

Working with Cisco UCS Manager

- Cisco UCS Domains and Cisco UCS Central, on page 1
- Policies in Cisco UCS Central and Cisco UCS Domains, on page 8
- Domains and Domain Groups, on page 16
- Domain Group Qualification Policy, on page 18
- Organization, on page 19

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.

  The shared secret can contain only alphanumeric characters (a-z, A-Z, 0-9) and the following special characters:

  - Period (.)
  - Hyphen (-)
  - Underscore (_)
  - Colon (:)

  Using only these allowed characters helps avoid the need to re-enter unsupported characters in the shared secret.

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.

Name	Earliest Supported Release	Description
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.
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.
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.

Name	Earliest Supported Release	Description
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.
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

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
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
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

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
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
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 14	See Consequences of Service Profile Changes on Policy Resolution, on page 14	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 14	See Consequences of Service Profile Changes on Policy Resolution, on page 14	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 14	See Consequences of Service Profile Changes on Policy Resolution, on page 14	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**.