Cisco UCS Central Deployment Guide, Release 1.0

First Published: November 20, 2012

Last Modified: April 02, 2013

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

Text Part Number: OL-28304-03

CONTENTS

Preface

This preface includes the following sections:

Audience

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

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

Conventions

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

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

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

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

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

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

Warning IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS

Related Cisco UCS Documentation

Documentation Roadmaps

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

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

Other Documentation Resources

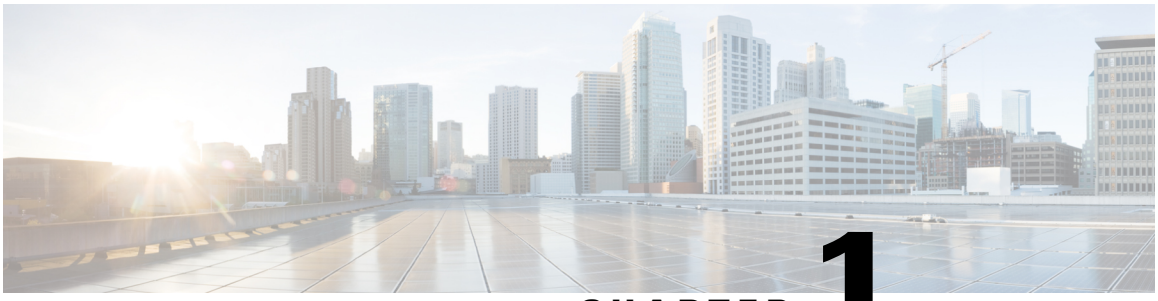
An ISO file containing all B and C-Series documents is available at the following URL: http://www.cisco.com/cisco/software/type.html?mdfid=283853163&flowid=25821. From this page, click **Unified Computing System (UCS) Documentation Roadmap Bundle**.

The ISO file is updated after every major documentation release.

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

Documentation Feedback

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



CHAPTER 1

Overview of Cisco UCS Central

This chapter includes the following sections:

About Cisco UCS Central

Cisco UCS Central allows you to manage multiple Cisco UCS domains or through a single management point. 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 replace Cisco UCS Manager, which is the basic engine for managing a Cisco UCS domain. Instead, it builds on the capabilities provided by Cisco UCS Manager and works with Cisco UCS Manager to effect changes in individual domains.

For a Cisco UCS domain to be managed by Cisco UCS Central, you must first register that domain with Cisco UCS Central.

Cisco UCS Central allows you to ensure global policy compliance, with subject-matter experts choosing the resource pools and policies that need to be enforced globally or managed locally. With a simple drag-and-drop operation, service profiles can be moved between geographies to enable fast deployment of infrastructure, when and where it is needed, to support business workloads.

You can use Cisco UCS Central to view and manage data that is distributed over a large number of individual domains. For example, you can do the following in Cisco UCS Central:

- View the hardware inventory in one or more registered domains.
- Launch the KVM Console to view an individual server in a registered domain.
- Launch Cisco UCS Manager in a registered domain.
- View faults, events, and audit logs in one or more registered domains.
- Handle one-to-many functions, such as global ID pools, global policies, and firmware management across all registered domains.

Cisco UCS Central does not reduce or change any local management capabilities of Cisco UCS Manager, such as its API. This allows administrators to continue usingCisco UCS Manager the way they did before even in the presence of Cisco UCS Central and also allows all existing third party integrations to continue to operate without change. Selectively they can allow polices to be globalized providing them with an easy transition to centralized management.

Cisco UCS Central Features

Cisco UCS Central includes the following features:

Centralized inventory

Manual inventory spreadsheets are no longer needed. Cisco UCS Central automatically aggregates a global inventory of all Cisco UCS components, organized by domain, with customizable refresh schedules. Cisco UCS Central provides even easier integration with ITIL processes, with direct access to the inventory through an XML interface.

Centralized fault summary

Quickly and easily view the status of all registered Cisco UCS domains with a quick-look global fault summary panel, a fault summary organized by domain and fault type, with views into individual Cisco UCS domains for greater fault detail and more rapid problem resolution.

Centralized policy-based firmware upgrades

Take the guesswork and manual errors out of updating infrastructure firmware. You can download firmware updates automatically from the Cisco.com website to a firmware library within Cisco UCS Central. Then you can update the firmware for registered domains, globally or selectively, on an automated schedule or as your business workloads allow. Managing firmware centrally helps ensure compliance with IT standards and makes reprovisioning of resources a point-and-click operation.

Global ID pooling

Eliminate identifier conflicts and help ensure portability of software licenses with Cisco UCS Central. 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, for example, move server identifiers between Cisco UCS domains anywhere in the world and reboot an existing workload to run on the new server.

Domain grouping and subgrouping

Simplify policy management by creating 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 subdomains, which makes it easy to manage policy exceptions when administering large numbers of Cisco UCS domains. Each subdomain has a hierarchical relationship with the parent domain.

Global administrative policies

Help ensure compliance and staff efficiency with global administrative policies. These 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.

Cisco UCS Central 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 is similar to the XML API for Cisco UCS Manager, making integration with high-level management software very fast.

Cisco UCS Manager backups

The backup facility in Cisco UCS Central enables you to quickly and efficiently back up the configuration from Cisco UCS Manager in registered Cisco UCS domains. You can configure automated backups to occur on a specific schedule, or perform manual backups as your business needs require.

Domain Groups

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

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

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

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

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

Policies

Cisco UCS Central acts as a global policy server for registered Cisco UCS domains. Configuring global Cisco UCS Central policies for remote Cisco UCS domains involves registering domains and assigning registered domains to domain groups.

In addition, the policy import capability allows a local policy to be globalized inside of Cisco UCS Central. You can then apply these global policies to other registered Cisco UCS domains.

You can define the following global policies in Cisco UCS Central that are resolved by Cisco UCS Manager in a registered Cisco UCS domain:

Backup Policies

The full state backup policy allows you to schedule regular full-state backups of a snapshot of the entire system. You can choose whether to configure the full-state backup to occur on a daily, weekly, or bi-weekly basis.

The all configuration backup policy allows you to schedule a regular backup and export of all system and logical configuration settings. This backup does not include passwords for locally authenticated users. You can choose whether to configure the all configuration backup to occur on a daily, weekly, or bi-weekly basis.

Call Home Policy

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

Capability Catalog

This policy is a set of tunable parameters, strings, and rules. Cisco UCS Manager uses the catalog to update the display and component configurations such as newly qualified DIMMs and disk drives for servers.

Core Files Export Policy

Cisco UCS Manager uses the Core File Exporter to export core files as soon as they occur to a specified location on the network through TFTP. This functionality allows you to export the tar file with the contents of the core file.

Fault Collection Policy

The fault collection policy controls the life cycle of a fault inCisco UCS domains, including when faults are cleared, the flapping interval (the length of time between the fault being raised and the condition being cleared), and the retention interval (the length of time a fault is retained in the system).

Firmware Image Management

Cisco UCS uses firmware obtained from and certified by Cisco to support the endpoints in Cisco UCS domains. Each endpoint is a component in Cisco UCS domains that requires firmware to function. The upgrade order for the endpoints in Cisco UCS domains depends upon the upgrade path, and includes Cisco UCS Manager, I/O modules, fabric interconnects, endpoints physically located on adapters, and endpoints physically located on servers. Cisco delivers all firmware updates to Cisco UCS components in bundles of images. Cisco UCS firmware updates are available for download to fabric interconnects in Cisco UCS domains.

Host Firmware Package

This policy enables you to specify a set of firmware versions that make up the host firmware package (host firmware pack). The host firmware pack includes the firmware for server and adapter endpoints including adapters, BIOS, board controllers, Fibre Channel adapters, HBA option ROM, and storage controllers.

Management Interface Monitoring Policy

This policy defines how the mgmt0 Ethernet interface on the fabric interconnect should be monitored. If Cisco UCS detects a management interface failure, a failure report is generated. If the configured number of failure reports is reached, the system assumes that the management interface is unavailable and generates a fault.

Role-Based Access Control and Remote Authentication Policies

Role-based access control is a method of restricting or authorizing system access for users based on user roles and locales. A role defines the privileges of a user in the system and the locale defines the organizations (domains) that a user is allowed access. Because users are not directly assigned privileges, management of individual user privileges is simply a matter of assigning the appropriate roles and locales.

SNMP Policy

Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network.

Syslog Policy

A syslog policy is a collection of four policy attributes including console, file, monitor, and remote destination attributes. The syslog policy includes creating, enabling, disabling, and setting attributes.

Time Zone and NTP Policies

Cisco UCS requires a domain-specific time zone setting and an NTP server to ensure the correct time display in Cisco UCS Manager. If you do not configure both of these settings in Cisco UCS domains, the time does not display correctly.

Equipment Policies

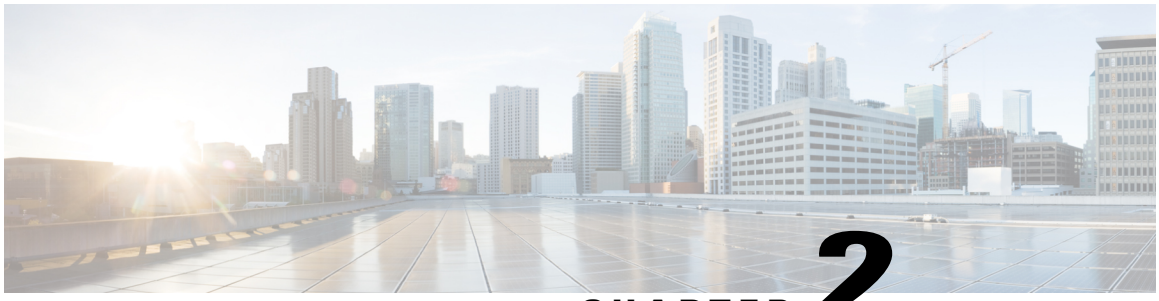
Cisco UCS Central supports global equipment policies defining the global power allocation policy (based on policy driven chassis group cap or manual blade level cap methods), power policy (based on grid, n+1 or non-redundant methods), and SEL policy. Registered Cisco UCS domains choosing to define power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

Pools

Pools are collections of identities, or physical or logical resources, that are available in the system. All pools increase the flexibility of service profiles and allow you to centrally manage your system resources. Pools that are defined in Cisco UCS Central are called **Global Pools** and can be shared between Cisco UCS domains. **Global Pools** allow centralized ID management across Cisco UCS domains that are registered with Cisco UCS Central. By allocating ID pools from Cisco UCS Central to Cisco UCS Manager, you can track how and where the IDs are used, prevent conflicts, and be notified if a conflict occurs. Pools that are defined locally in Cisco UCS Manager are called **Domain Pools**.

Note The same ID can exist in different pools, but can be assigned only once. Two blocks in the same pool cannot have the same ID.

You can pool identifying information, such as MAC addresses, to preassign ranges for servers that host specific applications. For example, you can configure all database servers across Cisco UCS domains within the same range of MAC addresses, UUIDs, and WWNs.



CHAPTER 2

Cisco UCS Central Prerequisites

This chapter includes the following sections:

System Requirements for Deploying Cisco UCS Central

Server Type

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

Required TCP Ports

The following TCP ports must be open between Cisco UCS Manager and a registered Cisco UCS domain for the firmware management and backup functionality to work correctly:

- LOCKD_TCPPORT=32803
- MOUNTD_PORT=892
- RQUOTAD_PORT=875
- STATD_PORT=32805
- NFS_PORT="nfs"(2049)
- RPC_PORT="sunrpc"(111)

Server Requirements

The following table describes the minimum requirements for the standalone rack server on which you deploy Cisco UCS Central.

Table 1: System Requirements for Cisco UCS Central by Hypervisor

Requirement	ESX Minimum Requirement	Hyper-V Minimum Requirement
Disk space	60 GB	60 GB
RAM	4 GB	4 GB
VCPU cores	1 core	2 cores
Disk read speed	> 75 MBps >125 MBps is the recommended speed.	> 75 MBps >125 MBps is the recommended speed.

Note Performance of Cisco UCS Central is not guaranteed if you deploy it on a server that does not meet the minimum disk read speed requirement.

If the disk read speed on the server is lower than the required minimum during the deployment of Cisco UCS Central, the installer displays a warning message but you can complete the deployment. However, if the disk read speed is lower than the required minimum during operation, Cisco UCS Central raises a fault, as shown in the following table, depending upon how low the disk read speed is:

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

Supported Hypervisors for Deploying Cisco UCS Central

The following table describes the support for hypervisors on which you can deploy Cisco UCS Central.

Table 2: Supported Hypervisors and Operating Systems

Hypervisors	Supported Versions
Microsoft Hyper-V	Windows 2008 R2 with SP1

Hypervisors	Supported Versions
VMware ESX	• ESX 4.0u2 • ESX 4.1u1 • ESX 5.0

Supported Web Browsers for the Cisco UCS Central GUI

Web browser support for the Cisco UCS Central GUI depends upon the operating system of the computer on which you plan to run Cisco UCS Central GUI.

Operating System	Supported Web Browsers
Microsoft Windows	• Internet Explorer 8 and above • Firefox 3.5 and above • Chrome 14 and above
Mac	• Firefox 3.5 and above • Chrome 14 and above • Safari 5 and above
Linux RHEL	• Firefox 3.5 and above • Chrome 14 and above

Information Required to Deploy Cisco UCS Central

When you deploy Cisco UCS Central, you need to provide the following information:

- Static IPv4 address for Cisco UCS Central
- IPv4 netmask
- Default gateway
- Password to be assigned to the Cisco UCS Central admin account
- Hostname for the virtual machine (VM)
- IPv4 address for the DNS server, if you plan to use one

- Name of the domain, if any, in which you plan to include Cisco UCS Central
- Shared secret, which is the password required when you register Cisco UCS domains with Cisco UCS Central

Guidelines for Cisco UCS Passwords

A password is required for each locally authenticated user account. A user with admin, aaa, or domain-group-management privileges can configure Cisco UCS Central to perform a password strength check on user passwords. If the password strength check is enabled, each user must have a strong password.

Cisco recommends that each user have a strong password. If you enable the password strength check for locally authenticated users, Cisco UCS Central rejects any password that does not meet the following requirements:

- Must contain a minimum of 8 characters and a maximum of 80 characters.
- Must contain at least three of the following:
  - Lower case letters
  - Upper case letters
  - Digits
  - Special characters
- Must not contain a character that is repeated more than 3 times consecutively, such as aaabbb.
- Must not be identical to the username or the reverse of the username.
- Must pass a password dictionary check. For example, the password must not be based on a standard dictionary word.
- Must not contain the following symbols: $ (dollar sign), ? (question mark), and = (equals sign).
- Should not be blank for local user and admin accounts.

CHAPTER 3

Deploying Cisco UCS Central

This chapter includes the following sections:

Obtaining the Cisco UCS Central Software from Cisco

Procedure

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

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

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

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

Step 5 In the right pane, click the link for the Cisco UCS Central software in the format that you want. You can download the Cisco UCS Central software in the following formats:

- An OVA file with a name such as `ucs-central.1.0.1a.ova`
- An ISO file with a name such as `ucs-central.1.0.1a.iso`

You can also download the admin password reset ISO image from this location. The Cisco UCS Central Provider Bundle should be downloaded from Cisco UCS Central and used to upgrade an existing Cisco UCS Central deployment.

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

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

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

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

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

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

What to Do Next

Deploy the VM in a supported hypervisor.

Using the Cisco UCS Central OVA File

Deploying the Cisco UCS Central OVA file in VMware

Note The Cisco UCS Central VM performs a one-time installation process the first time it starts up. Allow the installation to complete before you log in.

Procedure

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

Step 2 Open or import the Cisco UCS Central OVA file into a supported hypervisor, as required by the hypervisor. Do not continue with the next step until the VM has finished booting.

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

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

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

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

b) At the `Enter the UCS Central VM eth0 IPv4 Address :` prompt, enter the IP address assigned to Cisco UCS Central and press Enter.
You must enter a static IP address that is reserved for this Cisco UCS Central VM. Cisco UCS Central does not support Dynamic Host Configuration Protocol (DHCP).

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

d) At the `Enter the Default Gateway :` prompt, enter the default gateway used by Cisco UCS Central and press Enter.
e) At the `Enforce Strong Password (yes/no)` prompt, enter yes and press Enter.
We recommend that you choose to enforce a strong password. This setting affects the configuration of the admin and all locally authenticated user accounts for Cisco UCS Central. You can change this setting in Cisco UCS Central later, if desired.
f) At the `Enter the admin Password :` prompt, enter the password you want to use for the admin account and press Enter.
g) At the `Confirm admin Password :` prompt, re-enter the password you want to use for the admin account and press Enter.
h) At the `Enter the UCS Central VM eth0 IPv4 Address :` prompt, enter the hostname you want to use for the Cisco UCS Central VM and press Enter.
i) (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.
j) (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.
k) At the `Enter the Shared Secret :` prompt, enter the shared secret (or password) that you want to use to register one or more Cisco UCS domains with Cisco UCS Central and press Enter.
l) At the `Confirm Shared Secret :` prompt, re-enter the shared secret and press Enter.
m) 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.

Restoring the Cisco UCS Central VM from the OVA File

Before You Begin

You must have a backup file 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 the Cisco UCS Central configuration guides.

Procedure

Step 1 Save the Cisco UCS Central OVA file to a folder that you can access from the hypervisor.
Step 2 Open or import the Cisco UCS Central OVA file into a supported hypervisor, as required by the hypervisor. Do not continue with the next step until the VM has finished booting.

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

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

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

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

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

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

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

e) At the `Enter the File copy protocol[tftp/scp/ftp/sftp] :` prompt, enter the supported protocol that you want to use to copy the backup file to the Cisco UCS Central VM and press Enter.

f) At the `Enter the Backup server IPv4 Address :` prompt, enter the IP address assigned to the server where the backup file is stored and press Enter.

g) At the `Enter the Backup file path and name :` prompt, enter the full file path and name of the backup file on the server and press Enter.

h) At the `Enter the Username to be used for backup file transfer :` prompt, enter the username the system should use to log in to the remote server and press Enter.

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

j) At the `Proceed with this configuration. Please confirm[yes/no]` prompt, enter yes and press Enter.
If you think you made an error when completing any of these steps, enter no and press Enter. You will then be prompted to answer the questions again.

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

Using the Cisco UCS Central ISO File

Deploying the 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

Setting	Recommended Value
RAM	No less than 4096 MB
Network adapter	Default
Number of vCPU	2
Virtual drive	No less than 25GB of available disk space You also need to create a second virtual disk in Step 3.

Step 2 In the settings for the VM, do the following:
a) Delete the default network adapter.
b) Create a new legacy network adapter.
c) Click **Apply**.

Step 3 Under the same controller as the first virtual drive, create a second virtual drive for the VM with no less than 45GB of available disk space.

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

Step 5 Start the VM and connect to the console.

Step 6 From the **Cisco UCS Central Installation** menu on the ISO image, choose **Install Cisco UCS Central**. The Cisco UCS Central installer checks that the VM has the required RAM and disk space (two disks, one with 20GB and one with 40GB). If the VM meets the requirements, the installer formats the disks, transfers the files, and installs Cisco UCS Central.

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

Step 8 Reboot the Cisco UCS Central VM.

Deploying the 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
Data store	No less than 60GB available disk space

Setting	Recommended Value
Virtual machine type	7 or later
Guest operating system	A supported operating system, such as Linux RHEL 5.0(32-bit)
Number of vCPU	1 or 2
Memory	No less than 4GB
Virtual adapter	1 virtual adapter with VM network
SCSI controller	LSI Logic parallel
Virtual disk	No less than 20GB of available disk space You also need to create a second virtual disk in Step 2.
Advanced options	Virtual device node SCSI

Step 2 In **Edit Settings**, create a new hard disk for the VM with no less than 40GB of available disk space.

Step 3 From the **Options** menu, check **Force BIOS Setup** to change the boot options.

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

Step 5 Start the VM and connect to the console.

Step 6 From the **Cisco UCS Central Installation** menu on the ISO image, choose **Install Cisco UCS Central**. The Cisco UCS Central installer checks that the VM has the required RAM and disk space (two disks, one with 20GB and one with 40GB). If the VM meets the requirements, the installer formats the disks, transfers the files, and installs Cisco UCS Central.

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

Step 8 Reboot the Cisco UCS Central VM.

Reinstalling Cisco UCS Central from the ISO file

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

Before You Begin

We recommend that you backup your Cisco UCS Central data before you perform this procedure.

Procedure

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

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

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

Step 4 In the Cisco UCS Central installer, for the **What Would You Like To Do?** field, click the **Skip Boot Loader Updating** radio button and click **Next**.

Step 5 After the reinstallation is complete, unmount the Cisco UCS Central ISO image from the virtual CD/DVD drive.

Step 6 Reboot the Cisco UCS Central VM.

Upgrading Cisco UCS Central from the ISO file

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

Before You Begin

We recommend that you backup your Cisco UCS Central data before you perform this procedure.

Procedure

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

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

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

Step 4 In the Cisco UCS Central installer, for the **What Would You Like To Do?** field, click the **Create New Boot Loader Configuration** radio button and click **Next**.

Step 5 After the upgrade is complete, unmount the Cisco UCS Central ISO image from the virtual CD/DVD drive.

Step 6 Reboot the Cisco UCS Central VM.

Logging into and out of the Cisco UCS Central GUI

Logging in to the Cisco UCS Central GUI through HTTP

The default HTTP web link for the Cisco UCS Central GUI is `http://UCSCentral_IP`, where *`UCSCentral_IP`* represents the IP address assigned to Cisco UCS Central.

Procedure

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

Step 2 On the launch page, do the following:

a) Enter your username and password.

b) Click **Log In**.

Logging in to the Cisco UCS Central GUI through HTTPS

The default HTTPS web link for the Cisco UCS Central GUI is `https://UCSCentral_IP`, where *`UCSCentral_IP`* represents the IP address assigned to Cisco UCS Central.

Procedure

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

Step 2 On the launch page, do the following:

a) Enter your username and password.

b) Click **Log In**.

Logging out of the Cisco UCS Central GUI

Procedure

In the Cisco UCS Central GUI, click **Log Out** in the upper right.
The Cisco UCS Central GUI logs you out immediately and returns your browser to the launch page.

Logging into and out of the Cisco UCS Central CLI

Logging into the Cisco UCS Central CLI

Procedure

Step 1 In an SSH or telnet client, connect to the IP address assigned to Cisco UCS Central.

Step 2 At the `login as:` prompt, enter your Cisco UCS Central username and press Enter.

Step 3 At the `Password:` prompt, enter your password and press Enter.

Logging out of the Cisco UCS Central CLI

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

Procedure

Step 1 At the prompt, type exit and press Enter.

Step 2 Continue to type exit and press Enter at each prompt until the window closes.

Resetting the Admin Password for Cisco UCS Central

Procedure

Step 1 If you have not done so already, obtain the password reset ISO image for your release of Cisco UCS Central from Cisco.com.
The password reset ISO image has a name such as `ucs-central-passreset.1.0.1a.iso`.

Step 2 If necessary, reboot the VM and change the boot options to boot from CD ROM.

Step 3 Mount the Password Reset ISO image with the virtual CD/DVD drive.

Step 4 On the **UCS Central Admin Password Reset** page, do the following:

a) In the **Admin Password** field, enter the new admin password.

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

c) Click **Next**.

Step 5 After the password change is complete, unmount the Cisco UCS Central ISO image from the virtual CD/DVD drive.

Step 6 Reboot the Cisco UCS Central VM.

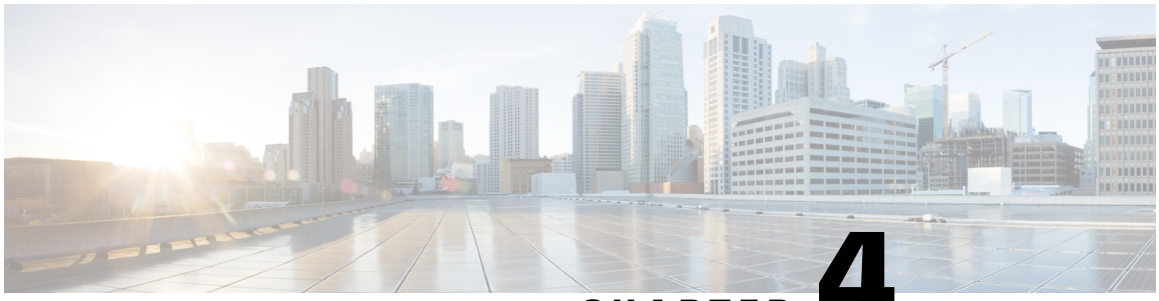
Resetting the Shared Secret

Procedure

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

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

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



CHAPTER 4

Registering Cisco UCS Domains with Cisco UCS Central

This chapter includes the following sections:

Registration of Cisco UCS Domains

You can have Cisco UCS Central manage some or all of the Cisco UCS domains in your data center.

If you want to have Cisco UCS Central manage a Cisco UCS domain, you need to register that domain. When you register, you need to choose which types of policies and other configurations, such as backups and firmware, will be managed by Cisco UCS Central and which by Cisco UCS Manager. You can have Cisco UCS Central manage the same types of policies and configurations for all registered Cisco UCS domains or you can choose to have different settings for each registered Cisco UCS domain.

Before you register a Cisco UCS domain with 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
- Obtain the shared secret that you configured when you deployed Cisco UCS Central

Note You cannot change or swap the IP addresses used by Cisco UCS Manager in a domain that is registered with Cisco UCS Central. If you need to change or swap that IP address, you must first unregister the domain from Cisco UCS Central. You can reregister the Cisco UCS domain after you have changed or swapped the IP address.

Policy Resolution between Cisco UCS Manager and Cisco UCS Central

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

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

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

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

Name	Description
Infrastructure & Catalog Firmware	Determines whether the Capability Catalog and infrastructure firmware policy are defined locally or come from Cisco UCS Central.
Time Zone Management	Determines whether the time zone and NTP server settings are defined locally or comes from Cisco UCS Central.
Communication Services	Determines whether HTTP, CIM XML, Telnet, SNMP, web session limits, and Management Interfaces Monitoring Policy settings are defined locally or in Cisco UCS Central.
Global Fault Policy	Determines whether the Global Fault Policy is defined locally or in Cisco UCS Central.
User Management	Determines whether authentication and native domains, LDAP, RADIUS, TACACS+, trusted points, locales, and user roles are defined locally or in Cisco UCS Central.

Name	Description
DNS Management	Determines whether DNS servers are defined locally or in Cisco UCS Central.
Backup & Export Policies	Determines whether the Full State Backup Policy and All Configuration Export Policy are defined locally or in Cisco UCS Central.
Monitoring	Determines whether Call Home, Syslog, and TFTP Core Exporter settings are defined locally or in Cisco UCS Central.
SEL Policy	Determines whether the SEL Policy is defined locally or in Cisco UCS Central.
Power Allocation Policy	Determines whether the Global Power Allocation Policy is defined locally or in Cisco UCS Central.
Power Policy	Determines whether the Power Policy is defined locally or in Cisco UCS Central.

Consequences of Policy Resolution Changes

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

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

Policies and Configuration	Policy Source		Behavior in Cisco UCS Manager on Registration with Cisco UCS Central		Behavior in Cisco UCS Manager when Registration Changed	
	Cisco UCS Central	Cisco UCS Manager	Domain Group Unassigned	Domain Group Assigned	Unassigned from Domain Group	Deregistered from Cisco UCS Central
Call Home	N/A Cisco UCS Manager only	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
SNMP configuration	N/A Cisco UCS Manager only	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
HTTP	N/A Cisco UCS Manager only	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy

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
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
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

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
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
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

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
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
Maintenance Policy Schedule Host Firmware Packs	N/A	Assigned domain group	See Consequences of Service Profile Changes on Policy Resolution, on page 27	See Consequences of Service Profile Changes on Policy Resolution, on page 27	Deletes remote policies	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 27	See Consequences of Service Profile Changes on Policy Resolution, on page 27	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 27	See Consequences of Service Profile Changes on Policy Resolution, on page 27	Deletes remote policies	Converted to a local policy

Consequences of Service Profile Changes on Policy Resolution

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

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

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

Cisco UCS Releases Supported for Registering a Cisco UCS Domain

The following table lists the Cisco UCS release for the Cisco UCS Manager and infrastructure in a Cisco UCS domain that you want to register with Cisco UCS Central. All patches for the maintenance release listed are supported.

Cisco UCS Central	Cisco UCS Domain
Cisco UCS Central, Release 1.0(1)	Cisco UCS Manager, Release 2.1(1)

Registering a Cisco UCS Domain with Cisco UCS Central using the Cisco UCS Manager GUI

Note You cannot change or swap the IP addresses used by Cisco UCS Manager in a domain that is registered with Cisco UCS Central. If you need to change or swap that IP address, you must first unregister the domain from Cisco UCS Central. You can reregister the Cisco UCS domain after you have changed or swapped the IP address.

Before You Begin

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.

Procedure

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

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

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

Step 4 In the **Work** pane, click the **UCS Central** tab.

Step 5 In the **Actions** area, click **Register With UCS Central**.

Step 6 In the **Register with UCS Central** dialog box, do the following:

a) Complete the following fields:

Name	Description
Hostname/IP Address field	The hostname or IP address of the virtual machine where Cisco UCS Central is deployed. **Note** If you use a hostname rather than an IP address, you must configure a DNS server. If the Cisco UCS domain is not registered with Cisco UCS Central or DNS management is set to **local**, configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to **global**, configure a DNS server in Cisco UCS Central.
Shared Secret field	The shared secret (or password) that was configured when Cisco UCS Central was deployed.

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

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

c) Click **OK**.

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

Procedure

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

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

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

Step 4 In the **Work** pane, click the **UCS Central** tab.

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

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

Step 6 Click **Save Changes**.

Unregistering a Cisco UCS Domain from Cisco UCS Central using the Cisco UCS Manager GUI

When you unregister a Cisco UCS domain from Cisco UCS Central, Cisco UCS Manager no longer receives updates to global policies.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, expand **All** > **Communication Management**.
Step 3 Click the **UCS Central** node.
Step 4 In the **Work** pane, click the **UCS Central** tab.
Step 5 In the **Actions** area, click **Unregister From UCS Central**.
Step 6 If the Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.
Step 7 Click **OK**.

Registering a Cisco UCS Domain with Cisco UCS Central using the Cisco UCS Manager CLI

Note You cannot change or swap the IP addresses used by Cisco UCS Manager in a domain that is registered with Cisco UCS Central. If you need to change or swap that IP address, you must first unregister the domain from Cisco UCS Central. You can reregister the Cisco UCS domain after you have changed or swapped the IP address.

Before You Begin

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.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.
Step 2	UCS-A/system # **create control-ep policy** *ucs-central*	Creates the policy required to register the Cisco UCS Domain with Cisco UCS Central. *ucs-central* can be the hostname or IP address of the virtual machine where Cisco UCS Central is deployed.

	Command or Action	Purpose
		Note If you use a hostname rather than an IP address, you must configure a DNS server. If the Cisco UCS domain is not registered with Cisco UCS Central or DNS management is set to **local**, configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to **global**, configure a DNS server in Cisco UCS Central.
Step 3	Shared Secret for Registration: *shared-secret*	Enter the shared secret (or password) that was configured when Cisco UCS Central was deployed.
Step 4	UCS-A/system/control-ep # **commit-buffer**	Commits the transaction to the system configuration.

The following example registers a Cisco UCS Domain with a Cisco UCS Central system at IP address 209.165.200.233, and commits the transaction:

```
UCS-A# scope system
UCS-A /system # create control-ep policy 209.165.200.233
Shared Secret for Registration: S3cretW0rd!
UCS-A /system/control-ep* # commit-buffer
UCS-A /system/control-ep #
```

What to Do Next

Configure policy resolution between Cisco UCS Manager and Cisco UCS Central.

Configuring Policy Resolution between Cisco UCS Manager and Cisco UCS Central using the Cisco UCS Manager CLI

Before You Begin

You must register the Cisco UCS Domain with Cisco UCS Central before you can configure policy resolution.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.
Step 2	UCS-A/system # **scope control-ep policy**	Enters control-ep policy mode.
Step 3	UCS-A/system/control-ep # **set backup-policy-ctrl source** {**local** | **global**}	Determines whether the Full State Backup Policy and All Configuration Export Policy are defined locally or in Cisco UCS Central.

	Command or Action	Purpose
Step 4	UCS-A/system/control-ep # **set communication-policy-ctrl source** {**local** | **global**}	Determines whether HTTP, CIM XML, Telnet, SNMP, web session limits, and Management Interfaces Monitoring Policy settings are defined locally or in Cisco UCS Central.
Step 5	UCS-A/system/control-ep # **set datetime-policy-ctrl source** {**local** | **global**}	Determines whether the time zone and NTP server settings are defined locally or comes from Cisco UCS Central.
Step 6	UCS-A/system/control-ep # **set dns-policy-ctrl source** {**local** | **global**}	Determines whether DNS servers are defined locally or in Cisco UCS Central.
Step 7	UCS-A/system/control-ep # **set fault-policy-ctrl source** {**local** | **global**}	Determines whether the Global Fault Policy is defined locally or in Cisco UCS Central.
Step 8	UCS-A/system/control-ep # **set infra-pack-ctrl source** {**local** | **global**}	Determines whether the Capability Catalog and infrastructure firmware policy are defined locally or come from Cisco UCS Central.
Step 9	UCS-A/system/control-ep # **set mep-policy-ctrl source** {**local** | **global**}	Determines whether the SEL Policy is defined locally or in Cisco UCS Central.
Step 10	UCS-A/system/control-ep # **set monitoring-policy-ctrl source** {**local** | **global**}	Determines whether Call Home, Syslog, and TFTP Core Exporter settings are defined locally or in Cisco UCS Central.
Step 11	UCS-A/system/control-ep # **set powermgmt-policy-ctrl source** {**local** | **global**}	Determines whether the Global Power Allocation Policy is defined locally or in Cisco UCS Central.
Step 12	UCS-A/system/control-ep # **set psu-policy-ctrl source** {**local** | **global**}	Determines whether the Power Policy is defined locally or in Cisco UCS Central.
Step 13	UCS-A/system/control-ep # **set security-policy-ctrl source** {**local** | **global**}	Determines whether authentication and native domains, LDAP, RADIUS, TACACS+, trusted points, locales, and user roles are defined locally or in Cisco UCS Central.
Step 14	UCS-A/system/control-ep # **commit-buffer**	Commits the transaction to the system configuration.

The following example configures policy resolution for a Cisco UCS Domain that is registered with Cisco UCS Central and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope control-ep policy
UCS-A /system/control-ep* # set backup-policy-ctrl source global
UCS-A /system/control-ep* # set communication-policy-ctrl source local
UCS-A /system/control-ep* # set datetime-policy-ctrl source global
UCS-A /system/control-ep* # set dns-policy-ctrl source global
UCS-A /system/control-ep* # set fault-policy-ctrl source global
UCS-A /system/control-ep* # set infra-pack-ctrl source global
UCS-A /system/control-ep* # set mep-policy-ctrl source global
```

```
UCS-A /system/control-ep* # set monitoring-policy-ctrl source global
UCS-A /system/control-ep* # set powermgmt-policy-ctrl source global
UCS-A /system/control-ep* # set psu-policy-ctrl source local
UCS-A /system/control-ep* # set security-policy-ctrl source global
UCS-A /system/control-ep* # commit-buffer
UCS-A /system/control-ep #
```

Unregistering a Cisco UCS Domain from Cisco UCS Central using the Cisco UCS Manager CLI

When you unregister a Cisco UCS domain from Cisco UCS Central, Cisco UCS Manager no longer receives updates to global policies.

Procedure

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

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

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