Overview

This chapter contains the following sections:

Network Device Management Tasks You Can Perform in Cisco UCS Director

You can use Cisco UCS Director to perform management, monitoring, and reporting tasks for network devices within a domain.

Configuration and Administration

You can configure the following network device protocols and components in Cisco UCS Director:

- Ports and trunks
- Multiple Spanning Tree (MST), Per VLAN Spanning Tree (PVST), and VLAN Trunking Protocol (VTP)
- Storage area network (SAN) zones and zonesets
- Virtual device contexts (VDCs), virtual Fibre Channels (VFCs), and virtual port channel (vPC) domains
- VLANs and private VLANs
- Virtual storage area networks (VSANs)

• Virtual extensible local area networks (VXLANs)

Monitoring and Reporting

You can also use Cisco UCS Director to monitor and report on network devices, including:

• Service detail requests

• Configurations

• Modules

• Interfaces

• Port capabilities and profiles

• Pool policies and usage

• MAC address table configurations

• Quality of Service (QoS) policy and class maps

• Service detail requests

• SAN zones and zonesets

• vPC information

• VSAN, VLAN, and Private VLAN information

Network Device Management Tasks You Cannot Perform in Cisco UCS Director

You cannot use Cisco UCS Director to perform certain network device management tasks within a Cisco UCS domain, such as the following:

• Firmware upgrades

• User management

Orchestration Tasks for Network Device Management

Cisco UCS Director includes orchestration features that allow you to automate configuration and management of network domain devices in workflows.

A complete list of the network device orchestration tasks is available in the Workflow Designer and in the Task Library.

For more information about orchestration in Cisco UCS Director, see the Cisco UCS Director Orchestration Guide.

Adding a Network Device Account

In order to create a network devices account, first add a network element in Cisco UCS Director. After a network device is added as a network element in Cisco UCS Director, it appears in the **Managed Network Element** screen.

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   In the **Add Network Element** screen, complete the required fields, including the following:

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.
Use Credential Policy check box	Click the check box to use a policy to assign the credentials for the device instead of manually entering them. You may browse and choose an existing policy or create a new policy. **Note** Ensure that you have provided the appropriate protocol value for the device category. For example, if the device category is F5 Load Balance, the protocol value could be HTTP or HTTPs. If the device category is Cisco ASA, the protocol value could be Telnet or SSH.
Credential Policy drop-down list	If you checked the **Use Credential Policy** check box, then you can choose a policy from the drop-down list, or you can create a new credential policy.

Name	Description
Protocol drop-down list	Choose the protocol to be used to communicate with the device. The list may include the following: • Telnet • SSH • HTTP • HTTPS **Note** The values in this drop-down list vary based on the selected device category. For example, if the device category is F5 Load Balance, the available options are HTTP and HTTPs. If the device category is Cisco ASA, the available options are Telnet and SSH.
Port field	The port to use to access the device. This value appears based on the value selected in the Protocol field. You can modify this value, if necessary.
Login field	The login name for the device.
Password field	The password associated with the login name.

Step 5 Click **Submit**.

Adding the device 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 test the connectivity to the device, choose the device, then click **Test Connection**. To edit the credentials of the network device, choose the device, then click **Edit Credentials**. To remove a network device, choose the device, then click **Delete Network Element**.

Collecting Inventory for a Network Device

Step 1	Choose **Physical** > **Network**.
Step 2	On the **Network** page, choose the pod.
Step 3	On the **Network** page, click **Managed Network Elements**.
Step 4	Select the network device for which you want to collect inventory.
Step 5	Choose **Collect Inventory**.

Configuring the Polling Interval

The polling interval specifies the frequency of inventory collection.

Step 1	On the menu bar, choose **Administration** > **System**.
Step 2	Click the **System Tasks** tab.
Step 3	Choose an inventory task of the account and click **Manage Task**.
Step 4	From the **Minutes** drop-down list, choose the polling interval.
Step 5	Click **Submit**.

Configuring Session Pool Properties

You can configure the session properties for all networking devices, except ISE and F5 devices.

Step 1	Choose **Physical** > **Network**.
Step 2	On the **Network** page, choose the pod.
Step 3	On the **Network** page, click **Managed Network Elements**.
Step 4	Select the network device for which you want to configure the session properties.
Step 5	Choose **Configure Session Pool Properties**.
Step 6	In the **Configure Session Properties** screen, complete the required fields, including the following:

Name	Description
Maximum Active Sessions field	Specify the maximum number of active sessions that are allowed for the device. You must enter a number.
	If you do not enter a number, the default value of 5 is set for the device.
Maximum Wait Time field	Specify the time, in milliseconds, that the system waits if all sessions for a device are occupied.
	If the maximum active sessions configured for a device is 5, and if all 5 sessions are occupied, then the system waits for the time period specified in this field. Within this time period if a currently running session ends, then a new session is initiated for the latest request. However, if no currently running sessions ends within the specified time period, then an error message is displayed.
	If you do not enter a number, the default value of 15 seconds is set for the device.

Step 7   Click **Submit**.

Viewing Connectivity and Topology for Network Devices

You can view the connectivity and topology diagram for any network device. You can choose to view a hierarchical, concentric, circular, or force-directed mode.

Step 1   On the menu tab, choose **Physical** > **Network**.

Step 2   In the **Network** pane, choose the pod.

Step 3   Click the **Managed Network Elements** tab.

Step 4   Select the network device that you want to view.

Step 5   Click **View Connectivity**.

Step 6   In the **Topology View - Network Device Connectivity** dialog box, complete the following fields:

Name	Description
View Mode drop-down list	Choose one of the following: • **Hierarchical** • **Concentric** • **Circular** • **Force directed**
Show Link Labels check box	Check this check box to show link labels in the topology.
Allow Item Spacing check box	Check this check box to allow line spacing in the view.

Step 7   Click **Close** when you are finished verifying the connectivity of the network devices and determining their topology.

Verifying Network Device Details in a Pod Environment

After the network device is added to the pod, all discovered components of the pod environment are displayed at the account level.

Step 1   On the menu bar, choose **Physical** > **Network**.

Step 2   In the **Network** pane, click the pod.

Step 3   Click the **Managed Network Elements** tab.

Step 4   Click the network device, and click **View Details**.

All information about the device appears in the **Summary** tab. You can choose other tabs to see specific details, such as interfaces, modules, VLANs, port profiles, and so on, depending on the network device.