Configuring Cisco UCS Central Accounts

This chapter contains the following sections:

Multi-Domain Managers

A multi-domain manager is an application that can manage more than one domain. For example, Cisco UCS Central is a multi-domain manager that manages one or more registered Cisco UCS domains.

Server Management

Server Management

When you add a Cisco UCS Central account, you can choose how you want Cisco UCS Director to manage the servers for that account. You can choose one of the following:

All Servers

All servers are managed by Cisco UCS Director. This option is the default.

If you choose this option, all servers are added in the Managed state.

Selected Servers

Only selected servers are managed by Cisco UCS Director. You can add and remove servers from the managed server list as needed. If you choose this option, all servers are added in the Unmanaged state.

Note In order to be able to use the servers, it would be required to manually move them to Managed state.

When you move the servers from Managed to Unmanaged state, initially, the servers are moved to a Transition state. After keeping them in that state for around 6 hours, Cisco UCS Director moves them to Unmanaged state. During this time, the servers are removed from the Servers report.

Server license usage includes servers in Managed, Transition, and Decommissioned states. It does not include unmanaged servers.

You can monitor the servers and view the details in the Monitoring and Reporting chapter.

Selecting a Server for Management

Before You Begin

You can choose which servers you want Cisco UCS Director to manage in a Cisco UCS Central Account. For this task, make sure that you choose the **Selected Servers** option under server management, while adding a Cisco UCS Central account.

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 Expand the **UCS Central Accounts**, and click the Cisco UCS Central account that you want to work on.

Step 4 On the **UCS Central Accounts** screen, click **All UCS Domains**.

Step 5 Click a Cisco UCS domain that you want to work on and from the **More Actions** drop-down list, choose **View Details**.

Step 6 Click **Discovered Servers**.
You can see all servers in the Cisco UCS domain discovered by Cisco UCS Manager.

Step 7 Click **Manage Servers**.

Step 8 On the **Manage Servers** screen, check the boxes for those servers that you want to have managed.
Cisco UCS Director moves the selected servers to the Managed state.

Step 9 Click **Submit**.

Unmanaging a Server

If you have configured the server management option as **Selected Servers** while adding a Cisco UCS Central account, you can edit server state through Cisco UCS Director.

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 Expand the **UCS Central Accounts**, and click the Cisco UCS Central account that you want to work on.

Step 4 On the **UCS Central Accounts** screen, click **All UCS Domains**.

Step 5 Click a Cisco UCS domain that you want to work on and from the **More Actions** drop-down list, choose **View Details**.

Step 6 Click **Discovered Servers**.
You can see all servers in the Cisco UCS domain discovered by Cisco UCS Manager.

Step 7 Click **Unmanage Servers**.

Step 8 On the **Unmanage Servers** screen, uncheck the boxes for those servers that you no longer want to have managed.
Cisco UCS Director moves the selected servers to the Transition state and removes them from the servers report. The servers remain in that Transition state for 6 hours before Cisco UCS Director completes the move to the Unmanaged state. While a server is in Transition state, it is counted in your license usage.

Step 9 Click **Submit**.

Cisco UCS Central Accounts

Each Cisco UCS Central account represents a single Cisco UCS Central, plus all the Cisco UCS domains registered with that Cisco UCS Central.

When you create a Cisco UCS Central account all Cisco UCS domains that are registered with that Cisco UCS Central, and their related Cisco UCS Manager accounts, are imported into Cisco UCS Director. You can assign one or more of those Cisco UCS Manager accounts from the Cisco UCS Central account to a pod if needed. You can also register a Cisco UCS Manager account with a Cisco UCS Central account.

Note Cisco UCS Central is a multi-domain manager; you do not create the Cisco UCS Central account in a pod.

Adding a Cisco UCS Central Account

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Multi-Domain Managers**.

Step 3 On the **Multi-Domain Managers** page, click **Add Account**.

Step 4 On the Add Account screen, from the **Account Type** drop-down list, choose UCS Central.

Step 5 Click **Submit**.

Step 6 On the **Multi-Domain Manager Account** screen, enter the information for the following fields:

Name	Description
Account Name field	A unique name that you assign to this account.
Description field	(Optional) A description of this account.
Account Type drop-down list	Is pre-populated with **UCS Central** by default. If not, choose **UCS Central**.
Server Management drop-down list	Choose the servers that you want to manage in this account. It can be one of the following: • **All Servers—**This is a default option. It allows you to add all the servers. If you choose this option, all servers are added in Managed state. • **Selected Servers—**Only selected servers are managed by Cisco UCS Director. You can view them in the Discovered Servers report. Viewing the Discovered Servers Report for Cisco UCS Central Domain You can add and remove servers from the Managed server list as needed. If you choose this option, all servers are added in the Unmanaged state.
Server Address field	The IP address of Cisco UCS Central.
Use Credential Policy check box	Check the box if you want to use a policy to provide the credentials. A **Credential Policy** drop-down list comes up. Choose a policy defined in UCS Central. Or add a new one. As a result, the User ID, Password, Transport Type, and Port fields become unavailable.

Name	Description
User ID field	The username that this account uses to access Cisco UCS Central. This username must be a valid account in Cisco UCS Central. **Note** When creating a UCS Central account integrated with LDAP, the username must be in the following format: **ucs-<*Domain Name*>*username*** For example: ucs-vxendomain.com\jdoe123
Password field	The password associated with the username.
Transport Type drop-down list	Choose the transport type that you want to use for this account. This can be one of the following: • **http** • **https**
Port field	The port used to access Cisco UCS Central.
Contact Email field	The email address that you can use to contact the administrator or other person responsible for this account.
Location field	The location of this account.

Step 7 Click **Submit**.

Cisco UCS Director tests the connection to Cisco UCS Central. If that test is successful, it adds the Cisco UCS Central account and discovers all infrastructure elements and registered Cisco UCS domains in that account, including chassis, servers, fabric interconnects, service profiles, and pools. This discovery process and inventory collection cycle takes approximately five minutes to complete.

The polling interval configured on the **Infrastructure System Parameters** tab specifies the frequency of inventory collection.

Testing the Connection to a Physical Account

You can test the connection at any time after you add an account to a pod.

Step 1 Choose **Administration** > **Physical Accounts**.
Step 2 On the **Physical Accounts** page, click **Multi-Domain Managers**.
Step 3 On the **Multi-Domain Managers** screen, click the row of the account for which you want to test the connection.
Step 4 Click **Test Connection**.
Step 5 When the connection test has completed, click **Close**.

What to Do Next

If the connection fails, verify the configuration of the account, including the username and password. If the username and password are correct, determine whether there is a network connectivity problem.

Verifying the Discovery of a Cisco UCS Central Account

Step 1 Choose **Physical** > **Compute**.
Step 2 On the **Compute** page, expand **Multi-Domain Managers**.
Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.
Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Assigning a Cisco UCS Domain to a Pod

After you assign a Cisco UCS domain to a pod, Cisco UCS Director displays it as a Cisco UCS Manager account, and you can configure, monitor, and obtain reports on that account.

Step 1 Choose **Physical** > **Compute**.
Step 2 On the **Compute** page, expand **Multi-Domain Managers**.
Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.
Step 4 Choose an Account, and click the **All UCS Domains** tab. Then click the row for the domain that you want to assign to a pod.
Step 5 From the **More Actions** drop-down list, choose **Assign to Pod**.
Step 6 On the **Assign to Pod** screen, complete the following fields:

Name	Description
Pod drop-down list	Choose the pod to which this account belongs.
Authentication Type drop-down list	Choose the type of authentication to be used for this account. This can be one of the following: • **Locally Authenticated—**A locally authenticated user account is authenticated directly through the fabric interconnect. It is enabled or disabled anyone with administrator or AAA privileges. • **Remotely Authenticated—**A remotely authenticated user account is any user account that is authenticated through LDAP, RADIUS, or TACACS+.
Server Management drop-down list	Choose how you want to have the servers in this account managed. This can be one of the following: • **All Servers—**All servers are managed by Cisco UCS Director. This option is the default. If you choose this option, all servers are added in the Managed state. • **Selected Servers—**Only selected servers are managed by Cisco UCS Director. You can add and remove servers from the managed server list as needed. If you choose this option, all servers are added in the Unmanaged state. For more information, see the Cisco UCS Director Management Guide for Cisco UCS Manager for the appropriate release.
Account Name field	A unique name that you assign to this account.
Description field	(Optional) A description of this account.
User ID field	The username that this account uses to access Cisco UCS Manager. This username must be a valid account in Cisco UCS Manager.
Password field	The password associated with the username.
Transport Type drop-down list	Choose the transport type that you want to use for this account. This can be one of the following: • **HTTP** • **Https**
Port field	The port used to access Cisco UCS Manager.
Contact Email field	The email address that you can use to contact the administrator or other person responsible for this account.

Name	Description
Location field	The location of this account.
Service Provider field	(Optional) The name of the service provider associated with this account, if any.

Step 7 Click **Submit**.

Unassigning a Cisco UCS Domain from a Pod

When you unassign a Cisco UCS domain from a pod, Cisco UCS Director does not delete the related Cisco UCS Manager account. If you want to delete the account, use **Administration** > **Physical Accounts**.

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Account** page, choose an Account, and click the **All UCS Domains** tab. Then click the row for the domain that you want to unassign from a pod.

Step 5 From the **More Actions** drop-down list, choose **Unassign from Pod**.

Step 6 On the **UCSM Account** screen, click **Submit**.

Organizations

Organizations in a Multitenancy Environment

Multi-tenancy allows you to divide the large physical infrastructure of an Cisco UCS domain into logical entities known as organizations. As a result, you can achieve a logical isolation between organizations without providing a dedicated physical infrastructure for each organization.

You can assign unique resources to each tenant through the related organization in the multi-tenant environment. These resources can include different policies, pools, and quality of service definitions. You can also implement locales to assign or restrict user privileges and roles by organization, if you do not want all users to have access to all organizations.

If you set up a multi-tenant environment, all organizations are hierarchical. The top-level organization is always root. The policies and pools that you create in root are system-wide and are available to all organizations in the system. However, any policies and pools created in other organizations are only available to organizations

that are above it in the same hierarchy. For example, if a system has organizations named Finance and HR that are not in the same hierarchy, Finance cannot use any policies in the HR organization, and HR cannot access any policies in the Finance organization. However, both Finance and HR can use policies and pools in the root organization.

If you create organizations in a mult-itenant environment, you can also set up one or more of the following for each organization or for a sub-organization in the same hierarchy:

- Resource pools
- Policies
- Service profiles
- Service profile templates

The root organization is always the top level organization.

Creating an Organization

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Organization**.

Step 6 Click **Add**.

Step 7 On the **Add Organization** screen, complete the following fields:

a) In the **Name** field, enter a name for the organization.
b) In the **Description** field, enter a description for the organization.
c) From the **Parent Organization** drop-down list, choose the organization under which this organization resides.

Time Zones

Cisco UCS requires a domain-specific time zone setting and an NTP server to ensure the correct time displays in Cisco UCS Central. If you do not configure time zones, the time might not display correctly.

In addition, if your environment includes Cisco UCS Central, you must configure an NTP server and the correct time zone in 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.

Adding a Time Zone

Step 1 Choose **Physical** > **Compute**.

Step 2 On the **Compute** page, expand **Multi-Domain Managers**.

Step 3 On the **Compute** page, choose the **UCS Central Account** under **Multi-Domain Managers**.

Step 4 On the **UCS Central Accounts** page, choose the account and click **View Details**.

Step 5 Click **Time Zones**.

Step 6 Click **Add**.

Step 7 On the **Add Time Zone** screen, do the following:

a) From the **NTP Server Name** drop-down list, enter the IP address or hostname of the NTP server for this time zone.
b) Click the **Domain Group**, check the boxes for the domains that you want to add to the domain group.
c) From the **Time Zone** drop-down list, select a Time Zone for your account.
d) Click **Submit**.