Managing a Physical Infrastructure

This chapter contains the following sections:

About Managing a Physical Infrastructure

Cisco UCS Director enables you to manage both physical and virtual infrastructures. While managing a physical account, you would need to first create a site, and add a pod to the site. After you create this account, Cisco UCS Director discovers all components within the newly created physical account. Typically, the discovery process takes about 5 minutes. In the system, you can either add a new pod or you can use the default pod that is available. A physical account can be associated with the default pod or with one that you add.

Note As an administrator, you can create either a physical account or a virtual account first in the system. A physical account in Cisco UCS Director has no dependency on a virtual (cloud) account.

Using the Converged View

The **Converged** view provides you with a graphical representation of the sites, and pods that you have configured in Cisco UCS Director. To access this view, choose **Converged** from the side navigation bar. If you have configured a site or multiple sites in the system, then this **Converged** view page displays a drop-down list from where you can select a site and view the pods that are associated with the site. However, you cannot add a site from this page. For information on adding a site, see Adding a Site, on page 2. After you have added a site in the system, you can either add a pod from the **Converged** page, or you can add a pod from the **Administration** > **Physical Accounts** > **Pods** screen.

The **Converged** page, in addition to letting you view the pods associated with each site, also provides the following options:

- Search—If your site has several pods, then you can use the search feature to locate a specific pod using the name as the search criteria.
- Add, Edit and Delete—Use these options to add, modify or delete pods.

- Collapse and expand the row of pods displayed for a site.
- View specific account information of each pod:
  - If you select a pod, and mouse over an account, then all account details are displayed. Alternatively, you can click an account to view the detailed information.
  - Power status of the account - the power icon on the account indicates if the account is powered on or powered off. Green color indicates that it is powered on, and red color indicates that it is powered off.

Adding a Site

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

Step 2 On the **Physical Accounts** page, click **Site Management**.

Step 3 Click **Add**.

Step 4 On the **Add Site** screen, complete the following fields:

Name	Description
Site Name field	A descriptive name for the site.
Description field	The description of the site, such as the location, significance, and so on.
Contact Name field	The name of the person responsible for this site.

Step 5 Click **Submit**.

Adding a Pod

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

Step 2 On the **Physical Accounts** page, click **Pods**.

Step 3 Click **Add**.

Step 4 On the **Add Pod** screen, complete the following fields:

Name	Description
Name field	A descriptive name for the pod.

Name	Description
Type drop-down list	Choose the type of pod that you want to add. This can be one of the following: • **Flexpod** • **VersaStack** • **Generic** • **ExpressPod Medium** • **VSPEX** • **ExpressPod Small** • **Vblock** • **HyperFlex** • **Virtual SAN Pod** The nongeneric pod types accommodate only specific physical and virtual components. A generic pod does not require a specific pod license. You can add any type of physical or virtual component to a generic pod. For more information about bundled pod licenses (FlexPod, Vblock, and VSPEX), which include the necessary individual device licenses to run a pod, see the Cisco UCS Director Installation and Upgrade Guides. **Note** Only VersaStack and Generic pods are supported in the IBM accounts in Cisco UCS Director.
Site drop-down list	Choose the site where you want to add the pod. If your environment does not include sites, you can omit this step.
Description field	(Optional) A description of the pod.
Address field	The physical location of the pod. For example, this field could include the city or other internal identification used for the pod.
Hide Pod check box	Check to hide the pod if you do not want it to show in the Converged Check View. You can continue to add or delete accounts from the pod. For example, you can use this check box to ensure that a pod that does not have any physical or virtual elements is not displayed in the Converged View.

Step 5 Click **Add**.

What to do next

Add one or more accounts to the pod.

Adding a Physical Account

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

Step 2 On the **Physical Accounts** page, click **Physical Accounts**.

Step 3 Click **Add**.

Step 4 On the **Add Account** screen, complete the following fields:

Name	Description
Pod drop-down list	Choose the pod to which this physical account belongs.
Category drop-down list	Choose the category type (Computing or Storage). If you chose Storage, continue to Step 6.
Account Type drop-down list	Choose from the following account types for this physical account: • **UCSM** • **HP ILO** • **Cisco Rack Server (CIMC)** • **IPMI**

Step 5 Click **Submit**.

Step 6 On the **Add Account** screen, complete the following fields:

Name	Description
Authentication Type drop-down list	Choose from the following authentication types to be used for this account: • **Locally Authenticated**—A locally authenticated user account is authenticated directly through the fabric interconnect and can be enabled or disabled by anyone with admin 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 servers are managed by this account by selecting one of the following options: • **All Servers** • **Selected Servers**
Account Name field	A unique name for the physical account that you want to add.
Server Address field	The IP address of the server.

Name	Description
Use Credential Policy check box	Check this check box if you want to use a credential policy for this account rather than enter the information manually.
Credential Policy drop-down list	If you checked **Use Credential Policy**, choose the credential policy that you want to use from this drop-down list. This field is only displayed if you choose to use a credential policy.
User ID field	The username for accessing this account. This field is not displayed if you choose to use a credential policy.
Password field	The password associated with the username. This field is not displayed if you choose to use a credential policy.
Transport Type drop-down list	Choose the transport type that you want to use for the account. This can be one of the following: • **HTTP** • **HTTPS** This field is not displayed if you choose to use a credential policy.
Port field	The server port number. This field is not displayed if you choose to use a credential policy.
Description field	The description of the account.
Contact Email field	The contact email address for the account.
Location field	The location.
Service Provider field	The service provider's name, if any.

Step 7 If this account is Storage, choose the appropriate account type: **NetApp ONTAP**, **NetApp OnCommand**, **EMC VNX**, **EMC VMAX Solutions Enabler** or **WHIPTAIL**.

Step 8 Click **Add**.

Adding a Multi-Domain Manager Account

You can add the following types of multi-domain manager accounts:

- PNSC—Cisco Prime Network Services Controller account

- DCNM—Cisco Prime Data Center Network Manager account
- UCS Central—Cisco UCS Central account
- APIC—Cisco Application Policy Infrastructure Controller account
- EMC RecoverPoint account
- EMC VPLEX account

Before you begin

You must be logged in to the appliance to complete this task.

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

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

Step 3 Click **Add**.

Step 4 On the **Add Account** screen, choose the account type from the drop-down list.

Step 5 Click **Submit**.

Step 6 On the **Multi-Domain Manager Account** screen, complete the following fields:

Name	Description
Account Name field	Choose the account name to which this multi-domain manager account belongs.
Description field	(Optional) The description of the account.
Server Address field	Enter the IP address of the server managing the multi-domain manager account.
Account Name field	A unique name for the physical account that you want to add.
Server Address field	The IP address of the server.
User ID field	The username for accessing this account.
Password field	The password associated with the username.
Transport Type drop-down list	Choose the transport type that you want to use for the account. This can be one of the following: • http • https
Port field	The server port number. The default port is 443.
Contact Email field	(Optional) The contact email address for the account.
Location field	(Optional) The location.

Step 7 Click **Submit**.

Adding a Network Element

In order to create a virtual server that supports load balancing, first add a network element in Cisco UCS Director. After a Load Balancer is added as a network element in Cisco UCS Director, it appears on the **Managed Network Element** screen.

Before you begin

You must be logged in to the appliance to complete this task.

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

Step 2 On the **Physical Accounts** page, click **Managed Network Elements**.

Step 3 Click **Add Network Element**.

Step 4 On the **Add Network Element** screen, complete the following fields:

Name	Description
Pod drop-down list	Choose the pod to which the network element belongs.
Device Category drop-down list	Choose the device category for this network element. For example: **F5 Load Balancer**.
Device IP field	The IP address for this device.
Protocol drop-down list	Choose the protocol to be used. The list may include the following: • Telnet • SSH • HTTP • HTTPS **Note** When working with an F5 load balancer device, HTTP and HTTPS are the only valid selections.
Port field	The port to use.
Login field	The login name.
Password field	The password associated with the login name.

Step 5 Click **Submit**.

Adding the F5 Load Balancer triggers the system task inventory collection. The polling interval configured on the **System Tasks** screen specifies the frequency of inventory collection.

What to do next

To modify or edit a virtual server, choose the server, and then click **Modify**. To remove a virtual server, choose the server, and then click **Delete**.

Enabling DHCP Logging

Before you begin

You must be logged in to the appliance to complete this task.

Step 1 Choose **Administration** > **Physical Accounts**.
Step 2 On the **Physical Accounts** page, choose the **Network Service Agents**.
Step 3 Click **Embedded Network Services**.
Step 4 On the **Embedded Network Services** screen, check the **Enable DHCP Logging**.

Testing Connectivity

You can test connectivity for managed network elements, virtual accounts, and physical accounts.

Testing Connectivity of Managed Network Elements

Step 1 Choose **Administration** > **Physical Accounts**.
Step 2 On the **Physical Accounts** page, click **Managed Network Elements**.
Step 3 Click the row with the pod for which you want to test connectivity.
Step 4 Click **Test Connection**.

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.

Enabling Device Discovery

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

Step 2 On the **Physical Accounts** page, click **Discovered Devices**.

Step 3 Click **Setup Discovery**.

Step 4 On the **Setup Discovery** screen, check **Enable Discovery**.

Step 5 On the **Setup Discovery** screen, complete the IP address range field and determine if the default values for the following fields are adequate for your environment:

Name	Description
Enable Discovery check box	The check box is checked by default to enable device discovery for this account.
IP Range field	The IP address range for device discovery. (For example, 10.1.1.1-10.1.1.12)
TCP Timeout (ms) field	The TCP timeout (ms) (default value is 2000 ms).
SNMP Timeout (ms) field	The SNMP timeout (ms) (default is 1500 ms).
SNMP Community Strings field	The SNMP community string (default is public).

Step 6 Click **Submit**.