Cisco UCS Central Overview

This chapter includes the following sections:

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

- Bandwidth statistics collection and aggregation with two week or one year retention
- 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:

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.

Feature	Description
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.
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.
Statistics management	Cisco UCS Central enables you to gain a better understanding of how Cisco UCS domains are functioning over time to improve operations to smoothly handle periodic peaks and shifts in workload. You can configure and generate reports from the Cisco UCS Central GUI. To accelerate the collection of statistics, the centralized database schema is open and data can be accessed directly or through the Cisco UCS Central Software GUI, command-line interface (CLI), or XML API.
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.
High availability	As with all Cisco UCS solutions, Cisco UCS Central is designed for no single point of failure. High availability for Cisco UCS Central Software allows organizations to run Cisco UCS Central using an active-standby model with a heartbeat that automatically fails over if the active Cisco UCS Central does not respond.
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.

Feature	Description
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.
Policy/policy component and resources import	Cisco UCS Central provides you the flexibility search for and import a perfect policy/policy component or a resource from one registered UCS domain into CCisco UCS Central. You can then deploy this policy or the resource to other managed domains.

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, and 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.

Important

- Make sure to create a separate domain groups for all modular server domains. Also make sure the modular server domain groups are not hierarchical.
- You must create separate infrastructure firmware policy for modular domains in Cisco UCS Central. The infrastructure firmware policies must be unique to modular servers. This will prevent any firmware policy resolution issues with other domain groups.

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 global policies in Cisco UCS Central that are resolved by Cisco UCS Manager in a registered Cisco UCS domain.

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.

Multi-version Management Support

Cisco UCS Central, release 1.1(2a) and newer provides you the ability to manage multiple Cisco UCS domains with different versions of Cisco UCS Manager at the same time. Cisco UCS Central identifies feature capabilities of each Cisco UCS domain at the time of domain registration. This ability enables you to seamlessly integrate multiple versions Cisco UCS Manager with Cisco UCS Central for management and global service profile deployment.

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

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

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

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

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

Supported Features in Cisco UCS Manager

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

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

Management Exclusion

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

- **Global service profile deployment**: If you deploy global service profile on a server pool, and you have disabled global service profile deployment in one of the servers in the pool, Cisco UCS Central excludes the server from the global service profile deployment.
- **In band management**: A service profile with inband management capability will not be deployed on the servers where you have excluded inband management feature.
- **Policy mapping**: This will disable importing policies or policy components from this Cisco UCS domain into Cisco UCS Central.
- **Remote management**: This will restrain controlling physical devices in a Cisco UCS domain from Cisco UCS Central.

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

Feature Support Matrix

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

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

Note

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

Cisco UCS Central CLI Overview

Managed Objects

Cisco UCS uses a managed object model, where managed objects are abstract representations of physical or logical entities that can be managed. For example, servers, chassis, I/O cards, and processors are physical entities represented as managed objects, and resource pools, user roles, service profiles, and policies are logical entities represented as managed objects.

Managed objects may have one or more associated properties that can be configured.

Command Modes

The CLI is organized into a hierarchy of command modes, with the EXEC mode being the highest-level mode of the hierarchy. Higher-level modes branch into lower-level modes. You use **create**, **enter**, and **scope** commands to move from higher-level modes to modes in the next lower level , and you use the **exit** command to move up one level in the mode hierarchy.

Note Most command modes are associated with managed objects, so you must create an object before you can access the mode associated with that object. You use **create** and **enter** commands to create managed objects for the modes being accessed. The **scope** commands do not create managed objects and can only access modes for which managed objects already exist.

Each mode contains a set of commands that can be entered in that mode. Most of the commands available in each mode pertain to the associated managed object. Depending on your assigned role and locale, you may have access to only a subset of the commands available in a mode; commands to which you do not have access are hidden.

The CLI prompt for each mode shows the full path down the mode hierarchy to the current mode. This helps you to determine where you are in the command mode hierarchy, and it can be an invaluable tool when you need to navigate through the hierarchy.

Object Commands

Four general commands are available for object management:

- **create** *object*

- **delete** *object*
- **enter** *object*
- **scope** *object*

You can use the **scope** command with any managed object, whether a permanent object or a user-instantiated object. The other commands allow you to create and manage user-instantiated objects. For every **create** *object* command, a corresponding **delete** *object* and **enter** *object* command exists.

In the management of user-instantiated objects, the behavior of these commands depends on whether the object exists, as described in the following tables:

Table 1: Command behavior if the object does not exist

Command	Behavior
create *object*	The object is created and its configuration mode, if applicable, is entered.
delete *object*	An error message is generated.
enter *object*	The object is created and its configuration mode, if applicable, is entered.
scope *object*	An error message is generated.

Table 2: Command behavior if the object exists

Command	Behavior
create *object*	An error message is generated.
delete *object*	The object is deleted.
enter *object*	The configuration mode, if applicable, of the object is entered.
scope *object*	The configuration mode of the object is entered.

Complete a Command

You can use the Tab key in any mode to complete a command. Partially typing a command name and pressing Tab causes the command to be displayed in full or to the point where another keyword must be chosen or an argument value must be entered.

Command History

The CLI stores all commands used in the current session. You can step through the previously used commands by using the Up Arrow or Down Arrow keys. The Up Arrow key steps to the previous command in the history, and the Down Arrow key steps to the next command in the history. If you get to the end of the history, pressing the Down Arrow key does nothing.

All commands in the history can be entered again by simply stepping through the history to recall the desired command and pressing Enter. The command is entered as if you had manually typed it. You can also recall a command and change it before you press Enter.

Committing, Discarding, and Viewing Pending Commands

When you enter a configuration command in the CLI, the command is not applied until you enter the **commit-buffer** command. Until committed, a configuration command is pending and can be discarded by entering a **discard-buffer** command.

You can accumulate pending changes in multiple command modes and apply them together with a single **commit-buffer** command. You can view the pending commands by entering the **show configuration pending** command in any command mode.

Note Committing multiple commands together is not an atomic operation. If any command fails, the successful commands are applied despite the failure. Failed commands are reported in an error message.

While any commands are pending, an asterisk (*) appears before the command prompt. The asterisk disappears when you enter the **commit-buffer** command.

The following example shows how the prompts change during the command entry process:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # create domain-group 12
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

Online Help for the CLI

At any time, you can type the ? character to display the options available at the current state of the command syntax.

If you have not typed anything at the prompt, typing ? lists all available commands for the mode you are in. If you have partially typed a command, typing ? lists all available keywords and arguments available at your current position in the command syntax.

Logging into and out of the Cisco UCS Central GUI

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.

Viewing Supported Features in a Cisco UCS Domain

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr)# **scope domain-mgmt**	Enters domain management.
Step 3	UCSC(resource-mgr) /domain-mgmt # **scope ucs-domain** *domain ID*	Enters the specified domain.
Step 4	UCSC(resource-mgr) /domain-mgmt/ucs-domain # **show server-feature-mask**	Displays the server feature mask details.
Step 5	UCSC(resource-mgr) /domain-mgmt/ucs-domain # **show network-feature-mask**	Displays the network feature mask details.
Step 6	UCSC(resource-mgr) /domain-mgmt/ucs-domain # **show storage-feature-mask**	Displays the storage feature mask details.

	Command or Action	Purpose
Step 7	UCSC(resource-mgr) /domain-mgmt/ucs-domain # **show envr-feature-mask**	Displays the environment feature mask details.

The following example shows how to view server, network, storage and environment feature masks:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain domain ID
UCSC(resource-mgr) /domain-mgmt/ucs-domain # show server-feature-mask

Server feature mask:
    Feature mask
    ------------
    Global Sp Feature Mask,Policy Map Feature Mask,In Band Mgmt Feature
Mask, Advanced Boot Order Feature Mask

UCSC(resource-mgr) /domain-mgmt/ucs-domain # show network-feature-mask

Network feature mask:
    Feature mask
    ------------
    None
UCSC(resource-mgr) /domain-mgmt/ucs-domain # show storage-feature-mask

Storage feature mask:
    Feature mask
    ------------
    Fc Zoning Feature Mask,Iscsi Ipv6 Feature Mask

UCSC(resource-mgr) /domain-mgmt/ucs-domain # show envr-feature-mask

Environment feature mask:
    Feature mask
    ------------
   Power Group Feature Mask,Remote Operation Feature Mask,Ucs Registration
 Feature Mask, Estimate Impact On Reconnect Feature Mask
UCSC(resource-mgr) /domain-mgmt/ucs-domain #
```

Viewing Supported Features for Global Service Profile Deployment

Before deploying a global service profile in a registered UCS domain, you can verify if the domain has the supported feature for this global service profile.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr)# **scope org**	Enters the organization root.
Step 3	UCSC(resource-mgr)#/org **scope service profile***Global Service Profile Name*	Enters the service profile.

	Command or Action	Purpose
Step 4	UCSC(resource-mgr) /org/service profile # **show server-feature-mask**	Displays the server feature mask details.
Step 5	UCSC(resource-mgr) /org/service profile #**show network-feature-mask**	Displays the network feature mask details.
Step 6	UCSC(resource-mgr) /org/service profile #**show storage-feature-mask**	Displays the storage feature mask details.
Step 7	UCSC(resource-mgr) /org/service profile # **show envr-feature-mask**	Displays the environment feature mask details.

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr)/org# scope service profile service profile name
Server feature mask:
    Feature mask
    ------------
    Global Sp Feature Mask,In Band Mgmt Feature Mask
UCSC(resource-mgr) /org/service-profile # show server-feature-masknenetwork-feature-mask

Network feature mask:
    Feature mask
    ------------
    None
UCSC(resource-mgr) /org/service-profile # show network-feature-mask

storage-feature-mask

Storage feature mask:
    Feature mask
    ------------
    None
UCSC(resource-mgr) /org/service-profile # show storage-feature-mask

envoir-feature-mask

Environment feature mask:
    Feature mask
    ------------
    Ucs Registration Feature Mask
UCSC(resource-mgr) /org/service-profile #
```

Configuring Identifier Policies

Identifier Policies

Cisco UCS Central supports an identifier policy for the **root** domain group. The identifier policy defines the soak interval, which is the number of seconds Cisco UCS Central waits before reassigning a pool entity that has been released by the Cisco UCS domain to which it was assigned.

Configuring the Identifier Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope identifier-policy**	Enters the identifier policy mode.
Step 4	UCSC(policy-mgr) /domain-group/identifier-policy # **set soak-interval** *soak-time*	Specifies the soak interval for the identifier policy. Specify an integer between 0 and 86400.
Step 5	UCSC(policy-mgr) /domain-group/identifier-policy # **commit-buffer**	Commits the transaction to the system.

The following example shows how to configure identifier policy and specify soak interval:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group dg1
UCSC(policy-mgr) /domain-group # scope identifier-policy
UCSC(policy-mgr) /domain-group/identifier-policy # set soak-interval 30
UCSC(policy-mgr) /domain-group/identifier-policy # commit-buffer
UCSC(policy-mgr) /domain-group #
```

Viewing the Identifier Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope identifier-policy**	Enters the identifier policy mode.
Step 4	UCSC(policy-mgr) /domain-group/identifier-policy # **show**	Displays the identifier policy with soak interval.

The following example shows how to view the identifier policy:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group dg1
UCSC(policy-mgr) /domain-group # scope identifier-policy
UCSC(policy-mgr) /domain-group/identifier-policy # show
Identifier Policy:
    Soak interval in seconds
    ------------------------
    30
UCSC(policy-mgr) /domain-group #
```