:

Ctrl+c

You may need to press the selected key combination multiple times before your screen displays the `loader` prompt.

Step 4 At the loader prompt, run the following command:

`loader >` **cmdline recoverymode=1**

Step 5 Boot the Cisco UCS 6400 Series Fabric Interconnect image on the fabric interconnect.

`loader >` **boot /installables/switch/***Cisco UCS 6400 FI Image*

Example:

`loader >` **boot /installables/switch/ucs-6400-k9-system.7.0.3.N2.3.40.173.gbin**

Step 6 Enter the config terminal mode.

`switch(boot)#` **config terminal**

Step 7 Reset the admin password.

```
switch(boot)(config)# admin-password New_password
```

Choose a strong password that includes at least one capital letter and one number. The password cannot be blank.

The new password displays in clear text mode.

Step 8 Exit the config terminal mode to reboot the FI.

```
switch(boot)(config)# exit
switch(boot)# exit
```

Step 9 Wait for the login prompt and use the new password to login.

```
Cisco UCS 6400 Series Fabric Interconnect
login: admin
Password:New_password
```

Step 10 Sync the new password with Cisco UCS Manager.

```
UCS-A # scope security
UCS-A/security  # set password
Enter new password: New_password
Confirm new password: New_password
UCS-A/security* # commit-buffer
```

Recovering the Admin Account Password in a Cluster Configuration for Cisco UCS 6200 and 6300 Series Fabric Interconnect

This procedure will help you to recover the password that you set for the admin account when you performed an initial system setup on the fabric interconnects. The admin account is the system administrator or superuser account.

Before you begin

1. Physically connect a console port on one of the fabric interconnects to a computer terminal or console server
2. Obtain the following information:
   - The firmware kernel version on the fabric interconnect
   - The firmware system version
   - Which fabric interconnect has the primary leadership role and which is the subordinate

Tip To find this information, you can log in with any user account on the Cisco UCS domain.

Procedure

Step 1 Connect to the console port of the subordinate fabric interconnect.

Step 2 For the subordinate fabric interconnect:

a) For Cisco UCS Mini, pull the fabric interconnect out of its chassis slot. For all other configurations, turn off the power to the fabric interconnect.

b) For Cisco UCS Mini, slide the fabric interconnect back into its chassis slot. For all other configurations, turn on the power to the fabric interconnect.

c) In the console, press one of the following key combinations as it boots to get the `loader` prompt:

- **Ctrl+l**
- **Ctrl+Shift+r**

You may need to press the selected key combination multiple times before your screen displays the `loader` prompt.

Step 3 Power cycle the primary fabric interconnect:

a) For Cisco UCS Mini, pull the fabric interconnect out of its chassis slot. For all other configurations, turn off the power to the fabric interconnect.

b) For Cisco UCS Mini, slide the fabric interconnect back into its chassis slot. For all other configurations, turn on the power to the fabric interconnect.

Step 4 In the console, press one of the following key combinations as it boots to get the `loader` prompt:

- **Ctrl+l**
- **Ctrl+Shift+r**

You may need to press the selected key combination multiple times before your screen displays the `loader` prompt.

Step 5 Boot the kernel firmware version on the primary fabric interconnect.

```
loader > boot /installables/switch/
kernel_firmware_version
```

Example:

```
loader > boot /installables/switch/ucs-6100-k9-kickstart.4.1.3.N2.1.0.11.gbin
```

```
loader > boot /installables/switch/ucs-mini-k9-kickstart.5.0.3.N2.3.01a.bin
```

Step 6 Enter config terminal mode.

```
Fabric(boot)# config terminal
```

Step 7 Reset the admin password.

```
Fabric(boot)(config)# admin-password password
```

Choose a strong password that includes at least one capital letter and one number. The password cannot be blank.

The new password displays in clear text mode.

Step 8 Exit config terminal mode and return to the boot prompt.

Step 9 Boot the system firmware version on the primary fabric interconnect.

```
Fabric(boot)# load /installables/switch/
system_firmware_version
```

Example:

```
Fabric(boot)# load
/installables/switch/ucs-6100-k9-system.4.1.3.N2.1.0.211.bin

Fabric(boot)# load /installables/switch/ucs-mini-k9-system.5.0.3.N2.3.01a.bin
```

Step 10 After the system image loads, log in to Cisco UCS Manager.

Step 11 In the console for the subordinate fabric interconnect, do the following to bring it up:

a) Boot the kernel firmware version on the subordinate fabric interconnect.

```
loader > boot /installables/switch/
kernel_firmware_version
```

b) Boot the system firmware version on the subordinate fabric interconnect.

```
Fabric(boot)# load /installables/switch/
system_firmware_version
```

Step 12 Sync the new password with Cisco UCS Manager and other FI.

```
UCS-B # scope security
UCS-B/security  # set password
Enter new password: New_password
Confirm new password: New_password
UCS-B/security* # commit-buffer
```

Recovering the Admin Account Password in a Cluster Configuration for Cisco UCS 6400 Series Fabric Interconnect

This procedure will help you to recover the password that you set for the admin account when you performed an initial system setup on the fabric interconnects. The admin account is the system administrator or superuser account.

Before you begin

1. Physically connect a console port on one of the fabric interconnects to a computer terminal or console server
2. Obtain the following information:
   - The Cisco UCS 6400 Series Fabric Interconnect image

Note Cisco UCS 6400 Series Fabric Interconnect does not have separate kernel and system images. It has a single unified image.

- Which fabric interconnect has the primary leadership role and which is the subordinate

Tip To find this information, you can log in with any user account on the Cisco UCS domain.

Procedure

Step 1 Connect to the console port of the subordinate fabric interconnect.

Step 2 UCS-B(local-mgmt)# **reboot**

This reboots the subordinate fabric interconnect.

You can also power cycle the subordinate fabric interconnect.

Step 3 In the console, press **Ctrl+c** key combinations as it boots to get the `loader` prompt:

Ctrl+c

You may need to press the selected key combination multiple times before your screen displays the `loader` prompt.

Step 4 At the loader prompt, run the following command:

```
loader > cmdline recoverymode=1
```

Step 5 Boot the Cisco UCS 6400 Series Fabric Interconnect image on the fabric interconnect.

```
loader > boot /installables/switch/Cisco UCS 6400 Series FI Image
```

Example:

```
loader > boot /installables/switch/ucs-6400-k9-system.7.0.3.N2.3.40.173.gbin
```

Step 6 Enter the config terminal mode.

```
switch(boot)# config terminal
```

Step 7 Reset the admin password.

```
switch(boot)(config)# admin-password New_password
```

Choose a strong password that includes at least one capital letter and one number. The password cannot be blank.

The new password displays in clear text mode.

Step 8 Exit the config terminal mode to reboot the FI.

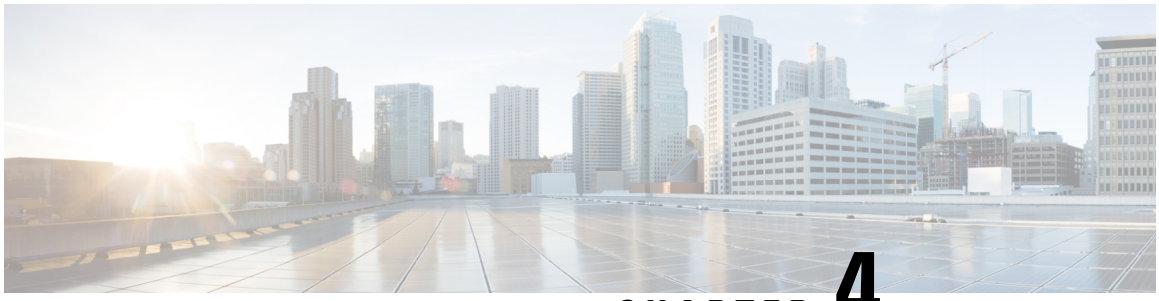
```
switch(boot)(config)# exit
switch(boot)# exit
```

Step 9 Wait for the login prompt and use the new password to login.

```
Cisco UCS 6400 Series Fabric Interconnect
login: admin
Password:New_password
```

Step 10 Sync the new password with Cisco UCS Manager and other FI.

```
UCS-B # scope security
UCS-B/security  # set password
Enter new password: New_password
Confirm new password: New_password
UCS-B/security* # commit-buffer
```



CHAPTER 4

Role-Based Access Configuration

- Role-Based Access Control Overview, on page 25
- User Accounts for Cisco UCS , on page 25
- Processor Node Utility Operating System , on page 27
- User Roles, on page 28
- Locales, on page 33
- Locally Authenticated User Accounts, on page 36
- Login Profile, on page 43
- Monitoring User Sessions, on page 44

Role-Based Access Control Overview

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

A user is granted write access to the required system resources only if the assigned role grants the access privileges and the assigned locale allows access. For example, a user with the Server Administrator role in the engineering organization can update server configurations in the Engineering organization. They cannot, however, update server configurations in the Finance organization, unless the locales assigned to the user include the Finance organization.

User Accounts for Cisco UCS

User accounts access the system. You can configure up to 48 local user accounts in each Cisco UCS Manager domain. Each user account requires a unique username and password.

You can set user accounts with an SSH public key. The public key can be set in either of the two formats: OpenSSH or SECSH.

Admin Account

An admin account comes with each Cisco UCS domain. The admin account is a default user account and cannot be modified or deleted. This account is the system administrator or superuser account s full privileges.

There is no default password assigned to the admin account; you must choose the password during the initial system setup.

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

Locally Authenticated User Accounts

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. After a local user account is disabled, the user cannot log in. The database does not delete the configuration details for disabled local user accounts. If you re-enable a disabled local user account, the account becomes active with the existing configuration, including the username and password.

Remotely Authenticated User Accounts

A remotely authenticated user account is any user account that is authenticated through LDAP, RADIUS, or TACACS+.

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

Expiration of User Accounts

You can configure user accounts to expire at a predefined time. When the expiration time is reached, the user account is disabled.

By default, user accounts do not expire.

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

Reserved Words: Locally Authenticated User Accounts

You cannot use the following words when creating a local user account in Cisco UCS.

- root
- bin
- daemon
- adm
- lp
- sync
- shutdown
- halt
- news
- uucp

- operator
- games
- gopher
- nobody
- nscd
- mailnull
- mail
- rpcuser
- rpc
- mtsuser
- ftpuser
- ftp
- man
- sys
- samdme
- debug

Web Session Limits for User Accounts

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

Each Cisco UCS Manager domain supports a maximum of 32 concurrent web sessions per user and 256 total user sessions. By default, the number of concurrent web sessions allowed by Cisco UCS Manager is set to 32 per user, but you can configure this value up to the system maximum of 256.

Processor Node Utility Operating System

Processor Node Utility Operating System (PNuOS) is a small utility that resides on the Cisco UCS Fabric Interconnect flash memory. This utility boots on a server (with no OS or service profile) and provides inventory discovery service. It is also used to preboot and provide configuration management during service-profile association and dis-association services. The PnuOS system boot is completely transparent to the server administrator.

PNuOS integrates a single static user account to assist in the configuration. The static account is accessible through a physical terminal or a KVM console that is connected to the Cisco IMC IP address of the server. The access is limited to the internal network VLANs and is available only temporarily during the duration of the maintenance operation for which the PNuOS was loaded on to the server. PNuOS is unloaded post the maintenance operation.

User Roles

User roles contain one or more privileges that define the operations that are allowed for a user. You can assign one or more roles to each user. Users with multiple roles have the combined privileges of all assigned roles. For example, if Role1 has storage-related privileges, and Role 2 has server-related privileges, users with Role1 and Role 2 have both storage-related and server-related privileges.

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

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

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

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

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

Note If a local and a remote user account have the same username, Cisco UCS Manager overrides any roles assigned to the remote user with those assigned to the local user.

Default User Roles

The system contains the following default user roles:

AAA Administrator

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

Administrator

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

Facility Manager

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

Network Administrator

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

Operations

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

Read-Only

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

Server Compute

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

Server Equipment Administrator

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

Server Profile Administrator

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

Server Security Administrator

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

Storage Administrator

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

Reserved Words: User Roles

You cannot use the following words when creating custom roles in Cisco UCS.

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

Privileges

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

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

Table 5: User Privileges

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

Privilege	Description	Default Role Assignment
service-profile-config	Service profile configuration	Server Profile Administrator
service-profile-config-policy	Service profile configuration policy	Server Profile Administrator
service-profile-ext-access	Service profile endpoint access	Server Profile Administrator
service-profile-network	Service profile network	Network Administrator
service-profile-network-policy	Service profile network policy	Network Administrator
service-profile-qos	Service profile QoS	Network Administrator
service-profile-qos-policy	Service profile QoS policy	Network Administrator
service-profile-security	Service profile security	Server Security Administrator
service-profile-security-policy	Service profile security policy	Server Security Administrator
service-profile-server	Service profile server management	Server Profile Administrator
service-profile-server-oper	Service profile consumer	Server Profile Administrator
service-profile-server-policy	Service profile pool policy	Server Security Administrator
service-profile-storage	Service profile storage	Storage Administrator
service-profile-storage-policy	Service profile storage policy	Storage Administrator

Creating a User Role

Procedure

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

Step 2 Expand **All** > **User Management** > **User Services**.

Step 3 Right-click **User Services** and choose **Create Role**.

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

Step 4 In the **Create Role** dialog box, complete the following fields:

Name	Description
Name field	A user-defined name for this user role. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.

Name	Description
Privileges list box	A list of the privileges defined in the system. Click a privilege to view a description of that privilege. Check the check box to assign that privilege to the selected user.
Help Section	
Description field	A description of the most recent privilege you clicked in the **Privileges** list box.

Step 5 Click **OK**.

Adding Privileges to a User Role

Procedure

Step 1 In the **Navigation** pane, click **Admin**.
Step 2 Expand **All** > **User Management** > **User Services**.
Step 3 Expand the **Roles** node.
Step 4 Choose the role to which you want to add privileges.
Step 5 In the **General** tab, check the boxes for the privileges you want to add to the role.
Step 6 Click **Save Changes**.

Removing Privileges from a User Role

Procedure

Step 1 In the **Navigation** pane, click **Admin**.
Step 2 Expand **All** > **User Management** > **User Services**.
Step 3 Expand the **Roles** node.
Step 4 Choose the role from which you want to remove privileges.
Step 5 In the **General** tab, uncheck the boxes for the privileges you want to remove from the role.
Step 6 Click **Save Changes**.

Deleting a User Role

When you delete a user role, Cisco UCS Manager removes that role from all user accounts to which the role was assigned.

Procedure

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

Step 2 Expand **All** > **User Management** > **User Services**.

Step 3 Expand the **Roles** node.

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

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

Locales

User Locales

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

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

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

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

- aaa
- admin
- fault
- operations

You can hierarchically manage organizations. A user who is assigned to a top-level organization has automatic access to all organizations below it. For example, an Engineering organization can contain a Software Engineering organization and a Hardware Engineering organization. A locale containing only the Software Engineering organization has access to system resources only within that organization. However, a locale that

contains the Engineering organization has access to the resources for both the Software Engineering and Hardware Engineering organizations.

Assigning an Organization to a Locale

Procedure

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

Step 2 Expand **All** > **User Management** > **User Services**.

Step 3 Expand the **Locales** node and click the locale to which you want to add an organization.

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

Step 5 In the **Organizations** area, click **+** on the table icon bar.

Step 6 In the **Assign Organizations** dialog box, do the following:

a) Expand the **Organizations** area to view the organizations in the Cisco UCS domain.
b) Expand the **root** node to see the sub-organizations.
c) Click an organization that you want to assign to the locale.
d) Drag the organization from the **Organizations** area and drop it into the design area on the right.
e) Repeat Steps b and c until you have assigned all desired organizations to the locale.

Step 7 Click **OK**.

Creating a Locale

Before you begin

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

Procedure

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

Step 2 Expand **All** > **User Management** > **User Services**.

Step 3 Right-click **Locales** and choose **Create a Locale**.

Step 4 In the **Create Locale** page, do the following:

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

This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.

b) Click **Next**.

Step 5 In the **Assign Organizations** dialog box, do the following:

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

b) Expand the **root** node to see the sub-organizations.
c) Click an organization that you want to assign to the locale.
d) Drag the organization from the **Organizations** area and drop it into the design area on the right.
e) Repeat Steps b and c until you have assigned all desired organizations to the locale.

Step 6 Click **Finish**.

What to do next

Add the locale to one or more user accounts. For more information, see Changing the Locales Assigned to a Locally Authenticated User Account, on page 40.

Deleting an Organization from a Locale

Procedure

Step 1 In the **Navigation** pane, click **Admin**.
Step 2 Expand **All** > **User Management** > **User Services**.
Step 3 Expand the **Locales** node and click the locale from which you want to delete an organization.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 In the **Organizations** area, right-click the organization that you want to delete from the locale and choose **Delete**.
Step 6 Click **Save Changes**.

Deleting a Locale

Procedure

Step 1 In the **Navigation** pane, click **Admin**.
Step 2 Expand **All** > **User Management** > **User Services**.
Step 3 Expand the **Locales** node.
Step 4 Right-click the locale you want to delete and choose **Delete**.
Step 5 If a confirmation dialog box displays, click **Yes**.

Locally Authenticated User Accounts

Creating a User Account

At a minimum, Cisco recommends that you create the following users:

- Server administrator account
- Network administrator account
- Storage administrator

Note After you create the user account, if you make any changes to any of the user account fields from the Cisco UCS Manager GUI, make sure to enter the password again.

Before you begin

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

- Remote authentication services—Ensures that the users exist in the remote authentication server with the appropriate roles and privileges.
- Multitenancy with organizations—Creates one or more locales. If you do not have any locales, all users are created in root and are assigned roles and privileges in all organizations.
- SSH authentication—Obtains the SSH key.

Procedure

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

Step 2 Expand **All** > **User Management** > **User Services**.

Step 3 Right-click **User Services** and choose **Create User** to open the **User Properties** dialog box.

You can also right-click **Locally Authenticated Users** to access that option.

Step 4 Complete the following fields with the required information about the user:

Name	Description

Login ID field	The account name that is used when logging into this account. This account must be unique and meet the following guidelines and restrictions for Cisco UCS Manager user accounts:
	• The login ID can contain between 1 and 32 characters, including the following:
	  • Any alphabetic character
	  • Any digit
	  • _ (underscore)
	  • - (dash)
	  • . (dot)
	• The login ID must be unique within Cisco UCS Manager.
	• The login ID must start with an alphabetic character. It cannot start with a number or a special character, such as an underscore.
	• The login ID is case-sensitive.
	• You cannot create an all-numeric login ID.
	• After you create a user account, you cannot change the login ID. You must delete the user account and create a new one.
	After you save the user, the login ID cannot be changed. You must delete the user account and create a new one.

First Name field	The first name of the user. This field can contain up to 32 characters.
Last Name field	The last name of the user. This field can contain up to 32 characters.
Email field	The email address for the user.
Phone field	The telephone number for the user.

Name	Description

Password field	The password associated with this account. If password strength check is enabled, a user's password must be strong and Cisco UCS Manager rejects any password that does not meet the following requirements:
	• Must contain a minimum of eight characters and a maximum of 80 characters.
	• If the password strength check is turned on, the minimum password length is variable and can be set from a minimum of 6 to a maximum of 80 characters.
	Note
	The default is 8 characters.
	• Must contain at least three of the following:
	  • Lower case letters
	  • Upper case letters
	  • Digits
	  • Special characters
	• Must not contain a character that is repeated more than three times consecutively, such as aaabbb.
	• Must not be identical to the username or the reverse of the username.
	• Must pass a password dictionary check. For example, the password must not be based on a standard dictionary word.
	• Must not contain the following symbols: $ (dollar sign), ? (question mark), and = (equals sign).
	• Should not be blank for local user and admin accounts.

Confirm Password field	The password a second time for confirmation purposes.
Account Status field	If the status is set to **Active**, a user can log into Cisco UCS Manager with this login ID and password.
Account Expires check box	If checked, this account expires and cannot be used after the date specified in the **Expiration Date** field. **Note** After you configure a user account with an expiration date, you cannot reconfigure the account to not expire. However, you can configure the account to use the latest expiration date available.

Name	Description
Expiration Date field	The date on which the account expires. The date should be in the format yyyy-mm-dd. Click the down arrow at the end of this field to view a calendar that you can use to select the expiration date. **Note** Cisco UCS Manager GUI displays this field when you check the **Account Expires** check box.

Step 5 In the **Roles** area, check one or more boxes to assign roles and privileges to the user account.

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

Step 6 (Optional) If the system includes organizations, check one or more check boxes in the **Locales** area to assign the user to the appropriate locales.

Step 7 In the **SSH** area, complete the following fields:

a) In the **Type** field, click the following:

- **Password Required**—The user must enter a password when they log in.
- **Key**—SSH encryption is used when this user logs in.

b) If you chose **Key**, enter the SSH key in the **SSH data** field.

Step 8 Click **OK**.

Enabling the Password Strength Check for Locally Authenticated Users

You must have admin or aaa privileges to enable the password strength check. If enabled, Cisco UCS Manager does not permit a user to choose a password that does not meet the guidelines for a strong password.

Procedure

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

Step 2 Expand **All** > **User Management** > **User Services**.

Step 3 Click the **Locally Authenticated Users** node.

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

Step 5 Click **Save Changes**.

Setting the Web Session Limits

Procedure

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

Step 2 Expand **All** > **Communication Management** > **Communication Services**.

Step 3 Click the **Communication Services** tab.

Step 4 In the **Web Session Limits** area, complete the following fields:

Note
The HTML-5 Interface supports one user session per browser.

Name	Description
Maximum Sessions Per User	The maximum number of concurrent HTTP and HTTPS sessions allowed for each user. Enter an integer between 1 and 256.
Maximum Sessions	The maximum number of concurrent HTTP and HTTPS sessions allowed for all users within the system. Enter an integer between 1 and 256.
Maximum Event Interval (in seconds)	The maximum time interval between two events. Tracks various types of event change notifications, such as responses to any user requests from the UI. If the interval expires, the UI session is terminated. Enter and integer between 120-3600

Step 5 Click **Save Changes**.

Changing the Locales Assigned to a Locally Authenticated User Account

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

Procedure

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

Step 2 On the **Admin** tab, expand **All** > **User Management** > **User Services** > **Locally Authenticated Users**.

Step 3 Click the user account that you want to modify.

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

Step 5 In the **Locales** area, do the following:

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

Step 6 Click **Save Changes**.

Changing the Roles Assigned to a Locally Authenticated User Account

Changes in user roles and privileges do not take effect until the next time the user logs in. If a user is logged in when you assign a new role to or remove an existing role from a user account, the active session continues with the previous roles and privileges.

Procedure

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

Step 2 On the **Admin** tab, expand **All** > **User Management** > **User Services** > **Locally Authenticated Users**.

Step 3 Click the user account that you want to modify.

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

Step 5 In the **Roles** area, do the following:

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

Step 6 Click **Save Changes**.

Enabling a User Account

You must have admin or aaa privileges to enable or disable a local user account.

Before you begin

Create a local user account.

Procedure

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

Step 2 Expand **All** > **User Management** > **User Services** > **Locally Authenticated Users**.

Step 3 Click the user that you want to enable.

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

Step 5 In the **Account Status** field, click the **active** radio button.

Step 6 Click **Save Changes**.

Disabling a User Account

You must have admin or aaa privileges to enable or disable a local user account.

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

Procedure

Step 1 In the **Navigation** pane, click **Admin**.
Step 2 Expand **All** > **User Management** > **User Services** > **Locally Authenticated Users**.
Step 3 Click the user that you want to disable.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 In the **Account Status** field, click the **inactive** radio button.

The admin user account is always set to active. It cannot be modified.

Step 6 Click **Save Changes**.

Clearing the Password History for a Locally Authenticated User

Procedure

Step 1 In the **Navigation** pane, click **Admin**.
Step 2 Expand **All** > **User Management** > **User Services** > **Locally Authenticated Users**.
Step 3 Click the user for whom you want to clear the password history.
Step 4 In the **Actions** area, click **Clear Password History**.
Step 5 If a confirmation dialog box displays, click **Yes**.

Deleting a Locally Authenticated User Account

Procedure

Step 1 In the **Navigation** pane, click **Admin**.
Step 2 Expand **All** > **User Management** > **User Services**.

Step 3 Expand the **Locally Authenticated Users** node.

Step 4 Right-click the user account you want to delete and choose **Delete**.

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

Login Profile

The login profile feature provides the ability to block login requests to Cisco UCS Manager for a specific period after failed login attempts.

This feature is currently supported on the Cisco UCS 6400 Series Fabric Interconnect, , Cisco UCS 6200 Series Fabric Interconnect and on Cisco UCS Manager Release 4.0(1) and later releases.

Configuring Login Profile

Procedure

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

Step 2 Expand **All** > **User Management** > **User Services** > **Login Profile**

Step 3 In the Work pane, click the **Enable** radio button in the **Admin State** field to allow blocking of login requests to Cisco UCS Manager for a specific period after failed login attempts.

If this feature is enabled, login requests to Cisco UCS Manager will be blocked for *x* seconds if there are *y* number of failed login attempts in *z* seconds. Here:

- *x* is specified in the **Block Login** field.
- *y* is specified in the **Failed Attempts** field.
- *z* is specified in the **Attempted Within** field.

Step 4 In the **Block Login** field, specify the number of seconds that login requests to Cisco UCS Manager will be blocked after a specified number of failed login attempts.

The default number of seconds for which login requests will be blocked is 60 seconds.

Step 5 In the **Failed Attempts** field, specify the number of failed attempts after which login requests to Cisco UCS Manager will be blocked.

The default number of failed attempts to be made in a specified duration after which login requests will be blocked is 5.

Step 6 In the **Attempted Within** field, specify the number of seconds in which a specific number of failed attempts must be made for login requests to Cisco UCS Manager to be blocked.

The default number of seconds in which the failed login attempts must be made is 30 seconds.

Monitoring User Sessions

Procedure

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

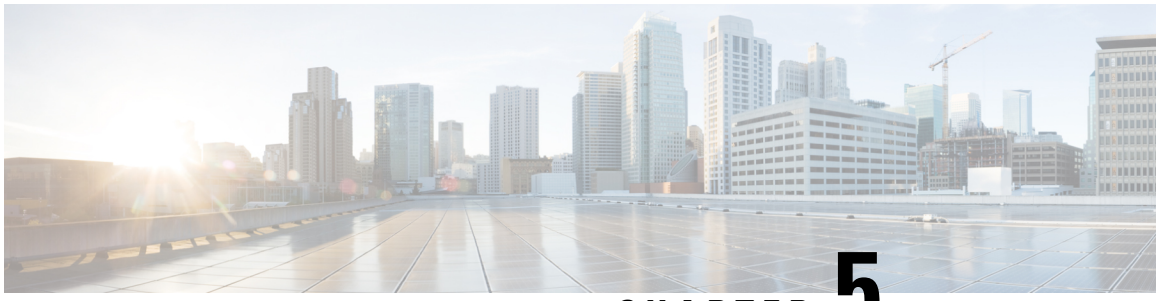
Step 2 In the **Admin** tab, expand **All** > **User Management**.

Step 3 Click the **User Services** node.

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

The tab displays the following details of user sessions:

Name	Description
Name column	The name for the session.
User column	The username that is involved in the session.
Fabric ID column	The fabric interconnect that the user logged in to for the session.
Login Time column	The date and time the session started.
Refresh Period column	When a web client connects to Cisco UCS Manager, the client must send refresh requests to Cisco UCS Manager to keep the web session active. This option specifies the maximum amount of time allowed between refresh requests for a user in this domain. If this time limit is exceeded, Cisco UCS Manager considers the web session inactive, but it does not terminate the session.
Session Timeout column	The maximum amount of time that can elapse after the last cookie/token refresh request has failed before Cisco UCS Manager considers a web session as inactive. If this time limit is exceeded, Cisco UCS Manager automatically terminates the web session.
Terminal Type column	The kind of terminal the user is logged in through.
Host column	The IP address from which the user is logged in.
Current Session column	If this column displays **Y**, the associated user session is currently active.



CHAPTER 5

Remote Authentication

- Authentication Services, on page 45
- Guidelines and Recommendations for Remote Authentication Providers, on page 45
- User Attributes in Remote Authentication Providers, on page 46
- Two-Factor Authentication, on page 48
- LDAP Providers and Groups, on page 48
- RADIUS Providers, on page 56
- TACACS+ Providers , on page 58
- Primary Authentication Service, on page 59
- Multiple Authentication Services Configuration, on page 63

Authentication Services

Cisco UCS supports the following two methods to authenticate user logins:

- Local user authentication - uses user accounts that exist locally in the Cisco UCS Manager
- Remote user authentication - uses one of the following protocols:
  - LDAP
  - RADIUS
  - TACACS+

Guidelines and Recommendations for Remote Authentication Providers

If a system is configured for one of the supported remote authentication services, you must create a provider for that service to ensure that Cisco UCS Manager can communicate with the system. The following guidelines impact user authorization:

User Accounts in Remote Authentication Services

User accounts can exist locally in Cisco UCS Manager or in the remote authentication server.

You can view the temporary sessions for users who log in through remote authentication services from the Cisco UCS Manager GUI and from the Cisco UCS Manager CLI.

User Roles in Remote Authentication Services

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

User Attributes in Remote Authentication Providers

For RADIUS and TACACS+ configurations, you must configure a user attribute for Cisco UCS in each remote authentication provider through which users log in to Cisco UCS Manager. This user attribute holds the roles and locales assigned to each user.

Note This step is not required for LDAP configurations that use the LDAP Group Mapping to assign roles and locales.

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

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

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

Table 6: Comparison of User Attributes by Remote Authentication Provider

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

Authentication Provider	Custom Attribute	Schema Extension	Attribute ID Requirements
RADIUS	Optional	Optional. You can choose to do one of the following: • Do not extend the RADIUS schema and use an existing unused attribute that meets the requirements. • Extend the RADIUS schema and create a custom attribute with a unique name, such as cisco-avpair.	The vendor ID for the Cisco RADIUS implementation is 009 and the vendor ID for the attribute is 001. The following syntax example shows how to specify multiples user roles and locales if you choose to create the cisco-avpair attribute: `shell:roles="admin,aaa" shell:locales="L1,abc"`. Use a comma "," as the delimiter to separate multiple values.
TACACS+	Required	Required. You must extend the schema and create a custom attribute with the name cisco-av-pair.	The cisco-av-pair name is the string that provides the attribute ID for the TACACS+ provider. The following syntax example shows how to specify multiples user roles and locales when you create the cisco-av-pair attribute: `cisco-av-pair=shell:roles="admin aaa" shell:locales*"L1 abc"`. Using an asterisk (*) in the cisco-av-pair attribute syntax flags the locale as optional, preventing authentication failures for other Cisco devices that use the same authorization profile. Use a space as the delimiter to separate multiple values.

Sample OID for LDAP User Attribute

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

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

```
lDAPDisplayName: CiscoAVPair
name: CiscoAVPair
objectCategory: CN=Attribute-Schema,CN=Schema,CN=Configuration,CN=X
```

Two-Factor Authentication

Cisco UCS Manager uses two-factor authentication for remote user logins, which adds a level of security to account logins. Two-factor authentication login requires a username, a token, and a password combination in the password field. You can provide a PIN, a certificate, or a token.

Two-factor authentication uses authentication applications that maintain token servers to generate one-time tokens for users during the login process and store passwords in the AAA server. Requests are sent to the token server to retrieve a vendor-specific attribute. Cisco UCS Manager expects the token server to integrate with the AAA server, therefore it forwards the request to the AAA server. The password and token are validated at the same time by the AAA server. Users must enter the token and password sequence in the same order as it is configured in the AAA server.

Two-factor authentication is supported by associating RADIUS or TACACS+ provider groups with designated authentication domains and enabling two-factor authentication for those domains. Two-factor authentication does not support IPM and is not supported when the authentication realm is set to LDAP, local, or none.

Web Session Refresh and Web Session Timeout Period

The **Web Session Refresh Period** is the maximum amount of time allowed between refresh requests for a Cisco UCS Manager GUI web session. The **Web Session Timeout** is the maximum amount of time that can elapse after the last cookie/token refresh request has failed before a Cisco UCS Manager GUI web session becomes inactive.

You can increase the **Web Session Refresh Period** to a value greater than 60 seconds up 172800 seconds to avoid frequent session timeouts that requires regenerating and re-entering a token and password multiple times. The default value is 7200 seconds when two-factor authentication is enabled, and is 600 seconds when two-factor authentication is not enabled.

You can specify a value between 300 and 172800 for the **Web Session Timeout Period**. The default is 8000 seconds when two-factor authentication is enabled, and 7200 seconds when two-factor authentication is not enabled.

LDAP Providers and Groups

Nested LDAP Groups

You can add an LDAP group as a member of another group and nest groups to consolidate member accounts and to reduce the replication of traffic. Cisco UCS Manager release 2.1(2) and higher enables you to search LDAP groups that are nested within another group defined in an LDAP group map.

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

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

You do not always need to create subgroups in a group map in Cisco UCS Manager.

LDAP Group Rule

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

Configuring Properties for LDAP Providers

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

Before you begin

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

Procedure

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

Step 2 Expand **All** > **User Management** > **LDAP**.

Step 3 In the **Properties** area, complete all fields.

Note
User login fails if the userDn for an LDAP user exceeds 255 characters.

Step 4 Click **Save Changes**.

What to do next

Create an LDAP provider.

Creating an LDAP Provider

Cisco UCS Manager supports a maximum of 16 LDAP providers.

Before you begin

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

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

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

  The Cisco LDAP implementation requires a unicode type attribute.

  If you choose to create the CiscoAVPair custom attribute, use the following attribute ID: 1.3.6.1.4.1.9.287247.1
- For a cluster configuration, add the management port IPv4 or IPv6 addresses for both fabric interconnects. This configuration ensures that remote users can continue to log in if the first fabric interconnect fails and the system fails over to the second fabric interconnect. All login requests are sourced from these IP addresses, not the virtual IPv4 or IPv6 address used by Cisco UCS Manager.

- If you want to use secure communications, create a trusted point containing the certificate of the root certificate authority (CA) of the LDAP server in Cisco UCS Manager.
- If you need to change the LDAP providers or add or delete them, change the authentication realm for the domain to local, make the changes to the providers, then change the domain authentication realm back to LDAP.

Attention LDAP remote usernames that include special characters cannot log in to systems that are running versions 2.2(3a) and later. The user cannot log in because of the Nexus OS limitations where special characters, !,%,^, are not supported in the username.

Procedure

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

Step 2 Expand **All** > **User Management** > **LDAP**.

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

Step 4 In the **Actions** area, click **Create LDAP Provider**.

Step 5 On the **Create LDAP Provider** page of the wizard, complete all fields with appropriate LDAP service information.

a) Complete the following fields with information about the LDAP service you want to use:

Name	Description
Hostname/FDQN (or IP Address) field	The hostname, or IPv4 or IPv6 address on which the LDAP provider resides. If SSL is enabled, this field must exactly match a Common Name (CN) in the security certificate of the LDAP database. **Note** If you use a hostname rather than an IPv4 or IPv6 address, you must configure a DNS server. If the Cisco UCS domain is not registered with Cisco UCS Central or DNS management is set to **local**, configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to **global**, configure a DNS server in Cisco UCS Central.
Order field	The order that the Cisco UCS uses this provider to authenticate users. Enter an integer between 1 and 16, or enter `lowest-available` or `0` (zero) if you want Cisco UCS to assign the next available order based on the other providers defined in this Cisco UCS domain.
Bind DN field	The distinguished name (DN) for an LDAP database account that has read and search permissions for all objects under the base DN. The maximum supported string length is 255 ASCII characters.
Base DN field	The specific distinguished name in the LDAP hierarchy where the server begins a search when a remote user logs in and the system attempts to obtain the user's DN based on their username. You can set the length of the base DN to a maximum of 255 characters minus the length of CN=username, where username identifies the remote user attempting to access Cisco UCS Manager using LDAP authentication. This value is required unless a default base DN has been set on the LDAP **General** tab.
Port field	The port through which Cisco UCS communicates with the LDAP database. The standard port number is 389.
Enable SSL check box	If checked, encryption is required for communications with the LDAP database. If unchecked, authentication information will be sent as clear text. LDAP uses STARTTLS. This allows encrypted communication using port 389. If checked, do not change the port to 636, leave it as 389. Cisco UCS negotiates a TLS session on port 636 for SSL, but initial connection starts unencrypted on 389.
Filter field	The LDAP search is restricted to those user names that match the defined filter. This value is required unless a default filter has been set on the LDAP **General** tab.

Name	Description
Attribute field	An LDAP attribute that stores the values for the user roles and locales. This property is always a name-value pair. The system queries the user record for the value that matches this attribute name. If you do not want to extend your LDAP schema, you can configure an existing, unused LDAP attribute with the Cisco UCS roles and locales. Alternatively, you can create an attribute named CiscoAVPair in the remote authentication service with the following attribute ID: `1.3.6.1.4.1.9.287247.1` This value is required unless a default attribute has been set on the LDAP **General** tab.
Password field	The password for the LDAP database account specified in the **Bind DN** field. You can enter any standard ASCII characters except for space, § (section sign), ? (question mark), or = (equal sign).
Confirm Password field	The LDAP database password repeated for confirmation purposes.
Timeout field	The length of time in seconds the system spends trying to contact the LDAP database before it times out. Enter an integer from 1 to 60 seconds, or enter 0 (zero) to use the global timeout value specified on the LDAP **General** tab. The default is 30 seconds.
Vendor radio button	The LDAP vendor that you want to use. This can be one of the following: • Open Ldap—The open source implementation of the LDAP protocol. • MS AD—Microsoft Active Directory.

b) Click **Next**.

Step 6 On the **LDAP Group Rule** page of the wizard, complete all fields with appropriate LDAP group rule information.

Note
Role and locale assignment is cumulative. If a user is included in multiple groups, or has a role or locale specified in the LDAP attribute, Cisco UCS assigns that user all the roles and locales mapped to any of those groups or attributes.

What to do next

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

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

Changing the LDAP Group Rule for an LDAP Provider

Procedure

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

Step 2 Expand **All** > **User Management** > **LDAP**.

Step 3 Expand **LDAP Providers** and choose the LDAP provider for which you want to change the group rule.

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

Step 5 In the **LDAP Group Rules** area, complete the following fields:

Name	Description
Group Authorization field	Whether Cisco UCS also searches LDAP groups when authenticating and assigning user roles and locales to remote users. This can be one of the following: • **Disable**—Cisco UCS does not access any LDAP groups. • **Enable**—Cisco UCS searches all LDAP groups mapped in this Cisco UCS domain. If the remote user is found, Cisco UCS assigns the user roles and locales defined for that LDAP group in the associated LDAP group map. **Note** Role and locale assignment is cumulative. If a user is included in multiple groups, or has a role or locale specified in the LDAP attribute, Cisco UCS assigns that user all the roles and locales mapped to any of those groups or attributes.
Group Recursion field	Whether Cisco UCS searches both the mapped groups and their parent groups. This can be one of the following: • **Non Recursive**—Cisco UCS searches only the groups mapped in this Cisco UCS domain. If none of the groups containing the user explicitly set the user's authorization properties, Cisco UCS uses the default settings. • **Recursive**—Cisco UCS searches each mapped group and all its parent groups for the user's authorization properties. These properties are cumulative, so for each group Cisco UCS finds with explicit authorization property settings, it applies those settings to the current user. Otherwise it uses the default settings.
Target Attribute field	The attribute Cisco UCS uses to determine group membership in the LDAP database. The supported string length is 63 characters. The default string is **`memberOf`**.

Name	Description
Use Primary Group field	The attribute Cisco UCS uses to determine if the primary group can be configured as an LDAP group map for membership validation. With this option Cisco UCS Manager can download and verify the primary-group membership of the user.

Step 6 Click **Save Changes**.

Deleting an LDAP Provider

Procedure

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

Step 2 Expand **All** > **User Management** > **LDAP**.

Step 3 Expand **LDAP Providers**.

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

Step 5 If a confirmation dialog box displays, click **Yes**.

LDAP Group Mapping

LDAP group mapping eliminates having to define role or locale information in the LDAP user object. UCSM can use group membership information to assign a role or locale to an LDAP user during login for organizations using LDAP groups to restrict access to LDAP databases.

When a user logs in to Cisco UCS Manager, the LDAP group map pulls information about the user's role and locale. If the role and locale criteria match the information in the policy, access is granted. Cisco UCS Manager supports a maximum of 28, 128, or 160 LDAP group maps depending on the release version.

Note Cisco UCS Manager Release 3.1(1) supports a maximum of 128 LDAP group maps, and Release 3.1(2) and later releases support a maximum of 160 LDAP group maps.

The role and locale definitions that you configure locally in the Cisco UCS Manager do not update automatically based on changes to an LDAP directory. When deleting or renaming LDAP groups in an LDAP directory, you must also update the Cisco UCS Manager with the change.

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

- Roles only
- Locales only
- Both roles and locales

For example, consider an LDAP group representing a group of server administrators at a specific location. The LDAP group map might include user roles such as server profile and server equipment. To restrict access to server administrators at a specific location, you can set the locale to a particular site name.

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

Creating an LDAP Group Map

Before you begin

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

Procedure

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

Step 2 Expand **All** > **User Management** > **LDAP**.

Step 3 Right-click **LDAP Group Maps** and choose **Create LDAP Group Map**.

Step 4 In the **Create LDAP Group Map** dialog box, specify all LDAP group map information, as appropriate.

Important
The name that you specify in the **LDAP Group DN** field must match the name in the LDAP database.

Note
If you use a special character in the **LDAP Group DN** field, you must prefix the special character with an escape character \ (single back slash).

What to do next

Set the LDAP group rule.

Deleting an LDAP Group Map

Procedure

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

Step 2 Expand **All** > **User Management** > **LDAP**.

Step 3 Expand **LDAP Group Maps**.

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

Step 5 If a confirmation dialog box displays, click **Yes**.

RADIUS Providers

Configuring Properties for RADIUS Providers

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

Note RADIUS authentication uses Password Authentication Protocol (PAP).

Procedure

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

Step 2 Choose**User Management** > **RADIUS**.

Step 3 In the **Properties** area, complete all fields.

Step 4 Click **Save Changes**.

What to do next

Create a RADIUS provider.

Creating a RADIUS Provider

Cisco UCS Manager supports a maximum of 16 RADIUS providers.

Before you begin

Perform the following configuration in the RADIUS server:

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

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

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

- For a cluster configuration, add the management port IPv4 or IPv6 addresses for both fabric interconnects. This configuration ensures that remote users can continue to log in if the first fabric interconnect fails and the system fails over to the second fabric interconnect. All login requests are sourced from these IP addresses, not the virtual IP address used by Cisco UCS Manager.

Procedure

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

Step 2 Expand **All** > **User Management** > **RADIUS**.

Step 3 In the **Create RADIUS Provider** dialog box, specify all appropriate RADIUS service information.

Note
If you use a hostname rather than an IPv4 or IPv6 address, you must ensure that a DNS server is configured for the hostname.

Step 4 Click **Save Changes**.

What to do next

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

For implementations involving multiple RADIUS databases, configure a RADIUS provider group.

Deleting a RADIUS Provider

Procedure

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

Step 2 Choose**User Management** > **RADIUS**.

Step 3 Right-click the RADIUS provider that you want to delete and choose **Delete**.

Step 4 If a confirmation dialog box displays, click **Yes**.

TACACS+ Providers

Configuring Properties for TACACS+ Providers

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

Procedure

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

Step 2 Choose**User Management** > **TACACS+**.

Step 3 In the **Properties** area, complete the **Timeout** field.

Step 4 Click **Save Changes**.

What to do next

Create a TACACS+ provider.

Creating a TACACS+ Provider

Cisco UCS Manager supports a maximum of 16 TACACS+ providers.

Before you begin

Perform the following configuration in the TACACS+ server:

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

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

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

- For a cluster configuration, add the management port IPv4 or IPv6 addresses for both fabric interconnects. This configuration ensures that remote users can continue to log in if the first fabric interconnect fails and the system fails over to the second fabric interconnect. All login requests are sourced from these IP addresses, not the virtual IP address used by Cisco UCS Manager.

Procedure

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

Step 2 Expand **All** > **User Management** > **TACACS+**.

Step 3 In the **Actions** area of the **General** tab, click **Create TACACS+ Provider**.

Step 4 In the **Create TACACS+ Provider** dialog box:

a) Complete all fields with TACACS+ service information, as appropriate.

Note
If you use a hostname rather than an IPv4 or IPv6 address, you must ensure a DNS server is configured for the hostname.

b) Click **OK**.

Step 5 Click **Save Changes**.

What to do next

For implementations involving a single TACACS+ database, select TACACS+ as the primary authentication service.

For implementations involving multiple TACACS+ databases, configure a TACACS+ provider group.

Deleting a TACACS+ Provider

Procedure

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

Step 2 Choose**User Management** > **TACACS+**.

Step 3 Right-click the TACACS+ provider that you want to delete and choose **Delete**.

Step 4 If a confirmation dialog box displays, click **Yes**.

Primary Authentication Service

Selecting the Console Authentication Service

Before you begin

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

Procedure

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

Step 2 Expand **All** > **User Management** > **Authentication**.

Step 3 Click **Native Authentication**.

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

Step 5 In the **Console Authentication** area, complete the following fields:

Name	Description
Realm field	The method by which a user logging into the console is authenticated. This can be one of the following: • **Local**—The user account must be defined locally in this Cisco UCS domain. • **Radius**—The user must be defined on the RADIUS server specified for this Cisco UCS domain. • **Tacacs**—The user must be defined on the TACACS+ server specified for this Cisco UCS domain. • **Ldap**—The user must be defined on the LDAP server specified for this Cisco UCS domain. • **None**—If the user account is local to this Cisco UCS domain, no password is required when the user logs into the console.
Provider Group drop-down list	The provider group to be used to authenticate a user logging into the console. **Note** The**Provider Group** drop-down list is displayed when you select Ldap, Radius, or Tacacs as the method by which a user is authenticated.
Two Factor Authentication	Two-factor authentication is available only when the **Realm** is set to **Radius** or **Tacacs**. When this checkbox is selected, the Console requires users whose accounts are authenticated by Radius or Tacacs servers to enter a token plus a password to log in.

Step 6 Click **Save Changes**.

Selecting the Default Authentication Service

Before you begin

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

Procedure

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

Step 2 Expand **All** > **User Management** > **Authentication**.

Step 3 Click **Native Authentication**.

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

Step 5 In the **Default Authentication** area, complete the following fields:

Name	Description
Realm drop-down list	The default method by which a user is authenticated during remote login. This can be one of the following: • **Local**—The user account must be defined locally in this Cisco UCS domain. • **Radius**—The user account must be defined on the RADIUS server specified for this Cisco UCS domain. • **Tacacs**—The user account must be defined on the TACACS+ server specified for this Cisco UCS domain. • **Ldap**—The user account must be defined on the LDAP server specified for this Cisco UCS domain. • **None**—If the user account is local to this Cisco UCS domain, no password is required when the user logs in remotely.
Provider Group drop-down list	The default provider group to be used to authenticate the user during remote login. **Note** The **Provider Group** drop-down is displayed when you select Ldap, Radius, or Tacacs as the method by which a user is authenticated.

Name	Description
Web Session Refresh Period (sec)	When a web client connects to Cisco UCS Manager, the client must send refresh requests to Cisco UCS Manager to keep the web session active. This option specifies the maximum amount of time allowed between refresh requests for a user in this domain. If this time limit is exceeded, Cisco UCS Manager considers the web session inactive, but it does not terminate the session. Specify an integer between 60 and 172800. The default is 600 seconds when Two-Factor Authentication is not enabled and 7200 seconds when it is enabled.
Web Session Timeout (sec)	The maximum amount of time that can elapse after the last cookie/token refresh request has failed before Cisco UCS Manager considers a web session as inactive. If this time limit is exceeded, Cisco UCS Manager automatically terminates the web session. Specify an integer between 300 and 172800. The default is 7200 seconds when Two-Factor Authentication is not enabled and 8000 seconds when it is enabled.
Two Factor Authentication checkbox	Two-Factor Authentication is available only when the **Realm** is set to **Radius** or **Tacacs**. When you select this check box, Cisco UCS Manager and the KVM launch manager require users whose accounts are authenticated by Radius or Tacacs servers to enter a token plus a password to log in. When 60 seconds remain for the **Web Session Refresh Period** to expire, users must generate a new token and enter the token plus their password to continue the session. **Note** After you enable two factor authentication and save the configuration, the default **Web Session Refresh Period (sec)** changes to 7200, and the default **Web Session Timeout (sec)** changes to 8000.

Step 6 Click **Save Changes**.

Role Policy for Remote Users

By default, if user roles are not configured in Cisco UCS Manager read-only access is granted to all users logging in to Cisco UCS Manager from a remote server using the LDAP, RADIUS, or TACACS protocols. For security reasons, it might be desirable to restrict access to those users matching an established user role in Cisco UCS Manager.

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

assign-default-role

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

This is the default behavior.

no-login

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

Configuring the Role Policy for Remote Users

Procedure

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

Step 2 Expand **All** > **User Management** > **Authentication**.

Step 3 Click **Native Authentication**.

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

Step 5 In the **Role Policy for Remote Users** field, click one of the following radio buttons to determine what happens when a user attempts to log in and the remote authentication provider does not supply a user role with the authentication information:

- **No Login**—The user is not allowed to log in to the system, even if the username and password are correct.
- **Assign Default Role**—The user is allowed to log in with a read-only user role.

Step 6 Click **Save Changes**.

Multiple Authentication Services Configuration

Multiple Authentication Services

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

- Provider groups
- Authentication domains

Provider Groups

A provider group is a set of providers that the Cisco UCS accesses during the authentication process. All of the providers within a provider group are accessed in the order that the Cisco UCS provider uses to authenticate users. If all of the configured servers are unavailable or unreachable, Cisco UCS Manager automatically falls back to the local authentication method using the local username and password.

Cisco UCS Manager allows you to create a maximum of 16 provider groups, with a maximum of eight providers allowed per group.

Creating an LDAP Provider Group

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

Before you begin

Create one or more LDAP providers.

Procedure

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

Step 2 Expand **All** > **User Management** > **LDAP**.

Step 3 Right-click **LDAP Provider Groups** and choose **Create LDAP Provider Group**.

Note
If you use a hostname rather than an IPv4 or IPv6 address, you must ensure a DNS server is configured for the hostname.

Step 4 In the **Create LDAP Provider Group** dialog box, specify all of the appropriate LDAP provider group information.

What to do next

Configure an authentication domain or select a default authentication service.

Deleting an LDAP Provider Group

Before you begin

Remove the provider group from an authentication configuration.

Procedure

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

Step 2 Expand **All** > **User Management** > **LDAP**.

Step 3 Expand **LDAP Provider Groups**.

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

Step 5 If a confirmation dialog box displays, click **Yes**.

Creating a RADIUS Provider Group

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

Before you begin

Create one or more RADIUS providers.

Procedure

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

Step 2 Expand **All** > **User Management** > **RADIUS**.

Step 3 Right-click **RADIUS Provider Groups** and choose **Create RADIUS Provider Group**.

Step 4 In the **Create RADIUS Provider Group** dialog box, do the following:

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

This name can be between 1 and 127 ASCII characters.

b) In the **RADIUS Providers** table, choose one or more providers to include in the group.

c) Click the >> button to add the providers to the **Included Providers** table.

You can use the << button to remove providers from the group.

d) (Optional) Use the **Move Up** or **Move Down** arrows in the **Included Providers** list to change the order in which the RADIUS providers authenticate providers.

e) After you add all of the required providers to the provider group, click **OK**.

What to do next

Configure an authentication domain or select a default authentication service.

Deleting a RADIUS Provider Group

You cannot delete a provider group if another authentication configuration is using that provider group.

Procedure

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

Step 2 Expand **All** > **User Management** > **RADIUS**.

Step 3 Expand **RADIUS Provider Groups**.

Step 4 Right-click the RADIUS provider group you want to delete and choose **Delete**.

Step 5 If a confirmation dialog box displays, click **Yes**.

Creating a TACACS+ Provider Group

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

Before you begin

Create one or more TACACS+ providers.

Procedure

Step 1 In the **Navigation** pane, click **Admin**.
Step 2 Expand **All** > **User Management** > **TACACS+**.
Step 3 Right-click **TACACS+ Provider Groups** and choose **Create TACACS+ Provider Group**.
Step 4 In the **Create TACACS+ Provider Group** dialog box, specify all TACACS+ provider group information, as appropriate.

Deleting a TACACS+ Provider Group

You cannot delete a provider group if another authentication configuration is using that provider group.

Procedure

Step 1 In the **Navigation** pane, click **Admin**.
Step 2 Expand **All** > **User Management** > **TACACS+**.
Step 3 Expand **TACACS+ Provider Groups**.
Step 4 Right-click the TACACS+ provider group that you want to delete and choose **Delete**.
Step 5 If a confirmation dialog box displays, click **Yes**.

Authentication Domains

The Cisco UCS Manager uses Authentication Domains to leverage multiple authentication systems. You can specify and configure each authentication domain during login; otherwise, Cisco UCS Manager uses the default authentication service configuration.

You can create up to eight authentication domains. Each authentication domain is associated with a provider group and a realm in the Cisco UCS Manager. The Cisco UCS Manager uses all servers within the realm if you do not specify a provider group.

Creating an Authentication Domain

Procedure

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

Step 2 Expand **All** > **User Management** > **Authentication**.

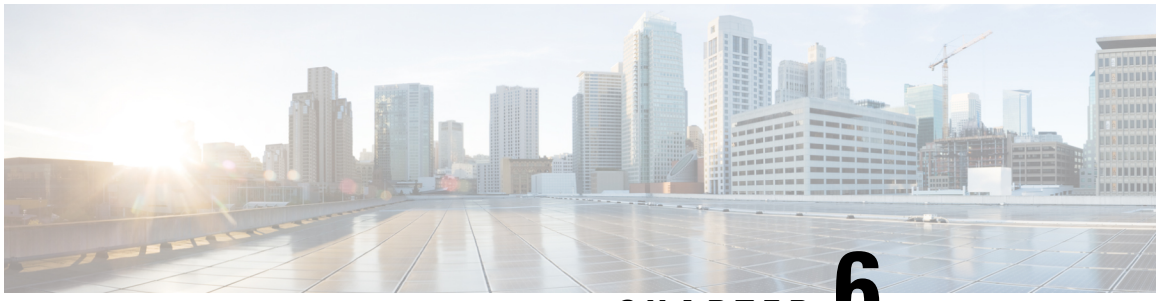
Step 3 Right-click **Authentication Domains** and choose **Create a Domain**.

Step 4 In the **Create a Domain** dialog box, complete the following fields:

Name	Description
Name	The name of the domain. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), and . (period), and you cannot change this name after the object is saved. **Note** For systems using the remote authentication protocol, the authentication domain name is considered part of the username and counts toward the 32-character limit for locally created usernames. Because Cisco UCS inserts 5 characters for formatting, authentication fails if the domain name and username combined characters total exceeds 27.
Web Session Refresh Period (sec)	When a web client connects to Cisco UCS Manager, the client must send refresh requests to Cisco UCS Manager to keep the web session active. This option specifies the maximum amount of time allowed between refresh requests for a user in this domain. If this time limit is exceeded, Cisco UCS Manager considers the web session inactive, but it does not terminate the session. Specify an integer between 60 and 172800. The default is 600 seconds when Two-Factor Authentication is not enabled and 7200 seconds when it is enabled. **Note** The number of seconds set for the **Web Session Refresh Period** must be less than the number of seconds set for the **Web Session Timeout**. Do not set the **Web Session Refresh Period** to the same value as the **Web Session Timeout**.
Web Session Timeout (sec)	The maximum amount of time that can elapse after the last cookie/token refresh request has failed before Cisco UCS Manager considers a web session as inactive. If this time limit is exceeded, Cisco UCS Manager automatically terminates the web session. Specify an integer between 300 and 172800. The default is 7200 seconds when Two-Factor Authentication is not enabled and 8000 seconds when it is enabled.

Name	Description
Realm	The authentication protocol to apply to users in this domain. This can be one of the following: • **Local**—The user account must be defined locally in this Cisco UCS domain. • **Radius**—The user must be defined on the RADIUS server specified for this Cisco UCS domain. • **Tacacs**—The user must be defined on the TACACS+ server specified for this Cisco UCS domain. • **Ldap**—The user must be defined on the LDAP server specified for this Cisco UCS domain.
Provider Group	The default provider group to use to authenticate users during remote login. **Note** The **Provider Group** drop-down list displays when you select Ldap Radius, or Tacacs as the method to authenticate users.
Two Factor Authentication	Two-Factor Authentication is available only when the **Realm** is set to **Radius** or **Tacacs**. When you select this check box, Cisco UCS Manager and the KVM launch manager require users whose accounts are authenticated by Radius or Tacacs servers to enter a token plus a password to log in. When 60 seconds remain for the **Web Session Refresh Period** to expire, users must generate a new token and enter the token plus their password to continue the session.

Step 5 Click **OK**.



CHAPTER 6

How to Enable and Disable the Call Home Feature

- Call Home in UCS Overview, on page 69
- Enabling Call Home, on page 70
- Disabling Call Home, on page 71
- Creating a Call Home Profile, on page 72
- Deleting a Call Home Profile, on page 74
- Configuring a Call Home Policy, on page 74
- Deleting a Call Home Policy, on page 75

Call Home in UCS Overview

Call Home provides an email-based notification for critical system policies. A range of message formats are available for compatibility with pager services or XML-based automated parsing applications. You can use this feature to page a network support engineer, email a Network Operations Center, or use Cisco Smart Call Home services to generate a case with the Technical Assistance Center.

The Call Home feature can deliver alert messages containing information about diagnostics and environmental faults and events.

The Call Home feature can deliver alerts to multiple recipients, referred to as Call Home destination profiles. Each profile includes configurable message formats and content categories. A predefined destination profile is provided for sending alerts to the Cisco TAC, but you also can define your own destination profiles.

When you configure Call Home to send messages, Cisco UCS Manager executes the appropriate CLI **show** command and attaches the command output to the message.

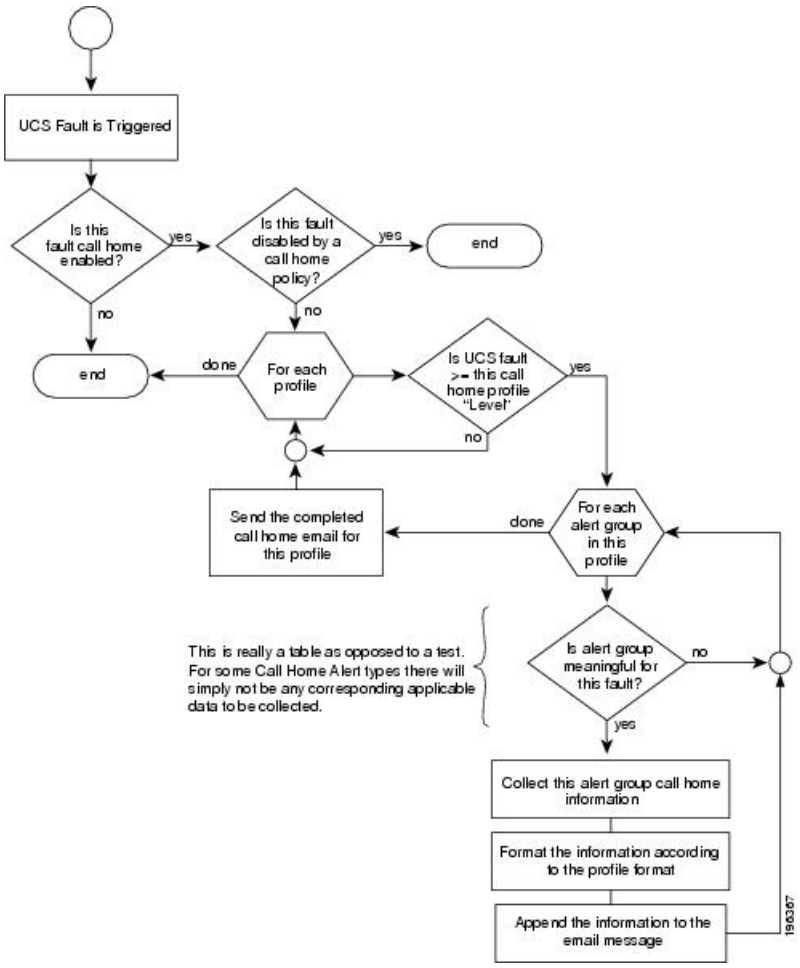
Cisco UCS delivers Call Home messages in the following formats:

- Short text format which provides a one or two line description of the fault that is suitable for pagers or printed reports.
- Full text format which provides fully formatted message with detailed information that is suitable for human reading.
- XML machine-readable format that uses Extensible Markup Language (XML) and Adaptive Messaging Language (AML) XML Schema Definition (XSD). The AML XSD is published on the Cisco.com website. The XML format enables communication with the Cisco Systems Technical Assistance Center.

For information about the faults that can trigger Call Home email alerts, see the *Cisco UCS Faults and Error Messages Reference*.

The following figure shows the flow of events after a Cisco UCS fault is triggered in a system with Call Home configured:

Figure 1: Flow of Events after a Fault is Triggered



Enabling Call Home

Procedure

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

Step 2 Expand **All** > **Communication Management** > **Call Home**.

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

Step 4 In the **Admin** area, complete the following fields to enable Call Home:

Name	Description
State field	This can be one of the following: • **Off**—Call Home is not used for this Cisco UCS domain. • **On**—Cisco UCS generates Call Home alerts based on the Call Home policies and profiles defined in the system. **Note** If this field is set to **On**, Cisco UCS Manager GUI displays the rest of the fields on this tab.
Switch Priority drop-down list	This can be one of the following: • **Alerts** • **Critical** • **Debugging** • **Emergencies** • **Errors** • **Information** • **Notifications** • **Warnings**
Throttling field	Indicates whether the system limits the number of duplicate messages received for the same event. This can be one of the following: • **On**—If the number of duplicate messages sent exceeds 30 messages within a 2-hour timeframe, then the system discards further messages for that alert type. • **Off**—The system sends all duplicate messages, regardless of how many are encountered.

Step 5 Click **Save Changes**.

Disabling Call Home

Procedure

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

Step 2 Expand **All** > **Communication Management** > **Call Home**.

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

Step 4 In the **Admin** area, click **off** in the **State** field.

Note
If this field is set to **off**, Cisco UCS Manager hides the rest of the fields on this tab.

Step 5 Click **Save Changes**.

What to do next

For more information on the Call Home feature, see the *Cisco UCS System Monitoring Guide*.

Creating a Call Home Profile

By default, you must configure the Cisco TAC-1 profile. However, you can also create additional profiles to send email alerts to one or more specified groups when events occur at the level that you specify.

Procedure

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

Step 2 Expand **All** > **Communication Management** > **Call Home**.

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

Step 4 On the icon bar to the right of the table, click +.

If the + icon is disabled, click an entry in the table to enable it.

Step 5 In the **Create Call Home Profile** dialog box, complete the following information fields:

Name	Description
Name field	A user-defined name for this profile. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.

Name	Description
Level field	Cisco UCS faults that are greater than or equal to this level trigger the profile. This can be one of the following: • **Critical** • **Debug** • **Disaster** • **Fatal** • **Major** • **Minor** • **Normal** • **Notification** • **Warning**
Alert Groups field	The group or groups that are alerted based on this Call Home profile. This can be one or more of the following: • **Cisco Tac**—Cisco TAC recipients • **Diagnostic**—POST completion server failure notification recipients • **Environmental**—Recipients of notifications about problems with PSUs, fans, etc.

Step 6 In the **Email Configuration** area, complete the following fields to configure the email alerts:

Name	Description
Format field	This can be one of the following: • **Xml**—A machine readable format that uses Extensible Markup Language (XML) and Adaptive Messaging Language (AML) XML schema definition (XSD). This format enables communication with the Cisco Systems Technical Assistance Center. • **Full Txt**—A fully formatted message with detailed information that is suitable for human reading. • **Short Txt**—A one or two line description of the fault that is suitable for pagers or printed reports.

Name	Description
Max Message Size field	The maximum message size that is sent to the designated Call Home recipients. Enter an integer between 1 and 5000000. The default is 5000000. For full text and XML messages, the maximum recommended size is 5000000. For short text messages, the maximum recommended size is 100000. For the Cisco TAC alert group, the maximum message size must be 5000000.

Step 7 In the **Recipients** area, do the following to add one or more email recipients for the email alerts:

a) On the icon bar to the right of the table, click +.

b) In the **Add Email Recipients** dialog box, enter the email address to which Call Home alerts should be sent in the **Email** field.

This email address receives Callhome Alerts/Faults.

After you save this email address, it can be deleted but it cannot be changed.

c) Click **OK**.

Step 8 Click **OK**.

Deleting a Call Home Profile

Procedure

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

Step 2 Expand **All** > **Communication Management** > **Call Home**.

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

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

Step 5 Click **Save Changes**.

Configuring a Call Home Policy

Tip By default, all Call Home policies are enabled to ensure that email alerts are sent for all critical system events.

Procedure

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

Step 2 Expand **All** > **Communication Management** > **Call Home**.

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

Step 4 On the icon bar to the right of the table, click **+**.

If the **+** icon is disabled, click an entry in the table to enable it.

Step 5 In the **Create Call Home Policy** dialog box, complete the following fields:

Name	Description
State field	If this field is **Enabled**, the system uses this policy when an error matching the associated cause is encountered. Otherwise, the system ignores this policy even if a matching error occurs. By default, all policies are enabled.
Cause field	The event that triggers the alert. Each policy defines whether an alert is sent for one type of event.

Step 6 Click **OK**.

Step 7 Repeat Steps 4 and 5 if you want to configure a Call Home policy for a different type of fault or event.

Deleting a Call Home Policy

Procedure

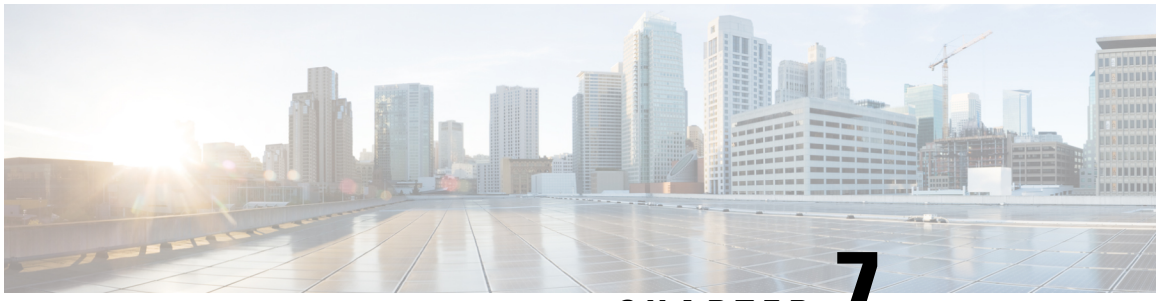
Step 1 In the **Navigation** pane, click **Admin**.

Step 2 Expand **All** > **Communication Management** > **Call Home**.

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

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

Step 5 Click **Save Changes**.



CHAPTER 7

UCS Manager Communication Services

- Communication Protocols, on page 77
- Communication Services, on page 77
- Non-Secure Communication Services , on page 79
- Secure Communication Services , on page 81
- Network-Related Communication Services, on page 89

Communication Protocols

Communication Services

You can use the communication services defined below to interface third-party applications with Cisco UCS.

Cisco UCS Manager supports IPv4 and IPv6 address access for the following services:

- CIM XML
- HTTP
- HTTPS
- SNMP
- SSH
- Telnet

Cisco UCS Manager supports out-of-band IPv4 address access to the **Cisco UCS KVM Direct** launch page from a web browser. To provide this access, you must enable the following service:

- CIMC Web Service

Communication Service	Description
CIM XML	The Common Information Model (CIM) XML) service is disabled by default and is only available in read-only mode. The default port is 5988. The CIM XML is a standards-based protocol for exchanging CIM information that the Distributed Management Task Force defines.

Communication Service	Description
CIMC Web Service	This service is disabled by default. When this service is enabled, users can directly access a server CIMC using one of the out-of-band management IP addresses assigned directly to the server, or associated with the server through a service profile. **Note** CIMC Web Service can only be enabled or disabled globally. You cannot configure KVM direct access for individual CIMC IP addresses.
HTTP	By default, HTTP is enabled on port 80. You can run the Cisco UCS Manager GUI in an HTTP or HTTPS browser. If you select HTTP, all data is exchanged in clear text mode. For a secure browser session, we recommend that you enable HTTPS and disable HTTP. By default, Cisco UCS implements a browser redirects to an HTTPS equivalent and recommends that you do not change this behavior. **Note** If you are upgrading to Cisco UCS, version 1.4(1), the browser redirect to a secure browser does not occur by default. To redirect the HTTP browser to an HTTPS equivalent, enable the **Redirect HTTP to HTTPS** in Cisco UCS Manager.
HTTPS	By default, HTTPS is enabled on port. With HTTPS, all data is exchanged in encrypted mode through a secure server. For a secure browser session, We recommend that you only use HTTPS and either disable or redirect HTTP communications.
SMASH CLP	This service is enabled for read-only access and supports a limited subset of the protocols, such as the **show** command. You cannot disable it. This shell service is one of the standards that the Distributed Management Task Force defines.
SNMP	By default, this service is disabled. If enabled, the default port is 161. You must configure the community and at least one SNMP trap. Enable this service only if your system includes integration with an SNMP server.
SSH	This service is enabled on port 22. You cannot disable it, and you cannot change the default port. This service provides access to the Cisco UCS Manager CLI.
Telnet	By default, this service is disabled. This service provides access to the Cisco UCS Manager CLI.

Non-Secure Communication Services

Web Session Limits for User Accounts

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

Each Cisco UCS Manager domain supports a maximum of 32 concurrent web sessions per user and 256 total user sessions. By default, the number of concurrent web sessions allowed by Cisco UCS Manager is set to 32 per user, but this value can be configured up to the system maximum of 256.

Setting Web Session Limits

Procedure

Step 1 Navigate to **Admin** > **Communication Management** > **Communication Services**

Step 2 Under Web Session Limits, complete the following fields:

Name	Description
Maximum Sessions Per User	The maximum number of concurrent HTTP and HTTPS sessions allowed for each user. Enter an integer between 1 and 256.
Maximum Sessions	The maximum number of concurrent HTTP and HTTPS sessions allowed for all users within the system. Enter an integer between 1 and 256.
Maximum Event Interval (in seconds)	The maximum time interval between two events. This tracks various types of event change notifications, such as responses to any user requests from the UI. If the interval expires, the UI session is terminated. Enter and integer between 120-3600

Step 3 Click **Save Changes**.

Setting Shell Session Limits

Procedure

Step 1 Navigate to **Admin** > **Communication Management** > **Communication Services**

Step 2 Under Shell Session Limits, complete the following fields:

Name	Description
Maximum Sessions Per User	The maximum number of concurrent shell sessions allowed per user. Enter an integer between 1-32.
Maximum Sessions	The maximum number of concurrent shell sessions allowed for all users within the system. Enter an integer between 1-32.

Step 3 Click **Save Changes**.

Configuring CIM-XML

Procedure

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

Step 2 Expand **All** > **Communication Management** > **Communication Services**.

Step 3 In the **CIM-XML** area, click the **Enabled** radio button.

The **CIM-XML** area expands to display the default **Port** number, 5988. You cannot change this port number.

Step 4 Click **Save Changes**.

Configuring HTTP

Procedure

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

Step 2 Expand **All** > **Communication Management** > **Communication Services**.

Step 3 In the **HTTP** area, click the **Enabled** radio button.

The **HTTP** area expands to display the available configuration options.

Step 4 (Optional) In the **Port** field, change the default port that Cisco UCS Manager GUI uses for HTTP.

The default port is 80.

Step 5 (Optional) In the **Redirect HTTP to HTTPS** field, click the **Enabled** radio button.

You must also configure and enable HTTPS to enable redirection of HTTP logins to the HTTPS login. Once enabled, you cannot disable the redirection until you have disabled HTTPS.

Note

If you redirect HTTP to HTTPS, you cannot use HTTP to access Cisco UCS Manager GUI. Redirection disables HTTP as it automatically redirects to HTTPS.

Step 6 Click **Save Changes**.

Secure Communication Services

Certificates, Key Rings, and Trusted Points

HTTPS uses components of the Public Key Infrastructure (PKI) to establish secure communications between two devices, such as a client's browser and Cisco UCS Manager.

Encryption Keys and Key Rings

Each PKI device holds a pair of asymmetric Rivest-Shamir-Adleman (RSA) encryption keys, one kept private and one made public, stored in an internal key ring. A message encrypted with either key can be decrypted with the other key. To send an encrypted message, the sender encrypts the message with the receiver's public key, and the receiver decrypts the message using its own private key. A sender can also prove its ownership of a public key by encrypting (also called 'signing') a known message with its own private key. If a receiver can successfully decrypt the message using the public key in question, the sender's possession of the corresponding private key is proven. Encryption keys can vary in length, with typical lengths from 512 bits to 2048 bits. In general, a longer key is more secure than a shorter key. Cisco UCS Manager provides a default key ring with an initial 1024-bit key pair, and allows you to create additional key rings.

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

This operation is only available in the UCS Manager CLI.

Certificates

To prepare for secure communications, two devices first exchange their digital certificates. A certificate is a file containing a device's public key along with signed information about the device's identity. To merely support encrypted communications, a device can generate its own key pair and its own self-signed certificate. When a remote user connects to a device that presents a self-signed certificate, the user has no easy method to verify the identity of the device, and the user's browser will initially display an authentication warning. By default, Cisco UCS Manager contains a built-in self-signed certificate containing the public key from the default key ring.

You can change the self-signed KVM certificate on CIMC for Cisco UCS servers to a user-generated public certificate. However, a password protected X.509 certificate private key is not supported. provides detailed information about this process.

Important The certificate must be in Base64 encoded X.509 (CER) format.

Trusted Points

To provide stronger authentication for Cisco UCS Manager, you can obtain and install a third-party certificate from a trusted source, or trusted point, that affirms the identity of your device. The third-party certificate is signed by the issuing trusted point, which can be a root certificate authority (CA) or an intermediate CA or trust anchor that is part of a trust chain that leads to a root CA. To obtain a new certificate, you must generate a certificate request through Cisco UCS Manager and submit the request to a trusted point.

Related Topics

Changing the KVM Certificate, on page 84

Creating a Key Ring

Cisco UCS Manager supports a maximum of 8 key rings, including the default key ring.

Procedure

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

Step 2 Expand **All** > **Key Management**.

Step 3 Right-click **Key Management** and choose **Create Key Ring**.

Step 4 In the **Create Key Ring** dialog box, do the following:

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

b) In the **Modulus** field, select one of the following radio buttons to specify the SSL key length in bits:

- **Mod2048**
- **Mod2560**
- **Mod3072**
- **Mod3584**
- **Mod4096**

c) Click **OK**.

What to do next

Create a certificate request for this key ring.

Creating a Certificate Request for a Key Ring

Procedure

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

Step 2 Expand **All** > **Key Management**.

Step 3 Click the key ring for which you want to create a certificate request.

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

Step 5 In the **General** tab, click **Create Certificate Request**.

Step 6 In the **Create Certificate Request** dialog box, complete the following fields:

Name	Description
DNS field	The domain name assigned to the network that is common to all host names.
Locality field	The city or town in which the company requesting the certificate is headquartered. Enter up to 64 characters. You can use any letters, numbers, or spaces, as well as the following special characters: , (comma), . (period), @ (at sign), ^ (carat), ((open parenthesis),) (close parenthesis), - (dash), _ (underscore), + (plus sign), : (colon), / (forward slash).
State field	The state or province in which the company requesting the certificate is headquartered. Enter up to 64 characters. You can use any letters, numbers, or spaces, as well as the following special characters: , (comma), . (period), @ (at sign), ^ (carat), ((open parenthesis),) (close parenthesis), - (dash), _ (underscore), + (plus sign), : (colon), / (forward slash).
Country field	The country code corresponding to the country in which the company resides. Enter two alphabetic characters.
Organization Name field	The organization requesting the certificate. Enter up to 64 characters. You can use any letters, numbers, or spaces, as well as the following special characters: , (comma), . (period), @ (at sign), ^ (carat), ((open parenthesis),) (close parenthesis), - (dash), _ (underscore), + (plus sign), : (colon), / (forward slash).
Organization Unit Name field	The organizational unit. Enter up to 64 characters. You can use any letters, numbers, or spaces, as well as the following special characters: , (comma), . (period), @ (at sign), ^ (carat), ((open parenthesis),) (close parenthesis), - (dash), _ (underscore), + (plus sign), : (colon), / (forward slash).
Email field	The email address associated with the request.
Password field	An optional password for this request.
Confirm Password field	If you specified a password, enter it again for confirmation.
Subject field	The fully qualified domain name of the fabric interconnect.

Step 7 To assign IP addresses, click the **IPv4** or **IPv6** tab. The choice you make depends upon how the fabric interconnects were configured when you set up Cisco UCS Manager.

- Click the IPv4 tab, and complete the following fields:

Name	Description
IP Address field	The IPv4 address of the Cisco UCS domain.
FI-A IP field	The IPv4 address of fabric interconnect A.
FI-B IP field	The IPv4 address of fabric interconnect B.

- Click the IPv6 tab, and complete the following fields:

Name	Description
IP Address field	The IPv6 address of the Cisco UCS domain.
FI-A IP field	The IPv6 address of fabric interconnect A.
FI-B IP field	The IPv6 address of fabric interconnect B.

Step 8 Click **OK**.

Step 9 Copy the text of the certificate request from the **Request** field and save in a file.

Step 10 Send the file with the certificate request to the trust anchor or certificate authority.

What to do next

Create a trusted point and set the certificate chain for the certificate of trust received from the trust anchor.

Changing the KVM Certificate

You can use this procedure to change the KVM certificate to a user-generated public certificate.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number*** > **Servers**.

Step 3 Click the server for which you want to change the KVM certificate.

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

Step 5 Click the **CIMC** subtab.

Step 6 In the **Actions** area, click **Change KVM Certificate**:

Step 7 In the **Change KVM Certificate** dialog box, complete the following fields:

Field	Description
Certificate field	A user-generated public certificate.

Field	Description
Key field	The corresponding user-generated private key. **Note** Password protected X.509 certificate private key is not supported.

Step 8 Click **OK**.

Step 9 If a confirmation dialog box appears, click **Yes**.

This operation will result in a reboot of the CIMC

Clearing the KVM Certificate

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number*** > **Servers**.

Step 3 Click the server for which you want to clear the KVM certificate.

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

Step 5 Click the **CIMC** subtab.

Step 6 In the **Actions** area, click **Clear KVM Certificate**:

Step 7 In the **Clear KVM Certificate** dialog box, click **Yes**.

This operation will result in a reboot of the CIMC

Creating a Trusted Point

Procedure

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

Step 2 Expand **All** > **Key Management**.

Step 3 Right-click **Key Management** and choose **Create Trusted Point**.

Step 4 In the **Create Trusted Point** dialog box, complete the following fields:

Name	Description
Name field	The name of the trusted point. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.
Certificate Chain field	The certificate information for this trusted point. **Important** The certificate must be in Base64 encoded X.509 (CER) format. For windows 2012 server, using RSASSA-PSS returns the following error occurs: Trustpoint's cert-chain is invalid, reason: unknown. UCS Manager does not support this algorithm.

Step 5 Click **OK**.

What to do next

When you receive the certificate from the trust anchor or certificate authority, import it in to the key ring.

Importing a Certificate into a Key Ring

Procedure

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

Step 2 Expand **All** > **Key Management**.

Step 3 Click the key ring into which you want to import the certificate.

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

Step 5 In the **Certificate** area, complete the following fields:

a) From the **Trusted Point** drop-down list, select the trusted point for the trust anchor that granted this certificate.

b) In the **Certificate** field, paste the text from the certificate you received from the trust anchor or certificate authority.

Important
The certificate must be in Base64 encoded X.509 (CER) format.

Tip
If the fields in an area do not display, click the **Expand** icon to the right of the heading.

Step 6 Click **Save Changes**.

What to do next

Configure your HTTPS service with the key ring.

Configuring HTTPS

Caution After you complete the HTTPS configuration, including changing the port and key ring for the HTTPS to use, all current HTTP and HTTPS sessions are closed without warning as soon as you save or commit the transaction.

Procedure

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

Step 2 Expand **All** > **Communication Management** > **Communication Services**.

Step 3 In the **HTTPS** area, click the **Enabled** radio button.

The **HTTPS** area expands to display the available configuration options.

Step 4 Complete the following fields:

Name	Description
Admin State field	This can be one of the following: • **Enabled** • **Disabled** If **Admin State** is enabled, Cisco UCS Manager GUI displays the remaining fields in this section.
Port field	The port to use for HTTPS connections. Specify an integer between 1 and 65535. By default, HTTPS is enabled on port.
Operational Port field	The port Cisco UCS Manager requires for system-level HTTPS communication. You cannot change this port.
Key Ring drop-down list	The key ring for HTTPS connections.

Name	Description
Cipher Suite Mode field	The level of Cipher Suite security used by the Cisco UCS domain. This can be one of the following: • **High Strength** • **Medium Strength** • **Low Strength** • **Custom**—Allows you to specify a user-defined Cipher Suite specification string.
Cipher Suite field	If you select **Custom** in the **Cipher Suite Mode** field, specify the user-defined Cipher Suite specification string in this field. The Cipher Suite specification string can contain up to 256 characters and must conform to the OpenSSL Cipher Suite specifications. You cannot use any spaces or special characters except ! (exclamation point), + (plus sign), - (hyphen), and : (colon). For details, see http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite. For example, the medium strength specification string Cisco UCS Manager uses as the default is: `ALL:!ADH:!EXPORT56:!LOW:RC4+RSA:+HIGH:+MEDIUM:+EXP:+eNULL`
Allowed SSL Protocols	Enables you to choose which SSL protocols can be used. This can be one of the following: • **Default (Allow all except SSLv2 and SSLv3)** • **Only TLSv1.2** **Note** If you choose Only TLSv1.2, all web client connections trying to use less secure versions of TLS are blocked.

Step 5 Click **Save Changes**.

Deleting a Key Ring

Procedure

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

Step 2 Expand **All** > **Key Management**.

Step 3 Right-click the key ring you want to delete and choose **Delete**.

Step 4 If a confirmation dialog box displays, click **Yes**.

Deleting a Trusted Point

Before you begin

Ensure that the trusted point is not used by a key ring.

Procedure

Step 1 In the **Navigation** pane, click **Admin**.
Step 2 Expand **All** > **Key Management**.
Step 3 Right-click the trusted point you want to delete and choose **Delete**.
Step 4 If a confirmation dialog box displays, click **Yes**.
Step 5 Click **OK**.

Network-Related Communication Services

Enabling SNMP and Configuring SNMP Properties

SNMP messages from a Cisco UCS domain display the fabric interconnect name rather than the system name.

Procedure

Step 1 In the **Navigation** pane, click **Admin**.
Step 2 Expand **All** > **Communication Management** > **Communication Services**.
Step 3 Select the **Communication Services** tab.
Step 4 In the **SNMP** area, complete the following fields:

Name	Description
Admin State field	This can be one of the following: • **Enabled** • **Disabled** Enable this service only if your system includes integration with an SNMP server. If **Admin State** is enabled, Cisco UCS Manager GUI displays the remaining fields in this section.

Step 5 Click **Save Changes**.

What to do next

Create SNMP traps and users.

Enabling the CIMC Web Service

The CIMC web service is enabled by default. Follow the steps below to enable the service if it is disabled.

Procedure

Step 1 In the **Navigation** pane, click **Admin**.
Step 2 Expand **All** > **Communication Management** > **Communication Services**.
Step 3 Select the **Communication Services** tab.
Step 4 In the **CIMC Web Service** area, click the **Enabled** radio button.
Step 5 Click **Save Changes**.

Disabling Communication Services

Note We recommend that you disable all communication services that are not required to interface with other network applications.

Procedure

Step 1 In the **Navigation** pane, click **Admin**.
Step 2 Expand **All** > **Communication Management** > **Communication Services**.

Step 3 On the **Communication Services** tab, click the **disable** radio button for each service that you want to disable.

Step 4 Click **Save Changes**.

Enabling Telnet

Procedure

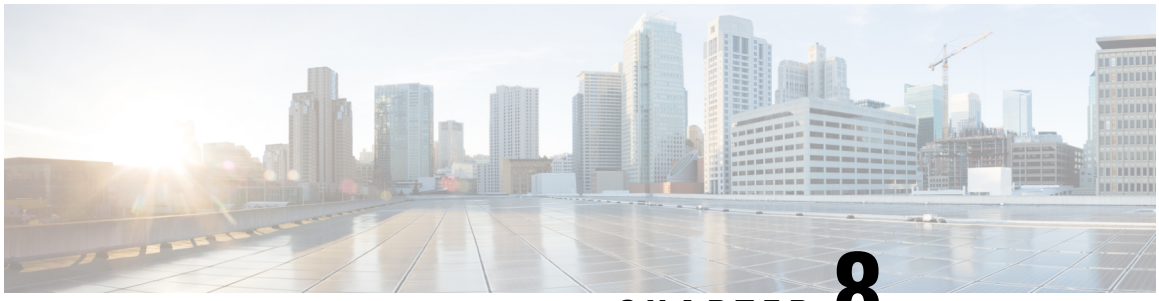
Step 1 In the **Navigation** pane, click **Admin**.

Step 2 Expand **All** > **Communication Management** > **Communication Services**.

Step 3 Click the **Communication Services** tab.

Step 4 In the **Telnet** area, click the **Enabled** radio button.

Step 5 Click **Save Changes**.



CHAPTER 8

CIMC Sessions Management

• CIMC Session Management, on page 93

CIMC Session Management

You can view and close any KVM, vMedia, and SOL sessions in Cisco UCS Manager. If you have administrator privileges, you can discontinue the KVM, vMedia, and SoL sessions of any user. . Cisco Integrated Management Controller (CIMC) provides session information to Cisco UCS Manager. When Cisco UCS Manager gets an event from CIMC, it updates its session table and displays the information to all users.

The session information consists of the following information:

- Name—The name of the user who launched the session.
- Session ID—The ID associated with the session. The format of the session ID for blades is [unique identifier] _ [chassis id] _ [Blade id]. The format of the session ID for racks is [unique identifier] _ 0 _ [Rack id].
- Type of session—KVM, vMedia, or SoL.
- Privilege level of the user—Read-Write, Read Only, or Granted.
- Administrative state—Active or Inactive. The value is active if the session is active. The value is inactive if the session terminate command has been issued but the session has not been terminated. This situation occurs when FSM of the server is in progress with another operation or when the connectivity to CIMC is lost.
- Source Address—The IP address of the computer from which the session was opened.
- Service Profile—The service profile associated with the session. The service profile attribute value for a CIMC session is displayed only if the session is opened on an IP address that is provided from the service profile.
- Server—The name of the server associated with the session.
- Login time—The date and time the session started.
- Last Update Time—The last time the session information was updated by CIMC.

A new session is generally added when a user connects to KVM, vMedia, or SOL. A Pnuos vMedia session will be displayed in the session table during the server discovery with the user name __vmediausr__.

The CIMC session data is available under the **CIMC Sessions** tab in Cisco UCS Manager GUI. Any CIMC session terminated by the user is audit logged with proper details.

Note To perform the GUI and CLI tasks that are described in this guide, a CIMC image version of 2.1(2a) or above is required for the session management support for the blade servers. The latest CIMC image version of 1.5(1l) and above is required for the rack-servers.

Viewing All Open CIMC Sessions

This task describes one way to view all CIMC sessions opened globally on Cisco UCS Manager. You can view CIMC sessions of all servers opened by local, remote, or IPMI users in a single page.

Procedure

Step 1 In the **Navigation** pane, click **Admin** > **User Management** > **User Services**.

Step 2 In the **Work** pane, click the **CIMC Sessions** tab.

Viewing the CIMC Sessions of a Server

This task describes how to view the CIMC sessions of a specific server. You can view the CIMC sessions opened on the server and the service profile.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Chassis** > **Chassis Number** > **Servers** > ***Server Number***.

Step 3 In the **Work** pane, click the **CIMC Sessions** tab.

Viewing the CIMC Sessions of a Service Profile

This task describes how to view the CIMC sessions of a specific service profile.

Note A CIMC session will only be displayed under a service profile if the session was opened on an IP address provided from that service profile.

Procedure

Step 1 In the **Navigation** pane, click **Servers**.
Step 2 Expand **Servers** > **Service Profiles** > **Root** > ***Service Profile Name***.
Step 3 In the **Work** pane, click the **CIMC Sessions** tab.

Viewing the CIMC Sessions Opened by a Local User

This task describes how to view CIMC sessions opened by a local user.

Procedure

Step 1 In the **Navigation** pane, click **Admin** > **User Management** > **User Services** > **Locally Authenticated Users** > ***User Name***
Step 2 In the **Work** pane, click the **CIMC Sessions** tab.

Viewing the CIMC Sessions Opened by a Remote User

This task describes how to view CIMC sessions opened by a remote user.

Procedure

Step 1 In the **Navigation** pane, click **Admin**.
Step 2 Under **Admin**, expand **User Management** > **User Services** > **Remotely Authenticated Users** > ***User Name***.
Step 3 In the **Work** pane, click the **CIMC Sessions** tab.

Clearing All Open CIMC Sessions

This task describes how to clear all open CIMC sessions. You can clear the CIMC sessions of all servers and service-profiles opened by the local, remote, or IPMI users.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, click **User Management**.

Step 3 In the **Work** pane, click the **CIMC Sessions** tab.

Step 4 Select the CIMC sessions you want to clear, right-click, and select **Clear CIMC Session**.

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

Clearing the CIMC Sessions of a Server

This task describes how to clear the CIMC session of a server. You can clear one or more CIMC sessions that are opened on a server.

Procedure

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

Step 2 On the **Equipment** tab, expand **Servers** > ***Server Name***.

Step 3 In the **Work** pane, click the **CIMC Sessions** tab.

Step 4 Select the CIMC sessions that you want to clear, right-click, and select **Clear CIMC Session**.

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

Clearing the CIMC Sessions of a Service Profile

This task describes how to clear the CIMC sessions of a service profile. You can clear one or more CIMC sessions opened with an IP address provided on the service-profile.

Procedure

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

Step 2 On the **Servers** tab, expand **Servers** > **Service Profiles** > **root** > ***Service Profile Name***.

Step 3 In the **Work** pane, click the **CIMC Sessions** tab.

Step 4 Select the CIMC sessions that you want to clear, right-click, and select **Clear CIMC Session**.

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

Clearing the CIMC Sessions of a Local User

This task describes how to clear the CIMC sessions of a local user. You can clear one or more CIMC sessions opened by a local user.

Procedure

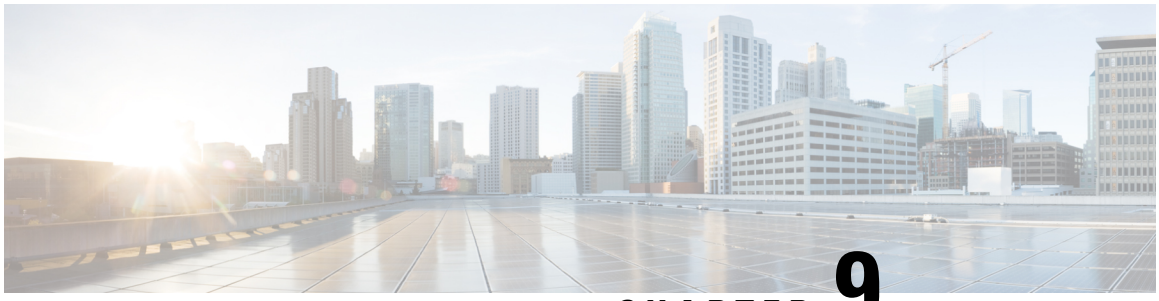
Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, expand **User Services** > **Locally Authenticated Users** > ***User Name***.
Step 3 In the **Work** pane, click the **General** tab.
Step 4 Under the **General** tab, expand the **CIMC Sessions** section.
Step 5 Select the CIMC sessions you want to clear, right-click, and select **Clear CIMC Session**.
Step 6 If the Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Clearing the CIMC Sessions of a Remote User

This task describes how to clear the CIMC sessions of a remote user. You can clear one or more CIMC sessions opened by a remote user.

Procedure

Step 1 In the **Navigation** pane, click **Admin**.
Step 2 Expand **User Management** > **User Services** > **Remotely Authenticated Users** > ***User Name***.
Step 3 In the **Work** pane, click the **General** tab.
Step 4 Under the **General** tab, expand the **CIMC Sessions** section.
Step 5 Select the CIMC sessions that you want to clear, right-click, and select **Clear CIMC Session**.
Step 6 If the Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.



CHAPTER 9

Setting the Management IP Address

- Management IP Address, on page 99
- Configuring the Management IP Address on a Server, on page 100
- Setting the Management IP Address on a Service Profile Template, on page 104
- Setting the Management IP Address on a Service Profile Template, on page 104
- Management IP Pools, on page 105
- Creating an IPv6 Address Block in the Management IP Pool, on page 105
- Deleting an IP Address Block from the Management IP Pool, on page 106
- Creating an IPv4 Address Block in the Management IP Pool, on page 106

Management IP Address

Each server in a Cisco UCS domain must have a one or more management IP addresses assigned to its Cisco Integrated Management Controller (CIMC) or to the service profile associated with the server. Cisco UCS Manager uses these IP addresses for external access that terminates in the CIMC. This external access can be through one of the following services:

- KVM console
- Serial over LAN
- An IPMI tool

The management IP addresses used to access the CIMC on a server can be out-of-band (OOB) addresses, through which traffic traverses the fabric interconnect via the management port, or inband addresses, through which traffic traverses the fabric interconnect via the fabric uplink port. Up to six IP addresses can be configured to access the CIMC on a server, two out-of-band (OOB) and four inband.

You can configure the following management IP addresses:

- A static OOB IPv4 address assigned directly to the server
- An OOB IPv4 address assigned to the server from a global ext-mgmt pool
- An inband IPv4 address derived from a service profile associated with the server
- An inband IPv4 address drawn from a management IP pool and assigned to a service profile or service profile template
- An static inband IPv6 address assigned directly to the server

- An inband IPv6 address derived from a service profile associated with the server

You can assign multiple management IP addresses to each CIMC on the server and to the service profile associated with the server. If you do so, you must use different IP addresses for each of them.

A management IP address that is assigned to a service profile moves with that service profile. If KVM or SoL sessions are active when you migrate the service profile to another server, Cisco UCS Manager terminates the sessions and does not restart them after the migration is completed. You configure the IP address when you create or modify a service profile.

Note You cannot assign a static IP address to a server or service profile if that IP address has already been assigned to a server or service profile in the Cisco UCS domain. If you attempt to do so, Cisco UCS Manager warns you that the IP address is already in use and rejects the configuration.

A unicast Internet Control Message Protocol (ICMP) request will be sent to the gateway IP address every second from each server that is configured with an inband IP address. This request is to check if connectivity for the inband traffic through the current Fabric Interconnect (FI) is up, and to initiate a failover to the other FI if it is down. The path selected for inband and the failover operations are completely independent of the server data traffic. The default polling interval is 1 second and the polling interval is configurable to a maximum of 5 seconds. After three failed polls, the CIMC will failover to the other FI. During failover, the CIMC will issue a Gratuitous Address Resolution Protocol (GARP) on the newly selected uplinks to notify the network that the MAC has been moved to a new location.

Configuring the Management IP Address on a Server

Configuring a Server to Use a Static IP Address

If this action is greyed out, the server has already been assigned a static IP address.

You can configure a total of three static management addresses per server:

- Outband IPv4
- Inband IPv4
- Inband IPv6

Note You are not required to configure all three.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Chassis** > **Chassis** *Number* > **Cartridges** > **Cartridge** *Number* > **Servers**

Step 3 Click the server for which you want to configure IP addresses.

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

Step 5 Click the **CIMC** subtab.

In the **Actions** area, two choices are available for management IP addresses:

- **Modify Outband Static Management IP**
- **Change Inband Management IP**

Step 6 To modify the outband static management IP address, in the **Actions** area, click **Modify Outband Static Management IP**:

Step 7 In the **Modify Outband Static Management IP** dialog box, complete the following fields:

Field	Description
IP Address	The static IPv4 address to be assigned to the server.
Subnet Mask	The subnet mask for the IP address.
Default Gateway	The default gateway that the IP address should use.

Step 8 Click **OK**.

Step 9 To modify the inband management IP address, click **Change Inband Management IP**.

In the **Change Management IP Address** dialog box, there are two tabs:

- **Inband IPv4**
- **Inband IPv6**

a) To change the static inband IPv4 management address, click the **Inband IPv4** subtab.

b) In the **Change Management IP Address** dialog box, complete the following fields:

Field	Description
Management IP Address Policy drop-down	Click **Static**.
IP Address	The static IPv4 address to be assigned to the server.
Subnet Mask	The subnet mask for the IP address.
Default Gateway	The default gateway that the IP address should use.

c) Click **OK**.

d) To change the static inband management IPv6 address, click the **Inband IPv6** subtab.

e) In the **Change Management IP Address** dialog box, complete the following fields:

Field	Description
Management IP Address Policy drop-down	Click **Static**.
IP Address	The static IPv6 address to be assigned to the server.
Prefix	The network prefix for the IP address.
Default Gateway	The default gateway that the IP address should use.

Step 10 Click **OK**.

Step 11 If a confirmation dialog box displays, click **Yes**.

Configuring a Server to Use a Management IP Pool

If any action is specified in this procedure is greyed out, it means that the configuration has already been completed. You can configure a total of three management IP pools per server:

- Outband IPv4
- Inband IPv4
- Inband IPv6

Note You are not required to configure all three.

Before you begin

Configure management IP pools before configuring servers to use management IP pools.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Chassis** > **Chassis** *Number* > **Cartridges** > **Cartridge** *Number* > **Servers**

Step 3 Click the server that you want to configure to use the management IP pool.

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

Step 5 Click the **CIMC** subtab.

- To configure an outband IP pooled management IP address policy, proceed with Step 6.
- To configure inband IPv4 and/or IPv6 management IP address policies, proceed to Step 8.

Step 6 In the **Actions** area, click **Use Outband Pooled Management IP**.

Step 7 Click **Yes** in the **Use Outband Pooled Management IP** confirmation dialog box, then click **OK**.
The management IP address policy is now switched to using an OOB IP address from the outband management IP pool.

Step 8 In the **Actions** area, click **Change Inband Management IP**.

Step 9 In the **Change Management IP Dialog** box, there are two tabs:

- **Inband IPv4**
- **Inband IPv6**

a) To change the inband IPv4 management IP pool, click the **Inband IPv4** tab, and complete the following fields:

Field	Description
Network drop-down list	A VLAN selected from the associated VLAN group.
Management IP Address Policy drop-down list	The management IP pool you want to assign to the server. There are two types of pools available: • **Domain Pools** • **Global Pools** Select one of the pools available from either the **Domain Pools** entries or the **Global Pools** entries.

b) To change the inband IPv6 management IP pool, click the **Inband IPv6** tab, and complete the following fields:

Field	Description
Network drop-down list	A VLAN selected from the associated VLAN group.
Management IP Address Policy drop-down list	The management IP pool you want to assign to the server. There are two types of pools available: • **Domain Pools** • **Global Pools** Select one of the pools available from either the **Domain Pools** entries or the **Global Pools** entries.

Step 10 Click **OK**.

Step 11 If a confirmation dialog box displays, click **Yes**.

Deleting the Inband Configuration from a Server

This procedure removes the inband management IP address configuration from a server. If this action is greyed out, no inband configuration was completed.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Chassis** > **Chassis** *Number* > **Cartridges** > **Cartridge** *Number* > **Servers**

Step 3 Choose the server for which you want to delete the inband management IP configuration.

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

Step 5 Click the **CIMC** subtab.

Step 6 In the **Actions** area, click **Delete Inband Configuration**.

Step 7 Click **Yes** in the **Delete** confirmation dialog box.

The inband configuration for the server is deleted.

Note
If an inband service profile is configured in Cisco UCS Manager with a default VLAN and pool name, the server CIMC will automatically get an inband configuration from the inband profile approximate one minute after deleting the inband configuration here.

Setting the Management IP Address on a Service Profile Template

Procedure

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 Expand **Servers** > **Service Profile Templates**.

Step 3 Expand the node for the organization that contains the service profile template for which you want to set the management IP address.

If the system does not include multi tenancy, expand the **root** node.

Step 4 Click the service profile template for which you want to set the management IP address.

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

Step 6 Expand the **Management IP Address** area.

Step 7 In the **Actions** area, click **Change Management IP Address**.

Step 8 Complete the fields in the **Change Management IP Address** dialog box.

Step 9 Click **Save Changes**.

Setting the Management IP Address on a Service Profile Template

Procedure

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 Expand **Servers** > **Service Profile Templates**.

Step 3 Expand the node for the organization that contains the service profile template for which you want to set the management IP address.

If the system does not include multi tenancy, expand the **root** node.

Step 4 Click the service profile template for which you want to set the management IP address.

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

Step 6 Expand the **Management IP Address** area.

Step 7 In the **Actions** area, click **Change Management IP Address**.

Step 8 Complete the fields in the **Change Management IP Address** dialog box.

Step 9 Click **Save Changes**.

Management IP Pools

The default management IP pool, **IP Pool ext-mgmt** is a collection of external IPv4 and IPv6 addresses. Cisco UCS Manager reserves each block of IP addresses in the management IP pool for external access that terminates in the CIMC on a server.

By default, the **IP Pool ext-mgmt** is used to configure the CIMC outbound management IP address. You cannot change this IP pool if already a static IP address is assigned to the server from this pool. If you want to configure the outbound management IP address for CIMC from a static IP address, then you can delete the IP addresses from the default management IP pool.

You can configure separate out-of-band IPv4 address pools, and in-band IPv4 or IPv6 address pools. You can configure in-band pools that contain both IPv4 and IPv6 address blocks.

Tip To avoid assigning an IP pool that contains only IPv4 addresses as the in-band IPv6 policy, or assigning an IP pool that contains only IPv6 addresses as the in-band IPv4 policy to a server CIMC, it is suggested that you configure separate in-band address pools, each with only IPv4 or IPv6 addresses.

You can configure service profiles and service profile templates to use IP addresses from the management IP pools. You cannot configure servers to use the management IP pool.

All IP addresses in the management IP pool must be in the same IPv4 subnet, or have the same IPv6 network prefix as the IP address of the fabric interconnect.

Note The management IP pool must not contain any IP addresses that were assigned as static IP addresses for a server or service profile.

Creating an IPv6 Address Block in the Management IP Pool

The management IP pool must not contain any IP addresses that were assigned as static IP addresses for a server or service profile.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.
Step 2 In the **LAN** tab, expand **LAN** > **Pools** > *Organization_Name* .
Step 3 Expand the **IP Pools** node.
Step 4 Right-click **IP Pool ext-mgmt** and select **Create Block of IP Addresses**.
Step 5 In the **Create a Block of IPv6 Addresses** dialog box, specify the required information.
Step 6 Click **OK**.

What to do next

Configure one or more service profiles or service profile templates to obtain the CIMC IP address from the management IP pool.

Deleting an IP Address Block from the Management IP Pool

Procedure

Step 1 In the **Navigation** pane, click **LAN**.
Step 2 In the **LAN** tab, expand **LAN** > **Pools** > *Organization_Name* .
Step 3 Expand the **IP Pools** node.
Step 4 Select **IP Pool ext-mgmt**.
Step 5 Right-click the IP address block that you want to delete and select **Delete**.
Step 6 If a confirmation dialog box displays, click **Yes**.

Creating an IPv4 Address Block in the Management IP Pool

The management IP pool must not contain any IP addresses that were assigned as static IP addresses for a server or service profile.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.
Step 2 In the **LAN** tab, expand **LAN** > **Pools** > *Organization_Name* .
Step 3 Expand the **IP Pools** node.
Step 4 Right-click **IP Pool ext-mgmt** and select **Create Block of IP Addresses**.

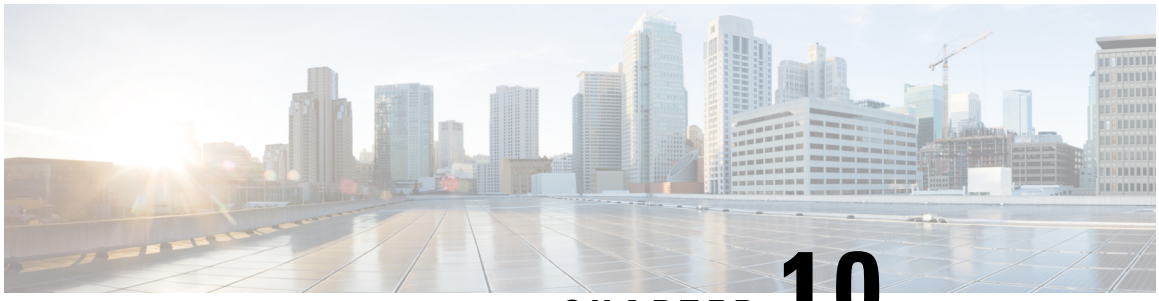
Step 5 In the **Create a Block of IPv4 Addresses** dialog box, complete the following fields:

Name	Description
Name column	The range of IPv4 addresses assigned to the block.
From column	The first IPv4 address in the block.
To column	The last IPv4 address in the block.
Subnet column	The subnet mask associated with the IPv4 addresses in the block.
Default Gateway column	The default gateway associated with the IPv4 addresses in the block.
Primary DNS column	The primary DNS server that this block of IPv4 addresses should access.
Secondary DNS column	The secondary DNS server that this block of IPv4 addresses should access.

Step 6 Click **OK**.

What to do next

Configure one or more service profiles or service profile templates to obtain the CIMC IP address from the management IP pool.



CHAPTER 10

Organizations in UCS Manager

- Organizations in a Multitenancy Environment, on page 109
- Hierarchical Name Resolution in a Multi-Tenancy Environment, on page 110
- Creating an Organization under the Root Organization, on page 112
- Creating an Organization under a Sub-Organization, on page 112
- Deleting an Organization, on page 113

Organizations in a Multitenancy Environment

Multi-tenancy allows you to divide the large physical infrastructure of an Cisco UCS domain into logical entities known as organizations. As a result, you can achieve a logical isolation between organizations without providing a dedicated physical infrastructure for each organization.

You can assign unique resources to each tenant through the related organization in the multi-tenant environment. These resources can include different policies, pools, and quality of service definitions. You can also implement locales to assign or restrict user privileges and roles by organization, if you do not want all users to have access to all organizations.

If you set up a multi-tenant environment, all organizations are hierarchical. The top-level organization is always root. The policies and pools that you create in root are system-wide and are available to all organizations in the system. However, any policies and pools created in other organizations are only available to organizations that are above it in the same hierarchy. For example, if a system has organizations named Finance and HR that are not in the same hierarchy, Finance cannot use any policies in the HR organization, and HR cannot access any policies in the Finance organization. However, both Finance and HR can use policies and pools in the root organization.

If you create organizations in a multi-tenant environment, you can also set up one or more of the following for each organization or for a sub-organization in the same hierarchy:

- Resource pools
- Policies
- Service profiles
- Service profile templates

The root organization is always the top level organization.

Hierarchical Name Resolution in a Multi-Tenancy Environment

In a multi-tenant environment, Cisco UCS uses the hierarchy of an organization to resolve the names of policies and resource pools. When Cisco UCS Manager searches for details of a policy or a resource assigned to a pool, the following occurs:

1. Cisco UCS Manager checks for policies and pools with the specified name within the organization assigned to the service profile or policy.
2. If a policy is found or an available resource is inside a pool, Cisco UCS Manager uses that policy or resource. If the pool does not have any available resources at the local level, Cisco UCS Manager moves up in the hierarchy to the parent organization and searches for a pool with the same name. Cisco UCS Manager repeats this step until the search reaches the root organization.
3. If the search reaches the root organization and has not found an available resource or policy, Cisco UCS Manager returns to the local organization and begins to search for a default policy or available resource in the default pool.
4. If an applicable default policy or available resource in a default pool is found, Cisco UCS Manager uses that policy or resource. If the pool does not have any available resources, Cisco UCS Manager moves up in the hierarchy to the parent organization and searches for a default pool. Cisco UCS Manager repeats this step until the search reaches the root organization.
5. If Cisco UCS Manager cannot find an applicable policy or available resource in the hierarchy, it returns an allocation error.

Example: Server Pool Name Resolution in a Single-Level Hierarchy

In this example, all organizations are at the same level below the root organization. For example, a service provider creates separate organizations for each customer. In this configuration, organizations only have access to the policies and resource pools assigned to that organization and to the root organization.

In this example, a service profile in the XYZcustomer organization is configured to use servers from the XYZcustomer server pool. When resource pools and policies are assigned to the service profile, the following occurs:

1. Cisco UCS Manager checks for an available server in the XYZcustomer server pool.
2. If the XYZcustomer server pool has an available server, Cisco UCS Manager associates that server with the service profile and discontinues the search. If the pool does not have an available server, Cisco UCS Manager checks the root organization for a server pool with the same name.
3. If the root organization includes an XYZcustomer server pool and that pool has an available server, Cisco UCS Manager associates that server with the service profile and discontinues the search. If the pool does not have an available server, Cisco UCS Manager returns to the XYZcustomer organization to check the default server pool.
4. If the default pool in the XYZcustomer organization has an available server, Cisco UCS Manager associates that server with the service profile and discontinues the search. If the default pool does not have an available server, Cisco UCS Manager checks the default server pool in the root organization.

5. If the default server pool in the root organization has an available server, Cisco UCS Manager associates that server with the service profile and discontinues the search. If the default pool does not have an available server, Cisco UCS Manager returns an allocation error.

Example: Server Pool Name Resolution in a Multi-Level Hierarchy

In this example, each organization includes at least one suborganization. For example, a company could create organizations for each major division in the company and for subdivisions of those divisions. In this configuration, each organization has access to its local policies and resource pools and to the resource pools in the parent hierarchy.

In this example, the Finance organization includes two sub-organizations, AccountsPayable and AccountsReceivable. A service profile in the AccountsPayable organization is configured to use servers from the AP server pool. When resource pools and policies are assigned to the service profile, the following occurs:

1. Cisco UCS Manager checks for an available server in the AP server pool defined in the service profile.
2. If the AP server pool has an available server, Cisco UCS Manager associates that server with the service profile and discontinues the search. If the pool does not have an available server, Cisco UCS Manager moves one level up the hierarchy and checks the Finance organization for a pool with the same name.
3. If the Finance organization includes a pool with the same name and that pool has an available server, Cisco UCS Manager associates that server with the service profile and discontinues the search. If the pool does not have an available server, Cisco UCS Manager moves one level up in the hierarchy and checks the root organization for a pool with the same name.
4. If the root organization includes a pool with the same name and that pool has an available server, Cisco UCS Manager associates that server with the service profile and discontinues the search. If the pool does not have an available server, Cisco UCS Manager returns to the AccountsPayable organization to check the default server pool.
5. If the default pool in the AccountsPayable organization has an available server, Cisco UCS Manager associates that server with the service profile and discontinues the search. If the default pool does not have an available server, Cisco UCS Manager moves one level up in the hierarchy and checks the default server pool in the Finance organization.
6. If the default pool in the Finance organization has an available server, Cisco UCS Manager associates that server with the service profile and discontinues the search. If the default pool does not have an available server, Cisco UCS Manager moves one level up in the hierarchy and checks the default server pool in the root organization.
7. If the default server pool in the root organization has an available server, Cisco UCS Manager associates that server with the service profile and discontinues the search. If the default pool does not have an available server, Cisco UCS Manager returns an allocation error.

Creating an Organization under the Root Organization

Procedure

Step 1 On the toolbar, choose **New** > **Create Organization**.

Step 2 In the **Name** field of the **Create Organization** dialog box, enter a unique name for the organization.

This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.

Step 3 In the **Description** field, enter a description for the organization.

Step 4 Click **OK**.

Creating an Organization under a Sub-Organization

Procedure

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 Expand **Service Profiles** > **root**.

You can also access the **Sub-Organizations** node under the **Policies** or **Pools** nodes.

Step 3 Expand the **Sub-Organizations** node and do one of the following:

- To create an organization directly under root, right-click **Sub-Organizations** and choose **Create Organization**.
- To create an organization under a lower-level sub-organization, expand the sub-organization nodes in the hierarchy and then right-click the sub-organization under which you want to create the new organization and choose **Create Organization**.

Step 4 In the **Name** field of the **Create Organization** dialog box, enter a unique name for the organization.

This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.

Step 5 In the **Description** field, enter a description for the organization.

Step 6 Click **OK**.

Deleting an Organization

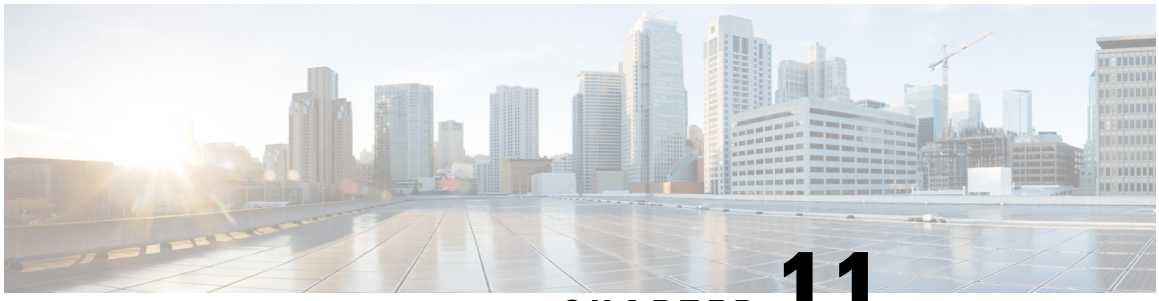
Procedure

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 Navigate to the organization that you want to delete.

Step 3 Right-click the organization and choose **Delete**.

Step 4 If a confirmation dialog box displays, click **Yes**.



CHAPTER 11

Backup and Restore

- Backup Operations in UCS, on page 115
- Considerations and Recommendations for Backup Operations, on page 115
- Required User Role for Backup and Import Operations, on page 116
- Creating a Backup Operation, on page 116
- Running a Backup Operation, on page 121
- Modifying a Backup Operation, on page 122
- Deleting One or More Backup Operations, on page 122
- Backup Types, on page 123
- System Restore, on page 132

Backup Operations in UCS

When you perform a backup through Cisco UCS Manager, you take a snapshot of all or part of the system configuration and export the file to a location on your network. You cannot use Cisco UCS Manager to back up data on the servers.

You can perform a backup while the system is up and running. The backup operation only saves information from the management plane. It does not have any impact on the server or network traffic.

Considerations and Recommendations for Backup Operations

Before you create a backup operation, consider the following:

Backup Locations

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

Potential to Overwrite Backup Files

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

Multiple Types of Backups

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

Scheduled Backups

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

Incremental Backups

You cannot perform incremental backups.

Encryption of Full State Backups

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

Backups from Cisco UCS Manager

Port configurations that include global VLANs and VSANs are not restored when you do an all-config backup in Cisco UCS Manager. Reconfigure the ports from Cisco UCS Central.

FSM Tasks for Backup Policy and Configuration Export Policy

When configuring both **Backup Policy** and **Config Export Policy** on the **Policy Backup & Export** tab and using the same hostname for both policies, Cisco UCS Manager will create only one **Backup Operation** in the **Backup Configuration** page to run both tasks. Each policy run will not have a separate FSM task.

To see a separate FSM task for each policy, you can create a hostname alias in your DNS server to point to the same FTP/TFTP/SCP/SFTP server. Then you can use one hostname for the **Backup Policy** and another hostname for the **Config Export Policy**.

Required User Role for Backup and Import Operations

You must have a user account that includes the admin role to create and run backup and import operations.

Creating a Backup Operation

Before you begin

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

Procedure

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

Step 2 Click the **All** node.

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

Step 4 In the **Actions** area, click **Backup Configuration**.

Step 5 In the **Backup Configuration** dialog box, click **Create Backup Operation**.

Step 6 In the **Create Backup Operation** dialog box, complete the following fields:

Name	Description
Admin State field	This can be one of the following: • **Enabled**—Cisco UCS Manager runs the backup operation as soon as you click **OK**. • **Disabled**—Cisco UCS Manager does not run the backup operation when you click **OK**. If you select this option, all fields in the dialog box remain visible. However, you must manually run the backup from the **Backup Configuration** dialog box.

Name	Description
Type field	The information saved in the backup configuration file. This can be one of the following: • **Full state**—A binary file that includes a snapshot of the entire system. You can use the file generated from this backup to restore the system during disaster recovery. This file can restore or rebuild the configuration on the original fabric interconnect, or recreate the configuration on a different fabric interconnect. You cannot use this file for an import. **Note** You can only use a full state backup file to restore a system that is running the same version as the system from which the backup file was exported. It is also important that the bundles from which the backup was taken remain present in the Cisco UCS Manager and should not be deleted. • **All configuration**—An XML file that includes all system and logical configuration settings. You can use the file generated from this backup to import these configuration settings to the original fabric interconnect or to a different fabric interconnect. You cannot use this file for a system restore. This file does not include passwords for locally authenticated users. • **System configuration**—An XML file that includes all system configuration settings such as usernames, roles, and locales. You can use the file generated from this backup to import these configuration settings to the original fabric interconnect or to a different fabric interconnect. You cannot use this file for a system restore. • **Logical configuration**—An XML file that includes all logical configuration settings such as service profiles, VLANs, VSANs, pools, and policies. You can use the file generated from this backup to import these configuration settings to the original fabric interconnect or to a different fabric interconnect. You cannot use this file for a system restore.

Name	Description
Preserve Identities check box	This checkbox remains selected for **All Configuration** and **System Configuration** type of backup operation, and provides the following functionality: • **All Configuration**—The backup file preserves all identities derived from pools, including vHBAs, WWPNs, WWNN, vNICs, MACs and UUIDs. Also, the identities for Chassis, FEX, Rack Servers, and user labels for Chassis, FEX, Rack Servers, IOMs and Blade Servers are preserved. **Note** If this check box is not selected the identities will be reassigned and user labels will be lost after a restore. • **System Configuration**—The backup file preserves identities for Chassis, FEX, Rack Servers, and user labels for Chassis, FEX, Rack Servers, IOMs and Blade Servers. **Note** If this check box is not selected the identities will be reassigned and user labels will be lost after a restore. If this checkbox is selected for **Logical Configuration** type of backup operation, the backup file preserves all identities derived from pools, including vHBAs, WWPNs, WWNN, vNICs, MACs and UUIDs. **Note** If this check box is not selected the identities will be reassigned and user labels will be lost after a restore.
Location of the Backup File field	Where the backup file should be saved. This can be one of the following: • **Remote File System**—The backup XML file is saved to a remote server. Cisco UCS Manager GUI displays the fields described below that allow you to specify the protocol, host, filename, username, and password for the remote system. • **Local File System**—The backup XML file is saved locally. HTML-based Cisco UCS Manager GUI displays the **Filename** field. Enter a name for the backup file in **<*filename*>.xml** format. The file is downloaded and saved to a location depending on your browser settings.

Name	Description
Protocol field	The protocol to use when communicating with the remote server. This can be one of the following: • **FTP** • **TFTP** • **SCP** • **SFTP** • **USB A**—The USB drive inserted into fabric interconnect A. This option is only available for certain system configurations. • **USB B**—The USB drive inserted into fabric interconnect B. This option is only available for certain system configurations.
Hostname field	The hostname, IPv4 or IPv6 address of the location where the backup file is stored. This can be a server, storage array, local drive, or any read/write media that the fabric interconnect can access through the network. **Note** If you use a hostname rather than an IPv4 or IPv6 address, you must configure a DNS server. If the Cisco UCS domain is not registered with Cisco UCS Central or DNS management is set to **local**, configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to **global**, configure a DNS server in Cisco UCS Central.
Remote File field	The full path to the backup configuration file. This field can contain the filename as well as the path. If you omit the filename, the backup procedure assigns a name to the file.
User field	The username the system should use to log into the remote server. This field does not apply if the protocol is TFTP.
Password field	The password for the remote server username. This field does not apply if the protocol is TFTP. Cisco UCS Manager does not store this password. Therefore, you do not need to enter this password unless you intend to enable and run the backup operation immediately.

Step 7 Click **OK**.

Step 8 If Cisco UCS Manager displays a confirmation dialog box, click **OK**.

If you set the **Admin State** field to enabled, Cisco UCS Manager takes a snapshot of the configuration type that you selected and exports the file to the network location. The backup operation displays in the **Backup Operations** table in the **Backup Configuration** dialog box.

Step 9 (Optional) To view the progress of the backup operation, do the following:

a) If the operation does not display in the **Properties** area, click the operation in the **Backup Operations** table.
b) In the **Properties** area, click the down arrows on the **FSM Details** bar.

The **FSM Details** area expands and displays the operation status.

Step 10 Click **OK** to close the **Backup Configuration** dialog box.

The backup operation continues to run until it is completed. To view the progress, re-open the **Backup Configuration** dialog box.

Running a Backup Operation

Procedure

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

Step 2 Click the **All** node.

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

Step 4 In the **Actions** area, click **Backup Configuration**.

Step 5 In the **Backup Operations** table of the **Backup Configuration** dialog box, click the backup operation that you want to run.

The details of the selected backup operation display in the **Properties** area.

Step 6 In the **Properties** area, complete the following fields:

a) In the **Admin State** field, click the **Enabled** radio button.
b) For all protocols except TFTP, enter the password for the username in the **Password** field.
c) (Optional) Change the content of the other available fields.

Note
If you change other fields -- such as resetting a scheduled backup from weekly to daily -- you must re-enter your user name and password. Otherwise, an FI backup will fail.

Step 7 Click **Apply**.

Cisco UCS Manager takes a snapshot of the configuration type that you selected and exports the file to the network location. The backup operation displays in the **Backup Operations** table in the **Backup Configuration** dialog box.

Step 8 (Optional) To view the progress of the backup operation, click the down arrows on the **FSM Details** bar.

The **FSM Details** area expands and displays the operation status.

Step 9 Click **OK** to close the **Backup Configuration** dialog box.

The backup operation continues to run until it is completed. To view the progress, re-open the **Backup Configuration** dialog box.

Modifying a Backup Operation

You can modify a backup operation to save a file of another backup type to that location or to change the filename and avoid overwriting previous backup files.

Note You can only use a full state backup file to restore a system that is running the same version as the system from which the backup file was exported. It is also important that the bundles from which the backup was taken remain present in the Cisco UCS Manager and should not be deleted.

Procedure

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

Step 2 Click the **All** node.

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

Step 4 In the **Actions** area, click **Backup Configuration**.

Step 5 In the **Backup Operations** area of the **Backup Configuration** dialog box, click the backup operation that you want to modify.

The details of the selected backup operation display in the **Properties** area. If the backup operation is in a disabled state, the fields are dimmed.

Step 6 In the **Admin State** field, click the **enabled** radio button.

Step 7 Modify the appropriate fields.

You do not have to enter the password unless you want to run the backup operation immediately.

Step 8 (Optional) If you do not want to run the backup operation immediately, click the **disabled** radio button in the **Admin State** field.

Step 9 Click **OK**.

Deleting One or More Backup Operations

Procedure

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

Step 2 Click the **All** node.

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

Step 4 In the **Actions** area, click **Backup Configuration**.

Step 5 In the **Backup Operations** table of the **Backup Configuration** dialog box, click the backup operations that you want to delete.

Tip
You cannot click a backup operation in the table if the admin state of the operation is set to **Enabled.**

Step 6 Click the **Delete** icon in the icon bar of the **Backup Operations** table.

Step 7 If a confirmation dialog box displays, click **Yes**.

Step 8 In the **Backup Configuration** dialog box, click one of the following:

Option	Description
Apply	Deletes the selected backup operations without closing the dialog box.
OK	Deletes the selected backup operations and closes the dialog box.

Backup Types

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

- **Full state**—A binary file that includes a snapshot of the entire system. You can use the file generated from this backup to restore the system during disaster recovery. This file can restore or rebuild the configuration on the original fabric interconnect, or recreate the configuration on a different fabric interconnect. You cannot use this file for an import.

Note You can only use a full state backup file to restore a system that is running the same version as the system from which the backup file was exported. It is also important that the bundles from which the backup was taken remain present in the Cisco UCS Manager and should not be deleted.

- **All configuration**—An XML file that includes all system and logical configuration settings. You can use the file generated from this backup to import these configuration settings to the original fabric interconnect or to a different fabric interconnect. You cannot use this file for a system restore. This file does not include passwords for locally authenticated users.
- **System configuration**—An XML file that includes all system configuration settings such as usernames, roles, and locales. You can use the file generated from this backup to import these configuration settings to the original fabric interconnect or to a different fabric interconnect. You cannot use this file for a system restore.
- **Logical configuration**—An XML file that includes all logical configuration settings such as service profiles, VLANs, VSANs, pools, and policies. You can use the file generated from this backup to import these configuration settings to the original fabric interconnect or to a different fabric interconnect. You cannot use this file for a system restore.

Configuring the Full State Backup Policy

Before you begin

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

Procedure

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

Step 2 Click the **All** node.

Step 3 In the **Work** pane, click the **Backup and Export Policy** tab.

Step 4 In the **Full State Backup Policy** area, complete the following fields:

Name	Description
Hostname field	The hostname, IPv4 or IPv6 address of the location where the policy backup file is stored. This can be a server, storage array, local drive, or any read/write media that the fabric interconnect can access through the network. **Note** If you use a hostname rather than an IPv4 or IPv6 address, you must configure a DNS server. If the Cisco UCS domain is not registered with Cisco UCS Central or DNS management is set to **local**, configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to **global**, configure a DNS server in Cisco UCS Central.
Protocol field	The protocol to use when communicating with the remote server. This can be one of the following: • **FTP** • **TFTP** • **SCP** • **SFTP** • **USB A**—The USB drive inserted into fabric interconnect A. This option is only available for certain system configurations. • **USB B**—The USB drive inserted into fabric interconnect B. This option is only available for certain system configurations.
User field	The username the system should use to log into the remote server. This field does not apply if the protocol is TFTP.
Password field	The password for the remote server username. This field does not apply if the protocol is TFTP.

Name	Description
Remote File field	The full path to the policy backup file. This field can contain the filename as well as the path. If you omit the filename, the backup procedure assigns a name to the file.
Admin State field	This can be one of the following: • **Enabled**—Cisco UCS Manager backs up all policy information using the schedule specified in the **Schedule** field. • **Disabled**—Cisco UCS Manager does not back up policy information.
Schedule field	The frequency with which Cisco UCS Manager backs up policy information.
Max Files field	The maximum number of backup files that Cisco UCS Manager maintains. This value cannot be changed.
Description field	The description of the backup policy. The default description is **Database Backup Policy**. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), or ' (single quote).

Step 5 (Optional) In the **Backup/Export Config Reminder** area, complete the following fields:

Name	Description
Admin State column	This can be one of the following: • **Enable**—Cisco UCS Manager raises a fault if a backup is not taken during the specified time period. • **Disable**—Cisco UCS Manager does not raise a fault if a backup is not taken during the specified time period.
Remind Me After (days) column	The number of days before you are reminded to take a backup. Enter an integer between 1 and 365. The default value is 30 days.

Step 6 Click **Save Changes**.

Configuring the All Configuration Export Policy

Before you begin

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

Procedure

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

Step 2 Click the **All** node.

Step 3 In the **Work** pane, click the **Policy Backup & Export** tab.

Step 4 In the **Config Export Policy** area, complete the following fields:

Name	Description
Hostname field	The hostname, IPv4 or IPv6 address of the location where the configuration backup file is stored. This can be a server, storage array, local drive, or any read/write media that the fabric interconnect can access through the network. **Note** If you use a hostname rather than an IPv4 or IPv6 address, you must configure a DNS server. If the Cisco UCS domain is not registered with Cisco UCS Central or DNS management is set to **local**, configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to **global**, configure a DNS server in Cisco UCS Central.
Protocol field	The protocol to use when communicating with the remote server. This can be one of the following: • **FTP** • **TFTP** • **SCP** • **SFTP** • **USB A**—The USB drive inserted into fabric interconnect A. This option is only available for certain system configurations. • **USB B**—The USB drive inserted into fabric interconnect B. This option is only available for certain system configurations.
User field	The username the system should use to log into the remote server. This field does not apply if the protocol is TFTP.
Password field	The password for the remote server username. This field does not apply if the protocol is TFTP.
Remote File field	The full path to the backup configuration file. This field can contain the filename as well as the path. If you omit the filename, the backup procedure assigns a name to the file.

Name	Description
Admin State field	This can be one of the following: • **Enabled**—Cisco UCS Manager backs up all policy information using the schedule specified in the **Schedule** field. • **Disabled**—Cisco UCS Manager does not back up policy information.
Schedule field	The frequency with which Cisco UCS Manager backs up policy information.
Max Files field	The maximum number of configuration backup files that Cisco UCS Manager maintains. This value cannot be changed.
Description field	The description of the configuration export policy. The default description is **Configuration Export Policy**. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), or ' (single quote).

Step 5 (Optional) In the **Backup/Export Config Reminder** area, complete the following fields:

Name	Description
Admin State column	This can be one of the following: • **Enable**—Cisco UCS Manager raises a fault if a backup is not taken during the specified time period. • **Disable**—Cisco UCS Manager does not raise a fault if a backup is not taken during the specified time period.
Remind Me After (days) column	The number of days before you are reminded to take a backup. Enter an integer between 1 and 365. The default value is 30 days.

Step 6 Click **Save Changes**.

Import Methods

You can use one of the following methods to import and update a system configuration through Cisco UCS:

- **Merge**—The information in the imported configuration file is compared with the existing configuration information. If there are conflicts, the import operation overwrites the information on the Cisco UCS domain with the information in the import configuration file.

- **Replace**—The current configuration information is replaced with the information in the imported configuration file one object at a time.

Import Configuration

You can import any configuration file that was exported from Cisco UCS. The file does not need to have been exported from the same Cisco UCS.

Note You cannot import configuration from a higher release to a lower release.

The import function is available for all configuration, system configuration, and logical configuration files. You can perform an import while the system is up and running. An import operation modifies information on the management plane only. Some modifications caused by an import operation, such as a change to a vNIC assigned to a server, can cause a server reboot or other operations that disrupt traffic.

You cannot schedule an import operation. You can, however, create an import operation in advance and leave the admin state disabled until you are ready to run the import.Cisco UCS will not run the import operation on the configuration file until you set the admin state to enabled.

You can maintain only one import operation for each location where you saved a configuration backup file.

Creating an Import Operation

You cannot import a Full State backup file. You can import any of the following configuration files:

- All configuration
- System configuration
- Logical configuration

Before you begin

Collect the following information to import a configuration file:

- Backup server IP address and authentication credentials
- Fully-qualified name of a backup file

Procedure

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

Step 2 Click the **All** node.

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

Step 4 In the **Actions** area, click **Import Configuration**.

Step 5 In the **Import Configuration** dialog box, click **Create Import Operation**.

Step 6 In the **Create Import Operation** dialog box, complete the following fields:

Name	Description
Admin State field	This can be one of the following: • **Enabled**—Cisco UCS Manager runs the import operation as soon as you click **OK**. • **Disabled**—Cisco UCS Manager does not run the import operation when you click **OK**. If you select this option, all fields in the dialog box remain visible. However, you must manually run the import from the **Import Configuration** dialog box.
Action field	This can be one of the following: • **Merge**—The configuration information is merged with the existing information. If there are conflicts, the system replaces the information on the current system with the information in the import configuration file. • **Replace**—The system takes each object in the import configuration file and overwrites the corresponding object in the current configuration.
Location of the Import File field	Where the backup file that you want to import is located. This can be one of the following: • **Remote File System**—The backup XML file is stored on a remote server. Cisco UCS Manager GUI displays the fields described below that allow you to specify the protocol, host, filename, username, and password for the remote system. • **Local File System**—The backup XML file is stored locally. Cisco UCS Manager GUI displays the **Filename** field with an associated **Browse** button that let you specify the name and location for the backup file to be imported.
Protocol field	The protocol to use when communicating with the remote server. This can be one of the following: • **FTP** • **TFTP** • **SCP** • **SFTP** • **USB A**—The USB drive inserted into fabric interconnect A. This option is only available for certain system configurations. • **USB B**—The USB drive inserted into fabric interconnect B. This option is only available for certain system configurations.

Name	Description
Hostname field	The hostname, IPv4 or IPv6 address from which the configuration file should be imported. **Note** If you use a hostname rather than an IPv4 or IPv6 address, you must configure a DNS server. If the Cisco UCS domain is not registered with Cisco UCS Central or DNS management is set to **local**, configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to **global**, configure a DNS server in Cisco UCS Central.
Remote File field	The name of the XML configuration file.
User field	The username the system should use to log into the remote server. This field does not apply if the protocol is TFTP.
Password field	The password for the remote server username. This field does not apply if the protocol is TFTP. Cisco UCS Manager does not store this password. Therefore, you do not need to enter this password unless you intend to enable and run the import operation immediately.

Step 7 Click **OK**.

Step 8 In the confirmation dialog box, click **OK**.

If you set the **Admin State** to enabled, Cisco UCS Manager imports the configuration file from the network location. Depending on the action that you select, the information in the file merges with the existing configuration or replaces the existing configuration. The import operation displays in the **Import Operations** table of the **Import Configuration** dialog box.

Step 9 (Optional) To view the progress of the import operation, do the following:

a) If the operation does not automatically display in the **Properties** area, click the operation in the **Import Operations** table.

b) In the **Properties** area, click the down arrows on the **FSM Details** bar.

The **FSM Details** area expands and displays the operation status.

Step 10 Click **OK** to close the **Import Configuration** dialog box.

The import operation continues to run until it is completed. To view the progress, re-open the **Import Configuration** dialog box.

Running an Import Operation

You cannot import a Full State backup file. You can import any of the following configuration files:

- All configuration
- System configuration

- Logical configuration

Procedure

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

Step 2 Click the **All** node.

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

Step 4 In the **Actions** area, click **Import Configuration**.

Step 5 In the **Import Operations** table of the **Import Configuration** dialog box, click the operation that you want to run.

The details of the selected import operation display in the **Properties** area.

Step 6 In the **Properties** area, complete the following fields:

a) In the **Admin State** field, click the **Enabled** radio button.

b) For all protocols except TFTP, enter the password for the username In the **Password** field.

c) (Optional) Change the content of the other available fields.

Step 7 Click **Apply**.

Cisco UCS Manager imports the configuration file from the network location. Depending upon which action you selected, the information in the file is either merged with the existing configuration or replaces the existing configuration. The import operation displays in the **Import Operations** table of the **Import Configuration** dialog box.

Step 8 (Optional) To view the progress of the import operation, click the down arrows on the **FSM Details** bar.

The **FSM Details** area expands and displays the operation status.

Step 9 Click **OK** to close the **Import Configuration** dialog box.

The import operation continues to run until it is completed. To view the progress, re-open the **Import Configuration** dialog box.

Modifying an Import Operation

Procedure

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

Step 2 Click the **All** node.

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

Step 4 In the **Actions** area, click **Import Configuration**.

Step 5 In the **Import Operations** area of the **Import Configuration** dialog box, click the import operation that you want to modify.

The details of the selected import operation display in the **Properties** area. If the import operation is in a disabled state, the fields are dimmed.

Step 6 In the **Admin State** field, click the **enabled** radio button.

Step 7 Modify the appropriate fields.

You do not have to enter the password unless you want to run the import operation immediately.

Step 8 (Optional) If you do not want to run the import operation immediately, click the **disabled** radio button in the **Admin State** field.

Step 9 Click **OK**.

Deleting One or More Import Operations

Procedure

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

Step 2 Click the **All** node.

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

Step 4 In the **Actions** area, click **Import Configuration**.

Step 5 In the **Import Operations** table of the **Backup Configuration** dialog box, click the import operations that you want to delete.

Tip
You cannot click an import operation in the table if the admin state of the operation is set to **Enabled.**

Step 6 Click the **Delete** icon in the icon bar of the **Import Operations** table.

Step 7 If a confirmation dialog box displays, click **Yes**.

Step 8 In the **Import Configuration** dialog box, click one of the following:

Option	Description
Apply	Deletes the selected import operations without closing the dialog box.
OK	Deletes the selected import operations and closes the dialog box.

System Restore

You can use the restore function for disaster recovery.

You can restore a system configuration from any full state backup file that was exported from Cisco UCS. The file does not need to have been exported from Cisco UCS on the system that you are restoring. When restoring using a backup file that was exported from a different system, we recommend that you use a system with the same or similar system configuration and hardware, including fabric interconnects, servers, adapters,

and I/O module or FEX connectivity. Mismatched hardware and system configuration can lead to the restored system not fully functioning. If there is a mismatch between the I/O module links or servers on the two systems, acknowledge the chassis and servers after the restore operation.

In Cisco UCS Manager Release 4.0(1) and later releases, if a full state backup is collected on a UCS 6200 Series Fabric Interconnect with the following unsupported features, then full state restore cannot be used to restore this file on a Cisco UCS 6400 Series Fabric Interconnect:

- Chassis Discovery Policy and Chassis Connectivity Policy are in non port channel mode
- Virtual Machine Management is enabled - VMware, Linux KVM, or Microsoft Hypervisor

The restore function is only available for a full state backup file. You cannot import a full state backup file. You perform a restore through the initial system setup. For more information, see the appropriate *Cisco UCS Central Installation and Upgrade Guide*.

Note You can only use a full state backup file to restore a system that is running the same version as the system from which the backup file was exported. It is also important that the bundles from which the backup was taken remain present in the Cisco UCS Manager and should not be deleted.

Restoring the Configuration for a Fabric Interconnect

It is recommended to use a full state backup file to restore a system running the same version as the source system from which the backup was exported. You can use a full state backup to restore a system within the same release train. For example, you can use a backup from a system running on Cisco UCS Manager 4.1(3b) release version to restore a system on release 4.1(3m). It is also important to ensure that the bundles from which the backup was taken remain present in Cisco UCS Manager and are not deleted.

To avoid issues with VSAN or VLAN configuration, a backup should be restored on the fabric interconnect that was the primary fabric interconnect at the time of backup.

Before you begin

Collect the following information to restore the system configuration:

- Fabric interconnect management port IPv4 address and subnet mask, or IPv6 address and prefix
- Default gateway IPv4 or IPv6 address
- Backup server IPv4 or IPv6 address and authentication credentials
- Fully-qualified name of a Full State backup file

Note You must have access to a Full State configuration file to perform a system restore. You cannot perform a system restore with any other type of configuration or backup file.

Procedure

Step 1 Connect to the console port.

Step 2 If the fabric interconnect is off, power on the fabric interconnect.

You will see the power on self-test message as the fabric interconnect boots.

Step 3 At the installation method prompt, enter **`gui`**.

Step 4 If the system cannot access a DHCP server, you may be prompted to enter the following information:

- IPv4 or IPv6 address for the management port on the fabric interconnect
- Subnet mask or prefix for the management port on the fabric interconnect
- IPv4 or IPv6 address for the default gateway assigned to the fabric interconnect

Step 5 Copy the web link from the prompt into a web browser and go to the Cisco UCS Manager GUI launch page.

Step 6 On the launch page, select **Express Setup**.

Step 7 Select **UCSM** to continue.

Step 8 On the **Express Setup** page, select **Restore From Backup** and click **Submit**.

Step 9 In the **Protocol** area of the **Cisco UCS Manager Initial Setup** page, select the protocol you want to use to upload the full state backup file:

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

Step 10 In the **Server Information** area, complete the following fields:

Name	Description
Server IP	The IPv4 or IPv6 address of the computer where the full state backup file is located. This can be a server, storage array, local drive, or any read/write media that the fabric interconnect can access through the network.
Backup File Path	The file path where the full state backup file is located, including the folder names and filename. **Note** You can only use a full state backup file to restore a system that is running the same version as the system from which the backup file was exported. It is also important that the bundles from which the backup was taken remain present in the Cisco UCS Manager and should not be deleted.
User ID	The username the system should use to log into the remote server. This field does not apply if the protocol is TFTP.

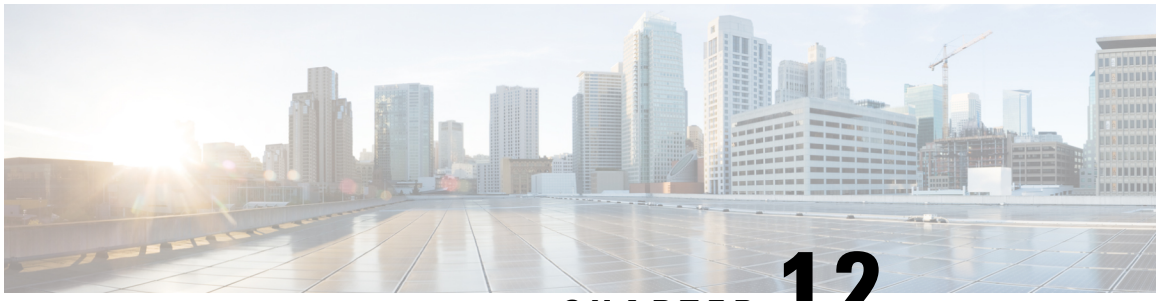
Name	Description
Password	The password for the remote server username. This field does not apply if the protocol is TFTP.

Step 11 Click **Submit**.

You can return to the console to watch the progress of the system restore.

The fabric interconnect logs in to the backup server, retrieves a copy of the specified full-state backup file, and restores the system configuration.

For a cluster configuration, you do not need to restore the secondary fabric interconnect. As soon as the secondary fabric interconnect reboots, Cisco UCS Manager synchronizes the configuration with the primary fabric interconnect.



CHAPTER 12

Scheduling Options

- Creating a Schedule, on page 137
- Creating a One Time Occurrence for a Schedule, on page 142
- Creating a Recurring Occurrence for a Schedule, on page 145
- Deleting a One Time Occurrence from a Schedule, on page 147
- Deleting a Recurring Occurrence from a Schedule, on page 148
- Deleting a Schedule, on page 148

Creating a Schedule

Procedure

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 On the **Servers** tab, right-click **Schedules** and choose **Create Schedule**.

Step 3 In the **Identify Schedule** page of the **Create Schedule** wizard, complete the following fields:

Name	Description
Name field	The name of the schedule. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.
Description field	A description of the schedule. We recommend including information about where and when the schedule should be used. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), or ' (single quote).

Name	Description
Owner field	The owner of the schedule. This can be one of the following: • **Local**—Cisco UCS Manager owns the schedule, which is configured in this Cisco UCS domain. • **Pending Global**—Cisco UCS Manager is in the process of transferring this schedule to Cisco UCS Central. • **Global**—Cisco UCS Central owns the schedule, which is configured on a remote server.

Step 4 Click **Next**.

Step 5 On the **One Time Occurrences** page, click one of the following:

Option	Description
Next	Moves to the next page. Choose this option if you do not want to create a one time occurrence for this schedule. If you choose this option, continue with Step 8.
Add	Opens the **Create a One Time Occurrence** dialog box, where you can specify a single time when this schedule should be run. If you choose this option, continue with Step 6.

Step 6 (Optional) In the **Create a One Time Occurrence** dialog box, do the following:

a) Complete the following fields:

Name	Description
Name field	The name of the one time occurrence of this schedule. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.
Start Time field	The date and time that the occurrence will run. Click the down arrow at the end of the field to select the date from a calendar.

b) Click the down arrows to expand the **Options** area.

c) In the **Options** area, complete the following fields:

Name	Description
Max Duration field	The maximum length of time that the scheduled occurrence can run. This can be one of the following: • **None**—The occurrence runs until all tasks are completed. • **other**—Cisco UCS Manager GUI displays the **dd:hh:mm:ss** field allowing you to specify the maximum amount of time that the occurrence can run. Cisco UCS completes as many scheduled tasks as possible within the specified time. By default, the maximum duration is set to **none**. If you do not change this setting and you do not set a maximum number of tasks, the maintenance window continues until all pending activities are completed.
Max Number of Tasks field	The maximum number of scheduled tasks that can be run during this occurrence. This can be one of the following: • **Unlimited**—Cisco UCS runs all scheduled tasks unless those tasks exceed the maximum time specified in the **Max Duration** field. If **Max Duration** is set to **none** and you select this option, the maintenance window continues until all pending activities are completed. • **other**—Cisco UCS Manager GUI displays a text field allowing you to specify the maximum number of tasks that can be run during this occurrence. Enter an integer between 1 and 65535. **Note** This option does not apply if this schedule is associated with a fault suppression task.
Max Number of Concurrent Tasks field	The maximum number of tasks that can run concurrently during this occurrence. This can be one of the following: • **Unlimited**—Cisco UCS runs as many concurrent tasks as the system can handle. • **other**—Cisco UCS Manager GUI displays a text field allowing you to specify the maximum number of concurrent tasks that can be run during this occurrence. Enter an integer between 1 and 65535. **Note** This option does not apply if this schedule is associated with a fault suppression task.

Name	Description
Minimum Interval Between Tasks field	The minimum length of time that the system should wait before starting a new task. This setting is meaningful only if the maximum number of concurrent tasks is set to a value other than None. This can be one of the following: • **None**—Cisco UCS runs the next task as soon as possible. • **other**—Cisco UCS Manager GUI displays the **dd:hh:mm:ss** field allowing you to specify the minimum amount of time that Cisco UCS will wait between tasks. **Note** This option does not apply if this schedule is associated with a fault suppression task.

d) Click **OK**.

Step 7 To add another one time occurrence, click **Add** and repeat step 6. Otherwise, click **Next**.

Step 8 (Optional) If you want to define a recurring occurrence for this schedule, on the **Recurring Occurrences** page, click **Add**.

a) In the **Create a Recurring Occurrence** dialog box, complete the following fields:

Name	Description
Name field	The name of the recurring occurrence of this schedule. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.
Day field	The day on which Cisco UCS runs an occurrence of this schedule. This can be one of the following: • **every day** • **Monday** • **Tuesday** • **Wednesday** • **Thursday** • **Friday** • **Saturday** • **Sunday** • **odd days** • **even days**

Name	Description
Hour field	The hour of the specified day at which this occurrence of the schedule starts. This can be an integer between 0 and 24, where 0 and 24 are both equivalent to midnight. **Note** Cisco UCS ends all recurring occurrences on the same day in which they start, even if the maximum duration has not been reached. For example, if you specify a start time of 11 p.m. and a maximum duration of 3 hours, Cisco UCS starts the occurrence at 11 p.m. but ends it at 11:59 p.m. after only 59 minutes. Ensure that the start time you specify is early enough so that the recurring occurrence finishes before 11:59 p.m.
Minute field	The minute of the hour at which the schedule occurrence starts. This can be an integer between 0 and 60.

b) Click the down arrows to expand the **Options** area.
c) In the **Options** area, complete the following fields:

Name	Description
Max Duration field	The maximum length of time that each occurrence of this schedule can run. This can be one of the following: • **None**—The occurrence runs until all tasks are completed. • **other**—Cisco UCS Manager GUI displays the **dd:hh:mm:ss** field allowing you to specify the maximum amount of time that the occurrence can run. Cisco UCS completes as many scheduled tasks as possible within the specified time.
Max Number of Tasks field	The maximum number of scheduled tasks that can be run during each occurrence. This can be one of the following: • **Unlimited**—Cisco UCS runs all scheduled tasks unless those tasks exceed the maximum time specified in the **Max Duration** field. If **Max Duration** is set to **none** and you select this option, the maintenance window continues until all pending activities are completed. • **other**—Cisco UCS Manager GUI displays a text field allowing you to specify the maximum number of tasks that can be run during this occurrence. Enter an integer between 1 and 65535. **Note** This option does not apply if this schedule is associated with a fault suppression task.

Name	Description
Max Number of Concurrent Tasks field	The maximum number of tasks that can run concurrently during each occurrence. This can be one of the following: • **Unlimited**—Cisco UCS runs as many concurrent tasks as the system can handle. • **other**—Cisco UCS Manager GUI displays a text field allowing you to specify the maximum number of concurrent tasks that can be run during this occurrence. Enter an integer between 1 and 65535. **Note** This option does not apply if this schedule is associated with a fault suppression task.
Minimum Interval Between Tasks field	The minimum length of time that the system should wait before starting a new task. This setting is meaningful only if the maximum number of concurrent tasks is set to a value other than None. This can be one of the following: • **None**—Cisco UCS runs the next task as soon as possible. • **other**—Cisco UCS Manager GUI displays the **dd:hh:mm:ss** field allowing you to specify the minimum amount of time that Cisco UCS will wait between tasks. **Note** This option does not apply if this schedule is associated with a fault suppression task.

d) Click **OK**.
e) To add another recurring occurrence, click **Add** and repeat this step.

Step 9 Click **Finish**.

Creating a One Time Occurrence for a Schedule

Note By default, the maximum duration and the maximum number of tasks are set to **none**. If you do not change either of these defaults, Cisco UCS Manager does not impose any limit to the length of time that the maintenance window lasts. All pending activities are applied as soon as the scheduled maintenance window begins, and Cisco UCS Manager continues to reboot the servers impacted by the pending activities until all of those tasks are complete.

Procedure

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 Expand **Schedules**.

Step 3 Right-click the schedule to which you want to add an occurrence and choose **Create a One Time Occurrence**.

Step 4 In the **Create a One Time Occurrence** dialog box, complete the following fields:

Name	Description
Name field	The name of the one time occurrence of this schedule. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.
Start Time field	The date and time that the occurrence will run. Click the down arrow at the end of the field to select the date from a calendar.

Step 5 Click the down arrows to expand the **Options** area.

Step 6 In the **Options** area, complete the following fields:

Name	Description
Max Duration field	The maximum length of time that the scheduled occurrence can run. This can be one of the following: • **None**—The occurrence runs until all tasks are completed. • **other**—Cisco UCS Manager GUI displays the **dd:hh:mm:ss** field allowing you to specify the maximum amount of time that the occurrence can run. Cisco UCS completes as many scheduled tasks as possible within the specified time. By default, the maximum duration is set to **none**. If you do not change this setting and you do not set a maximum number of tasks, the maintenance window continues until all pending activities are completed.

Name	Description
Max Number of Tasks field	The maximum number of scheduled tasks that can be run during this occurrence. This can be one of the following: • **Unlimited**—Cisco UCS runs all scheduled tasks unless those tasks exceed the maximum time specified in the **Max Duration** field. If **Max Duration** is set to **none** and you select this option, the maintenance window continues until all pending activities are completed. • **other**—Cisco UCS Manager GUI displays a text field allowing you to specify the maximum number of tasks that can be run during this occurrence. Enter an integer between 1 and 65535. **Note** This option does not apply if this schedule is associated with a fault suppression task.
Max Number of Concurrent Tasks field	The maximum number of tasks that can run concurrently during this occurrence. This can be one of the following: • **Unlimited**—Cisco UCS runs as many concurrent tasks as the system can handle. • **other**—Cisco UCS Manager GUI displays a text field allowing you to specify the maximum number of concurrent tasks that can be run during this occurrence. Enter an integer between 1 and 65535. **Note** This option does not apply if this schedule is associated with a fault suppression task.
Minimum Interval Between Tasks field	The minimum length of time that the system should wait before starting a new task. This setting is meaningful only if the maximum number of concurrent tasks is set to a value other than None. This can be one of the following: • **None**—Cisco UCS runs the next task as soon as possible. • **other**—Cisco UCS Manager GUI displays the **dd:hh:mm:ss** field allowing you to specify the minimum amount of time that Cisco UCS will wait between tasks. **Note** This option does not apply if this schedule is associated with a fault suppression task.

Step 7 Click **OK**.

Creating a Recurring Occurrence for a Schedule

Procedure

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 Expand **Schedules**.

Step 3 Right-click the schedule to which you want to add an occurrence and choose **Create a Recurring Occurrence**.

Step 4 In the **Create a Recurring Occurrence** dialog box, complete the following fields:

Name	Description
Name field	The name of the recurring occurrence of this schedule. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.
Day field	The day on which Cisco UCS runs an occurrence of this schedule. This can be one of the following: • **every day** • **Monday** • **Tuesday** • **Wednesday** • **Thursday** • **Friday** • **Saturday** • **Sunday** • **odd days** • **even days**

Name	Description
Hour field	The hour of the specified day at which this occurrence of the schedule starts. This can be an integer between 0 and 24, where 0 and 24 are both equivalent to midnight. **Note** Cisco UCS ends all recurring occurrences on the same day in which they start, even if the maximum duration has not been reached. For example, if you specify a start time of 11 p.m. and a maximum duration of 3 hours, Cisco UCS starts the occurrence at 11 p.m. but ends it at 11:59 p.m. after only 59 minutes. Ensure that the start time you specify is early enough so that the recurring occurrence finishes before 11:59 p.m.
Minute field	The minute of the hour at which the schedule occurrence starts. This can be an integer between 0 and 60.

Step 5 Click the down arrows to expand the **Options** area.

Step 6 In the **Options** area, complete the following fields:

Name	Description
Max Duration field	The maximum length of time that each occurrence of this schedule can run. This can be one of the following: • **None**—The occurrence runs until all tasks are completed. • **other**—Cisco UCS Manager GUI displays the **dd:hh:mm:ss** field allowing you to specify the maximum amount of time that the occurrence can run. Cisco UCS completes as many scheduled tasks as possible within the specified time.
Max Number of Tasks field	The maximum number of scheduled tasks that can be run during each occurrence. This can be one of the following: • **Unlimited**—Cisco UCS runs all scheduled tasks unless those tasks exceed the maximum time specified in the **Max Duration** field. If **Max Duration** is set to **none** and you select this option, the maintenance window continues until all pending activities are completed. • **other**—Cisco UCS Manager GUI displays a text field allowing you to specify the maximum number of tasks that can be run during this occurrence. Enter an integer between 1 and 65535. **Note** This option does not apply if this schedule is associated with a fault suppression task.

Name	Description
Max Number of Concurrent Tasks field	The maximum number of tasks that can run concurrently during each occurrence. This can be one of the following: • **Unlimited**—Cisco UCS runs as many concurrent tasks as the system can handle. • **other**—Cisco UCS Manager GUI displays a text field allowing you to specify the maximum number of concurrent tasks that can be run during this occurrence. Enter an integer between 1 and 65535. **Note** This option does not apply if this schedule is associated with a fault suppression task.
Minimum Interval Between Tasks field	The minimum length of time that the system should wait before starting a new task. This setting is meaningful only if the maximum number of concurrent tasks is set to a value other than None. This can be one of the following: • **None**—Cisco UCS runs the next task as soon as possible. • **other**—Cisco UCS Manager GUI displays the **dd:hh:mm:ss** field allowing you to specify the minimum amount of time that Cisco UCS will wait between tasks. **Note** This option does not apply if this schedule is associated with a fault suppression task.

Step 7 Click **OK**.

Deleting a One Time Occurrence from a Schedule

If this is the only occurrence in a schedule, that schedule is reconfigured with no occurrences. If the schedule is included in a maintenance policy and that policy is assigned to a service profile, any pending activities related to the server associated with the service profile cannot be deployed. You must add a one time occurrence or a recurring occurrence to the schedule to deploy the pending activity.

Procedure

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 Expand **Schedules** > ***Schedule_Name***.

Step 3 Expand **One Time Occurrences**.

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

Step 5 If a confirmation dialog box displays, click **Yes**.

Deleting a Recurring Occurrence from a Schedule

If this is the only occurrence in a schedule, that schedule is reconfigured with no occurrences. If the schedule is included in a maintenance policy and that policy is assigned to a service profile, any pending activities related to the server associated with the service profile cannot be deployed. You must add a one time occurrence or a recurring occurrence to the schedule to deploy the pending activity.

Procedure

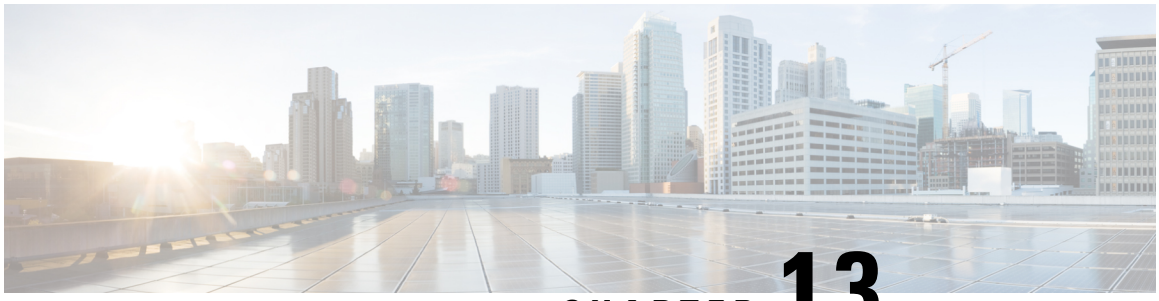
Step 1 In the **Navigation** pane, click **Servers**.
Step 2 Expand **Schedules** > ***Schedule_Name***.
Step 3 Expand **Recurring Occurrences**.
Step 4 Right-click the occurrence you want to delete and choose **Delete**.
Step 5 If a confirmation dialog box displays, click **Yes**.

Deleting a Schedule

If this schedule is included in a maintenance policy, the policy is reconfigured with no schedule. If that policy is assigned to a service profile, any pending activities related to the server associated with the service profile cannot be deployed. You must add a schedule to the maintenance policy to deploy the pending activity.

Procedure

Step 1 In the **Navigation** pane, click **Servers**.
Step 2 Expand **Schedules**.
Step 3 Right-click the schedule you want to delete and choose **Delete**.
Step 4 If a confirmation dialog box displays, click **Yes**.



CHAPTER 13

Deferred Deployments of Service Profile Updates

- Service Profile Deferred Deployments, on page 149
- Maintenance Policy, on page 151
- Pending Activities for Deferred Deployments, on page 155

Service Profile Deferred Deployments

Some modifications to a service profile or to an updating service profile template can be disruptive and require a reboot of the server. You can, however, configure deferred deployment to control when those disruptive configuration changes are implemented. For example, you can choose to deploy the service profile changes immediately or have them deployed during a specified maintenance window. You can also choose whether or not a service profile deployment requires explicit user acknowledgment.

Deferred deployment is available for all configuration changes that occur through the association of a service profile with a server. These configuration changes can be prompted by a change to a service profile, to a policy that is included in a service profile, or to an updating service profile template. For example, you can defer the upgrade and activation of firmware through host firmware packages and management firmware packages, such as server BIOS, RAID controller, host HBA, and network adapters. However, you cannot defer the direct deployment of firmware images for components that do not use either of the firmware packages, such as Cisco UCS Manager, fabric interconnects, and I/O modules.

Deferred deployment is not available for the following actions which require the reboot of a server:

- Initial association of a service profile with a server
- Final disassociation of a service profile from a server, without associating the service profile with a different server
- Decommissioning a server
- Re-acknowledging a server
- Resetting a server

If you want to defer the deployment of service profile changes, you must configure one or more maintenance policies and configure each service profile with a maintenance policy. If you want to define the time period when the deployment should occur, you also need to create at least one schedule with one or more recurring occurrences or one time occurrences, and include that schedule in a maintenance policy.

Schedules for Deferred Deployments

A schedule contains a set of occurrences. These occurrences can be one time only or can recur at a specified time and day each week. The options defined in the occurrence, such as the duration of the occurrence or the maximum number of tasks to be run, determine whether a service profile change is deployed. For example, if a change cannot be deployed during a given maintenance window because the maximum duration or number of tasks was reached, that deployment is carried over to the next maintenance window.

Each schedule checks periodically to see whether the Cisco UCS domain entered one or more maintenance windows. If so, the schedule executes the deployments that are eligible according to the constraints specified in the maintenance policy.

A schedule contains one or more occurrences, which determine the maintenance windows associated with that schedule. An occurrence can be one of the following:

One Time Occurrence

One time occurrences define a single maintenance window. These windows continue until the maximum duration of the window or the maximum number of tasks that can be run in the window is reached.

Recurring Occurrence

Recurring occurrences define a series of maintenance windows. These windows continue until the maximum number of tasks or the end of the day specified in the occurrence was reached.

Guidelines and Limitations for Deferred Deployments

Service Profile Association Changes and Maintenance Policy Options

When changing service profile association, the following maintenance policy options can affect how the changes are applied:

- If the **On Next Boot** and **User Ack** options are enabled in a maintenance policy, the service profile association change displays a warning that an acknowledgement is required. However, association will happen immediately.
- If the **On Next Boot** and **User Ack** options are not enabled in a maintenance policy, the service profile association change displays a warning that an acknowledgement is required, and will remain pending until acknowledged.

Cannot Undo All Changes to Service Profiles or Service Profile Templates

If you cancel a pending change, Cisco UCS Manager attempts to roll back the change without rebooting the server. However, for complex changes, Cisco UCS Manager may have to reboot the server a second time to roll back the change. For example, if you delete a vNIC, Cisco UCS Manager reboots the server according to the maintenance policy included in the service profile. You cannot cancel this reboot and change, even if you restore the original vNIC in the service profile. Instead, Cisco UCS Manager schedules a second deployment and reboot of the server.

Association of Service Profile Can Exceed Boundaries of Maintenance Window

After Cisco UCS Manager begins the association of the service profile, the scheduler and maintenance policy do not have any control over the procedure. If the service profile association does not complete within the

allotted maintenance window, the process continues until it is completed. For example, this can occur if the association does not complete in time because of retried stages or other issues.

Cannot Specify Order of Pending Activities

Scheduled deployments run in parallel and independently. You cannot specify the order in which the deployments occur. You also cannot make the deployment of one service profile change dependent upon the completion of another.

Cannot Perform Partial Deployment of Pending Activity

Cisco UCS Manager applies all changes made to a service profile in the scheduled maintenance window. You cannot make several changes to a service profile at the same time and then have those changes be spread across several maintenance windows. When Cisco UCS Manager deploys the service profile changes, it updates the service profile to match the most recent configuration in the database.

Maintenance Policy

The maintenance policy specifies how deploys the service profile changes. The deployment can occur in one of the following ways:

- Immediately
- When acknowledged by a user with administrator privileges
- Automatically at the time specified in a schedule
- On the next reboot or shutdown without waiting for the user acknowledgment or the timer scheduling option

A UCSM and CIMC version on blade or rack server must be running firmware from 3.1.x bundle, for **On Next Boot** to work.

If the **On Next Boot** option is enabled in a maintenance policy, and you downgrade from Cisco UCS Manager Release 3.1(1) or later releases to any release earlier than Cisco UCS Manager Release 2.2(8), firmware downgrade will fail. Disable **On Next Boot** from the maintenance policy to continue with the downgrade.

You can use the soft shutdown timer in the maintenance policy to configure the wait time for performing a hard shutdown. The soft shutdown timer is applicable when you reboot the server for the following:

- Reset the server using the **Gracefully Restart OS** option.
- Shut down the server with the **In case of graceful shutdown failure, a hard shutdown will be issued after X seconds** option.
- Modify a service profile that requires a server reboot.

If the maintenance policy is configured to deploy the change during a scheduled maintenance window, the policy must include a valid schedule. The schedule deploys the changes in the first available maintenance window.

Note A maintenance policy only prevents an immediate server reboot when a configuration change is made to an associated service profile. However, a maintenance policy does not prevent the following actions from taking place right away:

- Deleting an associated service profile from the system
- Disassociating a server profile from a server
- Directly installing a firmware upgrade without using a service policy
- Resetting the server

Creating a Maintenance Policy

Before you begin

If you plan to configure this maintenance policy for automatic deferred deployment, create a schedule.

Procedure

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 Expand **Servers** > **Policies**.

Step 3 Expand the node for the organization where you want to create the policy.

If the system does not include multi tenancy, expand the **root** node.

Step 4 Right-click **Maintenance Policies** and choose **Create Maintenance Policy**.

Step 5 In the **Create Maintenance Policy** dialog box, complete the following fields:

Name	Description
Name field	The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.
Description field	A description of the policy. Cisco recommends including information about where and when to use the policy. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), or ' (single quote).

Name	Description
Soft Shutdown Timer drop-down list	This timer allows you to specify the time in seconds when Cisco UCS Manager performs a server shut down and reboot. Cisco UCS Manager waits until the specified time in the maintenance policy before performing a hard shut down. This can be one of the following: • **150 Secs**—Cisco UCS Manager waits until 150 seconds before performing a hard shut down and reboot of the server. • **300 Secs**—Cisco UCS Manager waits until 300 seconds before performing a hard shut down and reboot of the server. • **600 Secs**—Cisco UCS Manager waits for 600 seconds before performing a hard shut down and reboot of the server. • **Never**—Cisco UCS Manager never performs a server shut down.

Name	Description
Reboot Policy field	When a service profile is associated with a server, or when changes are made to a service profile that is already associated with a server, you must reboot the server to complete the process. The **Reboot Policy** field determines when the reboot occurs for servers associated with any service profiles that include this maintenance policy. This can be one of the following: • **Immediate**—The server reboots automatically as soon as the service profile association is complete or when you save service profile changes. • **User Ack**—You must explicitly acknowledge the pending activities for the changes made to the service profile to be applied to the associated server. • **Timer Automatic**—Cisco UCS defers all service profile associations and changes until the maintenance window defined by the schedule shown in the **Schedule** field. • **On Next Boot**—This option is used in combination with either **User Ack** or **Timer Automatic**. When the **On Next Boot** option is enabled, the host OS reboot, shutdown, and reset, or server reset and shutdown also triggers the associated FSM to apply the changes waiting for the**User Ack**, or the **Timer Automatic** maintenance window. **Note** De-selecting the On Next Boot option disables the Maintenance Policy on the BMC.
Schedule drop-down list	If the **Reboot Policy** is set to **Timer Automatic**, the schedule specifies when maintenance operations can be applied to the server. Cisco UCS reboots the server and completes the service profile changes at the scheduled time.
Create Schedule link	Creates a new schedule that is available to all objects in this Cisco UCS domain.

Step 6 Click **OK**.

What to do next

Include the policy in a service profile or service profile template.

Deleting a Maintenance Policy

Procedure

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 Expand **Servers** > **Policies** > ***Organization_Name***.

Step 3 Expand **Maintenance Policies**.

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

Step 5 If a confirmation dialog box displays, click **Yes**.

Pending Activities for Deferred Deployments

If you configure a deferred deployment in a Cisco UCS domain, Cisco UCS Manager enables you to view all pending activities. You can see activities that are waiting for user acknowledgement and those that are scheduled.

If a Cisco UCS domain has pending activities, Cisco UCS Manager GUI notifies users with admin privileges when they log in.

Cisco UCS Manager displays information about all pending activities, including the following:

- Name of the service profile to deploy and associate with a server
- Server affected by the deployment
- Disruption caused by the deployment
- Change performed by the deployment

Note You cannot specify the maintenance window in which a specific pending activity is applied to the server. The maintenance window depends upon how many activities are pending and which maintenance policy is assigned to the service profile. However, any user with admin privileges can manually initiate a pending activity and reboot the server immediately, whether it is waiting for user acknowledgment or for a maintenance window.

Viewing Pending Activities

Procedure

Step 1 On the toolbar, click **Pending Activities**.

Step 2 Click one of the following tabs:

- **User Acknowledged Activities**—Contains the **Service Profiles** and **Fabric Interconnects** tabs that display the tasks requiring user acknowledgment before they can complete.
- **Scheduled Activities**—Displays the tasks that will be performed based on the associated maintenance schedule.

Step 3 Click a row in the table to view the details of that pending activity.

If you click the link in the **Server** column, Cisco UCS Manager displays the properties of that server.

Deploying a Service Profile Change Waiting for User Acknowledgement

Important You cannot stop Cisco UCS Manager from rebooting the affected server after you acknowledge a pending activity.

Procedure

Step 1 On the toolbar, click **Pending Activities**.

Step 2 In the **Pending Activities** dialog box, click the **User Acknowledged Activities** tab and then the **Service Profiles** tab.

Step 3 Check the check box in the **Reboot Now** column for each pending activity you want to deploy immediately.

Step 4 Click **OK**.

Cisco UCS Manager immediately reboots the server affected by the pending activity.

Deploying All Service Profile Changes Waiting for User Acknowledgement

Important You cannot stop Cisco UCS Manager from rebooting the affected server after you acknowledge a pending activity.

Procedure

Step 1 On the toolbar, click **Pending Activities**.

Step 2 In the **Pending Activities** dialog box, click the **User Acknowledged Activities** tab and then the **Service Profiles** tab.

Step 3 In the toolbar, check the **Acknowledge All** check box.

Cisco UCS Manager GUI checks the **Reboot Now** check boxes for all pending activities listed in the table.

Step 4 Click **OK**.

Cisco UCS Manager immediately reboots all servers affected by the pending activities listed in the table.

Deploying a Scheduled Service Profile Change Immediately

Important You cannot stop Cisco UCS Manager from rebooting the affected server after you acknowledge a pending activity.

Procedure

Step 1 On the toolbar, click **Pending Activities**.

Step 2 In the **Pending Activities** dialog box, click the **Scheduled Activities** tab.

Step 3 Check the check box in the **Reboot Now** column for each pending activity you want to deploy immediately.

Step 4 Click **OK**.

Cisco UCS Manager immediately reboots the server affected by the pending activity.

Deploying All Scheduled Service Profile Changes Immediately

Important You cannot stop Cisco UCS Manager from rebooting the affected server after you acknowledge a pending activity.

Procedure

Step 1 On the toolbar, click **Pending Activities**.

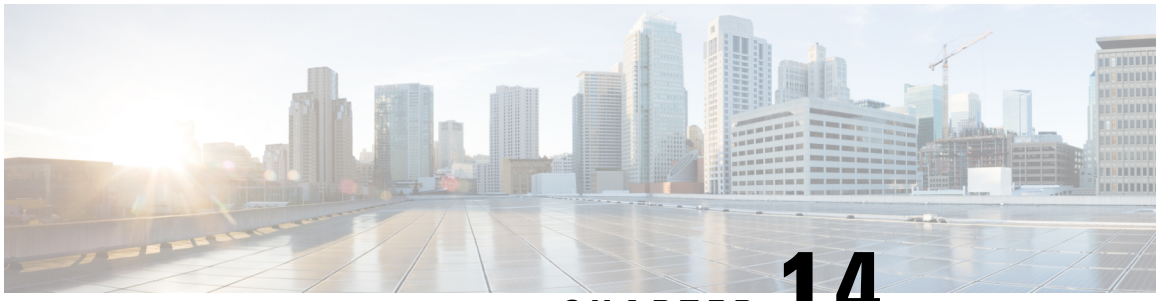
Step 2 In the **Pending Activities** dialog box, click the **Scheduled Activities** tab.

Step 3 In the toolbar, check the **Acknowledge All** check box.

Cisco UCS Manager GUI checks the **Reboot Now** check boxes for all pending activities listed in the table.

Step 4 Click **OK**.

Cisco UCS Manager immediately reboots all servers affected by the pending activities listed in the table.



CHAPTER 14

UCS Fault Suppression

- Global Fault Policy, on page 159
- Configuring the Global Fault Policy, on page 159

Global Fault Policy

The global fault policy controls the lifecycle of a fault in a Cisco UCS domain, including when faults are cleared, the flapping interval (the length of time between the fault being raised and the condition being cleared), and the retention interval (the length of time a fault is retained in the system).

A fault in Cisco UCS has the following lifecycle:

1. A condition occurs in the system and Cisco UCS Manager raises a fault. This is the active state.
2. When the fault is alleviated, it enters a flapping or soaking interval that is designed to prevent flapping. Flapping occurs when a fault is raised and cleared several times in rapid succession. During the flapping interval, the fault retains its severity for the length of time specified in the global fault policy.
3. If the condition reoccurs during the flapping interval, the fault returns to the active state. If the condition does not reoccur during the flapping interval, the fault is cleared.
4. The cleared fault enters the retention interval. This interval ensures that the fault reaches the attention of an administrator even if the condition that caused the fault has been alleviated and the fault has not been deleted prematurely. The retention interval retains the cleared fault for the length of time specified in the global fault policy.
5. If the condition reoccurs during the retention interval, the fault returns to the active state. If the condition does not reoccur, the fault is deleted.

Configuring the Global Fault Policy

Procedure

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

Step 2 Expand **All** > **Faults, Events, and Audit Log**.

Step 3 Click **Settings**.

Step 4 In the **Work** pane, click the **Global Fault Policy** tab.

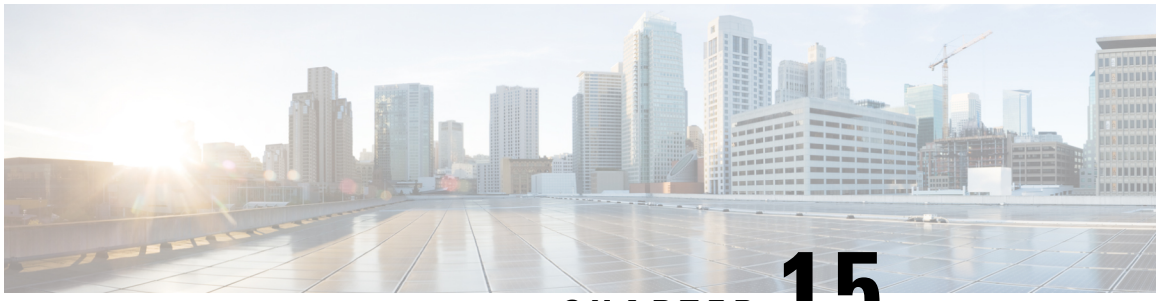
Step 5 In the **Global Fault Policy** tab, complete the following fields:

Name	Description
Flapping Interval field	Flapping occurs when a fault is raised and cleared several times in rapid succession. To prevent this, Cisco UCS Manager does not allow a fault to change its state until this amount of time has elapsed since the last state change. If the condition reoccurs during the flapping interval, the fault returns to the active state. If the condition does not reoccur during the flapping interval, the fault is cleared. What happens at that point depends on the setting in the **Clear Action** field. Enter an integer between 5 and 3,600. The default is 10.
Initial Severity field	This can be one of the following: • **Info** • **Condition** • **Warning**
Action on Acknowledgment field	Acknowledged actions are always deleted when the log is cleared. This option cannot be changed.
Clear Action field	The action Cisco UCS Manager takes when a fault is cleared. This can be one of the following: • **Retain**—Cisco UCS Manager GUI displays the **Length of time to retain cleared faults** section. • **Delete**—Cisco UCS Manager immediately deletes all fault messages as soon as they are marked as cleared.
Clear Interval field	Indicate whether Cisco UCS Manager automatically clears faults after a certain length of time. This can be one of the following: • **Never**—Cisco UCS Manager does not automatically clear any faults. • **other**—Cisco UCS Manager GUI displays the **dd:hh:mm:ss** field.
dd:hh:mm:ss field	The number of days, hours, minutes, and seconds that should pass before Cisco UCS Manager automatically marks that fault as cleared. What happens then depends on the setting in the **Clear Action** field.

Step 6 Click **Save Changes**.

What to do next

For more information on fault suppression, see the *Cisco UCS System Monitoring Guide*.



CHAPTER 15

KVM Console

- KVM Console, on page 163
- KVM Console for Cisco UCS B-Series M4, C-Series M4, and C-Series M5 Servers, on page 164
- KVM Direct Access, on page 167
- Starting the KVM Console from a Server, on page 168
- Starting the KVM Console from a Service Profile, on page 168
- Starting the KVM Console from the Cisco UCS KVM Direct Web Page, on page 169
- Starting the KVM Console from the KVM Launch Manager, on page 170
- KVM Folder Mapping, on page 171
- KVM Certificate, on page 171

KVM Console

The KVM console is an interface accessible from the Cisco UCS Manager GUI or the KVM Launch Manager that emulates a direct keyboard, video, and mouse (KVM) connection to the server. It allows you to connect and control the server from a remote location and also to map physical locations to virtual drives that can by accessed by the server during this Virtual KVM (vKVM) session. Unlike the KVM dongle, which requires you to be physically connected to the server, the KVM console allows you to connect to the server from a remote location across the network.

Beginning with Cisco UCS Manager Release 4.1(1), the KVM console is available as an HTML5-based application on Cisco UCS M4 and M5 servers. The console is no longer available as a Java-based application. For more information, see KVM Console for Cisco UCS B-Series M4, C-Series M4, and C-Series M5 Servers, on page 164

You must ensure that either the server or the service profile associated with the server is configured with a CIMC IP address if you want to use the KVM console to access the server. The KVM console uses the CIMC IP address assigned to a server or a service profile to identify and connect with the correct server in a Cisco UCS domain.

Instead of using CD/DVD or floppy drives directly connected to the server, the KVM console uses virtual media, which are actual disk drives or disk image files that are mapped to virtual CD/DVD or floppy drives. You can map any of the following to virtual drives:

- CD/DVD or floppy drives on your computer
- Disk image files on your computer
- CD/DVD or floppy drives on the network

- Disk image files on the network

Note When you launch the KVM console from the physical server, the system checks if the server is associated to a service profile. If the server is associated to a service profile with an associated management IP address, the KVM console is launched using that management IP address. If no management IP address is associated in the service profile, then the system launches the KVM console using the physical server.

Recommendations for Using the KVM Console to Install a Server OS

To install an OS from a virtual CD/DVD or floppy drive, you must ensure that the virtual CD/DVD or floppy drive is set as the first boot device in the service profile.

Installing an OS using the KVM console may be slower than using the KVM dongle because the installation files must be downloaded across the network to the server. If you map a disk drive or disk image file from a network share to a virtual drive, the installation may be even slower because the installation files must be downloaded from the network to the KVM console (your computer) and then from the KVM console to the server. When using this installation method, we recommend that you have the installation media as close as possible to the system with the KVM console.

KVM Console for Cisco UCS B-Series M4, C-Series M4, and C-Series M5 Servers

Beginning with Cisco UCS Manager Release 4.1(1), the UCS Manager provides the KVM console to access and mange the vKVM sessions on Cisco UCS M4 and M5 servers.

The following menu and the menu options are available on this KVM Console:

Server Actions Menu

Choose the remote server operation you want to execute on the system.

Menu Item	Description
Boot Server	Powers on the system from the virtual console session.
Shutdown Server	Powers off the system from the virtual console session.
Reset	Resets the system from the virtual console session.

File Menu

Menu Item	Description
Capture to File button	Opens the **Save** dialog box that allows you to save the current screen as a JPG image. **Note** This option is only available on the **KVM** tab.

Menu Item	Description
Paste Text From Clipboard	Allows you to paste content from the clipboard.
Exit button	Closes the KVM console.

View Menu

Menu Item	Description
Refresh	Updates the console display with the server's current video output.
Full Screen	Expands the KVM console so that it fills the entire screen.

Macros Menu

Choose the keyboard shortcut you want to execute on the remote system.

Menu Item	Description
Static Macros menu	Displays a predefined set of macros.
User Defined Macros menu	Displays the user-defined macros that have been created.
Server Defined Macros menu	Displays the server defined macros that have been created.
Manage button	Opens the **Configure User Defined Macros** dialog box, which allows you to create and manage macros. System-defined macros cannot be deleted.

Tools Menu

Menu Item	Description
Session Options	Opens the **Session Settings** dialog box that lets you specify: • Scaling allows you to choose how the aspect ratio is displayed on the KVM screen. • This defines which mouse acceleration to use on the target system. The default is **Absolute Positioning**.
Session User List	Opens the **Session User List** dialog box that shows all the user IDs that have an active KVM session.
Chat	Opens group chat window for any admins logged into the current KVM session.
Virtual Keyboard	Opens an onscreen keyboard for the current KVM session.
Playback Controls	Opens a dialog box to select DVC recording files.

Virtual Media Menu

Name	Description
Activate Virtual Devices	Activates a vMedia session that allows you to attach a drive or image file from your local computer or network. **Note** If you have not allowed unsecured connections, you will be prompted to accept the session. If you reject the session, the virtual media session is terminated.
CD/DVD	Choose the CD/DVD that you want to access, and click the **Map Drive** button to map it to the host server device. **Note** If the **Read Only** checkbox is checked, the server cannot write to the vMedia device even if the device has write capability.
Removable Disk	Choose the removable disk that you want to access, and click the **Map Drive** button to map it to the host server device. **Note** If the **Read Only** checkbox is checked, the server cannot write to the vMedia device even if the device has write capability.
Floppy Disk	Choose the floppy that you want to access, and click the **Map Drive** button to map it to the host server device. **Note** If the **Read Only** checkbox is checked, the server cannot write to the vMedia device even if the device has write capability.

Online Help Menu

Name	Description
Contents and Index	Opens Online Help.
About KVM Viewer	Displays build version information about HTML5 KVM Viewer.

KVM Direct Access

KVM direct access allows the administrators that manage the blade and rack servers in your Cisco UCS Manager domain to access the KVM console for their servers directly using a web browser. This feature allows you to restrict access to the IP addresses of the fabric interconnects, while still allowing your administrators to access the KVM console for the servers they manage.

Until Cisco UCS Manager Release 4.0, only out-of-band IPv4 management interface addresses were supported for KVM direct access. Cisco UCS Manager Release 4.0 introduces KVM direct access support for inband IPv4 or IPv6 management interface addresses as well.

Note KVM direct access over Inband is supported on blade servers only.

KVM direct access over outband also supports custom applications from which users can navigate to a server management IP address without using the Cisco UCS Manager GUI interface or the KVM Launch Manager.

KVM direct access is supported by providing a management IP address assigned directly to the server or associated to the server with a service profile by the server's administrator. The server administrator enters the assigned inband or outband IP address into a browser, and navigates to the Cisco UCS KVM Direct login page. In the login page, the users enter their username and password, and, for outband address, may choose an authentication domain. When they launch Cisco UCS KVM Direct, the console for the server is displayed, the same way it would if they had accessed the server from the Cisco UCS Manager GUI. Next to the **Launch** button, you can select a list of available outband and inband addresses associated with the server.Beginning with Cisco UCS Manager Release 4.1(1), the KVM Console GUI is available only as an HTML5-based application. It is no longer available as a Java-based application.

KVM direct access over inband employs self-signed certificates for authentication. When users access a server management IP address or service profile IP address for the first time, a dialog box will be displayed to alert them that they need to add a certificate exception to their browser's cache.

The default communications service that supports Cisco UCS KVM direct access is HTTPS. This cannot be disabled. When a user enters a management IP in a browser using HTTP as part of the address, they will be automatically redirected to the HTTPS service.

To accommodate KVM direct access over outband, ensure that the CIMC Web Service communication service in Cisco UCS Manager is enabled.

Note The CIMC Web Service is enabled by default in Cisco UCS Manager.

KVM Direct Users

Cisco UCS Manager users with appropriate privileges can log into any blade server in the chassis through KVM direct over inband. To have login credentials specific to a blade server, you can use login privileges based on the IPMI profile associated with the blade server. These login privileges are:

- Read-Only—User does not have access to Host keyboard or mouse inputs, vMedia, Power Controls, or Macros.
- Admin—User has all privileges.

Starting the KVM Console from a Server

You can start multiple KVM Console sessions using the addresses assigned to the server.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Chassis** > *Chassis Number* > **Servers**.

Step 3 Choose the server that you want to access through the **KVM Console**.

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

Step 5 Scroll down to the **Actions** area and then click the >> button to the right of **KVM Console**.

The **KVM Console** opens in a separate window and displays a list of available outband and inband addresses associated with the server.

Note
If you click **KVM Console** and not the >> button, your session will be started using server addresses in the preferential order of inband IPv6 first, inband IPv4 second, and out-of-band IPv4 third.

Step 6 Choose an address from the **Select IP Address** list.

Addresses displayed as **(Inband)** access the server via the uplink ports and those displayed as **(Outband)** access the server via the management interface port.

Step 7 Click **OK**.

The KVM Console is launched using the address you selected.

Tip
If the **Caps Lock** key on your keyboard is on when you open a KVM session, and you subsequently turn off your **Caps Lock** key, the **KVM Console** may continue to act as if Caps Lock is turned on. To synchronize the KVM Console and your keyboard, press **Caps Lock** once without the **KVM Console** in focus and then press **Caps Lock** again with the **KVM Console** in focus.

Step 8 To start another KVM session for the same server, repeat steps 5 through 7.

Another KVM session is started. You can start up to six sessions for a server, depending on the number of addresses that have been configured for it.

Starting the KVM Console from a Service Profile

Procedure

Step 1 In the **Navigation** pane, click **Servers**.

Step 2 Expand **Servers** > **Service Profiles**.

Step 3 Expand the node for the organization which contains the service profile for which you want to launch the KVM console.

If the system does not include multi tenancy, expand the **root** node.

Step 4 Choose the service profile for which you need KVM access to the associated server.

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

Step 6 Scroll down to the **Actions** area then click the >> button to the right of **KVM Console**.

The **KVM Console** opens in a separate window and displays a list of available out-of-band and inband addresses associated with the server.

Note
If you click **KVM Console** and not the >> button, your session will be started using server addresses in the preferential order of inband IPv6 first, inband IPv4 second, and outband IPv4 third.

Step 7 Choose an address from the **Select IP Address** list.

Addresses displayed as **(Inband)** access the server via the uplink ports and those displayed as **(Outband)** access the server via the management interface port.

Step 8 Click **OK**.

The KVM Console is launched using the address you selected.

Tip
If the **Caps Lock** key on your keyboard is on when you open a KVM session, and you subsequently turn off your **Caps Lock** key, the **KVM Console** may continue to act as if Caps Lock is turned on. To synchronize the KVM Console and your keyboard, press **Caps Lock** once without the **KVM Console** in focus and then press **Caps Lock** again with the **KVM Console** in focus.

Step 9 To start another session for the same server, repeat steps 6 through 8.

Another KVM session is started. You can start up to six sessions for a server, depending on the number of addresses that have been configured for it.

Starting the KVM Console from the Cisco UCS KVM Direct Web Page

The Cisco UCS KVM Direct login page enables you to access a server directly from a web browser without logging in to Cisco UCS Manager.

Before you begin

To access the KVM console for a server using the Cisco UCS KVM Direct login page, you need the following:

- A Cisco UCS username and password.
- The server CIMC or service profile IPv4 outband or IPv4/IPv6 inband management address for the server you want to access.

Procedure

Step 1 In your web browser, type or select the web link for the management IP address of the server you want to access.

Step 2 If a **Security Alert** dialog box appears, click **Yes** to create a security exception.
The security exception is permanently stored in your browser's cache.

Step 3 In the Cisco UCS **KVM Direct** dialog box, specify the name, password, and domain.

Step 4 Click the **Lauch KVM** button to start HTML5 KVM. Next to the Launch button, you can select a list of available outband and inband addresses associated with the server.

Starting the KVM Console from the KVM Launch Manager

To access the KVM console for a server through the KVM Launch Manager, you need the following:

- Cisco UCS username and password.
- Name of the service profile associated with the server for which you want KVM access.

The KVM Launch Manager enables you to access a server through the KVM console without logging in to Cisco UCS Manager.

Procedure

Step 1 In your web browser, type or select the web link for Cisco UCS Manager GUI.

Example:

The default web link for HTTP access is `http://UCSManager_IP` for an IPv4 address, or `http://UCSManager_IP6` for an IPv6 address. The default web link for HTTPS access is `https://UCSManager_IP` for an IPv4 address, or `https://UCSManager_IP6` for an IPv6 address. In a standalone configuration, *UCSManager_IP* or *UCSManager_IP6* are the IPv4 or IPv6 addresses, respectively, for the management port on the fabric interconnect. In a cluster configuration, *UCSManager_IP* or *UCSManager_IP6* are the IPv4 or IPv6 addresses, respectively, assigned to Cisco UCS Manager.

Step 2 On the Cisco UCS Manager launch page, click **Launch KVM Manager**.

Step 3 If a **Security Alert** dialog box appears, click **Yes** to accept the security certificate and continue.

Step 4 On the **UCS - KVM Launch Manager Login** page, do the following:

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

Step 5 In the **Service Profiles** table of the KVM Launch Manager, do the following:

a) Locate the row containing the service profile and associated server for which you need KVM access.

b) In the **Launch KVM** column for that server, click **Launch**. Next to the Launch button, you can select a list of available outband and inband addresses associated with the server.

The KVM console opens in a separate window.

Tip
If the **Caps Lock** key on your keyboard is on when you open a KVM session, and you subsequently turn off your **Caps Lock** key, the **KVM Console** may continue to act as if Caps Lock is turned on. To synchronize the KVM Console and your keyboard, press **Caps Lock** once without the **KVM Console** in focus and then press **Caps Lock** again with the **KVM Console** in focus.

KVM Folder Mapping

KVM Folder Mapping is supported in UCS Manager 3.2(1). Folder mapping provides external file access to the KVM console through the HTML5 KVM interface for remote system updates. This feature is available for B-series and C-series servers with systems running Google Chrome version 57 and higher.

Procedure

Step 1 Start the KVM console.

Step 2 Click the **Create Image** button.

Step 3 Drag and drop any files into the Create Image dialog box.

Step 4 Click **Download ISO Image File** to create the ISO image. Only ISO images are available through the HTML5 KVM interface.

Step 5 Click the **Virtual Media** button, then select **Activate Virtual Devices**. Wait a few seconds for the virtual devices to load.

Step 6 Click the **Virtual Media** button, then select **CD/DVD**.

Step 7 Drag the new ISO file or a folder into the Virtual Disk Management dialog box then click **Map Drive**. The new files are now mapped to this KVM session for read only access.

KVM Certificate

Changing the KVM Certificate

You can use this procedure to change the KVM certificate to a user-generated public certificate.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number*** > **Servers**.

Step 3 Click the server for which you want to change the KVM certificate.

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

Step 5 Click the **CIMC** subtab.

Step 6 In the **Actions** area, click **Change KVM Certificate**:

Step 7 In the **Change KVM Certificate** dialog box, complete the following fields:

Field	Description
Certificate field	A user-generated public certificate.
Key field	The corresponding user-generated private key. **Note** Password protected X.509 certificate private key is not supported.

Step 8 Click **OK**.

Step 9 If a confirmation dialog box appears, click **Yes**.

This operation will result in a reboot of the CIMC

Clearing the KVM Certificate

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number*** > **Servers**.

Step 3 Click the server for which you want to clear the KVM certificate.

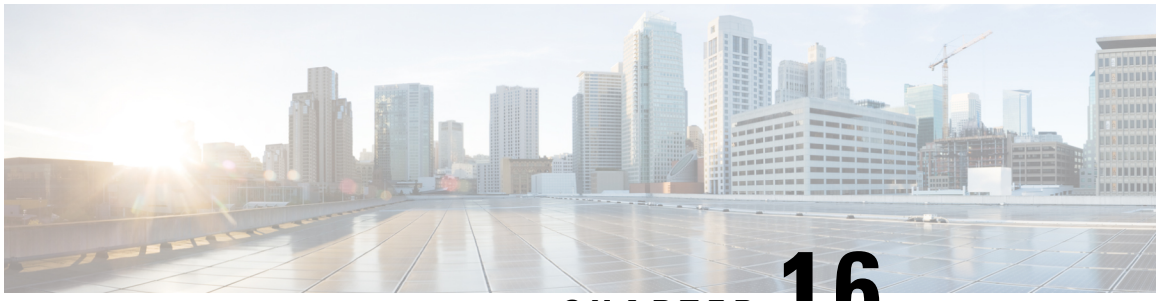
Step 4 In the **Work** pane, click the **Inventory** tab.

Step 5 Click the **CIMC** subtab.

Step 6 In the **Actions** area, click **Clear KVM Certificate**:

Step 7 In the **Clear KVM Certificate** dialog box, click **Yes**.

This operation will result in a reboot of the CIMC



CHAPTER 16

Cisco Intersight Management

- Intersight Management Mode, on page 173
- Device Connector, on page 173

Intersight Management Mode

Cisco Intersight™ is a management platform delivered as a service with embedded analytics for your Cisco and 3rd party IT infrastructure. Intersight Managed Mode (IMM) is a new architecture that manages the UCS Fabric Interconnected systems through a Redfish-based standard model. Intersight Managed Mode unifies the capabilities of the UCS Systems and the cloud-based flexibility of Intersight, thus unifying the management experience for the standalone and Fabric Interconnect attached systems. Intersight Management Model standardizes policy and operation management for UCSX-S9108-100G, UCS-FI-6454, UCS-FI-64108, UCS-FI-6536 and Cisco UCS B-Series (M5, M6), Cisco UCS C-Series (M5, M6, M7, M8), and Cisco UCS X-Series (M6, M7, M8) servers.

You can choose between the native UCSM Managed Mode (UMM) or Intersight Managed Mode (IMM) for the Fabric attached UCS Systems during initial setup of the Fabric Interconnects. If you choose to switch back between UMM and IMM, you must erase the present configuration and start from initial setup. Before erasing the configuration, you must ensure to unclaim the device from Intersight and decommission all rack servers.

Note For more information, see https://intersight.com/help/resources#intersight_managed_mode.

Device Connector

Device connector connects Cisco UCS Manager to Cisco Intersight, the cloud-hosted server management system. It enables Cisco UCS Manager to be managed and monitored through Cisco Intersight.

To register a device with Cisco Intersight in the cloud, you must do the following:

1. Connect Cisco UCS Manager with Cisco Intersight by configuring the device connector proxy settings, if they are required.
2. Use the device serial number and security code to validate your access to the device from Cisco Intersight and claim the device.

Enabling or Disabling Cisco Intersight Management

When you enable Cisco Intersight management, it establishes a bidirectional communication between the Intersight Cloud application and the device.

Before you begin

You must be an administrator to configure the device connector.

Procedure

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

Step 2 Expand **All** > **Device Connector**.

The **Device Connector** tab displays the connection status and the set access mode. The device ID and claim code displayed in the **Device Connector** tab is used in Cisco Intersight to claim Cisco UCS Manager.

Step 3 Click **Settings**.

Step 4 In the **Settings** wizard, click **General**.

Step 5 Enable the **Device Connector** slider to enable Intersight management or disable the **Device Connector** slider to disable Intersight management.

By default, the Cisco Intersight Management state is **Enabled**.

Step 6 Select the **Access Mode** as **Read-only** or **Allow Control**.

You cannot configure the device through Cisco Intersight when the **Read-only** access mode is selected. Therefore, any configuration that comes to the device connector through the cloud is rejected with an error code.

You have full control to configure the device through Cisco Intersight when the **Allow Control** mode is selected.

Step 7 To disable the Intersight management, disable the **Device Connector** slider.

When you disable the Intersight management, the **Device Connector** page displays the connection status as **Administratively Disabled**.

Step 8 Click **Save**.

Viewing Intersight Device Connector Properties

Procedure

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

Step 2 Expand **All** > **Device Connector**.

The **Device Connector** tab displays the connection status and the set access mode. The device ID and claim code displayed in the **Device Connector** tab is used in Cisco Intersight to claim Cisco UCS Manager.

Step 3 Click **Settings**.

Step 4 In the **Settings** wizard, review the following information:

Name	Description
General tab	The state of the connection between Cisco UCS Manager and Cisco Intersight. **Device Connector** slider— Allows you to enable or disable the Cisco Intersight management. You can do one of the following: • Turn on **Device Connector** slider—To enable Cisco Intersight management. You can claim this system and leverage the capabilities of Cisco Intersight. This is the default connection status. • Turn off **Device Connector** slider—To disable Cisco Intersight management. No communication will be allowed with Cisco Intersight. **Access Mode**—Configure access as **Read-only** or **Allow Control**. • **Read-only**—When the **Read-only** access mode is selected, you cannot configure the device through Intersight. • **Allow Control**—When the**Allow Control** access mode is selected, you have full control to configure the device through Intersight.
DNS Configuration tab	Configure the DNS Settings • **Domain name** field—Add a domain name. • **DNS Server** field—Configure at least one DNS server to enable DNS name resolution. The Intersight Device Connector must be able to successfully resolve DNS records. **Note** When the DNS settings is managed by a global policy in Cisco UCS Central, the DNS settings will be grayed. In such cases, update the DNS settings from Cisco UCS Central.

Name	Description
NTP Configuration tab	Configure the NTP Settings. Cisco strongly recommends configuring at least one NTP Server for time synchronization. If the system clock time is not synchronized with the Internet time, the Intersight device connector may be able to communicate with the Intersight service, as long as the time offset is not too large. If the time offset is outside the validity period of the Intersight X.509 Certificate, the device connector will not be able to communicate with the Intersight service. • **NTP Server** field—Configure at least one NTP server. **Note** When the NTP settings is managed by a global policy in Cisco UCS Central, the NTP settings will be grayed. In such cases, update the NTP settings from Cisco UCS Central.
Proxy Configuration tab	Whether HTTPS proxy settings are disabled or manually configured. This can be one of the following: • Turn off **Enable Proxy**—To disable the HTTPS proxy settings configuration. • Turn on**Enable Proxy**—To enable the HTTPS proxy settings configuration. • **Proxy Hostname/IP**—Enter the proxy hostname or IP address. • **Proxy Port**— Enter the proxy port number. • **Authentication**—Enable this option to authenticate access to the proxy server. Enter the **Username** and **Password** to authenticate access. **Note** The device connector does not mandate the format of the login credentials, they are passed as-is to the configured HTTP proxy server. Whether or not the username must be qualified with a domain name will depend on the configuration of the HTTP proxy server.

Name	Description
Certificate Manager tab	Allows you to view a list of trusted certificates and import a valid trusted certificate. • **Import**—Allows you to select and import a CA signed certificate. **Important** The imported certificate must be in the *.pem (base64 encoded) format. • You can view the list of certificates with the following information: • **Name**—Common name of the CA certificate • **In Use**—Whether the certificate in the trust store was used to successfully verify the remote server • **Issued By**—The issuing authority for the certificate • **Expires**—The expiry date of the certificate **Note** You cannot delete bundled certificates.

Step 5 Click **Close**.

Updating Device Connector

When you upgrade Cisco UCS Manager, the device connector is automatically updated to the image integrated with the Cisco UCS Manager version. The device connector does not get downgraded when you downgrade the Cisco UCS Manager version.

You can update the device connector through the Cisco Intersight GUI. You can also update the device connector through the local management shell in Cisco UCS Manager CLI.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **connect local-mgmt**	Enters local management mode.
Step 2	UCS-A(local-mgmt)# **copy** [*from-filesystem*:] [*from-path*] *filename to-path* [*dest-filename*]	Copies the device connector image file from a remote server to a local destination by using the specified file transfer protocol. You need to copy the file to one fabric interconnect only. • *from-filesystem*—The remote file system containing the file to be copied.

	Command or Action	Purpose
		This file system can be specified by using one of the following options: • **ftp:** [// [*username@*] *server*] • **scp:** [// [*username@*] *server*] • **sftp:** [// [*username@*] *server*] • **tftp:** [//*server* [:*port*]] If the file system is not specified, the current working file system is assumed. If a remote protocol is specified with no server name, you are prompted to enter the server name. • *from-path*—Absolute or relative path to the file to be copied. If no path is specified, the current working directory is assumed. • *filename*—The name of the source file to be copied. • *to-path*—Absolute or relative path to the copied file. If no path is specified, the current working directory is assumed. The path includes the local file system to contain the copied file. This file system can be specified from one of the following options: • **volatile:** • **workspace:** • *dest-filename*—The new name for the copied file. If a dest-filename is specified, the copied file is renamed at the destination location. **Note** You cannot download the device connector image file through Cisco UCS Manager GUI.
Step 3	UCS-A(local-mgmt)# **update-device-connector workspace:** | **volatile:**/*filename* [**skip-upgrade-on-peer**]	Updates the device connector image on the peer fabric interconnect and then the local fabric interconnect. Using the **skip-upgrade-on-peer** option skips update on the peer fabric interconnect.

Example

The following example updates the device connector on both fabric interconnects:

```
UCS-A# connect local-mgmt
UCS-A(local-mgmt)# copy scp://username@10.100.100.100/filepath/filename.bin workspace:/
UCS-A(local-mgmt)# update-device-connector workspace:/filename.bin
Update Started
Updating Device Connector on peer Fabric interconnect
Successfully updated device connector on peer Fabric interconnect
Updating Device Connector on local Fabric interconnect
Successfully updated device connector on local Fabric interconnect
UCS-A(local-mgmt)#
```

The following example updates the device connector on the local fabric interconnect only:

```
UCS-A# connect local-mgmt
UCS-A(local-mgmt)# copy scp://username@10.100.100.100/filepath/filename.bin workspace:/
UCS-A(local-mgmt)# update-device-connector workspace:/filename.bin skip-upgrade-on-peer
Update Started
Updating Device Connector on local Fabric interconnect
Successfully updated device connector on local Fabric interconnect
UCS-A(local-mgmt)#
```