Cisco UCS Central Installation and Upgrade Guide, Release 2.0

First Published: 2017-05-16

Last Modified: 2020-08-13

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

CONTENTS

Preface

Audience

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

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

Conventions

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

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

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

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

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

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

Warning IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS

Related Cisco UCS Documentation

Documentation Roadmaps

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

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

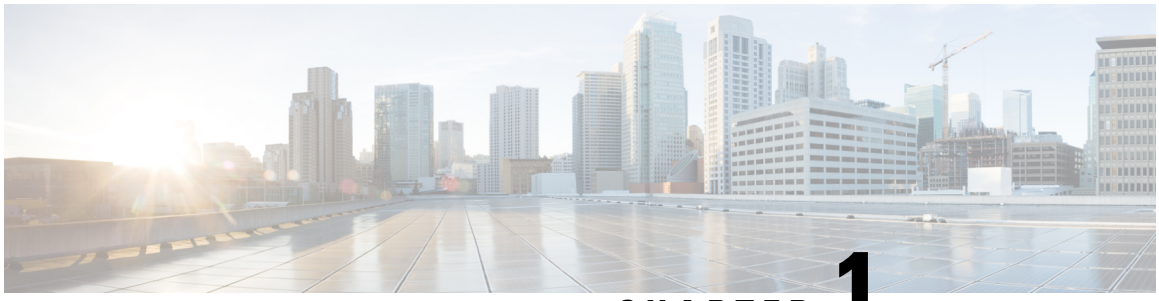
For information on supported firmware versions and supported UCS Manager versions for the rack servers that are integrated with the UCS Manager for management, refer to Release Bundle Contents for Cisco UCS Software.

Other Documentation Resources

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

Documentation Feedback

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



CHAPTER 1

Overview

This chapter includes the following sections:

Installing Cisco UCS Central, Release 2.0

You can install Cisco UCS Central, release 2.0 in the Standalone Mode.

The standalone installation enables you to install Cisco UCS Central on a virtual machine in the same way as the releases prior to release 1.3.

Upgrading Cisco UCS Central to Release 2.0

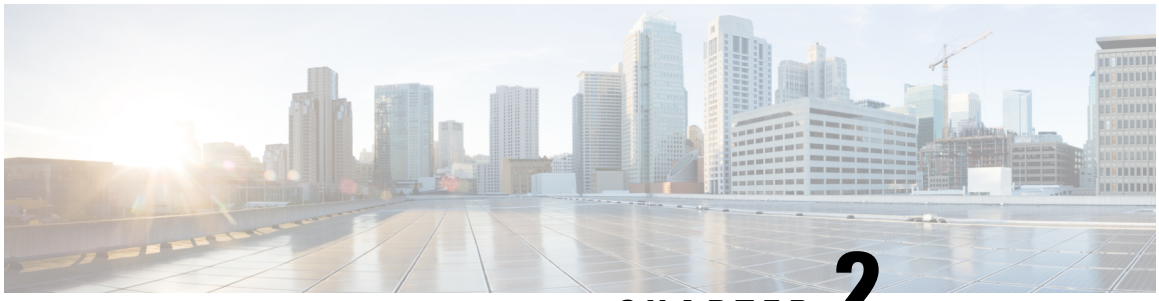
When you upgrade Cisco UCS Central to release 2.0, you can upgrade to a standalone mode.

Important Before upgrading Cisco UCS Central, make sure the registered domains are upgraded to the supported Cisco UCS Manager release version. Cisco UCS Central, release 2.0 requires Cisco UCS Manager, release 2.1(2) or newer. If you do not upgrade Cisco UCS Manager before upgrading Cisco UCS Central, any registered Cisco UCS domains will stop receiving updates from Cisco UCS Central after the upgrade.

Before upgrading Cisco UCS Central to 2.0 you must do the following:

- Make sure you have Cisco UCS Manager 2.1(2) or newer. It is recommended to upgrade Cisco UCS Manager to the latest version to ensure complete feature support.
- If you are planning to upgrade Cisco UCS Central from release 1.0, 1.1, 1.2, or 1.3, you must first upgrade to Cisco UCS Central 1.4 and then upgrade to release 2.0. To upgrade Cisco UCS Central release 1.0, 1.1, 1.2, or 1.3, see the appropriate installation guide at http://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-central-software/products-installation-guides-list.html.

For supported upgrade options, requirements and procedures, see Upgrading Cisco UCS Central to Release 2.0, on page 39.



CHAPTER 2

Introducing Cisco UCS Central 2.0

This chapter includes the following sections:

Overview of Cisco UCS Central 2.0 Features

Cisco UCS Central, release 2.0 allows you to take charge of the data center environment by delivering easy to use, integrated solution for managing Cisco UCS Domains from a single management point, both in data centers and remote management locations. With Cisco UCS Central 2.0, you can efficiently manage server, storage, and network policies and generate network traffic reports for your data center.

Note The flash-based user interface is deprecated, and is not supported in Cisco UCS Central.

Release 2.0(1a) supports the following new features:

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

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

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

Overview of Cisco UCS Central HTML 5 UI

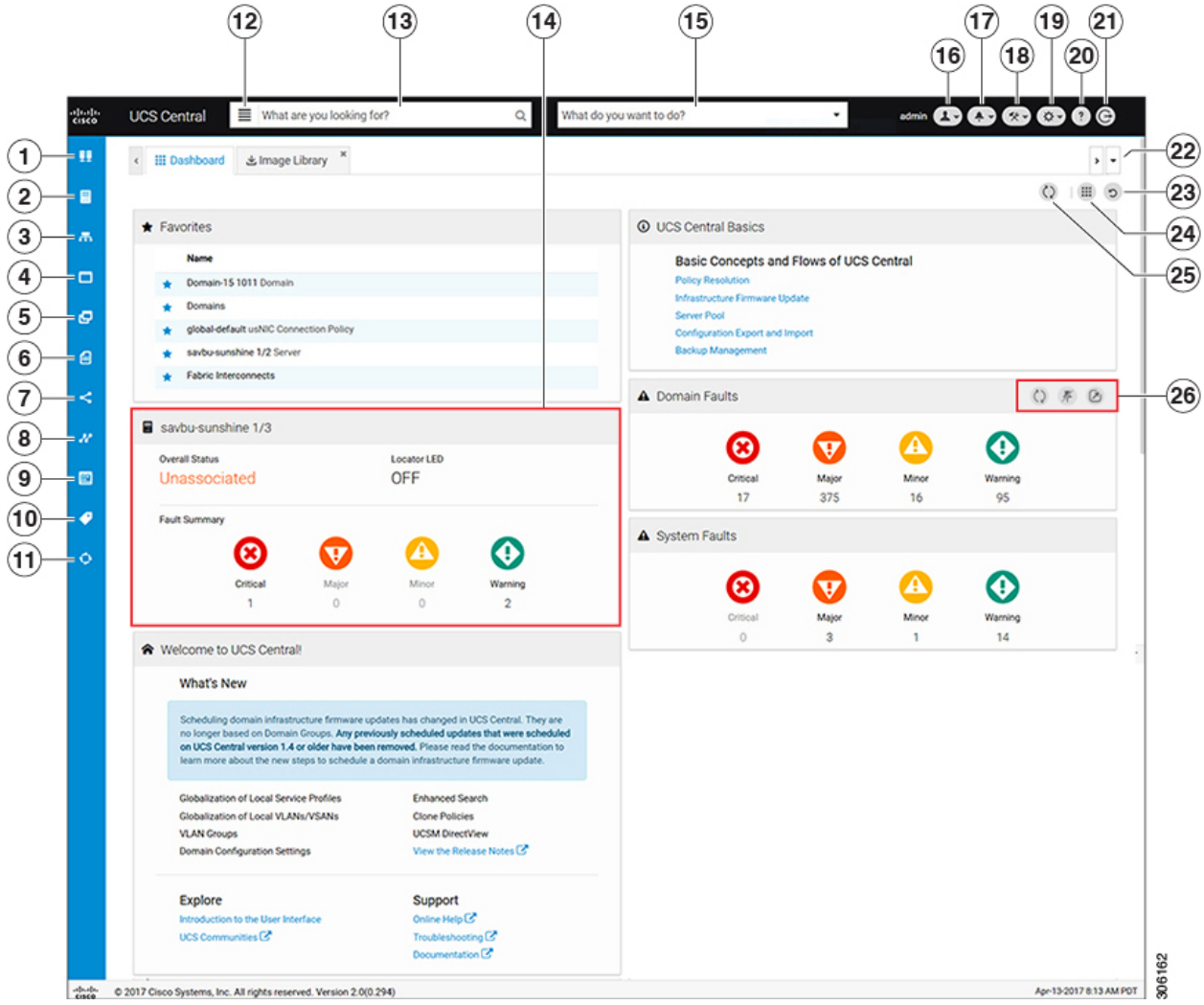
Cisco UCS Central HTML5 based user interface provides flexibility and task based usability for your management purposes.

The dashboard provides a quick overview of components in the system. You can pin the components you use frequently and customize the dashboard to suit your operational requirements. You can click on any object on the dashboard to go to the related page in the system.

Using the HTML5 UI

Dashboard

You can pin dashboard widgets and customize the dashboard based on your operational requirements. The following describes the basic dashboard structure, and the navigation icons, for performing management tasks:



Item	Description
1	Domain group navigation icon. Click to display domain group **root** and other domain groups in the system. You can click a domain group to launch the details page.
2	Browse Tables icon. Click to display physical and logical inventory-related entities in the system such as: **Equipment**, **Domains**, **Fabric Interconnects**, **Servers**, **Chassis**, **FEX**, **Hardware Components**. Click any of these entities to launch related pages and view details.
3	Organization navigation icon. Click to display org **root** and other sub organizations in the system. You can click the root, or any suborganization, to launch the details page for a selected organization.
4	Profiles icon. Click to display a list of **Service** and **Chassis** Profiles and their **Scope**, **Fault Level**, and the associated **Org**. Click to view corresponding Profile details.

Item	Description
5	Templates icon. Click to display templates available in Cisco UCS Central such as **Service Profiles**, **Chassis Profiles**, **vHBAs**, and **vNIC** templates.
6	Policies icon. Click to display all the policies available in Cisco UCS Central. Click to view details of a policy from the Policies table.
7	LAN and SAN icon. Click to view details of **VLANs**, **VLAN Groups** and **VSANs**.
8	Identifiers icon. Click to view details of Identifiers, Pools, and ID Universe.
9	Schedules icon. Click to view details of **Schedules** in the system, **Schedule Type, Start Date** and **Frequency**.
10	Tag Management icon. Click to view **Tags** and **Tag Types**. Click a Tag to view the **Tag Type, Multiple Tags Per Object, Value Type,** and **System-Based Tag**.
11	Globalization tasks icon. Click to view **Globalization Tasks**, **Globalization Type**, and the **Status** of the globalization operation.
12	Search Categories icon. Click to search for an item in a specific category.
13	Spotlight Search bar. Type the name of a Pool, Policy, Tag Type, VLAN, VSAN, Equipment, Template, Domain, or other objects in Cisco UCS Central. The search result displays the top 10 matches and also provides a list of potential matches to the search term.
14	Dashboard widget. You can pin any widget on this dashboard. When you mouse over on the widget, other options are enabled on the widget menu bar.
15	Actions bar. What do you want to do? You can Create, Schedule, Install, Export, and Import from here: • Click the drop-down arrow to display available actions. • Select a task, or type the task into the actions bar. • Launch the dialog box to perform the task.

Item	Description
16	**Profile Configuration** icon. Click to launch **User Profile**, or **Change Password**. You can perform the following actions: • In the Basic tab, set **Language** preference. • **Restore Tabs** to save the open tabs and access them directly when you back in to Cisco UCS Central. You can select one of the following options from the **Restore Tabs** drop-down menu: • **Prompt to restore tabs** • **Automatically restore tabs** • **Do not restore tabs** The **Prompt to Restore** Tabs option is enabled by default when you log in to Cisco UCS Central. If you select the Auto Restore option, the selected tabs are restored automatically when you log back in to Cisco UCS Central. You can set User Roles from the **Roles** tab and set Locales from the **Locales** tab.
17	System Alerts icon. Click to display and navigate to **Pending Activities, System Faults, Domain Faults, Events, Audit Logs, Core Dumps**, and **Internal Services**.
18	System Tools icon. Click to display and navigate to **Firmware Management, Backup & Restore, Export & Import, Tech Support, Image Library, Domain Management, Hardware Compatibility Reports, Unified KVM Launcher, Active Sessions,** and **Start Logging Session**.
19	System Configuration icon. Click to display and navigate to **System Profiles, System Policies, Users, Authentication, SNMP, Smart Call Home**, and **Licenses**.
20	Help icon. Click to access online help.
21	Log out icon. Click to log out from the active Cisco UCS Central session.
22	Tab navigator. Allows you to navigate through the open tabs, or close all tabs at once.
23	Log out icon. Click to log out from the active Cisco UCS Central session.
24	Dashboard widgets library icon. Click to view available widgets. Click the widget to pin it to the dashboard.
25	Refresh icon. Click to refresh the information in all pinned widgets or table pages.
26	**Refresh, Pin,** and **Show Detail** icons. Click to perform these actions for a widget.

Behavior Changes in Release 2.0

Deprecation Announcements

- Cisco UCS Central no longer includes the Flex-based UI. The HTML5 UI is the only graphical interface available.
- The Statistics Management feature is deprecated and is no longer supported in Cisco UCS Central.
- After March 3, 2017, Cisco UCS Central version 1.4 or earlier will be unable to fetch the updated firmware image list from Cisco.com. If you are running Cisco UCS Central version 1.4 or earlier, you can manually download firmware images directly from Cisco.com and import them to Cisco UCS Central. To continue to have Cisco UCS Central fetch the available image data from Cisco.com and place the firmware image in the **Image Library**, Cisco recommends that you upgrade to Cisco UCS Central release 1.5 or later.

Feature Support

Behavior Changes Based on Design

- The Spotlight search bar replaces the search bar, and allows you to search for profiles, policies, pools, VLANs/VSANs, templates, domains, orgs, domain groups etc by their names, descriptions, and labels. Spotlight auto-completes the search field with suggestions as you type and displays the top 10 potential matches to the term you type.
- Icons in the Sidebar navigation menu enable direct and easy access to all objects in Cisco UCS Central. Browse tables, Organization navigation, and Domain group navigation are now part of Sidebar navigation.
- From the Organizations tree view, you can directly navigate to that org's Profiles, Templates, Pools, Policies, and Permitted VLANs. The corresponding tab in the selected org is highlighted and opened when you click these objects.
- Cisco UCS Central 2.0 prevents you from deleting critical objects such as service profiles, domain groups, organizations, and service profile templates from the Cisco UCS Central GUI and the command line. When you attempt to delete any of these items from Cisco UCS Central, an error message with the potential impact displays.
- You must create the global service profile template before you can create a service profile.
- vNIC and vHBA Placement is now referred to as Interface Placement.
- Registration Policy is now referred to as Domain Group Qualification Policy.
- ID Range Qualification Policy is now referred to as ID Range Access Control Policy.
- There are no qualified IP addresses for ID Range Access Control Policy.
- Only the configuration export (all-config) and backup (full-state) options are used in Cisco UCS Central. Other backup types such as config logical and config system are not supported.

Multi-version Management Support

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

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

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

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

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

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

Supported Features in Cisco UCS Manager

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

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

Management Exclusion

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

- **Global service profile deployment**: If you deploy global service profile on a server pool, and you have disabled global service profile deployment in one of the servers in the pool, Cisco UCS Central excludes the server from the global service profile deployment.

- **In band management**: A service profile with inband management capability will not be deployed on the servers where you have excluded inband management feature.
- **Policy mapping**: This will disable importing policies or policy components from this Cisco UCS domain into Cisco UCS Central.
- **Remote management**: This will restrain controlling physical devices in a Cisco UCS domain from Cisco UCS Central.

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

Feature Support Matrix

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

Note Some features are built in Cisco UCS Central to be compatible with upcoming Cisco UCS Manager releases.

Feature Support for Release 2.0

Cisco UCS Central Features	Supported Cisco UCS Central Versions	Supported Cisco UCS Manager Versions			
		2.1	2.2	3.0	3.1 /3.2/4.0
Support for Second RAID Controller in the IO Expander on Cisco UCS S3260 Storage Server (UCS-C3K-M4RAID)	2.0(1a)	No	No	No	3.1(3) and later
Support for Dual HBA Controller on Cisco UCS S3260 Storage Server (UCS-S3260-DHBA)	2.0(1a)	No	No	No	3.1(3) and later
Support for Dual SIOC	2.0(1a)	No	No	No	3.1(3) and later
Globalization of Service Profiles	2.0(1a)	No	2.2(8f)	No	3.1(2) and later
BIOS Asset Tag	2.0(1a)	No	No	No	3.1(3) and later

Cisco UCS Central Features	Supported Cisco UCS Central Versions	Supported Cisco UCS Manager Versions			
		2.1	2.2	3.0	3.1 /3.2/4.0
Hot patching/ Lightweight Upgrades	2.0(1a)	No	No	No	3.1(3) and later
User-Defined Zone Profiles	2.0(1a)	No	No	No	3.1(3) and later
Integrated Server Diagnostics	2.0(1a)	No	No	No	3.1(3) and later
SED Security Policies, Smart SSD, and KMIP Support	2.0(1a)	No	No	No	3.1(3) and later
Automatic Configuration of FI-Server Ports	2.0(1a)	No	No	No	3.1(3) and later
Set KVM IP on physical servers	2.0(1a)	No	No	No	3.1(3) and later
Fabric Evacuation in Firmware Auto Install	2.0(1a)	No	No	No	3.1(3) and later
Direct Fabric Interconnect Evacuation	2.0(1a)	No	2.2(4) and later	No	3.1(1) and later
Launch HTML5 KVM Client	2.0(1a)	No	No	No	3.1(3) and later
Multicast Policy	2.0(1a)	No	No	No	3.1(3) and later
Power Sync Policy	2.0(1a)	No	2.2(8)	No	3.1(2) and later
Statistics Threshold Policy	2.0(1a)	No	No	No	3.1(3) and later
Graphics Card Policy	2.0(1a)	No	No	No	3.1(3) and later
QoS System Class	2.0(1a)	No	No	No	3.1(3) and later
Hardware Change Discovery Policy	2.0(1a)	No	No	No	3.1(3) and later
Port Auto-Discovery Policy	2.0(1a)	No	No	No	3.1(3) and later

Cisco UCS Central Features	Supported Cisco UCS Central Versions	Supported Cisco UCS Manager Versions			
		2.1	2.2	3.0	3.1 /3.2/4.0
KMIP Certification Policy	2.0(1a)	No	No	No	3.1(3) and later
Server Reboot Logs	2.0(1a)	No	No	No	3.1(3) and later
Delete Decommissioned Rack Server, Chassis, FEX	2.0(1a)	Yes	Yes	No	3.1(1) and later
VLAN Group	2.0(1b)	No	No	No	3.1(2) and later

Feature Support for Release 1.5

Cisco UCS Central Features	Supported Cisco UCS Central Versions	Supported Cisco UCS Manager Versions			
		2.1	2.2	3.0	3.1
Cisco UCS S3260 Storage Server support	1.5(1a)	No	No	No	3.1(2) and later
vNIC/vHBA pairing	1.5(1a)	No	2.2(7) and later	No	3.1(2) and later
Traffic monitoring	1.5(1a)	No	2.2(7) and later	No	3.1(1) and later
UUID sync	1.5(1a)	No	2.2(7) and later	No	3.1(2) and later
Admin host port for PCI placement	1.5(1a)	No	No	No	3.1(1e) and later
Support for 160 LDAP group maps	1.5(1a)	No	2.2(8) and later	No	3.1(2) and later

Feature Support for Release 1.4

Cisco UCS Central Features	Supported Cisco UCS Central Versions	Supported Cisco UCS Manager Versions				
		2.1	2.2	2.5	3.0	3.1
Port Configuration	1.4(1a)	No	2.2(7) and later	No	No	3.1(1) and later

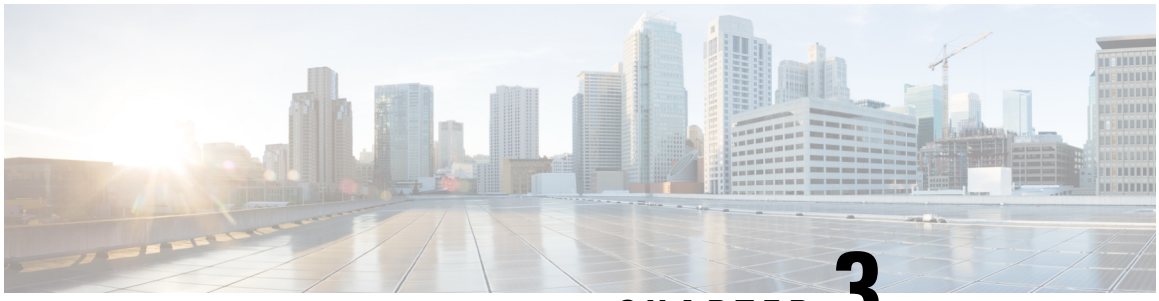
Cisco UCS Central Features	Supported Cisco UCS Central Versions	Supported Cisco UCS Manager Versions				
		2.1	2.2	2.5	3.0	3.1
Advanced Local Storage Configuration	1.4(1a)	No	2.2(7) and later	2.5(1) and later	No	3.1(1) and later
Multiple LUNs in Boot Policy	1.4(1a)	No	2.2(7) and later	2.5(1) and later	No	3.1(1) and later
Consistent Device Naming	1.4(1a)	No	2.2(4) and later	2.5(1) and later	3.0(1) and later	3.1(1) and later
Direct-Attached Storage/FC Zoning	1.4(1a)	No	2.2(7) and later	No	No	3.1(1) and later
Advanced Host Firmware Pack	1.4(1a)	No	2.2(6) and later	No	No	3.1(1) and later
usNIC Connection Policy	1.4(1a)	No	2.2(6) and later	No	No	3.1(1) and later
VMQ Connection Policy	1.4(1a)	No	2.2(6) and later	No	No	3.1(1) and later
Equipment Policies	1.4(1a)	No	2.2(7) and later	No	No	3.1(1) and later
Maintenance Policy on Next Reboot	1.4(1a)	No	No	No	No	3.1(1) and later

Feature Support for Release 1.3 and earlier

Cisco UCS Central Features	Supported Cisco UCS Central Versions	Supported Cisco UCS Manager Versions				
		2.1	2.2	2.5	3.0	3.1
Multi-version management support and viewing supported Cisco UCS Manager features	1.1(2a)	No	2.2(1b) and later	2.5(1a) and later	3.0(1c) and later	3.1(1a) and later
Importing policy/policy component and resources		No	2.2(1b) and later	2.5(1a) and later	3.0(1c) and later	3.1(1a) and later
Specifying remote location for backup image files		No	2.2(2b) and later	2.5(1a) and later	3.0(1c) and later	3.1(1a) and later
3rd party certificate		No	2.2(2c) and later	2.5(1a) and later	3.0(1c) and later	3.1(1a) and later
IPv6 inband management support		No	2.2(2c) and later	2.5(1a) and later	3.0(1c) and later	3.1(1a) and later
Estimate Impact on Reconnect	1.2(1a)	No	2.2(3a) and later	2.5(1a) and later	3.0(1c) and later	3.1(1a) and later
Precision Boot Order Control		No	2.2(1b) and later	2.5(1a) and later	3.0(1c) and later	3.1(1a) and later
Scriptable vMedia	1.2(1e) and later	No	2.2(2c) and later	2.5(1a) and later	3.0(2c) and later	3.1(1a) and later

Note

- Searching for policy/policy components or resources is supported in Cisco UCS Manager, releases 2.1(2x) and 2.1(3x). To import policies, you must have Cisco UCS Manager, releases 2.2(1b) or higher.
- For precision boot order control, the blade server must have CIMC version 2.2(1b) or above.



CHAPTER 3

Installation Prerequisites

This chapter includes the following sections:

Supported Browsers

To access the Cisco UCS Central GUI, your computer must meet or exceed the following minimum system requirements:

- Windows
  - Internet Explorer 11 and above
  - Firefox 45.0.2 and above
  - Chrome 49 and above
- Linux RHEL
  - Firefox 45.0.2 and above
  - Chrome 49 and above
- MacOS
  - Firefox 45.0.2 and above
  - Chrome 49 and above
  - Safari 9.0.3 and above

Supported Operating Systems

The released ISO is supported by the following:

- VMWare ESXi 5.x, ESXi 6.x and ESXi 7.x
- Microsoft Hyper-V Server 2012 R2, Microsoft Hyper-V Server 2016, Microsoft Hyper-V Server 2019
- KVM Hypervisor on Redhat Enterprise Linux 6.5, 6.8, 7.2, 7.3, and 7.4

The released OVA is supported by VMWare ESXi 5.x, and ESXi 6.x.

Required Ports

Cisco UCS Manager communicates with Cisco UCS Central using the individual IP addresses of the FIs (FI-A or FI-B IP address) as the source destination. Cisco UCS Central communicates back to Cisco UCS Manager using the VIP as the destination address.

Communication between Cisco UCS Central and Cisco UCS Domain

Typically, the IP addresses for all existing Cisco UCS Management domains exist on a common administrative network. If this is not the case, Cisco UCS Central will work, provided that routing access is assured from Cisco UCS Central to all subordinate management domains. For this reason, care must be taken to ensure that any firewalls, proxies, and other security systems are configured to permit read/write access on the following ports for continuous communications between Cisco UCS Central and all registered Cisco UCS domains.

The ports listed in the following tables need to be opened on Cisco UCS Central. These ports are accessed by UCS domains.

Note Depending on the version and UI that you are using, some ports may not be necessary. For example, NFS ports are not required for Cisco UCS Manager release 2.2(2) and above.

Table 1: Ports required for Cisco UCS Manager release versions 2.1(x) and 2.2(1) and below.

Port Number	Daemon	Protocol	Usage
32803	LOCKD_TCPPORT	TCP/UDP	Linux NFS lock
892	MOUNTD_PORT	TCP/UDP	Linux NFS mount
875	RQUOTAD_PORT	TCP/UDP	Linux remote quota server port (NFS)
32805	STATD_PORT	TCP/UDP	Linux lock recovery - used by NFS file locking service
2049	NFS_PORT	TCP/UDP	Linux NFS listening port
111	SUNRPC	TCP/UDP	Linux RCPBIND listening port (NFS)
443	HTTPS_PORT	TCP/UDP	Enable communication through firewall from Cisco UCS Central to Cisco UCS Domain(s) and UCS Central GUI

Port Number	Daemon	Protocol	Usage
80	HTTP	TCP	Communication from Cisco UCS Central to UCS domains with the Flash UI. This port can be configured using the Cisco UCS Central CLI. **Note** This port is not required if you are using the Cisco UCS Manager HTML5 UI.

Table 2: Ports required for Cisco UCS Manager release versions 2.2(2) and above, including UCS Mini, Cisco UCS Manager 3.0(1) or 3.0(2).

Port Number	Daemon	Protocol	Usage
443	HTTPS_PORT	TCP/UDP	Enable communication from Cisco UCS Central to Cisco UCS Domain(s) and the UCS Central GUI.
80	HTTP	TCP	Communication from Cisco UCS Central to UCS domains with the Flash UI. This port can be configured using the Cisco UCS Central CLI. **Note** This port is not required if you are using the Cisco UCS Manager HTML5 UI.

Communication between Cisco UCS Central and Client browser

The following ports must be open on Cisco UCS Manager. The ports are accessed by Cisco UCS Central to enable communication between Cisco UCS Central and the client browser:

Port Number	Daemon	Protocol	Usage
443	HTTPS_PORT	TCP	Enable communication from Cisco UCS Central to UCS domains. This port is always required.

AD Server Communication

The LDAP port 389 must be open on the AD server. This port is accessed by Cisco UCS Central for MS AD LDAP integration and communication.

Note Cisco UCS Central uses STARTTLS for supporting LDAP over SSL/TLS. Port 389 is the only port required.

System Requirements

Standalone Installation

If you are installing Cisco UCS Central in a standalone mode, make sure you have the following system requirements.

Server Type

We recommend that you deploy Cisco UCS Central on a VMware or Hyper-V hypervisor running on standalone rack server(s) that is not managed by Cisco UCS Manager or integrated into a Cisco UCS domain. The server must have a high-speed data store, preferably one provisioned from a high-speed storage array.

Server Requirements

The following table describes the minimum requirements for installing Cisco UCS Central in the following platforms:

- ESX
- Hyper-V
- KVM Hypervisor

Item	Minimum Requirements for EXS, Hyper-V and KVM Hypervisor
Disk 1	40 GB
Disk 2	40 GB
RAM	12 GB 32 GB for large scale
vCPU cores	4 cores
Disk read speed	> 75 MBps >125 MBps is the recommended speed.

Note

- If you want to manage more servers, for example 500 domains/10000 servers, make sure to increase RAM to at least 32 GB.
- Performance of Cisco UCS Central is not guaranteed if you deploy it on a server that does not meet the minimum requirements for vCPU, RAM or Disk Speed.
- Make sure to power off before making any changes to the VM settings.
-

If the disk read speed on the server is lower than the required minimum during the deployment of Cisco UCS Central, the installer displays a warning message but you can complete the deployment. However, if the disk

read speed is lower than the required minimum during operation, Cisco UCS Central raises a fault, as shown in the following table, depending upon how low the disk read speed is:

Disk Read Speed on Server	Fault Level
<75 MBps	Critical fault
75 to 100 MBps	Major fault
100 to 125 MBps	Minor fault
>125 MBps	N/A

Supported Database Servers

The following are the supported database servers for statistics collection:

- Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - 64-bit Production or higher
- PostgreSQL Server 9.1.8 64-bit or higher
- Microsoft SQL Server 2012 (SP1) - 11.0.3000.0 (X64) or higher
- Microsoft SQL Server 2008 R2 10.50.1600.1 (X64) SP1 or higher

When the statistics data is stored in external database server, consider the following as a reference data for disk space requirements on the database server:

- If you register 20 Cisco UCS domains , the minimum storage space required to store statistics data for 1 year would be 400 GB.
- If you register 100 Cisco UCS domains , the minimum storage space required to store statistics data for 1 year would be 2 TB.

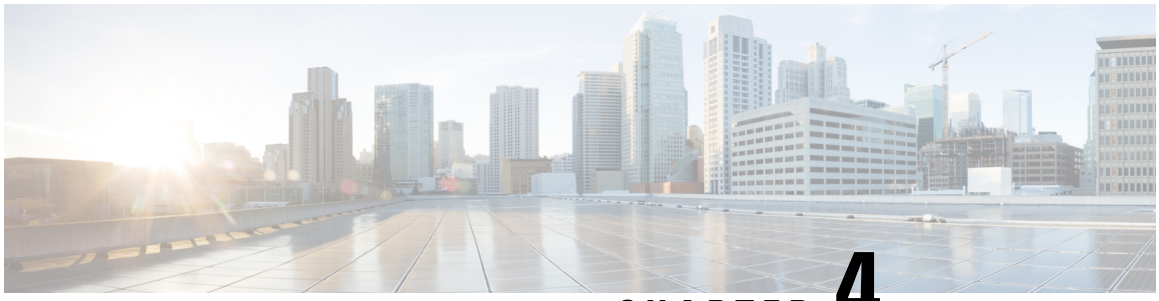
Client System

The minimum memory required for client system is 4 GB. However if you have 40 or more registered Cisco UCS Domains, it is recommended to have at least 8 GB memory on the client system.

Managing Cisco UCS Domains in Remote Locations

To manage Cisco UCS domains in remote locations such as remote branch offices, the following are the minimum requirements for network connectivity between Cisco UCS domain and Cisco UCS Central:

- Bandwidth - 1.5 Mbps or higher
- Latency - 500 ms (round trip) or lower



CHAPTER 4

Installing Cisco UCS Central

This chapter includes the following sections:

Overview of Installation

Cisco UCS Central provides you the option to install in a standalone mode. You must obtain the software from Cisco.com and save it in your local drive before installation.

You can install Cisco UCS Central using either one of the following:

- OVA file
- ISO Image

Obtaining the Cisco UCS Central Software from Cisco.com

Before you begin

Make sure that you have your Cisco.com username and password ready to be able to successfully download the Cisco UCS Central software.

Procedure

Step 1 In a web browser, navigate to Cisco.com.

Step 2 Under **Support**, click **All Downloads**.

Step 3 In the center pane, click **Unified Computing and Servers**.

Step 4 If prompted, enter your Cisco.com username and password to log in.

Step 5 In the right pane, click the link for the Cisco UCS Central software in the format that you want.

You can download the Cisco UCS Central software in the following formats:

- An OVA file with a name such as `ucs-central.2.0.1a.ova`
- An ISO file with a name such as `ucs-central.2.0.1a.iso`

You can also download the admin password reset ISO image from this location.

Step 6 On the page from which you download the software, click the **Release Notes** link to download the latest version of the Release Notes.

Step 7 Click the link for the release of the Cisco UCS Central software that you want to download.

Step 8 Click one of the following buttons and follow the instructions provided:

- **Download Now**—Allows you to download the Cisco UCS Central software immediately.
- **Add to Cart**—Adds the Cisco UCS Central software to your cart to be downloaded at a later time.

Step 9 Follow the prompts to complete your download of the software.

Step 10 Read the Release Notes before deploying the Cisco UCS Central VM.

Installing Cisco UCS Central in Standalone Mode

You can install Cisco UCS Central through either the OVA file or ISO Image in standalone mode.

Installing the Cisco UCS Central OVA File in VMWare

Note After the Cisco UCS Central VM starts up for the first time, it performs a one-time initial configuration process. Allow this process to complete before you log in.

Procedure

Step 1 Save the Cisco UCS Central OVA file to a folder that you can access from the hypervisor.

Step 2 From the VMware Virtual Center Console, choose **File** > **Deploy OVF Template**.

Step 3 Deploy the OVA file by choosing the ESX host on which you want to host the Cisco UCS Central VM.

Follow the steps to boot VM and wait until the process is 100% complete to proceed to the next step.

Step 4 If have not powered up the VM as part of importing the OVA file , power up the Cisco UCS Central VM.

Step 5 Open up a console window for the Cisco UCS Central VM.

Step 6 When the Cisco UCS Central VM has completed the initial part of the installation process, answer the following questions in the VM console window:

a) `Setup new configuration or restore full-state configuration from backup [setup/restore]` prompt, enter **`setup`** and press **`Enter`**.

b) At the `Enter the UCS Central VM eth0 IPv4 Address :` prompt, enter the IP address assigned to Cisco UCS Central and press **`Enter`**.

You must enter a static IP address that is reserved for this Cisco UCS Central VM. Cisco UCS Central does not support Dynamic Host Configuration Protocol (DHCP).

c) At the `Enter the UCS Central VM eth0 IPv4 Netmask :` prompt, enter the netmask assigned to Cisco UCS Central and press **Enter**.

d) At the `Enter the Default Gateway :` prompt, enter the default gateway used by Cisco UCS Central and press **Enter**.

e) At the `Is this VM part of a cluster(select 'no' for standalone) (yes/no)` prompt, select no and press **Enter**.

f) At the `Enter the UCS Central VM host name :` prompt, enter the host name you want to use for the Cisco UCS Central VM and press **Enter**.

g) (Optional) At the `Enter the DNS Server IPv4 Address :` prompt, enter the IP address for the DNS server you want to use for Cisco UCS Central and press **Enter**.

If you do not plan to use a DNS server for Cisco UCS Central, leave this blank and press **Enter**.

h) (Optional) At the `Enter the Default Domain Name :` prompt, enter the domain in which you want to include Cisco UCS Central and press **Enter**.

If you do not plan to include Cisco UCS Central in a domain, leave this blank and press **Enter**. Cisco UCS Central will use the default domain named localdomain.

i) At the `Enforce Strong Password(Yes/No)` prompt, if you want to set up strong password alert, select yes and press **Enter**.

j) At the `Enter the admin Password :` prompt, enter the password you want to use for the admin account and press **Enter**.

k) At the `Confirm admin Password :` prompt, re-enter the password you want to use for the admin account and press **Enter**.

l) At the `Enter the Shared Secret :` prompt, enter the shared secret (or password) that you want to use to register one or more Cisco UCS domains with Cisco UCS Central and press **Enter**.

m) At the `Confirm Shared Secret :` prompt, re-enter the shared secret and press **Enter**.

n) At the `Proceed with this configuration. Please confirm[yes/no]` prompt, enter **yes** and press **Enter**.

If you think you made an error when completing any of these steps, enter **no** and press **Enter**. You will then be prompted to answer the questions again.

After you confirm that you want to proceed with the configuration, the network interface reinitializes with your settings and Cisco UCS Central becomes accessible via the IP address.

Installing Cisco UCS Central ISO File in VMware

Note For VMware, we recommend that you install from the OVA file. Installing from the ISO file works with limitations. See https://tools.cisco.com/bugsearch/bug/CSCuv32055 for more information.

Procedure

Step 1 Create a VM with the following settings:

Setting	Recommended Value
Configuration	Custom configuration
Name	A descriptive name that includes information about the Cisco UCS Central deployment
Virtual machine type	7 or later
Guest operating system	A supported operating system, such as Linux RHEL 5.0(64-bit)
Number of vCPU	4
Memory	No less than 12GB
Virtual adapter	1 virtual adapter with VM network
SCSI controller	LSI Logic parallel
Virtual disk	No less than 40GB of available disk space You also need to create a second 40 GB virtual disk in Step 2.
Advanced options	Virtual device node SCSI

Step 2 In **Edit Settings**, add a new hard disk for the VM with no less than 40GB of available disk space for Standalone Installations and an additional 40GB for remote disk Cluster Installations.

Step 3 From the **Options** menu, do the following:

a) Check **Force BIOS Setup** to change the boot options.
b) Specify **Power on Boot Delay**.
c) Check **Failed Boot Recovery**.

Step 4 Mount the Cisco UCS Central ISO image to the CD/DVD drive.

Step 5 Start the VM and connect to the console.

Step 6 From the **Cisco UCS Central Installation** menu on the ISO image, choose **Install Cisco UCS Central**.

The Cisco UCS Central installer checks that the VM has the required RAM and disk space (two disks, both disks should be 40GB). If the VM meets the requirements, the installer formats the disks, transfers the files, and installs Cisco UCS Central.

Step 7 When the Cisco UCS Central VM has completed the initial part of the installation process, answer the following questions in the VM console window:

a) `Setup new configuration or restore full-state configuration from backup [setup/restore]` prompt, enter **`setup`** and press **`Enter`**.
b) At the `Enter the UCS Central VM eth0 IPv4 Address :` prompt, enter the IP address assigned to Cisco UCS Central and press **`Enter`**.

You must enter a static IP address that is reserved for this Cisco UCS Central VM. Cisco UCS Central does not support Dynamic Host Configuration Protocol (DHCP).

c) At the `Enter the UCS Central VM eth0 IPv4 Netmask :` prompt, enter the netmask assigned to Cisco UCS Central and press **Enter**.

d) At the `Enter the Default Gateway :` prompt, enter the default gateway used by Cisco UCS Central and press **Enter**.

e) At the `Is this VM part of a cluster(select 'no' for standalone) (yes/no)` prompt, select no and press **Enter**.

f) At the `Enter the UCS Central VM host name :` prompt, enter the host name you want to use for the Cisco UCS Central VM and press **Enter**.

g) (Optional) At the `Enter the DNS Server IPv4 Address :` prompt, enter the IP address for the DNS server you want to use for Cisco UCS Central and press **Enter**.

If you do not plan to use a DNS server for Cisco UCS Central, leave this blank and press **Enter**.

h) (Optional) At the `Enter the Default Domain Name :` prompt, enter the domain in which you want to include Cisco UCS Central and press **Enter**.

If you do not plan to include Cisco UCS Central in a domain, leave this blank and press **Enter**. Cisco UCS Central will use the default domain named localdomain.

i) At the `Enforce Strong Password(Yes/No)` prompt, if you want to set up strong password alert, select yes and press **Enter**.

j) At the `Enter the admin Password :` prompt, enter the password you want to use for the admin account and press **Enter**.

k) At the `Confirm admin Password :` prompt, re-enter the password you want to use for the admin account and press **Enter**.

l) At the `Enter the Shared Secret :` prompt, enter the shared secret (or password) that you want to use to register one or more Cisco UCS domains with Cisco UCS Central and press **Enter**.

m) At the `Confirm Shared Secret :` prompt, re-enter the shared secret and press **Enter**.

n) At the `Proceed with this configuration. Please confirm[yes/no]` prompt, enter **yes** and press **Enter**.

If you think you made an error when completing any of these steps, enter **no** and press **Enter**. You will then be prompted to answer the questions again.

Step 8 Unmount the Cisco UCS Central ISO image from the virtual CD/DVD drive.

Step 9 Reboot the Cisco UCS Central VM.

Installing Cisco UCS Central ISO File in Microsoft Hyper-V

Procedure

Step 1 Create a VM with the following settings:

Setting	Recommended Value
Name	A descriptive name that includes information about the Cisco UCS Central deployment
RAM	No less than 12GB
Network adapter	Default
Number of vCPU	4
Virtual disk	No less than 40GB of available disk space You also need to create a second 40GB virtual disk under IDE Controller in Step 3.

Step 2 In the settings for the VM, do the following:

a) Delete the default network adapter.
b) Create a new legacy network adapter.
c) Click **Apply**.

Step 3 Under the same IDE controller as the first virtual drive, create a second virtual drive for the VM with no less than 40GB of available disk space.

Step 4 In the **VM settings** > **Management** > **Integration Services**, uncheck **Time synchronization** to disable it.

Step 5 Mount the Cisco UCS Central ISO image to the CD/DVD drive.

Step 6 Start the VM and connect to the console.

Step 7 From the **Cisco UCS Central Installation** menu on the ISO image, choose **Install Cisco UCS Central**.

The Cisco UCS Central installer checks that the VM has the required RAM and disk space (two disks, both with 40GBs). If the VM meets the requirements, the installer formats the disks, transfers the files, and installs Cisco UCS Central.

Step 8 When the Cisco UCS Central VM has completed the initial part of the installation process, answer the following questions in the VM console window:

a) `Setup new configuration or restore full-state configuration from backup [setup/restore]` prompt, enter **`setup`** and press **`Enter`**.
b) At the `Enter the UCS Central VM eth0 IPv4 Address :` prompt, enter the IP address assigned to Cisco UCS Central and press **`Enter`**.

   You must enter a static IP address that is reserved for this Cisco UCS Central VM. Cisco UCS Central does not support Dynamic Host Configuration Protocol (DHCP).

c) At the `Enter the UCS Central VM eth0 IPv4 Netmask :` prompt, enter the netmask assigned to Cisco UCS Central and press **`Enter`**.
d) At the `Enter the Default Gateway :` prompt, enter the default gateway used by Cisco UCS Central and press **`Enter`**.
e) At the `Is this VM part of a cluster(select 'no' for standalone) (yes/no)` prompt, select no and press **`Enter`**.
f) At the `Enter the UCS Central VM host name :` prompt, enter the host name you want to use for the Cisco UCS Central VM and press **`Enter`**.
g) (Optional) At the `Enter the DNS Server IPv4 Address :` prompt, enter the IP address for the DNS server you want to use for Cisco UCS Central and press **`Enter`**.

If you do not plan to use a DNS server for Cisco UCS Central, leave this blank and press **Enter**.

h) (Optional) At the `Enter the Default Domain Name :` prompt, enter the domain in which you want to include Cisco UCS Central and press **Enter**.

If you do not plan to include Cisco UCS Central in a domain, leave this blank and press **Enter**. Cisco UCS Central will use the default domain named localdomain.

i) At the `Enforce Strong Password(Yes/No)` prompt, if you want to set up strong password alert, select yes and press **Enter**.
j) At the `Enter the admin Password :` prompt, enter the password you want to use for the admin account and press **Enter**.
k) At the `Confirm admin Password :` prompt, re-enter the password you want to use for the admin account and press **Enter**.
l) At the `Enter the Shared Secret :` prompt, enter the shared secret (or password) that you want to use to register one or more Cisco UCS domains with Cisco UCS Central and press **Enter**.
m) At the `Confirm Shared Secret :` prompt, re-enter the shared secret and press **Enter**.
n) At the `Proceed with this configuration. Please confirm[yes/no]` prompt, enter **yes** and press **Enter**.

If you think you made an error when completing any of these steps, enter **no** and press **Enter**. You will then be prompted to answer the questions again.

Step 9 Unmount the Cisco UCS Central ISO image from the virtual CD/DVD drive.

Step 10 Reboot the Cisco UCS Central VM.

Installing Cisco UCS Central ISO File in KVM Hypervisor

Note When you install Cisco UCS Central on KVM Hypervisor, the set up runs in graphics mode. Installing in text mode is not supported.

Procedure

Step 1 Create a VM with the following settings:

Setting	Recommended Value
Name	A descriptive name that includes information about the Cisco UCS Central deployment
RAM	No less than 12GB
Network adapter	Default
Number of vCPU	4

Setting	Recommended Value
Virtual disk	No less than 40GB of available disk space You also need to create a second 40GB virtual disk under IDE Controller in Step 3.

Step 2 Under the same IDE controller as the first virtual drive, create a second virtual drive for the VM with no less than 40GB of available disk space.

Step 3 Mount the Cisco UCS Central ISO image to the CD/DVD drive.

Step 4 Start the VM and connect to the console.

Step 5 From the **Cisco UCS Central Installation** menu on the ISO image, choose **Install Cisco UCS Central**.

The Cisco UCS Central installer checks that the VM has the required RAM and disk space (two disks, both with 40GBs). If the VM meets the requirements, the installer formats the disks, transfers the files, and installs Cisco UCS Central.

Step 6 When the Cisco UCS Central VM has completed the initial part of the installation process, answer the following questions in the VM console window:

a) `Setup new configuration or restore full-state configuration from backup [setup/restore]` prompt, enter **`setup`** and press **`Enter`**.

b) At the `Enter the UCS Central VM eth0 IPv4 Address :` prompt, enter the IP address assigned to Cisco UCS Central and press **`Enter`**.

You must enter a static IP address that is reserved for this Cisco UCS Central VM. Cisco UCS Central does not support Dynamic Host Configuration Protocol (DHCP).

c) At the `Enter the UCS Central VM eth0 IPv4 Netmask :` prompt, enter the netmask assigned to Cisco UCS Central and press **`Enter`**.

d) At the `Enter the Default Gateway :` prompt, enter the default gateway used by Cisco UCS Central and press **`Enter`**.

e) At the `Is this VM part of a cluster(select 'no' for standalone) (yes/no)` prompt, select no and press **`Enter`**.

f) At the `Enter the UCS Central VM host name :` prompt, enter the host name you want to use for the Cisco UCS Central VM and press **`Enter`**.

g) (Optional) At the `Enter the DNS Server IPv4 Address :` prompt, enter the IP address for the DNS server you want to use for Cisco UCS Central and press **`Enter`**.

If you do not plan to use a DNS server for Cisco UCS Central, leave this blank and press **`Enter`**.

h) (Optional) At the `Enter the Default Domain Name :` prompt, enter the domain in which you want to include Cisco UCS Central and press **`Enter`**.

If you do not plan to include Cisco UCS Central in a domain, leave this blank and press **`Enter`**. Cisco UCS Central will use the default domain named localdomain.

i) At the `Enforce Strong Password(Yes/No)` prompt, if you want to set up strong password alert, select yes and press **`Enter`**.

j) At the `Enter the admin Password :` prompt, enter the password you want to use for the admin account and press **`Enter`**.

k) At the `Confirm admin Password :` prompt, re-enter the password you want to use for the admin account and press **`Enter`**.

l) At the `Enter the Shared Secret :` prompt, enter the shared secret (or password) that you want to use to register one or more Cisco UCS domains with Cisco UCS Central and press **Enter**.

m) At the `Confirm Shared Secret :` prompt, re-enter the shared secret and press **Enter**.

n) At the `Proceed with this configuration. Please confirm[yes/no]` prompt, enter **yes** and press **Enter**.

If you think you made an error when completing any of these steps, enter **no** and press **Enter**. You will then be prompted to answer the questions again.

Step 7 Unmount the Cisco UCS Central ISO image from the virtual CD/DVD drive.

Step 8 Reboot the Cisco UCS Central VM.

Restoring the Cisco UCS Central VM in Standalone Mode

You cannot use a Cisco UCS Central, release 1.1 OVA file to restore a full-state backup from Cisco UCS Central, release 1.0.

Note This procedure describes the process to restore using an OVA file.

Before you begin

You must have a backup file with extension .tgz from a Cisco UCS Central system that you want to use to restore the configuration of the Cisco UCS Central VM. For information on how to back up a Cisco UCS Central system, see Managing Back up and Restore in Cisco UCS Central User Manual and CLI Reference Manual.

Procedure

Step 1 Save the Cisco UCS Central OVA file to a folder that you can access from the hypervisor.

Step 2 Open or import the Cisco UCS Central OVA file into a supported hypervisor, as required by the hypervisor.

Do not continue with the next step until the VM has finished booting.

Step 3 If you have not already done so as part of importing the OVA file, power up the Cisco UCS Central VM.

Step 4 Open up a console window to the Cisco UCS Central VM.

Step 5 When the Cisco UCS Central VM has completed the initial part of the installation process, answer the following questions in the VM console window:

a) `Setup new configuration or restore full-state configuration from backup [setup/restore]` prompt, enter **restore** and press **Enter**.

b) At the `Enter the UCS Central VM eth0 IPv4 Address :` prompt, enter the IP address assigned to Cisco UCS Central and press **Enter**.

c) At the `Enter the UCS Central VM eth0 IPv4 Netmask :` prompt, enter the netmask assigned to Cisco UCS Central and press **Enter**.

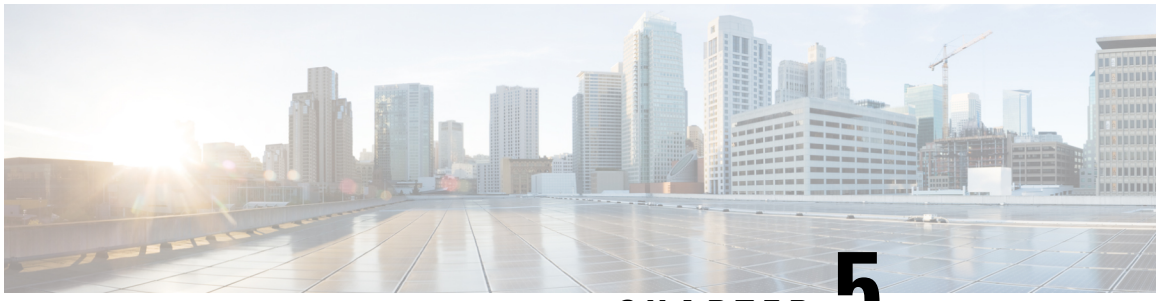
d) At the `Enter the Default Gateway :` prompt, enter the default gateway used by Cisco UCS Central and press **Enter**.
e) At the `Enter the File copy protocol[tftp/scp/ftp/sftp] :` prompt, enter the supported protocol that you want to use to copy the backup file to the Cisco UCS Central VM and press **Enter**.
f) At the `Enter the Backup server IPv4 Address :` prompt, enter the IP address assigned to the server where the backup file is stored and press **Enter**.
g) At the `Enter the Backup file path and name :` prompt, enter the full file path and name of the backup file on the server and press **Enter**.
h) At the `Enter the Username to be used for backup file transfer :` prompt, enter the username the system should use to log in to the remote server and press **Enter**.
i) (Optional) At the `Enter the Password to be used for backup file transfer :` prompt, enter the password for the remote server username and press **Enter**.
j) At the `Proceed with this configuration. Please confirm[yes/no]` prompt, enter **yes** and press **Enter**.

   If you think you made an error when completing any of these steps, enter **no** and press **Enter**. You will then be prompted to answer the questions again.

After you confirm that you want to proceed with the configuration, the network interface reinitializes with your settings and Cisco UCS Central becomes accessible via the IP address.

What to do next

After Cisco UCS Central is restored, login to Cisco UCS Central and download the firmware images into Image library. If any firmware images are referenced in the service profiles, then you must make sure that the images are downloaded and available in the image library before you re-acknowledge a Cisco UCS domain from the suspended state.



CHAPTER 5

Logging In and Setting Up

This chapter includes the following sections:

Overview of Logging In and Setting Up

You can log in and work with Cisco UCS Central using both Cisco UCS Central GUI and Cisco UCS Central CLI. You can perform almost all of the Cisco UCS Central operations, with very few exceptions, using both the interfaces.

To access the Cisco UCS Central GUI, you can use both HTTP and HTTPS protocols.

Access to some features requires that a user have the required privileges. For more information, see the Cisco UCS Central configuration guides.

Logging into and out of the Cisco UCS Central GUI

The following are the default HTTP and HTTPS web links to log into the Cisco UCS Central GUI.

- **HTTP**—The default HTTP web link for the HTML5 Cisco UCS Central GUI is `http://UCSCentral_IP`. If you are using the flash-based GUI, then the path is `http://UCSCentral_IP/flex.html`.
- **HTTPS**—The default HTTPS web link for the HTML5 Cisco UCS Central GUI is `https://UCSCentral_IP`. If you are using the flash-based GUI, then the path is `https://UCSCentral_IP/flex.html`.

Note *UCSCentral_IP* represents the IP address assigned to Cisco UCS Central.

Procedure

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

Step 2 On the launch page, do the following:

a) Enter your user name and password.

b) Click **Log In**.

What to do next

Logging Out

After you have completed your tasks on the Cisco UCS Central GUI, click the Log Out icon on the upper right corner. The Cisco UCS Central GUI logs you out immediately and returns your browser to the launch page.

Logging into and out of the Cisco UCS Central CLI

Use an SSH or telnet client to access the Cisco UCS Central CLI.

The default address to log into the Cisco UCS Central CLI is *UCSCentral_IP*

Note The **UCSCentral_IP** in represents the IP address assigned to Cisco UCS Central.

Procedure

Step 1 From the SSH client, connect to the IP address assigned to Cisco UCS Central.

Step 2 At the `log in as:` prompt, enter your Cisco UCS Central user name and press enter.

Step 3 At the `password:` prompt, enter your Cisco UCS Central password and press enter.

What to do next

Logging Out

After you have completed your tasks on the Cisco UCS Central CLI, type **exit** and press enter. Continue to type **exit** and press enter until the window closes.

Note Cisco UCS Central CLI clears the buffer of all uncommitted transactions when you exit.

Resetting the Admin Password

If you misplaced the admin password that you created for your account when you first installed the Cisco UCS Central software, you must reset your password before you can perform any admin-specific tasks. Make sure you have obtained the password reset image when obtaining the software from Cisco.com. If not, you can obtain the password reset image any time. Example of password reset image name: `ucs-central-passreset.2.0.1a.iso`

Procedure

Step 1 If necessary, reboot the VM and change the boot options to boot from CD ROM.

Step 2 Mount the Password Reset ISO image with the virtual CD/DVD drive.

Step 3 On the **UCS Central Admin Password Reset** page, do the following:

a) In the **Admin Password** field, enter the new admin password.
b) In the **Confirm Admin Password** field, re-enter the new admin password.
c) Click **Next**.

Step 4 After the password change is complete, unmount the Cisco UCS Central ISO image from the virtual CD/DVD drive.

Step 5 Reboot the Cisco UCS Central VM.

Password and Shared Secret Guidelines

Cisco recommends that each Cisco UCS Central user have a strong password. A password is required when you create each locally authenticated user account in Cisco UCS Central. A user with admin, aaa or domain-group-management privileges can configure Cisco UCS Central to perform a password strength check on the user passwords. The password that you create need to be unique.

If the password strength check is enabled, each user must have a strong password. Cisco UCS Central rejects any password or shared secret that does not meet the following requirements:

- Must contain a minimum of 8 characters and a maximum of 80 characters.
- Must contain at least three of the following:
  - Upper case letter
  - Lower case letters
  - Numbers
  - Special characters
- Must not contain a character that is repeated more than 3 times consecutively. **For example**: aaabbb111@@@
- Must not be identical to the user name or the reverse of the user name.

- Must pass 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 = (equal sign).
- Must not be blank for local users and admin users.
- If you are creating strong password, then the password must not contain three consecutive characters or number in any order.

Resetting the Shared Secret

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect local-mgmt**	Enters local management mode.
Step 2	UCSC (local-mgmt) # **set shared-secret**	Allows you to set a new shared secret.
Step 3	At the prompt, enter the new shared secret.	

Example

The following example shows how to reset the shared secret for Cisco UCS Central:

```
UCSC # connect local-mgmt
UCSC(local-mgmt) # set shared-secret
Enter Shared Secret: passW0rd2
```

What to do next

If you reset the shared secret in Cisco UCS Central, you must update the shared secret in Cisco UCS Manager for each registered Cisco UCS domain.

Important Do not unregister the Cisco UCS domains.

Resetting the Shared Secret in Cisco UCS Manager

If you reset the shared secret in Cisco UCS Central, you must update the shared secret in Cisco UCS Manager for each registered Cisco UCS domain.

Important Do not unregister the Cisco UCS domains.

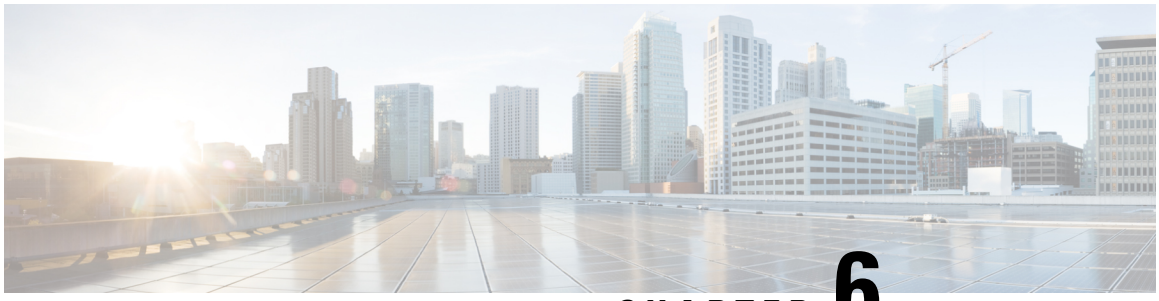
Procedure

	Command or Action	Purpose
Step 1	Log into the Cisco UCS Manager CLI for the registered domain.	
Step 2	UCS-A# **scope system**	Enters system mode.
Step 3	UCS-A /system # **scope control-ep policy**	Enters control-ep policy mode.
Step 4	UCS-A /system/control-ep # **set shared-secret**	Enter the shared secret (or password) that matches the new shared secret in Cisco UCS Central.
Step 5	UCS-A /system/control-ep # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to update the shared secret in Cisco UCS Manager:

```
UCS-A # scope system
UCS-A /system # scope control-ep policy
UCS-A /system/control-ep # set shared-secret
Shared Secret for Registration: passW0rd2
UCS-A /system/control-ep* # commit-buffer
UCS-A /system/control-ep #
```



CHAPTER 6

Upgrading Cisco UCS Central

Upgrading Cisco UCS Central to Release 2.0

You can upgrade Cisco UCS Central in standalone mode.

Make sure your system meets the system requirements for Cisco UCS Central, release 2.0. See System Requirements, on page 20.

Important

- Cisco UCS Central, release 2.0 requires a minimum of 12GB RAM and 40 GB storage space. Make sure that the VM RAM meets this requirement and disk1 size is upgraded to 40 GB. Otherwise, the upgrade will fail.
- After the upgrade, make sure to clear browser cache before logging into the Cisco UCS Central HTML5 UI.
- After the upgrade, Cisco UCS Central refreshes the inventory data of all registered Cisco UCS domains. Depending on the number of domains, the system may be sluggish until the inventory finishes.

Caution

Cisco UCS Central, release 2.0 supports Cisco UCS Manager, release 2.1(2), 2.1(3), 2.2(x), 3.0(x), and 3.1(x). You must first upgrade Cisco UCS Manager to one of the supported release versions before upgrading Cisco UCS Central. If you do not upgrade Cisco UCS Manager first, Cisco UCS Central generates version mismatch errors and any registered Cisco UCS domains stop receiving updates from Cisco UCS Central.

Supported Upgrade Path to Release 2.0

You can only upgrade Cisco UCS Central to release 2.0 from any of the following two releases:

- From 1.4 to 2.0(1a)
- From 1.5 to 2.0(1a)

Important

- Before upgrading Cisco UCS Central to 2.0 you must do the following:
  - Make sure you have Cisco UCS Manager 2.1(2) or newer. It is recommended to upgrade Cisco UCS Manager to the latest version to ensure complete feature support.
  - Upgrade Cisco UCS Central 1.0, 1.1, 1.2, 1.3 to Cisco UCS Central 1.4 release.

    Note
    1. You must upgrade releases 1.0, 1.1, 1.2, and 1.3 to 1.4 before you can upgrad to 2.0.
    2. Only ISO upgrade is supported for upgrade from release 1.0 or 1.1 to 1.2.

  - Make sure to take a full state backup before starting the upgrade process.
- You can use backup and restore option to ensure that you can recreate the environment in case of any failure. Backup and restore is not recommended for upgrades. The following is the recommended best practice for back up and restore:
  - Use full state backup for disaster recovery scenario, where the Cisco UCS Central VM is lost.
  - Use configuration import for importing configuration from a backup file on an existing Cisco UCS Central VM.
  - Full State backup does not backup firmware images downloaded in Cisco UCS Central. When deploying new Cisco UCS Central VM and restoring from a full state backup, make sure to download the firmware images again in Cisco UCS Central. After a full state restore, you must download the firmware images before acknowledging the Cisco UCS domains from suspend mode.
- The following options are not supported in 2.0:
  - Erase samdb config import.
  - Upgrade from Cisco UCS Central releases 1.0, 1.1, 1.2, and 1.3.
  - Taking a full state back up from Cisco UCS Central releases 1.4 and earlier to restore Cisco UCS Central release 2.0.
  - Taking a config export from Cisco UCS Central releases 1.4 and earlier to config import from Cisco UCS Central release 2.0.
  - Downgrade from Cisco UCS Central release 1.5 to Cisco UCS Central releases 1.2 or earlier.
  - If Statistics Collection is enabled in the previous releases of Cisco UCS Central, it will be disabled when you upgrade to release 2.0.

Upgrading Cisco UCS Central in Standalone Mode

This procedure upgrades the current running version of the RHEL kernel and all Cisco UCS Central components. It also retains all Cisco UCS Central data.

Before you begin

You must have obtained the Cisco UCS Central, release 2.0 ISO image. See Obtaining the Cisco UCS Central Software from Cisco.com, on page 23. We recommend that you backup your Cisco UCS Central data before you perform this procedure.

Procedure

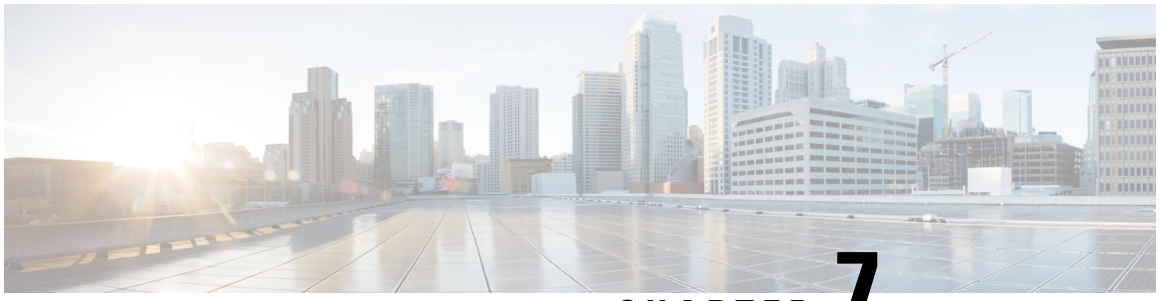
Step 1 If necessary, reboot the VM and change the boot options to boot from CD ROM.

Step 2 Mount the Cisco UCS Central ISO image with the virtual CD/DVD drive.

Step 3 From the **Cisco UCS Central Installation** menu on the ISO image, choose **Upgrade Existing Cisco UCS Central**.

Step 4 After the upgrade is complete, unmount the Cisco UCS Central ISO image from the virtual CD/DVD drive.

Step 5 Reboot the Cisco UCS Central VM.



CHAPTER 7

Working with Cisco UCS Manager

This chapter includes the following sections:

Cisco UCS Domains and Cisco UCS Central

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

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

Registering Cisco UCS Domains

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

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

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

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

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

Note

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

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

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

Registering a Cisco UCS Domain Using Cisco UCS Manager GUI

Procedure

Step 1 In Cisco UCS Manager **Navigation** pane, click **Admin** tab.

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

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

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

Step 5 In the **Register with UCS Central** dialog box,

a) Enter the host name or IP address in the **Hostname/IP Address** field.

We recommend that you use a hostname rather than an IP address. To use a hostname, you must configure a DNS server. If the Cisco UCS domain is not registered with Cisco UCS Central, or DNS management

is set to local, configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to global, configure a DNS server in Cisco UCS Central.

b) Enter the shared secret or password in the **Shared Secret** field.

Step 6 In the **Policy Resolution Control** area, click **Global** if you want the policy or configuration to be managed by Cisco UCS Central or click **Local** to manage the policy or configuration by Cisco UCS Manager.

Step 7 Click **OK**.

Unregistering a Cisco UCS Domain Using Cisco UCS Manager GUI

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

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

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

Procedure

Step 1 In Cisco UCS Manager **Navigation** pane, click **Admin** tab.

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

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

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

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

Step 6 Click **OK**.

Registering a Cisco UCS Domain Using Cisco UCS Manager CLI

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.

	Command or Action	Purpose
Step 2	UCS-A/system # **create control-ep policy** *ucs-central*	Creates the policy required to register the Cisco UCS Domain with Cisco UCS Central. *ucs-central* can be the hostname or IP address of the virtual machine where Cisco UCS Central is deployed. **Note** We recommend that you use a hostname rather than an IP address. To use a hostname, you must configure a DNS server. If the Cisco UCS domain is not registered with Cisco UCS Central, or DNS management is set to local, configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to global, configure a DNS server in Cisco UCS Central.
Step 3	Shared Secret for Registration: *shared-secret*	Enter the shared secret (or password) that was configured when Cisco UCS Central was deployed.
Step 4	UCS-A/system/control-ep # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example registers a Cisco UCS Domain with a Cisco UCS Central system with a FQDN, and commits the transaction:

```
UCS-A# scope system
UCS-A /system # create control-ep policy UCSCentral.MyCompany.com
Shared Secret for Registration: S3cretW0rd!
UCS-A /system/control-ep* # commit-buffer
UCS-A /system/control-ep #
```

Unregistering a Cisco UCS Domain Using Cisco UCS Manager CLI

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

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

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

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.
Step 2	UCS-A/system # **delete control-ep policy**	Deletes the policy and unregisters the Cisco UCS Domain from Cisco UCS Central.
Step 3	UCS-A/system # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example unregisters a Cisco UCS Domain from Cisco UCS Central and commits the transaction:

```
UCS-A# scope system
UCS-A /system # delete control-ep policy
UCS-A /system* # commit-buffer
UCS-A /system #
```

Changing Cisco UCS Central IP Address

Cisco recommends that you always register Cisco UCS domains using Cisco UCS Central's Fully Qualified Domain Name (FQDN). If domains are registered with FQDN, any change in the Cisco UCS Central IP address is transparent to the domain. Changing Cisco UCS Central's IP address is supported only when Cisco UCS Central has a Fully Qualified Domain Name (FQDN), and when the Cisco UCS domain is registered using a Cisco UCS Central domain name.

Note

- Changing Cisco UCS Central's hostname (FQDN) is not officially supported. However, if your business needs dictate that this be done, please engage Cisco Technical Support, so that we can evaluate accommodating this request.
- Changing Cisco UCS Central's IP address is not officially supported if Cisco UCS domains are registered using Cisco Cisco UCS Central's IP address. However, if your business needs dictate that this be done, please engage Cisco Technical Support, so that we can evaluate accommodating this request.

Procedure

Step 1 Delete the existing Cisco UCS Central IP address from the DNS server for the hostname and enter the new IP address and the Cisco UCS Central hostname.

Step 2 On the virtual infrastructure management platform (for example, VMware vCenter), change the virtual network interface (VIF) to point to the new subnet.

Step 3 From the Cisco UCS Central VM console, change the IP address of the network interface.

Step 4 Launch Cisco UCS Central from the GUI using the hostname. If the Cisco UCS Central GUI is inaccessible, then restart **pmon** command from the Cisco UCS Central CLI.

Step 5 Verify the Cisco UCS Central registration status on the Cisco UCS Manager GUI.

Step 6 For a High Availability setup, IP addresses of both the nodes and the virtual IP can be changed only at the primary node as shown in the example below.

Example

The following example is for a standalone setup of a network interface.

```
Changing IP for a UCS Central system in Standalone mode:

UCSC # scope network-interface a
UCSC/network-interface # set net ip 10.10.10.2 gw 10.10.10.1 netmask 255.255.255.0
Warning: When committed, this change may disconnect the current CLI session
UCSC/network-interface* # commit-buffer
UCSC/(local-mgmt)# pmon restart
  Shutting down pmon:       [  OK  ]
  Starting pmon:            [  OK  ]
--------------------------------------------------------------------------------

Changing node IP for a UCS Central system in High-Availability mode:

UCSC # scope network-interface a
UCSC/network-interface # set net ip 10.10.10.2 gw 10.10.10.1 netmask 255.255.255.0
Warning: When committed, this change may disconnect the current CLI session
UCSC/network-interface* # commit-buffer
UCSC # scope network-interface b
UCSC/network-interface # set net ip 10.10.10.2 gw 10.10.10.1 netmask 255.255.255.0
Warning: When committed, this change may disconnect the current CLI session
UCSC/network-interface* # commit-buffer
UCSC/(local-mgmt)# pmon restart
  Shutting down pmon:       [  OK  ]
  Starting pmon:            [  OK  ]
--------------------------------------------------------------------------------
Changing virtual IP for a UCS Central system in High-Availability mode

UCSC# scope system
UCSC/system # set virtual-ip
    a.b.c.d System IP Address
    ipv6    System IPv6 Address

UCSC/system # set virtual-ip 10.106.227.206
UCSC/system*# commit buffer
```

Changing Cisco UCS Manager IP Address

You can change the Cisco UCS Manager IP address if Cisco UCS domains are registered to Cisco UCS Central through an IP address. Use the following steps to change the Cisco UCS Manager IP address:

Before you begin

Ensure that the Fabric Interconnects have connectivity to the new subnet.

Procedure

Step 1 Delete the existing Cisco UCS Manager IP address from the DNS server for the hostname, and enter the new IP address and the same Cisco UCS Manager hostname.

Step 2 From the primary FI console, run the following commands:

Example:

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # set out-of-band ip 10.193.190.61 netmask 255.255.255.0 gw
10.193.190.1
UCS-A /fabric-interconnect* # scope fabric-interconnect b
UCS-A /fabric-interconnect* # set out-of-band ip 10.193.190.62 netmask 255.255.255.0 gw
10.193.190.1
UCS-A /fabric-interconnect* # scope system
UCS-A /system* # set virtual-ip 10.193.190.60
UCS-A /system* # commit-buffer
```

Step 3 After running the commands shown above, launch Cisco UCS Manager using the hostname and verify that the registration status is not changed.

Step 4 Under **service-reg** in the Cisco Cisco UCS Central CLI, verify that the **show clients** commands point to the new IP address for the UCS Domain.

Step 5 (Optional) To check if the IP address is changed, launch Cisco UCS Manager GUI from Cisco UCS Central, and verify that the new IP address is updated in the UI.

You can perform an additional check by updating one of the global service profile labels from the Cisco UCS Central GUI and ensure that the updated label is pushed down to Cisco UCS Manager. You can also create new global service profiles or policies and push them down to Cisco UCS Manager to verify that the new IP address is updated in the UI.

Cisco UCS Central Instance Migration

You can migrate a Cisco UCS Central instance to support Data Center migration or Disaster Recovery use cases. The following are required to successfully migrate a Cisco UCS Central instance:

- Cisco UCS Central has a Fully Qualified Domain Name (FQDN). In order to migrate a Cisco UCS Central instance, the FQDN (hostname) of the instance must remain the same.

- Any registered Cisco UCS Manager instances must continue to be reachable from the Cisco UCS Central instance by how they were registered (domain hostname or IP address).

Note Cisco UCS Central supports changing of the Cisco UCS Central IP address during migration.