Working with Policies

This chapter includes the following sections:

Global Policies

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.

Creating a Global Policy

You can create global policies under the **Servers**, **Network** and **Storage** tabs.

Before You Begin

You must be logged in as an admin or as a user with admin privileges to perform this task.

Procedure

Step 1 On the menu bar, click **Servers.**

Step 2 Expand **Policies** and then **root.**
If you want to create a global policy in a sub-organization, expand **Sub-Organizations** > **Organization_Name**

Step 3 Select the item in the tree under which you want to create a global policy.

Step 4 Click **Create** on the right pane of the screen.

Step 5 Enter the **Name**, **Description** and other information in the create window.

Step 6 Click **Ok.**
Global policy is created and appears in the tree.

Note To create global policies under the **Network** and **Storage** tabs, click on the respective tab and perform Steps 2 through 6 in the preceding procedure.

Including a Global Policy in a Local Service Profile

Procedure

Step 1 Launch Cisco UCS Manager.
You can launch Cisco UCS Manager through the Cisco UCS Central GUI, as described in Launching Cisco UCS Manager for a Cisco UCS Domain.

Step 2 In the **Navigation** pane of Cisco UCS Manager, click the **Servers** tab.

Step 3 On the **Servers** tab, expand **Servers** > **Service Profiles**.

Step 4 Expand the node for the organization that contains the service profile for which you want to include a global policy.
If the system does not include multitenancy, expand the **root** node.

If the service profile is in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 5 Choose the service profile in which you want to include a global policy.

Step 6 In the **Work** pane, click the **Policies** tab.

Step 7 Click the policy for which you want to include a global policy.

Step 8 From the **Policy** drop-down list, choose the global policy.

Step 9 Click **Save Changes**.

Policy Conversion Between Global and Local

Under certain circumstances you can convert a global policy to a local policy or a local policy to a global policy in Cisco UCS Manager.

Global service profiles and templates can only refer to global policies. Upon deployment, you cannot convert global policies that are included in global service profiles and templates to local policies. You must first convert the service profile or any policies that use the global policy, such as a LAN or SAN connectivity policy or a vNIC or vHBA template, to local.

When a service profile refers to a global template in Cisco UCS Central and the template includes a global policy, the ownership of the template is with the service profile. The ownership of the global policy remains with Cisco UCS Central, and you cannot make any changes to the policy ownership using Cisco UCS Manager. You can make changes to the policy ownership locally only if the policy is included in a local service profile or template.

Converting a Global Policy to a Local Policy

You can convert a policy from global to local only if the policy is included in a local service profile or service profile template.

Before You Begin

You must be logged in as an admin or as a user with admin privileges to perform this task.

Procedure

Step 1 Launch Cisco UCS Manager.
You can launch Cisco UCS Manager through the Cisco UCS Central GUI, as described in Launching Cisco UCS Manager for a Cisco UCS Domain.

Step 2 In the **Navigation** pane of Cisco UCS Manager, click the tab where the policy is located.
For example, click the **Servers** tab to convert a server-related policy, the **LAN** tab to convert a network-related policy, or the **SAN** tab to convert a storage-related policy.

Step 3 In the **Navigation** pane, expand **Policies**.

Step 4 Expand the node for the organization that contains the policy you want to convert.
If the system does not include multitenancy, expand the **root** node.

If the policy is in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 5 Choose the global policy that you want to convert to local.

Step 6 In the **Actions** section, click **Use Local.**

Step 7 If the Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

The policy is now a local policy that can be managed by Cisco UCS Manager.

Converting a Local Policy to a Global Policy

You can change the ownership of the local policies to global only if they are associated with a service profile.

Before You Begin

You must be logged in as an admin or as a user with admin privileges to perform this task.

Procedure

Step 1 Launch Cisco UCS Manager.
You can launch Cisco UCS Manager through the Cisco UCS Central GUI, as described in Launching Cisco UCS Manager for a Cisco UCS Domain.

Step 2 In the **Navigation** pane of Cisco UCS Manager, click the tab where the policy is located.
For example, click the **Servers** tab to convert a server-related policy, the **LAN** tab to convert a network-related policy, or the **SAN** tab to convert a storage-related policy.

Step 3 In the **Navigation** pane, expand **Policies**.

Step 4 Expand the node for the organization that contains the policy you want to convert.
If the system does not include multitenancy, expand the **root** node.

If the policy is in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 5 Choose the local policy that you want to convert to global.

Step 6 In the **Actions** area, click **Use Global**.

Step 7 If the Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

The policy is now a global policy that can only be managed by Cisco UCS Central and displays as read-only policy in the Cisco UCS Manager.

Policy Resolution between Cisco UCS Manager and Cisco UCS Central

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:

Name	Description
Infrastructure & Catalog Firmware	Determines whether the Capability Catalog and infrastructure firmware policy are defined locally or come from Cisco UCS Central.

Name	Description
Time Zone Management	Determines whether the date and time is defined locally or comes from Cisco UCS Central.
Communication Services	Determines whether HTTP, CIM XML, Telnet, SNMP, web session limits, and Management Interfaces Monitoring Policy settings are defined locally or in Cisco UCS Central.
Global Fault Policy	Determines whether the Global Fault Policy is defined locally or in Cisco UCS Central.
User Management	Determines whether authentication and native domains, LDAP, RADIUS, TACACS+, trusted points, locales, and user roles are defined locally or in Cisco UCS Central.
DNS Management	Determines whether DNS servers are defined locally or in Cisco UCS Central.
Backup & Export Policies	Determines whether the Full State Backup Policy and All Configuration Export Policy are defined locally or in Cisco UCS Central.
Monitoring	Determines whether Call Home, Syslog, and TFTP Core Exporter settings are defined locally or in Cisco UCS Central.
SEL Policy	Determines whether managed endpoints are defined locally or in Cisco UCS Central.
Power Management	Determines whether the power management is defined locally or in Cisco UCS Central.
Power Supply Unit	Determines whether power supply units are defined locally or in Cisco UCS Central.

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
Authentication Domains	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
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
Syslog	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
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 9	See Consequences of Service Profile Changes on Policy Resolution, on page 9	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 9	See Consequences of Service Profile Changes on Policy Resolution, on page 9	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 9	See Consequences of Service Profile Changes on Policy Resolution, on page 9	Deletes remote policies	Converted to a local policy

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	Local	Local, but any "default" policies are updated on domain group assignment	Local/Remote (if resolved to "default" post registration)

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	
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)

Modifying Policy Resolutions between Cisco UCS Manager and Cisco UCS Central using the Cisco UCS Manager GUI

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All** > **Communication Management**.

Step 3 Click the **UCS Central** node.

Step 4 In the **Actions** area, click **UCS Central**.

Step 5 In the **Policy Resolution Control** area, click one of the following radio buttons for each of the fields:

- **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.

Step 6 Click **Save Changes**.

Policy and Policy Component Import in Cisco UCS Central

Cisco UCS Central enables you to import policies, pools, vLANs, vSANs directly from one registered Cisco UCS domain into Cisco UCS Central. When you have a perfect policy or a policy component in one of your UCS domains, you can import the policy and apply it to multiple domains. This import option enables you to import and apply a policy from one registered UCS domain to multiple UCS domains with a single click.

Using the Cisco UCS Central GUI, you can search for a policy or a component in the registered UCS domains. You can also refine your search using the available filters. From the search results, select the policy or component and import that into Cisco UCS Central.

Note If the search results are more than 1000, the results truncates. Make sure to refine the search using filters.

Depending on the policy or component you are importing, you can import them into either of the following destinations:

- Domain group root or to a specific domain
- Org root or a specific org

Estimate Impact During Import

Cisco UCS Central provides you the option to estimate the impact of most of the management actions you perform using the GUI. Make sure to run estimate impact during an import. Make sure to review the estimate impact results. The results will help you to identify any potential issues such as unintentional server reboot or policy overwrite and take proper precautionary measures before importing the selected policy or component.

Cautions and Guidelines for Policy or Component Import

Make sure to review the following information before importing a policy or a policy component:

- In the registered Cisco UCS Domains, if you have Cisco UCS Manager releases 2.1(2x) and 2.1(3x), you can only search for policies or components in the domains. You must have Cisco UCS Manager, release 2.2 and above to be able to import policies.
- When you import a policy to the root or any domain, if a policy with the same name already exist in the domain, Cisco UCS Central displays a confirmation dialog box that warns you about the policy overwrite. If you select import, the imported policy overwrites the existing policy. You can not retrieve the existing policy after the import.
- Cisco UCS Central does not maintain back up copies of any policy in the registered UCS domains. For example, if you have a specific BIOS policy in a domain, and you import another BIOS policy without estimating impact, the existing BIOS policy will get overwritten and you will not be able to recover that. When you click **Estimate Impact** and review the impacts, you can identify the potential risk and take precautionary measures.
- To avoid losing any customized policies from the domains by import, before importing, make sure to run **Estimate Impact**. Estimate impact provides you a detailed list of potential issues. You can review the results and make import decision based on the information.
- If the policy you are importing causes server reboot, when you run the estimate impact you can review that and take proper precautionary measures before performing the import. Sometimes, even if the estimate impact warns about a reboot, the reboot may not happen immediately. The reboot option in the global default maintenance policy would trigger the reboot action based on the selected option.
- When you import a policy from a Cisco UCS Domain, if Cisco UCS Central does not support some component of that policy, the unsupported components are dropped from the policy during import.
- If you are importing a policy that causes a server reboot, sometimes the server reboot may not happen immediately after the import. It will happen based on the schedule associated with the maintenance policy.

Policies and Policy Dependents

The following tables lists the policies or dependents that you can import from Cisco UCS Manager:

Polices or Dependents	Description
Policies	You can import the following policies: • BIOS Policy • Boot Policy • CIM XML Policy • Call Home Policy • DNS Policy • Dynamic vNIC Connection Policy • Ethernet Adapter Policy • Fibre Channel Adapter Policy • Global Fault Policy • Global Power Allocation Policy • HTTP Policy • Interface Monitoring Policy • LAN Connectivity Policy • Local Disk Configuration Policy • Maintenance Policy • SEL Policy • SNMP Policy • Scrub Policy • Serial over LAN Policy • Server Pool Policy • Server Pool Policy Qualification • Shell Session Limits Policy • Syslog Policy • TFTP Core Export Policy • Telnet Policy • Threshold Policy • Time Zone Policy • Web Session Limits Policy • iSCSI Channel Adapter Policy • vNIC. vHBA Placement Policy

Polices or Dependents	Description
Pools	• IP Pools • IQN Pool • MAC Pool • UUID Suffix Pool • WWN Pool
Policy dependents	• Host Firmware Package • IPMI Access Profile • Schedule • Service Profile Template • iSCSI Authentication Profile • vHBA Template • vNIC Template • vLAN • vSAN

Policies that Cause Server Reboot During Import

The following policies cause server reboot in the destination after import:

- Boot Policy

Importing a Policy or a Policy Component from a UCS Domain

Make sure the policy you are importing does not cause a server reboot in the destination. For information on policies or policy component you can import and policies that cause server reboot, see Policies and Policy Dependents, on page 12

Important

- When you import a policy to the root or any domain, if a policy with the same name already exist in the domain, Cisco UCS Central displays a confirmation dialog box that warns you about the policy overwrite. If you select import, the imported policy overwrites the existing policy. You can not retrieve the existing policy after the import.
- To avoid losing any customized policies from the domains by import, before importing, make sure to run **Estimate Impact**. Estimate impact provides you a detailed list of potential issues. You can review the results and make import decision based on the information.

Procedure

Step 1 Click **Import** tab.

Step 2 **Search** for the policy you want to import.
You can search for the policy in one of the following two ways:

- Click **Select Type** drop down option to find the policy you want to import, and click **Search**.
- If you know the policy name, type the name in **Search policies, pools, vLANs, vSAns in UCS Domains by name** field and click **Search**.

Note Click the arrow next to Search to expand search filter options to refine your search for a policy. You can narrow your search by specifying options in fields such as, **Select Ownership**, **Domain Group**, **UCS Domain**, and **Org**.

Step 3 From the displayed list of search results, click and select the policy you want to import.
Selecting the policy displays **Import** and **Properties (UCS View)**.

Step 4 Click **Import** to launch the **Import** dialog box.
Options in the **Import** dialog box depends on the policy you have selected for import. Certain policies will display **Import As** option. You can import the selected policy with a different name in the selected destination.

Step 5 Specify the Destination for import.
Depending on the policy or component you are importing, you can import them into either of the following destinations:

- Domain group root or to a specific domain
- Policy name or org level

Step 6 Click **Estimate Impact**.
Progress bar displays the estimate impact status. When that reaches **100%**, click **Review Impact** to review the impact of the import in the specified destination.

Step 7 Click **Import**.
If the import is successful system displays **Import Successful** message.

Local Policies

The policies you create and manage in Cisco UCS Manager are local to the registered Cisco UCS domain. In Cisco UCS Central you can view the policies available in the registered Cisco UCS Domains as local policies. These policies can only be included in local service profiles or service profile templates that are created and managed within that Cisco UCS domain.

Statistics Threshold Policy

A statistics threshold policy monitors statistics about certain aspects of the system and generates an event if the threshold is crossed. You can set both minimum and maximum thresholds. For example, you can configure

the policy to raise an alarm if the CPU temperature exceeds a certain value, or if a server is overutilized or underutilized.

These threshold policies do not control the hardware or device-level thresholds enforced by endpoints, such as the CIMC. Those thresholds are burned in to the hardware components at manufacture.

Cisco UCS enables you to configure statistics threshold policies for the following components:

- Servers and server components
- Uplink Ethernet ports
- Ethernet server ports, chassis, and fabric interconnects
- Fibre Channel port

Note You cannot create or delete a statistics threshold policy for Ethernet server ports, uplink Ethernet ports, or uplink Fibre Channel ports. You can only configure the existing default policy.

Creating a Threshold Policy

You can create and configure threshold policies within the appropriate organization in the Policies node on the **Network** tab, the **Servers** tab, and the **Equipment** tab.

Procedure

Step 1 On the menu bar, click **Network**.

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Right-click **Threshold Policies** and choose **Create Threshold Policy**.

Step 4 In the **Create Threshold Policy** dialog box, enter the **Name** and optional description.

Note You can create a threshold class and threshold definition at this time, or close the dialog box and add them later later. Click **Create Threshold Class** to create a threshold class, and then click **Create Threshold Definition** on the **Create Threshold Class** dialog box.

Step 5 Click **OK**.

What to Do Next

- Add a threshold class to the threshold policy
- Add a threshold definition to the threshold class

Adding a Threshold Class to an Existing Threshold Policy

Procedure

Step 1 On the menu bar, click **Network**.

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Threshold Policies**.

Step 4 Select the policy for which you want to create a threshold class.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the **Threshold Classes** table, click **Create Threshold Class**.

Step 7 In the **Create Threshold Class** dialog box, choose the statistics class that you want to configure.

Step 8 Click **OK**.
The new class appears in the **Threshold Classes** table.

Step 9 In the **Work** pane, click **Save**.

What to Do Next

- Add additional threshold classes to the threshold policy.
- Add a threshold definition.

Adding a Threshold Definition to an Existing Threshold Class

Procedure

Step 1 On the menu bar, click **Network**.

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Threshold Policies**.

Step 4 Select the policy for which you want to create a threshold definition.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the **Threshold Classes** table, right-click the threshold class that you want to modify and choose **Create Threshold Definition**.

Step 7 In the **Create Threshold Definition** dialog box, choose the **Property Type**, enter the **Normal Value (packets)**, and choose the alarm triggers above and below normal value.

Step 8 Click **OK**.

Step 9 In the **Work** pane, click **Save**.

Deleting a Threshold Policy

Procedure

Step 1 On the menu bar, click **Network**.

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Threshold Policies**.

Step 4 Right-click the policy that you want to delete and choose **Delete**.

Step 5 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Deleting a Threshold Class from a Threshold Policy

Procedure

Step 1 On the menu bar, click **Network**.

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Threshold Policies**.

Step 4 Select the policy for which you want to delete a threshold class.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the **Threshold Classes** table, right-click the threshold definition you want to delete and choose **Delete**

Step 7 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Deleting a Threshold Definition from a Threshold Class

Procedure

Step 1 On the menu bar, click **Network**.

Step 2 In the **Navigation** Pane, expand **Network** > **Policies** > **root**.
If you want to create or access a policy in a sub-organization, expand **Sub-Organizations** > ***Organization_Name***.

Step 3 Expand **Threshold Policies**.

Step 4 Select the policy for which you want to delete a threshold definition.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the **Threshold Classes** table, expand the threshold class for which you want to delete a threshold definition.

Step 7 Right-click the threshold definition you want to delete and choose **Delete**.

Step 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.