Cisco UCS Central Getting Started Guide, Release 2.1

First Published: 2025-05-12

Last Modified: 2025-07-28

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

CHAPTER 1

Overview

Overview

This guide provides an overview of the Cisco Unified Computing System (Cisco UCS) and its key components-Cisco UCS Manager, and Cisco UCS Central.

Cisco UCS Central User Documentation Reference

The Cisco UCS Central following use case-based documents to understand and configure Cisco UCS Central:

Guide	Description
Cisco UCS Central Release Notes	Provides a scalable management solution for a growing Cisco Unified Computing System (Cisco UCS) environment.
Cisco UCS Central Getting Started Guide	Provides a brief introduction to the Cisco UCS infrastructure, Cisco UCS Manager, and Cisco UCS Central. Includes an overview of the HTML5 UI, how to register Cisco UCS domains in Cisco UCS Central, and how to activate licenses.

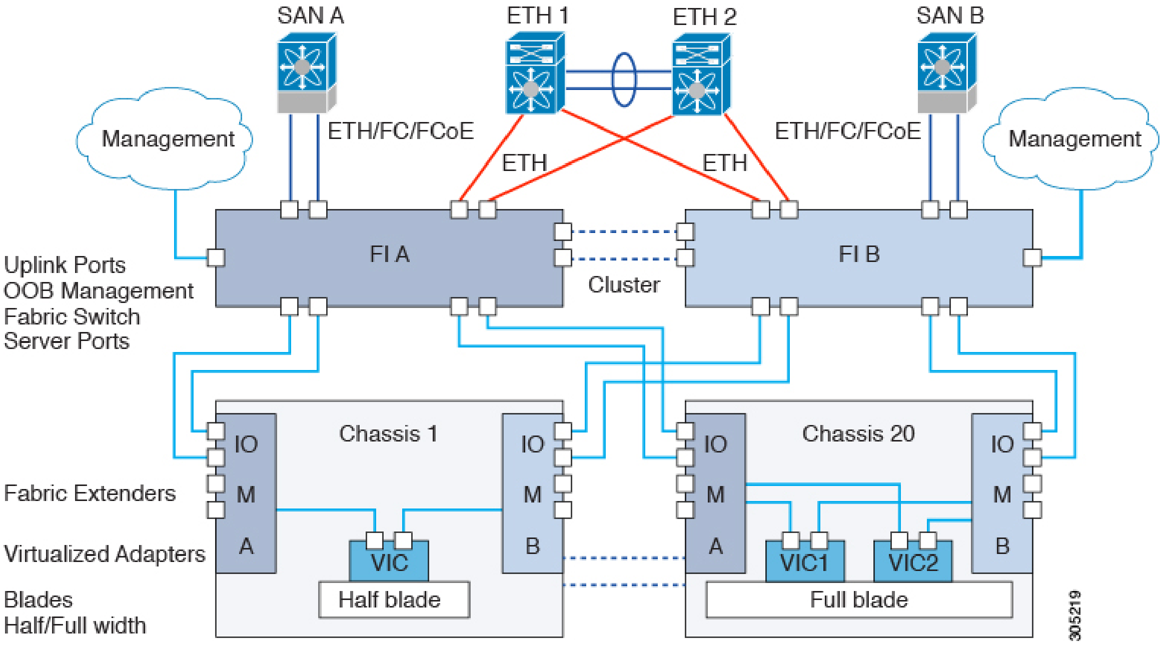
Guide	Description
Cisco UCS Central GUI User Guide	The guide provides the combined information from the following task: • **Administration**—Provides information on administrative tasks, such as user management, communication, firmware management, backup management, and Smart Call Home. • **Authentication**—Provides information on authentication tasks, such as passwords, users and roles, RBAC, TACACS+, RADIUS, LDAP, and SNMP. • **Server Management**—Provides information on server management, such as equipment policies, physical inventory, service profiles and templates, server pools, server boot, and server policies. • **Storage Management**—Provides information on storage management, such as ports and port channels, VSAN and vHBA management, storage pools, storage policies, storage profiles, disk groups, and disk group configuration. • **Network Manageent**—Provides information on network management, such as ports and port channels, VLAN and vNIC management, network pools, and network policies.
Cisco UCS Central CLI User Guide	Provides detailed instructions, examples, and reference materials for executing various administrative and operational tasks using the UCS Central CLI. It enables users to efficiently manage compute, network, and storage resources, as well as to configure and maintain policies, templates, and profiles across UCS domains.
Cisco UCS Central Faults Reference Manual	Provides administrators to identify and address issues proactively to maintain the health and performance of the infrastructure.

CHAPTER 2

Introduction to Cisco Unified Computing System Infrastructure

Cisco Unified Computing System Overview

Figure 1: Cisco UCS Architecture



Cisco UCS has a unique architecture that integrates compute, data network access, and storage network access into a common set of components under a single-pane-of-glass management interface.

Cisco UCS fuses access layer networking and servers. This high-performance, next-generation server system provides a data center with a high degree of workload agility and scalability. The hardware and software components support Cisco's unified fabric, which runs multiple types of data center traffic over a single converged network adapter.

Architectural Simplification

The simplified architecture of Cisco UCS reduces the number of required devices and centralizes switching resources. By eliminating switching inside a chassis, network access-layer fragmentation is significantly reduced. Cisco UCS implements Cisco unified fabric within racks and groups of racks, supporting Ethernet and Fibre Channel protocols over 10 Gigabit Cisco Data Center Ethernet and Fibre Channel over Ethernet (FCoE) links. This radical simplification reduces the number of switches, cables, adapters, and management points by up to two-thirds. All devices in a Cisco UCS domain remain under a single management domain, which remains highly available through the use of redundant components.

Scalability

A single Cisco UCS domain supports multiple chassis and their servers, all of which are administered through one Cisco UCS Manager. For more detailed information about the scalability, speak to your Cisco representative.

Flexibility

A Cisco UCS domain allows you to quickly align computing resources in the data center with rapidly changing business requirements. This built-in flexibility is determined by whether you choose to fully implement the stateless computing feature. Pools of servers and other system resources can be applied as necessary to respond to workload fluctuations, support new applications, scale existing software and business services, and accommodate both scheduled and unscheduled downtime. Server identity can be abstracted into a mobile service profile that can be moved from server to server with minimal downtime and no need for additional network configuration. With this level of flexibility, you can quickly and easily scale server capacity without having to change the server identity or reconfigure the server, LAN, or SAN. During a maintenance window, you can quickly do the following:

- Deploy new servers to meet unexpected workload demand and rebalance resources and traffic.
- Shut down an application, such as a database management system, on one server and then boot it up again on another server with increased I/O capacity and memory resources.

Optimized for Server Virtualization

Cisco UCS has been optimized to implement VM-FEX technology. This technology provides improved support for server virtualization, including better policy-based configuration and security, conformance with a company's operational model, and accommodation for VMware's VMotion.

Cisco UCS Manager Overview

Cisco UCS Manager is embedded software that resides on the fabric interconnects, providing complete configuration and management capabilities for all of the components in the Cisco UCS system. This configuration information is replicated between the two fabric interconnects, providing a highly available solution for this critical function. The most common way to access UCS Manager for simple tasks is to use a Web browser to open the Java-based GUI. For command-line or programmatic operations against the system, a command-line interface (CLI) and an XML API are also included with the system.

The Cisco UCS Manager GUI provides role-based access control (RBAC) to allow multiple levels of users granular administrative rights to system objects. Users can be restricted to certain portions of the system based on locale, which corresponds to an optional organizational structure that can be created within the system. Users can also be classified based on their access levels or areas of expertise, such as “Storage Administrator,” “Server Equipment Administrator,” or “Read-Only”. RBAC allows the comprehensive capabilities of the

Cisco UCS Manager GUI to be properly shared across multiple individuals or teams within your organization in a flexible, secure manner.

Cisco UCS Manager provides unified, embedded management of all software and hardware components. Every instance of Cisco UCS Manager and all of the components managed by it form a domain. For organizations that deploy multiple Cisco UCS domains, Cisco UCS Central software providesa centralized user interface that allows you to manage multiple, globallydistributed Cisco UCS domains with thousands of servers. Cisco UCS Central integrates with Cisco UCS Manager and utilizes it to provide globalconfiguration capabilities for pools, policies, and firmware.

CHAPTER 3

Introduction to Cisco UCS Central

Introducing Cisco UCS Central

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

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

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

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

Cisco UCS Central Features

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

Note For a full list of new features, see the Release Notes for Cisco UCS Central.

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

Feature	Description
Global service profiles and templates	Global service profiles and templates in Cisco UCS Central enables fast and simplified infrastructure deployment and provides consistency of configurations throughout the enterprise. This feature enables global bare-metal workload mobility very similar to how hypervisor enables virtualized workload mobility.
Backup	Cisco UCS Central provides an automatic backup facility that enables quick and efficient backing up the configuration information of the registered Cisco UCS domains and the UCS Central configuration.
XML API	Cisco UCS Central, just like Cisco UCS Manager, has a high-level industry-standard XML API for interfacing with existing management frameworks and orchestration tools. The XML API for Cisco UCS Central Software is similar to the XML API for Cisco UCS Manager, making integration with high-level managers very fast.
Remote Management	Cisco UCS Central enables you to manage various end points in the registered Cisco UCS domains from one management point. You can manage chassis, servers, fabric interconnects, and fabric extenders from Cisco UCS Central GUI or CLI. You can also access tech support files for registered UCS domains from Cisco UCS Central.

Overview of Cisco UCS Central HTML 5 UI

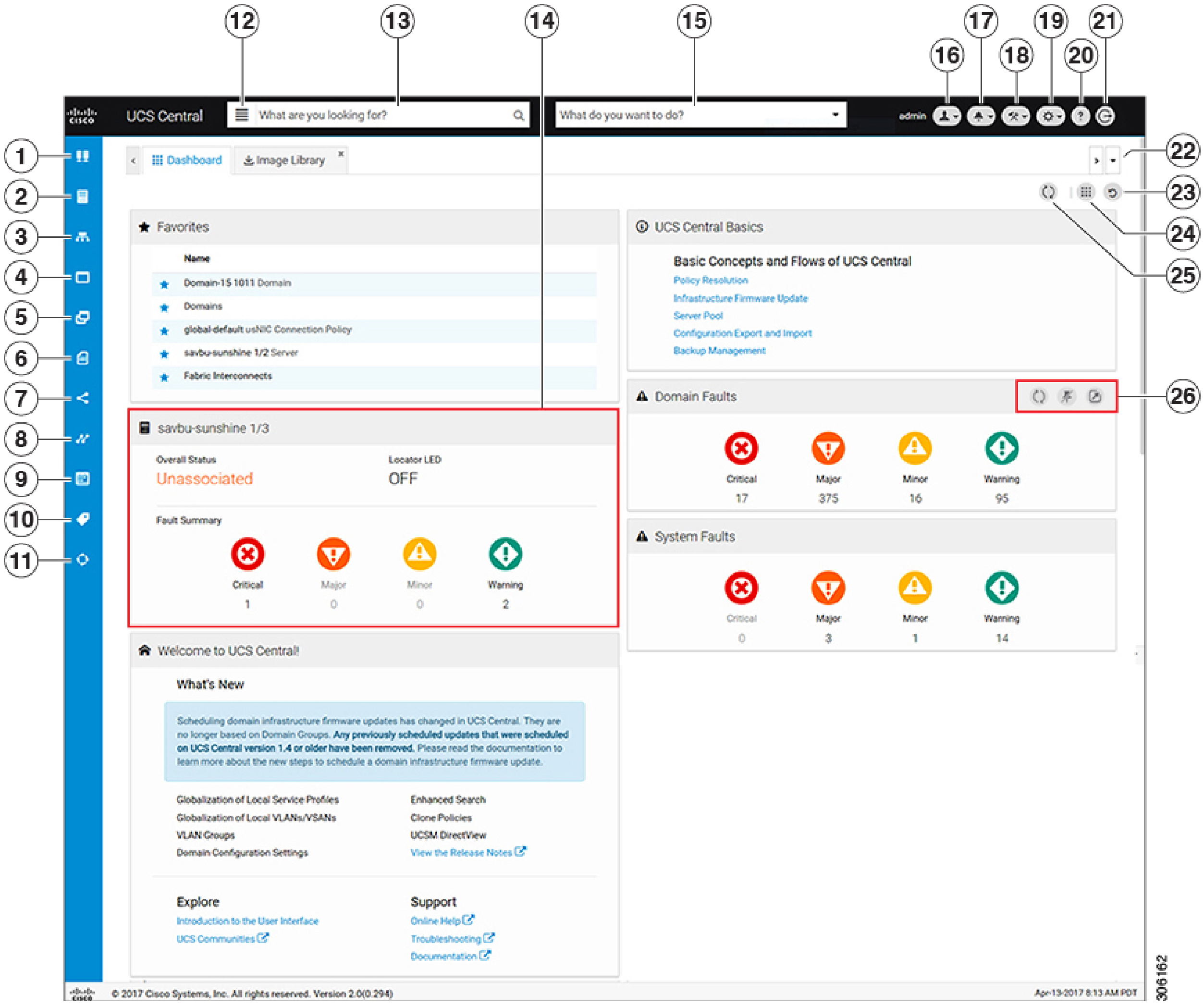
Cisco UCS Central HTML5 based user interface provides flexibility and task based usability for your management purposes.

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:



Favorites

Name
Domain-15 1011 Domain
Domains
global-default usNIC Connection Policy
savbu-sunshine 1/2 Server
Fabric Interconnects

Basic Concepts and Flows of UCS Central

Domain Faults

Critical	Major	Minor	Warning
17	375	16	95

savbu-sunshine 1/3

Overall Status: Unassociated
Locator LED: OFF

Fault Summary

Critical	Major	Minor	Warning
1	0	0	2

System Faults

Critical	Major	Minor	Warning
0	3	1	14

What's New

Scheduling domain infrastructure firmware updates has changed in UCS Central. They are no longer based on Domain Groups. **Any previously scheduled updates that were scheduled on UCS Central version 1.4 or older have been removed.** Please read the documentation to learn more about the new steps to schedule a domain infrastructure firmware update.

Globalization of Local Service Profiles
Globalization of Local VLANs/VSANs
VLAN Groups
Domain Configuration Settings
Enhanced Search
Clone Policies
UCSM DirectView

Explore

Support

© 2017 Cisco Systems, Inc. All rights reserved. Version 2.0(0.294)
Apr-13-2017 8:13 AM PDT

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.

Dashboard Widgets

Dashboard widgets allow you to customize the dashboard based on your operational requirements. Cisco UCS Central contains the following types of widgets:

Default Widgets

Default widgets are listed in the widgets library on the dashboard. Click the widgets library to pin the widget to the dashboard. The widgets library includes the following widgets:

- **Welcome to UCS Central!**—Displays introductory links and videos to get you started with Cisco UCS Central.
- **UCS Central Basics**— Displays basic concepts and flows for Cisco UCS Central.
- **Licenses**—Displays the total number of licenses and their status.
- **Backup & Restore**—Displays the current backup and restore status.
- **Config Export & Import**—Displays the current config export and import status.
- **Firmware Management**—Displays the total number of scheduled Firmware update jobs.
- **Inventory Status**—Displays the number of domains, FIs, servers, chassis, and FEX, as well as the overall status.
- **ID Universe**—Displays the number of IDs that are available or in conflict.
- **System Faults**—Displays the number of system faults with the top four severities.

  Click the Expand icon to view the Faults Log page for all system faults. Click on a fault icon to view the system faults with the selected severity pre-selected.
- **Domain Faults**—Displays the number of domain faults with the top four severities.

  Click the Expand icon to view the Faults Log page for all domain faults. Click on a fault icon to view the domain faults with the selected severity pre-selected.
- **Pending Activities**—Displays Pending activities. Some may need user acknowledgment.
- **Domains**—Displays current number of domains registered with Cisco UCS Central.

Table Summary Widgets

Table summary widgets displays the total number of items and the status for the following:

- **Domains**
- **Fabric Interconnects**
- **Servers**
- **Chassis**
- **FEX**
- **Service Profiles**

Up to two status bars can be displayed, with the top four errors displayed in each status bar.

Click the Expand icon to view the full table.

Detailed Instance Summary Widgets

Detailed instance summary widgets display the overall status and fault summary. Click the pin icon to create a widget for the following instances:

- Domain
- Domain Group
- Organization
- Fabric Interconnect
- Server
- Chassis
- FEX
- Service Profile

Click the Expand icon to view the full instance page. Click on a fault icon to view a faults window with the selected severity pre-selected.

Instance Shortcut Widgets

Shortcut widgets create a read-only link to a particular instance of a policy or template. Click the pin icon on an instance to create the widget.

Adding Table Summary Widgets to the Dashboard

Procedure

Step 1 Click the **Search** icon and choose one of the following:

- **Domains**
- **Fabric Interconnects**
- **Servers**
- **Chassis**
- **FEX**
- **Service Profiles**

Step 2 On the table page that displays, click the **Pin** icon.

Step 3 Click the **Dashboard** link to view the new widget.

Adding Instance Summary Widgets to the Dashboard

Procedure

Step 1 Click the **Search** icon and select one of the following:

- **Domains**
- **Fabric Interconnects**
- **Servers**
- **Chassis**
- **FEX**
- **Service Profiles**

Step 2 Click on an instance.

Step 3 On the instance page that displays, click the **Pin** icon.

Step 4 Click the **Dashboard** link to view the new widget.

Tab Navigator

The tab navigator appears on all screens, and allows you to navigate quickly through the tabs that you have opened. You can also close all tabs at once.

Using the Tab Navigator

Procedure

Step 1 On the tab bar, click the drop-down on the far right.

A list of all currently opened tabs is displayed.

Step 2 Select the tab that you want to navigate to, or select **Close All Tabs** to close all of the tabs.

Note
You cannot close the dashboard tab.

Common User Interface Options

The following table describes user interface options:

Icon	Label	Description
✓	Acknowledge	Acknowledge the changes most recently made.
⏻	Acknowledge reboot	Grant permission for Cisco UCS Central to reboot the selected hardware.
+	Add	Add the settings selected.
✓	Apply	Apply the settings that you configured.
≡	Browse Tables	Display physical and logical inventory entities in the system.
▦	Dashboard	Access to the Dashboard widgets.
🗑	Delete	Delete selected items.
🖧	Domain Group Navigation	Search through all of the registered domains.
⤓	Download and Import Selected Images	Download and import selected images from the Image Library.
</>	Download CSV file	Download data in table as a *.csv (comma delineated) file.
📄	Download PDF file	Download data in table as a *.pdf (Adobe PDF) file.
X	Download XLS file	Download data in table as an *.xls (Microsoft Excel) file.
☰	Dual Table View	Splits the table view into two views.
✎	Edit	Edit the item selected.
↗	Launch	Launch the submenu for the selected item.
🖧	Organization Navigation	Access to organizations and their service profiles, templates, pools, policies, and permitted vLANs.

Icon	Label	Description
📌	Pin	Pin the widget to the dashboard.
👤	Profile Configuration	Configure user settings, such as password and preferences.
☑	Register Domain	Register a Cisco UCS Manager domain with Cisco UCS Central.
🔄	Re-run report	Re-run the Hardware Compatibility List report.
⟲	Reset	Reset service profile assigned IDs manually.
🔗	Share tab	Copy a service profile's URL. When you send the link to another user, it opens to the same view. The other user does not have to search for the view.
🔔	System Alerts	Access to system alerts menu, logs, faults, core dumps, internal services, events, and pending activities.
⚙	System Configuration	Access to the system configuration menu when on the system level. In other views, configuration menu is contextual.
🏷	Tag	Tag items to assign them to groups for specific functions.
🛠	Tools	Access to the system tools menu when on the system level. In other views, tools menu is contextual.
☒	Unregister Domain	Unregister a Cisco UCS Manager domain from Cisco UCS Central.
▦	Usage Table	Opens a table to show data associated with the object.
★	Favorites	Saves your most used components, tabs, and dialogs for creating or editing policies and enables quick access.

CHAPTER 4

Working with Cisco UCS Manager

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 Cisco UCS Central's 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 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 4.1(3) 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

Before you begin

- Configure an NTP server and set the correct time zone in both Cisco UCS Manager and Cisco UCS Central. If the timezone and date are different, the registration may fail.
- Enable HTTPS on Cisco UCS Manager before you register a domain with Cisco UCS Central.

To register using the Cisco UCS Central hostname, you must also configure a DNS server. The DNS record must be created properly, and the DNS configuration must be in place for both Cisco UCS Manager and Cisco UCS Central.

Procedure

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

Step 2 Expand **All** > **Communication Management >UCS Central**.

Step 3 Click **Register With UCS Central**.

Step 4 In the **Register With UCS Central** area, perform the following:

- **Hostname/IP Address**—Enter the hostname of the IP address.
- **Shared Secret**—Enter the UCS Central shared secret.

Name	Earliest Supported Release	Description
Infrastructure & Catalog Firmware	4.1(3)	Determines whether the Capability Catalog and infrastructure firmware policy are defined locally in Cisco UCS Manager or come from Cisco UCS Central.
Time Zone Management	4.1(3)	Determines whether the time zone and NTP server settings are defined locally in Cisco UCS Manager or comes from Cisco UCS Central.
Communication Services	4.1(3)	Determines whether HTTP, CIM XML, Telnet, SNMP, web session limits, and Management Interfaces Monitoring Policy settings are defined locally in Cisco UCS Manager or in Cisco UCS Central.
Global Fault Policy	4.1(3)	Determines whether the Global Fault Policy is defined locally in Cisco UCS Manager or in Cisco UCS Central.
User Management	4.1(3)	Determines whether authentication and native domains, LDAP, RADIUS, TACACS+, trusted points, locales, and user roles are defined locally in Cisco UCS Manager or in Cisco UCS Central.
DNS Management	4.1(3)	Determines whether DNS servers are defined locally in Cisco UCS Manager or in Cisco UCS Central.
Backup & Export Policies	4.1(3)	Determines whether the Full State Backup Policy and All Configuration Export Policy are defined locally in Cisco UCS Manager or in Cisco UCS Central.
Monitoring	4.1(3)	Determines whether Call Home, Syslog, and TFTP Core Exporter settings are defined locally in Cisco UCS Manager or in Cisco UCS Central.
SEL Policy	4.1(3)	Determines whether the SEL Policy is defined locally in Cisco UCS Manager or in Cisco UCS Central.
Power Allocation Policy	4.1(3)	Determines whether the Power Allocation Policy is defined locally in Cisco UCS Manager or in Cisco UCS Central.
Power Policy	4.1(3)	Determines whether the Power Policy is defined locally in Cisco UCS Manager or in Cisco UCS Central.
Power Save Policy	4.1(3)	Globally manages the chassis to maximize energy efficiency or availability.
Cisco UCSX-9508 Chassis Power Extended Policy	4.1(3)	Manages the chassis to maximize energy efficiency or availability. Power Extended Policy is effective only when we have PSU Redundant Policy Mode. For example, the total power available can be extended when we have N+1, N+2 and Grid to PSU Redundancy modes.
Cisco UCSX-9508 Chassis Fan Control Policy	4.1(3)	Manages you to control the fan speed to bring down server power consumption and noise levels.

Name	Earliest Supported Release	Description
Equipment Policy	4.1(3)	Determines whether the Equipment Policy is defined locally in Cisco UCS Manager or in Cisco UCS Central.
Port Configuration	4.1(3)	Determines whether port configuration is defined locally in Cisco UCS Manager or in Cisco UCS Central.

The infrastructure and catalog firmware policy is set to local by default. All other policies are set to global.

Step 5 Click **OK**.

Domain Registration Management

On the Domain Management page, you can view the domain registrations and lost domains.

Domain Registrations

The **Domain Registrations** tab displays all Cisco UCS domains that you have attempted to register to Cisco UCS Central.

From this tab, you can do the following:

- Filter the Cisco UCS domains that are displayed.
- Delete Cisco UCS domains that failed to register.
- View the configuration status of the Cisco UCS domain.
- Unregister a successfully registered domain.

Important We recommend that you contact Cisco TAC before attempting to unregister a Cisco UCS domain.

Lost Domains

The **Lost Domains** tab displays all Cisco UCS domains that have lost connectivity. These domains may or may not be listed as **Registered**. You can delete these domains.

Unregistering a Cisco UCS Domain in Cisco UCS Central

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 continue to operate as local entities. When you reregister the domain, the service profiles and polices remain local.

Note You can also choose to remove the service profiles and policies entirely.

- Unregistering a Cisco UCS domain from Cisco UCS Central will be unsuccessful if you try to unregister immediately after registration, and you will be unable to perform remote operations. Cisco recommends that you check the **Inventory** status to move from **In Progress** to **OK** before you attempt to unregister again.

In a case where you choose certain policies to be resolved locally using the Policy Resolution Control feature in Cisco UCS Central, or when a Cisco UCS Domain is unregistered from Cisco UCS Central, the global settings/unnamed policies (such as QoS Settings, Discovery policies) stay as previously configured. You must manually change the policy details to the desired state.

Caution Unregistering a Cisco UCS Domain has serious implications. You must not unregister the Cisco UCS Domain unless you choose to permanently not manage it from Cisco UCS Central.

Procedure

Step 1 Click the **System Tools** icon and select **Domain Management**.

Step 2 On the **Domain Management** page, click the **Domain Registration** tab and choose the domain that you want to unregister.

Step 3 Click the **Unregister Domain** icon.

Step 4 Click **Unregister Domain** to continue.

Step 5 Choose the cleanup mode that you want to use:

- **Deep Remove Global**—Removes all policies inherited from the global configuration.
- **Localize Global**—Turns all global policies into local policies.

Step 6 Click **Unregister Domain**.

Viewing Domain Registration Configuration Status

Procedure

Step 1 Click the **System Tools** icon and choose **Domain Management**.

Step 2 To view the domain configuration status, select the domain, click the **Notification** icon (bell icon representation), and then click **Configuration Status**.

The **Domain Registrations Configuration Status** page displays the status of the registration.

Step 3 Click **Close** to close the window.

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
--------------------------------------------------------------------------------
```

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
```

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.

Policies in Cisco UCS Central and Cisco UCS Domains

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

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

- Global service profiles or service profile templates that are created and managed by Cisco UCS Central. You can associate global service profiles with servers in one or more registered Cisco UCS domains.

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

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

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

Policy Resolution between Cisco UCS Manager and Cisco UCS Central

Policy Resolution Control

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

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

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

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

Note The policy resolution options in Cisco UCS Central are not supported on all versions of Cisco UCS Manager. If your Cisco UCS Manager version is earlier than the earliest supported release, the policy resolution screen may display the value as global even if it is not applicable.

In a case where you choose certain policies to be resolved locally using the Policy Resolution Control feature in Cisco UCS Central, or when a Cisco UCS Domain is unregistered from Cisco UCS Central, the global settings/unnamed policies (such as QoS Settings, Discovery policies) stay as previously configured. You must manually change the policy details to the desired state.

Caution Unregistering a Cisco UCS Domain has serious implications. You must not unregister the Cisco UCS Domain unless you choose to permanently not manage it from Cisco UCS Central.

Name	Earliest Supported Release	Description
Infrastructure & Catalog Firmware	4.1(3)	Determines whether the Capability Catalog and infrastructure firmware policy are defined locally in Cisco UCS Manager or come from Cisco UCS Central.

Name	Earliest Supported Release	Description
Time Zone Management	4.1(3)	Determines whether the time zone and NTP server settings are defined locally in Cisco UCS Manager or comes from Cisco UCS Central.
Communication Services	4.1(3)	Determines whether HTTP, CIM XML, Telnet, SNMP, web session limits, and Management Interfaces Monitoring Policy settings are defined locally in Cisco UCS Manager or in Cisco UCS Central.
Global Fault Policy	4.1(3)	Determines whether the Global Fault Policy is defined locally in Cisco UCS Manager or in Cisco UCS Central.
User Management	4.1(3)	Determines whether authentication and native domains, LDAP, RADIUS, TACACS+, trusted points, locales, and user roles are defined locally in Cisco UCS Manager or in Cisco UCS Central.
DNS Management	4.1(3)	Determines whether DNS servers are defined locally in Cisco UCS Manager or in Cisco UCS Central.
Backup & Export Policies	4.1(3)	Determines whether the Full State Backup Policy and All Configuration Export Policy are defined locally in Cisco UCS Manager or in Cisco UCS Central.
Monitoring	4.1(3)	Determines whether Call Home, Syslog, and TFTP Core Exporter settings are defined locally in Cisco UCS Manager or in Cisco UCS Central.
SEL Policy	4.1(3)	Determines whether the SEL Policy is defined locally in Cisco UCS Manager or in Cisco UCS Central.
Power Allocation Policy	4.1(3)	Determines whether the Power Allocation Policy is defined locally in Cisco UCS Manager or in Cisco UCS Central.
Power Policy	4.1(3)	Determines whether the Power Policy is defined locally in Cisco UCS Manager or in Cisco UCS Central.
Equipment Policy	4.1(3)	Determines whether the Equipment Policy is defined locally in Cisco UCS Manager or in Cisco UCS Central.
Port Configuration	4.1(3)	Determines whether port configuration is defined locally in Cisco UCS Manager or in Cisco UCS Central.
Power Save Policy	4.1(3)	Globally manages the chassis to maximize energy efficiency or availability.
Cisco UCS X9508 Chassis Power Extended Policy	4.1(3)	Manages the chassis to maximize energy efficiency or availability.

Name	Earliest Supported Release	Description
Cisco UCS X9508 Chassis Fan Control Policy	4.1(3)	Manages you to control the fan speed to bring down server power consumption and noise levels.

Policies

To assign a policy or a Management IP pool/policy to a domain profile, click on the policy and then click on the drop-down list to select the policy you want to assign to a profile. You can assign the following policies to a domain:

- **QoS System Class** - Defines a configurable set of system classes that you can include in a QoS Policy.
- **Port Auto-Discovery Policy**- Determines whether Server Port Auto-Discovery enabled or disabled in Cisco UCS Central.
- **Hardware Change Discovery Policy**- Determines if a hardware replacement deep discovery is triggered automatically, or after user acknowledgement from Cisco UCS Central.
- **KMIP Certification Policy** - KMIP Certification Policy enables using Self-Encrypting Drives (SEDs) through key management servers. This policy aims to generate a certificate that will be used by CIMC to communicate with KMIP server to get the key. You can configure this policy to a domain if it is created in a global scope.

Management IP

You can assign the following pools/policies from the **Management IP** pool:

- **Inband Policy** - Policy to configure the Inband IP address on a server directly, or through an Inband policy.
- **Outband Pool** - Sets the Management IP Pool created for Outband network management.

Note The **Management IP** tab in the **Domain Configuration Settings** window is enabled only when the registered Cisco UCS Domain is Cisco UCS Manager 4.1(3) and later. For all earlier Cisco UCS Manager releases, the Management IP tab is hidden.

Consequences of Policy Resolution Changes

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

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

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

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

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

Policies and Configuration	Policy Source		Behavior in Cisco UCS Manager on Registration with Cisco UCS Central		Behavior in Cisco UCS Manager when Registration Changed	
	Cisco UCS Central	Cisco UCS Manager	Domain Group Unassigned	Domain Group Assigned	Unassigned from Domain Group	Deregistered from Cisco UCS Central
Maintenance Policy Schedule Host Firmware Packs	N/A	Assigned domain group	See Consequences of Service Profile Changes on Policy Resolution, on page 32	See Consequences of Service Profile Changes on Policy Resolution, on page 32	Deletes remote policies	Converted to a local policy
Maintenance Policy Schedule Host Firmware Packs	N/A	Assigned domain group	See Consequences of Service Profile Changes on Policy Resolution, on page 32	See Consequences of Service Profile Changes on Policy Resolution, on page 32	Deletes remote policies	Converted to a local policy
Maintenance Policy Schedule Host Firmware Packs	N/A	Assigned domain group	See Consequences of Service Profile Changes on Policy Resolution, on page 32	See Consequences of Service Profile Changes on Policy Resolution, on page 32	Deletes remote policies	Converted to a local policy
Password Profile	Domain group root	N/A	N/A	N/A	N/A	N/A
Password Encryption key	Domain group root	N/A	N/A	N/A	N/A	N/A

Consequences of Service Profile Changes on Policy Resolution

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

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

Policy	Behavior in Cisco UCS Manager on Registration with Cisco UCS Central		Domain Group Assigned after Registration with Cisco UCS Central
	Domain Group Unassigned / Domain Group Assigned		
	Service Profile not Modified	Service Profile Modified	
Maintenance Policy **Note** If you are using a global maintenance policy in a local service profile, all pending activities must be acknowledged on the Cisco UCS Central **Pending Activities** page.	Local	Local, but any "default" policies are updated on domain group assignment	Local/Remote (if resolved to "default" post registration)
Schedule	Local	Local, but any "default" policies are updated on domain group assignment	Local/Remote (if resolved to "default" post registration)
Host Firmware Packages	Local	Local, but any "default" policies are updated on domain group assignment	Local/Remote (if resolved to "default" post registration)

Cloning a Policy

Cisco UCS Central enables you to clone a policy with a new name, parent organization or domain group, and description if applicable, to help you make minor edits without having to create a new policy.

Before you begin

- You must have Create/Edit access to the policy.
- You can clone only one policy at a time.
- None of the 'oper' based properties are included in a cloned policy.

⚠

Caution Cloning is not enabled on the following:

- Schedules
- Pools
- Organizations
- Domain Groups
- Tag types
- VLANs
- VSANs

Procedure

Step 1 In the **Browse Tables** icon, click **Policies**.

Step 2 Click the check box next to the policy you want to clone, and click on the **Clone** icon.

Step 3 Choose the **Organization** or **Domain Group** where you want to create the policy, and enter the **Name** for the cloned policy and optional **Description**.

The name is case sensitive.

Step 4 Click **Clone**.

When you clone a policy, you should click **Evaluate** to estimate the impact of the changes before saving the cloned policy. You cannot duplicate policy names when you clone a policy. All cloned policies must have a unique name.

Domains and Domain Groups

When you register a Cisco UCS Manager instance in Cisco UCS Central, that instance becomes an ungrouped domain in Cisco UCS Central. You must assign this domain to a domain group to start managing this domain using global policies in Cisco UCS Central.

Cisco UCS Central creates a hierarchy of Cisco UCS domain groups for managing multiple Cisco UCS domains.

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

If you have created a domain group policy, and a new registered Cisco UCS domain meets the qualifiers defined in the policy, it is automatically be placed under the domain group specified in the policy. If not, it is placed in the ungrouped domains category until the domain group is assigned to a domain group.

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

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

Creating or Editing a Domain Group

Procedure

Step 1 In the **Actions** bar, type **Create Domain Group** and press Enter.

Step 2 In the **Domain Group** dialog box, click **Basic** and choose the **Domain Group Location** in which you want to create the domain group.

Step 3 Enter a **Name** and optional **Description**.

The name is case sensitive.

Step 4 In **Qualification**, select the **Qualification Policies** that you want to use to identify the Cisco UCS Manager domains.

All domains that meet the qualification policy are automatically added to the domain group.

Step 5 In **Domains**, select the Cisco UCS Manager domains that you want to add to the domain group.

Step 6 Click **Create**.

Adding a Domain to a Domain Group

Procedure

Step 1 In the **Actions** bar, type **Assign Domain to Domain Group**.

Step 2 In the **Domain to Domain Group** dialog box, in the **Domain** drop-down, select the Cisco UCS Manager domain that you want to add to the domain group.

Note
You can also select a domain, click the Operations icon, and select **Assign Domain to Domain Group**. In this case, the Cisco UCS Manager domain is pre-populated in the **Domain** drop-down.

Step 3 In the **Domain Group Location** drop-down, select domain group where you want to add the domain.

Step 4 Click **Assign**.

Managing Domain Group SNMP

Procedure

Step 1 Click the **Domain Group Navigation** icon and choose a domain group.

Step 2 Click the **Configuration** icon and choose **SNMP**.

Step 3 In **Basic**, click **Enabled**, then enter the **Community/User Name**.

Cisco UCS includes the SNMP v2c community name or the SNMP v3 username when it sends the trap to the SNMP host. This must be the same as the community or username that is configured in **SNMP Traps**.

Step 4 Enter the optional **System Contact** and **System Location**.

Step 5 In **SNMP Traps**, click **Add** and complete the following:

a) Enter the same **Community/User Name** from the **Basic** section.
b) Enter the **Port**, and select values for the SNMP **Version**, the **Type**, and the **V3 Privilege**.

Step 6 In **SNMP Users**, click **Add** and complete the following:

a) Enter the **SNMP User Name**.
b) Select the **Authentication Type** and whether to enable **AES-128 Encryption**.
c) Enter and confirm the values for the password and privacy password.

Step 7 Click **Save**.

Domain Group Qualification Policy

Domain group qualification policy enables you to automatically place new Cisco UCS domains under domain groups. You can create qualifiers based on Owner, Site and IP Address of various Cisco UCS domains based on your management requirements. When you register a new Cisco UCS domain, Cisco UCS Central analyses the domain based on the pre defined qualifiers in the domain group qualification policy and places the domain under a specific domain group for management.

Creating or Editing a Domain Group Qualification Policy

Procedure

Step 1 In the **Actions** bar, type **Create Domain Group Qualification Policy** and press Enter.

Step 2 In the **Domain Group Qualification Policy** dialog box, click **Basic** and choose the **Organization** in which you want to create the domain group qualification policy.

Step 3 Enter a **Name** and optional **Description**.

The policy name is case sensitive.

Step 4 In **Owner**, enter the owner name and regex.

Step 5 In **Site**, enter the site name and regex.

Step 6 In **IP Address**, add the IP address ranges.

Step 7 Click **Create**.

Organization

The **Organization** page enables you to view logical entities created under an organization that exists in a registered Cisco UCS domain.

Click one of the following icons to launch the specific page.

- **Service Profiles**—Displays all service profiles in the organization.
- **Service Profile Templates**—Displays all service profile templates in the organization.
- **Pools**—Displays all pools in the organization.
- **Policies**—Displays all policies in the organization.
- **Permitted VLANs**—Displays VLANs permitted in the organization.

Updating Organization Descriptions

After an organization is created, you can update the description.

Procedure

Step 1 In the **Edit Organization** dialog box, enter the **Description** for the organization.

Step 2 Click **Save**.

CHAPTER 5

Installation of Cisco UCS Central

Overview of Cisco UCS Central 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

Note Cisco UCS Central images are delivered in digitally signed OVA file.

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 **Products and Downloads**.

Step 3 In the center pane, click **All Downloads**.

Step 4 Click **Browse All** or enter your product in the search bar.

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

Step 5 Select **Servers - Unified Computing** > **UCS Central SoftwareUCS Central x.x**.

Choose the version that you want to download. For example, UCS Central 2.x.

Step 6 In the right pane, click the link for the Cisco UCS Central software in the format that you want:

- An OVA file with a name such as `ucs-central.2.x.x.ova`
- An ISO file with a name such as `ucs-central.2.x.x.iso`

Step 7 On the page from which you download the software, click the **Release Notes** link to download the latest version of the Release Notes.

Step 8 Click the link for the release of the Cisco UCS Central software that you want to download.

Step 9 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 10 Follow the prompts to complete your download of the software.

What to do next

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

Hardware Requirements

Hardware Requirements

The minimum memory required for client system is 32 GB. However if you have 40 or more registered Cisco UCS Domains, it is recommended to have at least 48 GB memory on the client system.

The minimum system requirements for Cisco UCS Central include a disk space of 200 GB, at least 32 GB of RAM, and a minimum of 10 vCPUs.

For virtual machine types 8.0 or later, it is recommended to select the Guest operating system as Alma Linux (64-bit). For earlier versions, select the guest OS as Red Hat Enterprise Linux 6 (64-bit).

Supporting Browsers

We recommend using the most recent version of one of the following supported browsers for Windows, LinuxRHEL, and MacOS:

- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Apple Safari

Note Cisco UCS Central does not support browser full screen mode.

We recommend the below screen resolutions to launch the Cisco UCS Central GUI:

- 1920 x 1080
- 1600 x 900
- 1440 x 900
- 1360 x 768
- 1280 x 768
- 1280 x 720
- 1280 x 600

Supported Operating Systems

The released ISO is supported by the following:

- VMware ESXi 7.x, ESXi 8.0 and later

  See the VMware Product Lifecycle website at *https://lifecycle.vmware.com/#/*
- Microsoft Hyper-V Server 2022, Microsoft Hyper-V Server 2025, and later
- KVM Hypervisor on Red Hat Enterprise Linux 8.7 and later

The released OVA is supported by VMware ESXi 7.x, ESXi 8.0 and later.

Installing Cisco UCS Central ISO File

Installing Cisco UCS Central ISO File in VMware

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 For virtual machine types 8.0 or later, it is recommended to select the Guest operating system as Alma Linux (64-bit). For earlier versions, select the guest OS as Red Hat Enterprise Linux 9 (64-bit). For ESXi 8, Secure boot option must be disabled.
Guest operating system	A supported operating system, such as RHEL 9.4.
Number of vCPU	10
Memory	No less than 32GB
Virtual adapter	1 virtual adapter with VM network
SCSI controller	LSI Logic parallel
Virtual disk	No less than 200GB (100GB +100GB) of available disk space You also need to create a second 100 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 100GB of available disk space and an additional 100GB for remote disk Cluster Installations.

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 disks should be 100GB). 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) `Cisco Smart Licensing is mandatory for UCS Central 2.1 and later..`

   At the following prompt, choose Yes if Smart Licensing is available; otherwise, select No.

   `Please confirm that you have UCS Central licenses in the Cisco Smart Licensing system to proceed [yes/no].`

   If no, `Cisco Smart Licensing is mandatory for UCS Central 2.1 installation to proceed. Installation is terminating. Press any key to shut down.`

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

   To restore, you must enter the password encryption key.

c) 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).

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

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

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 32GB
Network adapter	Default
Number of vCPU	10
Virtual disk	No less than 200GB (100GB +100GB) of available disk space You also need to create a second 100 GB virtual disk in Step 2.

Note

- Choose **Generation 2** in the **Select Generation** pane.
- Choose the template **Microsoft UFFI Certificate Authority**.

Step 2 Under the same IDE controller as the first virtual drive, create a second virtual drive for the VM with no less than 100GB 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 100GBs). 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) `Cisco Smart Licensing is mandatory for UCS Central 2.1 and later..`

At the following prompt, choose Yes if Smart Licensing is available; otherwise, select No.

```
Please confirm that you have UCS Central licenses in the Cisco Smart Licensing
system to proceed [yes/no].
```

If no, `Cisco Smart Licensing is mandatory for UCS Central 2.1 installation to proceed. Installation is terminating. Press any key to shut down.`

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

You must provide a password encryption key to restore the configuraiton.

c) 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).

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

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

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 32GB
Network adapter	Default
Number of vCPU	10
Virtual disk	No less than 100GB of available disk space You also need to create a second 100GB virtual disk under IDE Controller in Step 2. Configure the two virtual SATA disks, you can choose the **Disk bus** as **SATA** and ensure that each disk has a minimum of 100GB.

Note
To enable UEFI boot, from the **Overview** section, choose **UEFI X86_64...** option from the **Firmware** drop-down box.

Step 2 Under the same IDE controller as the first virtual drive, create a second virtual drive for the VM with no less than 100GB 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 100GBs). 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) `Cisco Smart Licensing is mandatory for UCS Central 2.1 and later..`

At the following prompt, choose Yes if Smart Licensing is available; otherwise, select No.

```
Please confirm that you have UCS Central licenses in the Cisco Smart Licensing
system to proceed [yes/no].
```

If no, `Cisco Smart Licensing is mandatory for UCS Central 2.1 installation to proceed. Installation is terminating. Press any key to shut down.`

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

   You must provide a password encryption key to restore the configuration.

c) 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).

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

e) At the `Enter the Default Gateway :` prompt, enter the default gateway used by Cisco UCS Central 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 Central 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.

Installing Cisco UCS Central OVA File

OVA Installation in VCenter

Procedure

Step 1 On the Cisco.com download site for Cisco UCS Central Software, download the Cisco UCS Central OVA.

The files are stored in your local download folder.

Step 2 Log in to the vCenter server, right-click on any inventory object and select **Deploy OVF Template**.

The **Deploy OVF Template wizard** is displayed.

Step 3 Specify the location of the OVA on the **Select an OVF template** page, and click **Next**.

Step 4 Enter a unique name for the virtual machine, and select a deployment location on the next page. Click **Next**.

Step 5 Select a resource to run the deployed OVA. Click **Next**.

Step 6 Verify the OVA details, and click **Next**.

Step 7 Select a storage location. Click **Next**.

(Optional) Select virtual disk format as **Thin provision**.

Step 8 Select a source network, and map it to a destination network. Click **Next**.

Note
Proceed with the default settings.

Step 9 Review the information on the **Ready to complete** page, and click **Finish**.

Step 10 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 11 If have not powered up the VM as part of importing the OVA file , power up the Cisco UCS Central VM.

Step 12 Open up a console window for the Cisco UCS Central VM.

Step 13 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) `Cisco Smart Licensing is mandatory for UCS Central 2.1 and later..`

At the following prompt, choose Yes if Smart Licensing is available; otherwise, select No.

```
Please confirm that you have UCS Central licenses in the Cisco Smart Licensing
system to proceed [yes/no].
```

If no, `Cisco Smart Licensing is mandatory for UCS Central 2.1 installation to proceed. Installation is terminating. Press any key to shut down.`

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

c) 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).

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

e) At the `Enter the Default Gateway :` prompt, enter the default gateway used by Cisco UCS Central 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 Central 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.

Importing the IdenTrust Certificate Chain

The Cisco UCS Central OVA file is signed with an IdenTrust CA certificate, which is not included in VMware's default truststore. As a result, the Review details page in the Deploy OVF Template wizard indicates that you are using an invalid certificate while completing the wizard.

You can prevent this by importing the IdenTrust certificate chain to the host or cluster on which you want to deploy the OVA file.

Procedure

Step 1 On the VMware ESXi host or cluster where your virtual appliance will reside, download the **Issuing CA Cert (PEM)** (trustidevcodesigning4.pem) and **Root CA Cert** (identrustcommercialrootca1.pem) for **TrustID EV Code Signing CA 4** from https://www.cisco.com/security/pki/codesign.

Step 2 Log in to the vSphere Web Client.

Step 3 Select **Administration** > **Certificates** > **Certificate Management**.

Step 4 In the **Trusted Root Certificates** field, click **Add**.

Step 5 Check the **Start Root certificate push to vCenter Hosts** check box. Click **Add**.

Step 6 In the **Add Trusted Root** dialog box, click **Browse**.

Step 7 Navigate and select the certificate chain you downloaded in Step 1 (**trustidevcodesigning4.pem** and **identrustcommercialrootca1.pem**). Click **Open**.

The files gets displayed in the **Add Trusted Root Certificate** page.

Step 8 Click **Add**.

A message indicates that the certificate chain was imported.

When you complete the Deploy OVF Template wizard, the Publisher field in the Review details page indicates that you are using a trusted certificate.

What to do next

OVA Installation in VCenter, on page 48

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.

Mount the ISO from ESXi:

- Click **Edit Settings** and do the following:
- In the **CD/DVD Media** settings, select the **Browse** option and choose the most recent UCS Central ISO file.
- Under the **Boot Options**, enable **Force BIOS Setup**.
- Click **Save**.
- Reboot the VM instance.
- From the GRUB boot options, choose **Reset UCS Central Admin Password** option.

  For additional assistance, please reach out to TAC for further guidance.

  Ensure that the ISO image is unmounted after completing the password reset process.

Mount the ISO from Hyper-V:

- Select the VM settings.
- Modify the boot sequence in the Firmware settings.
- Mount the ISO inage.
- Restart the VM instance.
- Choose the Reset UCS Central password option from the GRUB menu.

  For additional assistance, please reach out to TAC for further guidance.
- Before rebooting, update the boot order to prioritize the disk containing Cisco UCS Central.

Mount the ISO from RHEL KVM:

- Choose the **Details** option under the **View** section.
- Mount the ISO under SATA CD-ROM drive.
- Update the boot order and ensure both the SATA CD-ROM and the disk containing Cisco UCS Central are selected under Boot options.
- Apply the settings
- Restart the VM instance.
- Choose the **Reset UCS Central password** option from the GRUB menu.

  For further assistance, please contact TAC for additional support.
- Unmount the ISO file before rebooting.

Upgrading from Cisco UCS Central 2.0 or an Earlier Release

- There is no direct upgrade path supported to Cisco UCS Central release 2.1 from an earlier release.
- Backup restoration to Cisco UCS Central Release 2.1 is supported from Cisco UCS Central Release 2.0(1s) and later.

For more information, see Installation of Cisco UCS Central.

Restoring the Cisco UCS Central VM

- This procedure describes the process to restore using an OVA and ISO file.
- Backup restoration to Cisco UCS Central Release 2.1(1a) is compatible with Cisco UCS Central version 2.0(1s) and later.
- As a general recommendation, wait approximately 20 to 30 minutes after the restore operation before attempting GUI login. This ensures that system initialization is complete and CPU utilization has normalized, which can be verified through the CLI. Execute the following commands:

```
ucsCentral#connect local-mgmt
ucsCentral(local-managament)#show processes
```

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) `Cisco Smart Licensing is mandatory for UCS Central 2.1 and later..`

At the following prompt, choose Yes if Smart Licensing is available; otherwise, select No.

`Please confirm that you have UCS Central licenses in the Cisco Smart Licensing system to proceed [yes/no].`

If no, `Cisco Smart Licensing is mandatory for UCS Central 2.1 installation to proceed. Installation is terminating. Press any key to shut down.`

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

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

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

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

f) 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**.

g) 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**.

h) 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**.

i) 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**.

j) At the `Enter the Password to be used for backup file transfer` : prompt, enter the password for the remote server username and press **Enter**.

k) At the `Enter the key for decrypting the backup file (if backup taken from 201u or before, press enter to proceed` **:** prompt, enter the password encryption key to restore the configuration and press **`Enter`**.

l) 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 6

Tags

Tags and Tag Types

Cisco UCS Central uses tags to allow users to group objects outside of the Organization or Domain Group structures. You can use the following types of tags:

- System-defined tags—Tags that are defined by Cisco UCS Central. This includes the Maintenance Group tag, the Operating System for HCR tag, and the Adapter Driver for HCR tag.
- User-defined tags—Tags that are created by users but have specific values.
- Basic tags—Free text tags that can allow any value.

From the **Tag Management** page in the GUI, you can view all Tag Types that have been created in Cisco UCS Central. However, you can view only the Tags that are associated with an object and are in active use at any given time.

Creating a Tag Type

Only users with the Tag permission can create tag types.

Procedure

Step 1 In the **Actions** bar, type **Create Tag Type** and press Enter.

Step 2 In the **Basic** tab, enter the **Name** and optional **Description**.

Step 3 Select a color to assign to the tag, or accept the default.

Step 4 Choose whether you want to allow this tag to be assigned more than once to the same object.

Step 5 Choose one of the following:

- **Free Text**—Allows any text to be entered when the tag is assigned.
- **Predefined List**—You can create a list of values, or add additional values to a list of values. When the tag is assigned, you choose one of the values from the list.

Click the **Values** tab to add the specific values.

Step 6 Click **Create**.

Adding a Tag

You can add tags to policies, logical resources such as service profiles and ID pools, and physical inventory components such as domains or servers.

Procedure

Step 1 Navigate to the item that you want to tag.

Step 2 Click the **Tag** icon.

Step 3 In the **Add Tag** drop-down, select the tag type that you want to use.

Note
All user-defined tag types are displayed, but only system-defined tag types that can be applied to the specific object are listed. For example, you cannot apply a Maintenance Group tag type to a VLAN, so that tag type is hidden.

Step 4 Enter the values for the tag or select the tag value from the drop-down list.

Step 5 Click **Add**.

CHAPTER 7

License Management

Overview

Cisco Smart licensing is simple, flexible and a smart way of procuring, deploying and managing licenses in your environment. For more information on smart licensing, see http://www.cisco.com/web/ordering/smart-software-licensing/index.html

Smart Licensing

- Dynamic licensing. Licenses are associated with products and transferable within the virtual account.
- No license installation is necessary.
- License pools are account-specific. Any device in your company can use them.
- Licenses can be transferred between product instances without any software installation. You can transfer unused licenses from one virtual account to another.

Smart Licensing

Smart licenses are server based licenses. You will purchase, deploy and track licenses for servers instead of domains. Instead of registering individual products with license files or PAKs, Smart Licensing provides the option to create a pool of licenses that can be used across your company's portfolio.

Smart licensing uses Virtual Accounts, Product Instances and Registration Tokens to procure, deploy and manage licenses in your environment.

Virtual Accounts

Virtual accounts are collections of licenses and product instances. You can create virtual accounts in Cisco Smart Software Manager to organize the licenses for your company into logical entities. You can use virtual accounts to organize licenses by business unit, product type, IT group, or whatever makes sense for your organization. For example, if you segregate your company into different geographic regions, you can create a virtual account for each region to hold the licenses and product instances for that region.

All new licenses and product instances are placed in a virtual account. You choose the virtual account when you register a product instance. You can transfer existing licenses or product instances from one virtual account to another.

For more information on creating virtual accounts in Cisco Smart Software Manager, see http://www.cisco.com/web/ordering/smart-software-manager/docs/smart-software-manager-user-guide.pdf.

Product Instances

A Cisco UCS Central product instance has a unique device identifier (UDI) that is registered using a product instance registration token. You can register several instances of a product with a single registration token. Each product instance can have one or more licenses that reside in the same virtual account.

Registration Tokens

Registration tokens are stored in the Product Instance Registration Token Table that is associated with your smart account. After you enable Smart Licensing in Cisco UCS Central, you can generate a new token in a virtual account on the Smart Software Licensing portal to register in Cisco UCS Central.

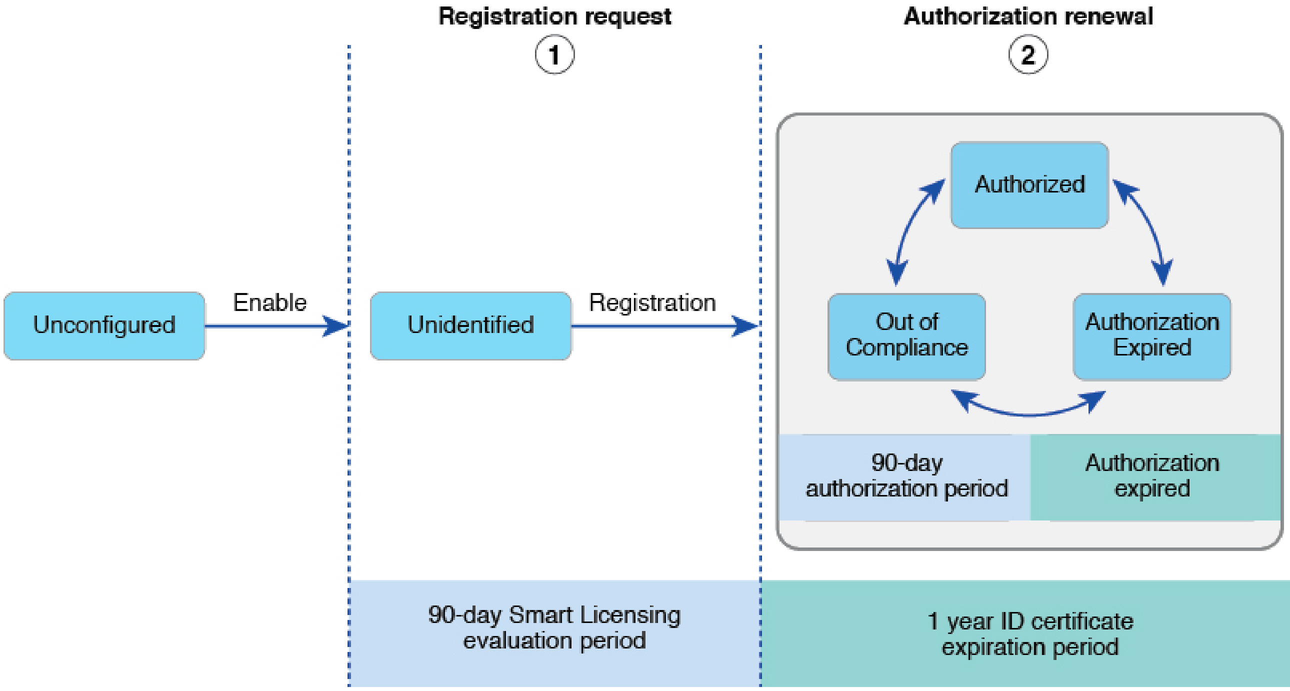
For more information on creating virtual accounts in Cisco Smart Software Manager, see http://www.cisco.com/web/ordering/smart-software-manager/docs/smart-software-manager-user-guide.pdf.

Obtaining Licenses

To obtain licenses using smart licensing, you will have to do the following:

- Generate tokens in Cisco Smart Software Manager virtual accounts.
- Register licenses for product instances in Cisco UCS Central.

The following illustrations explains the smart licensing process:



1	**Registration request**	The Smart Licensing 90-evaluation period starts when the product instance begins using the licensing feature. It not renewable. When the evaluation period expires, the agent sends a notification to the platform.
2	**Authorization renewal**	Authorization requests can result in an **Authorized** or **Out of Compliance (OOC)** response, or in an error due to a communication failure. Authorization periods are renewed every 30 days as long as authorization requests return **Authorized** or **Out of Compliance (OOC)** responses. When the authorization period expires, the agent continues to retry renewal with authorization requests. If successful, a new authorization period starts. If ID cert renewal (authorization renewal) fails, the product instance moves to an Unidentified state and begins consuming the evaluation period.

Enabling Smart Licensing

Before you begin

- Specify a DNS server.

Procedure

Step 1 Click the **System Configuration** icon and choose **Licenses**.

Step 2 Click **Enable Smart Software Licensing**.

System enables smart licensing and information related to traditional licensing is replaced with smart licensing related information.

Registering UCS Central Using a License Token

Before you begin

Make sure Smart Licensing is enabled.

Procedure

Step 1 Click the **System Configuration** icon and choose **Licenses**.

Step 2 Click the **Smart Software Manager** link to go to the Smart Software Manager portal.

Step 3 In the Smart Software Manager portal:

a) Select a Cisco UCS Central virtual account.

b) Click **New Token** in the **Product Instance Registration Tokens** panel and select **Copy**.

Step 4 In the Cisco UCS Central **Smart Software Licensing** panel, click **Register Smart Software Licensing**.

Step 5 In the **Register Smart Licensing** dialog box, enter the following:

- **HTTP Proxy**—Enter the IP address or hostname of the HTTP proxy server.
- **HTTP Proxy Port**—Enter the port number for the proxy server.
- **Product Instance Registration Token**—Paste the new token you generated.

Step 6 Click **Register**.

You will receive notifications on registration in progress, successful registration or failure to register.

Renewing Authorization

License authorization is used to show if you have enough licenses for your system, or if you are out of compliance. Authorization is renewed automatically by the Smart Licensing agent every 30 days, provided the network is up and Cisco UCS Central can reach the Smart License server.

If authorization is not renewed for 90 days, the authorization will expire.

Procedure

Step 1 Click the **System Configuration** icon and choose **Licenses**.

Step 2 In the Cisco UCS Central **Smart Software Licensing** panel, click the **Tools** menu.

Step 3 Select **Renew Authorization Now**.

Renewing Registration

The agent automatically renews the Smart Software Licensing registration certificate or the ID certificate every six months. Certification lasts for one year. If Cisco UCS Central cannot communicate with the Smart License Server, it may fail to renew the certificate. If this occurs, the certification will revert to evaluation state after one year.

Procedure

Step 1 Click the **System Configuration** icon and choose **Licenses**.

Step 2 In the Cisco UCS Central **Smart Software Licensing** panel, click the **Tools** menu.

Step 3 Select **Renew Registration Now**.

Deregistering Smart Software Licensing

When you deregister a product instance from Smart Software Licensing, the product will not be associated with the license. The product will be removed from the list of registered products for the associated virtual account. You can use the license to register another product, or reregister a product that has been deregistered.

Procedure

Step 1 Click the **System Configuration** icon and choose **Licenses**.

Step 2 In the Cisco UCS Central **Smart Software Licensing** panel, click the **Tools** menu.

Step 3 Select **Deregister** to remove Cisco UCS Central from Smart Software Manager.

Disabling Smart Software Licensing

If you disable Smart Software Licensing, Cisco UCS Central automatically returns to the Evaluation mode.

Note Only one licensing mode is supported at a time.

Procedure

Step 1 Click the **System Configuration** icon and choose **Licenses**.

Step 2 In the Cisco UCS Central **Smart Software Licensing** panel, click the **Action** menu.

Step 3 Select **Disable Smart Software Licensing**.