Domain Management

This chapter includes the following sections:

Registering Cisco UCS Domains

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 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 the active Cisco UCS Manager GUI sessions will be 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. For standalone mode, use individual VM IP address. If you plan to setup in cluster mode, use virtual IP address.

- Obtain the shared secret that you configured when you deployed Cisco UCS Central.

Note

- After you register a Cisco UCS domain in Cisco UCS Central, you cannot change or swap the IP used by the Cisco UCS Manager. If you need to change or swap the IP address, make sure to unregister the domain from Cisco UCS Central, change the IP address and then re-register in Cisco UCS Central.

- You can register or un-register a Cisco UCS domain using Cisco UCS Manager GUI or CLI.

- 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.

Warning

You should upgrade Cisco UCS Manager to Release 2.1(2) before registering with Cisco UCS Central. If you try to register Cisco UCS Manager, Release 2.1(1) with Cisco UCS Central Release 1.1, Cisco UCS Manager will display the registration as positive, but the Cisco UCS Central inventory will not display the registered Cisco UCS Domain. Cisco UCS Central faults will display a critical fault on the registration failure.

Estimate Impact on Reconnect

Cisco UCS Central, release 1.2 or later with Cisco UCS Manager, releases 2.2(3x) and 3.0(1) or later provides you the option to estimate impact on reconnect. If a registered Cisco UCS domain is disconnected from Cisco UCS Central or when you place a Cisco UCS domain in a suspended state, when you reconnect the domain or bring it out of suspended state, you can run Estimate Impact on Reconnect on the domain. The estimate impact on reconnect evaluates all accumulated changes to the domain when it was disconnected or suspended and provides you the status. This enables you to make informed decision on whether to proceed.

Unregistering Cisco UCS Domains

You can not unregister a Cisco UCS domain directly from Cisco UCS Central. If you want to unregister a Cisco UCS domain, you must use Cisco UCS Manager. See the appropriate *Cisco UCS Central Installation and Upgrade Guide* for more information.

Note

Unregistering a Cisco UCS domain can impact your global policies. See Consequences of Policy Resolution Changes for more information.

Domain Groups

Cisco UCS Central creates a hierarchy of Cisco UCS domain groups for managing multiple Cisco UCS domains. You will have the following categories of domain groups in Cisco UCS Central:

- **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 will automatically be placed under the domain group specified in the policy. If not, it will be placed in the ungrouped domains category. You can assign this ungrouped domain to a domain group.

Each Cisco UCS domain can only be assigned 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 will automatically inherit 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 will avoid 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 will protect the Cisco UCS domain from accidentally overwriting policies.

Creating a Domain Group

You can create a domain group under the domain group root from the **Equipment** tab or from the **Operations Management** tab. You can create up to five hierarchical levels of domain groups under the root. This procedure describes the process to create a domain group from the equipment tab, under the domain group root.

Procedure

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

Step 2   On the **Equipment** tab, expand **UCS Domains**.

Step 3   Right click on **Domain Group root**, and select **Create Domain Group**.

Step 4   In the **Create Domain Group** dialog box, enter **Name** and **Description**.

Step 5   Click **OK**.

Deleting a Domain Group

Procedure

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

Step 2   On the **Equipment** tab, **UCS Domains** > **Domain Group root**.

Step 3   Right click on domain group name you want to delete, and select **Delete**.

Step 4   If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Changing Group Assignment for a Cisco UCS Domain

You can assign a Cisco UCS domain to a domain group using any one of the following options:

• Changing the group assignment using the **Change Group Assignment** dialog box.

- Using the group assignment link under a specific domain group.

- Using domain group policy qualifiers.

This procedure describes the process to change the group assignment for a Cisco UCS domain.

Procedure

Step 1	On the menu bar, click **Equipment**.
Step 2	On the **Equipment** tab, expand **UCS Domains**.
Step 3	In the **Navigation** pane, expand **Ungrouped Domains**.
Step 4	Right click on the domain name and click **Change Group Assignment**.
Step 5	In the **Change Group Assignment** dialog box, choose the domain group and click **OK**.
Step 6	If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Domain Group and Registration Policies

Creating a Domain Group Policy

Procedure

Step 1	On the menu bar, click **Equipment**.
Step 2	In the **Navigation** Pane, on the **Equipment** tab, expand **UCS Domains** > **Policies**.
Step 3	Right-click **Domain Group Policies** and choose **Create Domain Group Policy**.
Step 4	In the **Create Domain Group Policy** dialog box, enter the **Name** and optional description.
Step 5	Choose a **Domain Group** and **Domain Group Policy Qualification** from the drop-down lists.
Step 6	Click **OK**.

Deleting a Domain Group Policy

Procedure

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

Step 2 In the **Navigation** Pane, on the **Equipment** tab, expand **UCS Domains** > **Policies**.

Step 3 Expand **Domain Group Policies**.

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

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

Creating a Registration Policy

Procedure

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

Step 2 In the **Navigation** Pane, on the **Equipment** tab, expand **UCS Domains** > **Policies**.

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

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

Step 5 Click **OK**.

What to Do Next

Add an address qualifier, owner qualifier, and site qualifier to the policy qualification.

Creating a Site Qualifier

Procedure

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

Step 2 In the **Navigation** Pane, on the **Equipment** tab, expand **UCS Domains** > **Policies**.

Step 3 Expand **Registration Policies**.

Step 4 Right-click the registration policy that you want to update, and choose **Create Site Qualifier**.

Step 5 In the **Create Site Qualifier** dialog box, enter the **Name** and **Regex**.

Step 6 Click **OK**.

Deleting a Site Qualifier

Procedure

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

Step 2 In the **Navigation** Pane, on the **Equipment** tab, expand **UCS Domains** > **Policies**.

Step 3 Expand **Registration Policies**.

Step 4 In the **Work** pane, expand **Sites**.

Step 5 Right-click the site that you want to delete, and choose **Delete**.

Step 6 If the Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Creating an Address Qualifier

Procedure

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

Step 2 In the **Navigation** Pane, on the **Equipment** tab, expand **UCS Domains** > **Policies**.

Step 3 Expand **Registration Policies**.

Step 4 Right-click the registration policy that you want to update, and choose **Create Address Qualifier**.

Step 5 In the **Create Address Qualifier** dialog box, enter the minimum and maximum IP addresses.

Step 6 Click **OK**.

Deleting an Address Qualifier

Procedure

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

Step 2 In the **Navigation** Pane, on the **Equipment** tab, expand **UCS Domains** > **Policies**.

Step 3 Expand **Registration Policies**.

Step 4 In the **Work** pane, expand **Addresses**.

Step 5 Right-click the address range that you want to delete, and choose **Delete**.

Step 6 If the Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Creating an Owner Qualifier

Procedure

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

Step 2 In the **Navigation** Pane, on the **Equipment** tab, expand **UCS Domains** > **Policies**.

Step 3 Expand **Registration Policies**.

Step 4 Right-click the registration policy that you want to update, and choose **Create Owner Qualifier**.

Step 5 In the **Create Owner Qualifier** dialog box, enter the **Name** and **Regex**.

Step 6 Click **OK**.

Deleting an Owner Qualifier

Procedure

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

Step 2 In the **Navigation** Pane, on the **Equipment** tab, expand **UCS Domains** > **Policies**.

Step 3 Expand **Registration Policies**.

Step 4 In the **Work** pane, expand **Owners**.

Step 5 Right-click the owner that you want to delete, and choose **Delete**.

Step 6 If the Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Deleting a Registration Policy

Procedure

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

Step 2 In the **Navigation** Pane, on the **Equipment** tab, expand **UCS Domains** > **Policies**.

Step 3 Expand **Registration 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**.

ID Range Qualification Policies

ID range qualification policies allow you to create policies and assign them to qualified domain groups and domain IP addresses. The ID range qualification policy is then visible to those domain groups and domain IP addresses. You can also create ID range qualification policies without assigning qualified domain groups or IP addresses. If you do not set qualifiers, the policy is available to all domain groups. ID resolution occurs hierarchically in the organization structure in the same manner as other global policies.

After you create an ID range qualification policy, you can apply it to a block in a new pool or an existing pool.

ID range qualification policies are not automatically pushed from Cisco UCS Central to the Cisco UCS Manager instances in a qualified domain group. If you change a domain group qualifier, a domain group ID, or the IP address of a Cisco UCS Manager domain group in Cisco UCS Central, the reference must be reset in the Cisco UCS Manager local service profile.

Note   Global service profiles in Cisco UCS Central do not support ID range qualification policies in this release.

Creating an ID Range Qualification Policy

Procedure

Step 1	On the menu bar, click **Equipment**.
Step 2	In the **Navigation** Pane, on the **Equipment** tab, expand **UCS Domains** > **Policies**.
Step 3	Right-click **ID Range Qualification Policies** and choose **Create ID Range Qualification Policy**.
Step 4	In the **Create ID Range Qualification Policy** dialog box, enter the **Name** and optional description.
Step 5	In the **Qualified Domain Groups** area, choose a **Context**. The contexts you choose appear next to the **Selected** field.
Step 6	In the **Qualified Domain IP Addresses** area, enter an **IP Address**, and click the plus sign. The IP addresses you enter appear next to the **Selected** field.
Step 7	Click **OK**.

What to Do Next

Assign the ID range qualification policy to a block.

Deleting an ID Range Qualification Policy

Procedure

Step 1	On the menu bar, click **Equipment**.
Step 2	In the **Navigation** Pane, on the **Equipment** tab, expand **UCS Domains** > **Policies**.
Step 3	Expand **ID Range Qualification Policies**.
Step 4	Right-click the policy that you want to delete and choose **Delete**.
Step 5	If the Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Call Home Policies

Cisco UCS Central supports global call home policies for notifying all email recipients defined in call home profiles to specific Cisco UCS Manager events. (There is no call home support for Cisco UCS Central in this release.) Profiles define lists of email recipients that receive alert notifications (to a maximum defined message size in full text, short text, or XML format) and alert criteria for triggering notifications.

Alert notifications are sent with predefined content based on alert levels (including major, minor, normal, notification and warning) and selected alert groups identifying events that trigger notification (such as diagnostic, environmental, inventory, license and other predefined events). Individual email recipients may be individually added to existing profiles. Registered Cisco UCS domains choosing to define security policies globally within that client's policy resolution control will defer all call home policies to its registration with Cisco UCS Central.

Configuring a Call Home Policy

A call home policy is created from a domain group under the domain group root. Call home policies under the Domain Groups root were already created by the system and ready to configure.

Procedure

Step 1	On the menu bar, click **Operations Management**.
Step 2	In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.
Step 3	In the **Navigation** pane, click **Operational Policies**.
Step 4	In the **Work** pane, click **CallHome**.
Step 5	(Optional) In the **Actions** area, click **Create**. Call home policies under the domain groups root were created by the system and ready to configure by default
Step 6	In the **Work** pane, click the **General** tab.
Step 7	In the **Actions** area, complete all applicable fields.

Name	Description
Create button	Creates an instance of the policy that will be used by all Cisco UCS domains included in the selected domain group.
Import button	Allows you to import the policy from one of the Cisco UCS domains registered with Cisco UCS Central.
Delete button	Deletes the instance of the policy defined for the selected domain group. After you delete the policy, it remains greyed-out until you click **Save**. When you do so, Cisco UCS Central deletes the policy and any configuration data you may have specified. While you can create a new instance of the policy later, you cannot restore the configuration data from a deleted instance. To cancel the delete request, click **Reset**.
State field	Whether Call Home is used for the Cisco UCS domains included in the Cisco UCS Central domain group. This can be one of the following: • **Off**—Call Home is not used for the Cisco UCS domains. • **On**—Cisco UCS generates Call Home alerts based on the Call Home policies and profiles defined in the domain group. **Note** If this field is set to **On**, Cisco UCS Central GUI displays the rest of the fields on this tab.
Throttling field	Whether the system limits the number of duplicate messages received for the same event. This can be one of the following: • **On**—If the number of duplicate messages sent exceeds 30 messages within a 2-hour time frame, then the system discards further messages for that alert type. • **Off**—The system sends all duplicate messages, regardless of how many are encountered.
Phone field	The telephone number for the main contact. Enter the number in international format, starting with a + (plus sign) and a country code. You can use hyphens but not parentheses.
Email field	The email address for the main contact. Cisco Smart Call Home sends the registration email to this email address. **Note** If an email address includes special characters, such as # (hash), spaces, or & (ampersand), the email server may not be able to deliver email messages to that address. Cisco recommends that you use email addresses which comply with RFC2821 and RFC2822 and include only 7bit ASCII characters.

Name	Description
Address field	The mailing address for the main contact. Enter up to 255 ASCII characters.
From field	The email address that should appear in the From field on Call Home alert messages sent by the system.
Reply To field	The return email address that should appear in the From field on Call Home alert messages sent by the system.
Switch Priority drop-down list	This can be one of the following: • **Alerts** • **Critical** • **Debugging** • **Emergencies** • **Errors** • **Information** • **Notifications** • **Warnings**
Hostname field	The IP address or hostname of the SMTP server. **Note** If you use a hostname rather than an IPv4 or IPv6 address, you must configure a DNS server. If the Cisco UCS domain is not registered with Cisco UCS Central or DNS management is set to **local**, configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to **global**, configure a DNS server in Cisco UCS Central.
Port field	The port number the system should use to talk to the SMTP server. Enter an integer between 1 and 65535. The default is 25.
Customer ID field	The CCO ID that includes the contract numbers for the support contract in its entitlements. Enter up to 510 ASCII characters.
Contract ID field	The Call Home contract number for the customer. Enter up to 510 ASCII characters.
Site field	The unique Call Home identification number for the customer site. Enter up to 510 ASCII characters.

Step 8 In the **Work** pane, click the **Profiles** tab.

Step 9 In the **Actions** area, complete all applicable fields.

Name	Description
Create button	Creates an instance of the policy that will be used by all Cisco UCS domains included in the selected domain group.
Import button	Allows you to import the policy from one of the Cisco UCS domains registered with Cisco UCS Central.
Delete button	Deletes the instance of the policy defined for the selected domain group. After you delete the policy, it remains greyed-out until you click **Save**. When you do so, Cisco UCS Central deletes the policy and any configuration data you may have specified. While you can create a new instance of the policy later, you cannot restore the configuration data from a deleted instance. To cancel the delete request, click **Reset**.
Filter button	Allows you to filter the data in the table. When you apply a filter, this button name changes to **Filter (on)**.
Create Profile button	Allows you to create a Call Home profile.
Add Email Recipient button	Allows you to add an email recipient to an existing Call Home profile.
Properties button	Displays detailed properties for the object selected in the table.
Delete button	Deletes the object selected in the table.
Name column	The name of the Call Home profile.
Level column	The lowest fault level that triggers the profile. Cisco UCS generates a Call Home alert for every fault that is at or above this level.
Alert Groups column	The group or groups that are alerted based on this Call Home profile.

Step 10 In the **Work** pane, click the **Policies** tab.

Step 11 In the **Actions** area, complete all applicable fields.

Name	Description
Create button	Creates an instance of the policy that will be used by all Cisco UCS domains included in the selected domain group.
Import button	Allows you to import the policy from one of the Cisco UCS domains registered with Cisco UCS Central.

Name	Description
Delete button	Deletes the instance of the policy defined for the selected domain group.
	After you delete the policy, it remains greyed-out until you click **Save**. When you do so, Cisco UCS Central deletes the policy and any configuration data you may have specified. While you can create a new instance of the policy later, you cannot restore the configuration data from a deleted instance.
	To cancel the delete request, click **Reset**.
Filter button	Allows you to filter the data in the table. When you apply a filter, this button name changes to **Filter (on)**.
Create Policy button	Allows you to create a new Call Home policy.
Properties button	Displays detailed properties for the object selected in the table.
Delete button	Deletes the object selected in the table.
Cause column	The event that triggers the alert. Each policy defines whether an alert is sent for one type of event.
State column	If this is **enabled**, Cisco UCS uses this policy when an error matching the associated cause is encountered. Otherwise, Cisco UCS ignores this policy even if a matching error occurs.
	By default, all policies are enabled.

Step 12 In the **Work** pane, click the **System Inventory** tab.

Step 13 In the **Actions** area, complete all applicable fields.

Name	Description
Create button	Creates an instance of the policy that will be used by all Cisco UCS domains included in the selected domain group.
Import button	Allows you to import the policy from one of the Cisco UCS domains registered with Cisco UCS Central.
Delete button	Deletes the instance of the policy defined for the selected domain group.
	After you delete the policy, it remains greyed-out until you click **Save**. When you do so, Cisco UCS Central deletes the policy and any configuration data you may have specified. While you can create a new instance of the policy later, you cannot restore the configuration data from a deleted instance.
	To cancel the delete request, click **Reset**.

Name	Description
Send Periodically field	If this field is set to **on**, Cisco UCS sends the system inventory to the Call Home database. When the information is sent depends on the other fields in this area.
Send Interval field	The number of days that should pass between automatic system inventory data collection. Enter an integer between 1 and 30.
Hour of Day to Send field	The hour that the data should be sent using the 24-hour clock format.
Minute of Hour to Send field	The number of minutes after the hour that the data should be sent.

Step 14 Click **Save**.

Deleting a Call Home Policy

A call home policy is deleted from a domain group under the domain group root. Call home policies under the domain groups root cannot be deleted.

Deleting a call home policy will remove all profiles, policies and system inventory settings within that policy.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 In the **Navigation** pane, click **Operational Policies**.

Step 4 In the **Work** pane, click **CallHome**.

Step 5 In the **Actions** area, click **Delete**.
A policy that is deleted will inherit its settings from its domain group's parent until it is reconfigured.

Step 6 Click **Save**.

Configuring a Profile for a Call Home Policy

Before You Begin

Before configuring a profile for a call home policy in a domain group under the Domain Group root, this profile and policy must first be created.

Procedure

Step 1   On the menu bar, click **Operations Management**.

Step 2   In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3   Under the **Domain Groups root** node, click **Operational Policies**.

Step 4   In the **Work** pane, click **CallHome**.

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

Step 6   In the **Actions** area, click **Create Profile** and complete all applicable fields.

a) In the **Create Profile** dialog, click and complete the following fields:

Name	Description
Name field	The user-defined name for this profile.
Level field	The lowest fault level that triggers the profile. Cisco UCS generates a Call Home alert for each fault that is at or above this level. This can be one of the following: • **critical** • **debug** • **disaster** • **fatal** • **major** • **minor** • **normal** • **notification** • **warning**

b) In the **Alert Groups** area, complete the following fields:

Name	Description
Alert Groups field	The group or groups that are alerted based on this Call Home profile. This can be one or more of the following: • **ciscoTac** • **diagnostic** • **environmental** • **inventory** • **license** • **lifeCycle** • **linecard** • **supervisor** • **syslogPort** • **system** • **test**

c) In the **Email Configuration** area, complete the following fields:

Name	Description
Format field	This can be one of the following: • **xml**—A machine readable format that uses Extensible Markup Language (XML) and Adaptive Messaging Language (AML) XML schema definition (XSD). This format enables communication with the Cisco Systems Technical Assistance Center. • **fullTxt**—A fully formatted message with detailed information that is suitable for human reading. • **shortTxt**—A one or two line description of the fault that is suitable for pagers or printed reports.
Max Message Size field	The maximum message size that is sent to the designated Call Home recipients. Enter an integer between 1 and 5000000. The default is 5000000. For full text and XML messages, the maximum recommended size is 5000000. For short text messages, the maximum recommended size is 100000. For the Cisco TAC alert group, the maximum message size must be 5000000.

d) In the **Email Recipients** area, complete the following fields:

Name	Description
Filter button	Allows you to filter the data in the table. When you apply a filter, this button name changes to **Filter (on)**.
Add Email Recipients button	Allows you to add an email recipient.
Properties button	Displays detailed properties for the object selected in the table.
Delete button	Deletes the object selected in the table.
Email column	The email address of the recipient.

e) Click **OK**.

Step 7 Click **Save**.

Adding Email Recipients to a Call Home Profile

Before You Begin

Before adding email recipients to a profile for a call home policy, this profile must first be created.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, click **Operational Policies**.

Step 4 In the **Work** pane, click **CallHome**.

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

Step 6 In the **Work** pane, click an existing profile for adding the email recipient.

Step 7 In the **Action** are, click **Add Email Recipients**.

Step 8 In the **Add Email Recipients** dialog box, enter an email address for the recipient.

Step 9 Click **OK**.

Step 10 Click **Save**.

Deleting a Profile for a Call Home Policy

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, click **Operational Policies**.

Step 4 In the **Work** pane, click **CallHome**.

Step 5 In the **Actions** area, click the profile in call home you want to delete.
You can also right-click the profile in call home you want to delete to access that option. A profile that is deleted will inherit its settings from its domain group's parent until it is reconfigured.

Step 6 In the **Actions** area, click **Delete**.
Deleting a profile for a call home policy will delete all email recipients and other settings defined for that profile.

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

Configuring a Policy for a Call Home Policy

Before You Begin

Before configuring a policy for a call home policy under a domain group, this policy must first be created. Policies for call home policies under the Domain Groups root were already created by the system and ready to configure.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3 Under the **Domain Groups root** node, click **Operational Policies**.

Step 4 In the **Work** pane, click **CallHome**.

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

Step 6 In the **Actions** area, click **Create Policy** and complete all applicable fields.

   a) In the **Create Policy** dialog, click and complete the following fields:

Name	Description
State field	If this is **enabled**, Cisco UCS uses this policy when an error matching the associated cause is encountered. Otherwise, Cisco UCS ignores this policy even if a matching error occurs. By default, all policies are enabled.

Name	Description
Cause field	The event that triggers the alert. Each policy defines whether an alert is sent for one type of event. You cannot change the cause after the policy has been saved.

    b) Click **OK**.

Step 7   Click **Save**.

Deleting a Policy for a Call Home Policy

Procedure

Step 1   On the menu bar, click **Operations Management**.

Step 2   In the **Navigation** pane, expand **Domain Groups** > **Domain Group root**.

Step 3   Under the **Domain Groups root** node, click **Operational Policies**.

Step 4   In the **Navigation** pane, click **Operational Policies**.

Step 5   In the **Work** pane, click **CallHome**.

Step 6   In the **Actions** area, click the policy in call home you want to delete.
You can also right-click the policy in call home you want to delete to access that option. A policy that is deleted will inherit its settings from its domain group's parent until it is reconfigured.

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

Port Configuration

You can configure the fixed and expansion module ports in a Fabric Interconnect from Cisco UCS Central for both classic and mini Cisco UCS domains.

- **Ethernet ports**: By default the Ethernet ports are unconfigured. You can configure an Ethernet port as a **Server Port** or an **Uplink Port** in any Cisco UCS domain from Cisco UCS Central .

    ◦ Server ports handle the data traffic between the fabric interconnect and the adapter cards on the servers.

    ◦ Uplink ports handles Ethernet traffic between the fabric interconnect and the next layer of the network. All network-bound Ethernet traffic is pinned to one of these ports.

- **Scalability ports**: Mini Cisco UCS domain has the scalability port. You can configure this scalability port only as a **Server Port**.

When you configure a port on a fabric interconnect, the administrative state is automatically set to enabled. You can disable the port after it is configured.

Note   You can perform these two types of port configuration from Cisco UCS Central. All other port configuration options are available for you from Cisco UCS Manager. For more details on port configuration, see Configuring Ports and Port Channels section in Cisco UCS Manager Configuration Guides.

Configuring Ethernet Port

You can configure the Ethernet port either as a **Server Port** or as an **Uplink Port**. When you configure the port, the port is automatically enabled. You can also **Disable** or **UnConfigure** a port.

Procedure

Step 1   From **Domains** tab, click **Equipment** > **UCS Domains**.

Step 2   In the **Navigation** pane, expand **Domain Groups** or **Ungrouped Domains** as applicable.

Step 3   In the **Navigation** pane, expand the UCS Domain name and expand **Fabric Interconnects** > **Fabric Interconnect A or B** > **Fixed Module 1 or 2** and click **Ethernet Ports**.
The **Work** pane displays a list of available Ethernet ports in this module.

Step 4   Right click on one of the ports to display port configuration options.

Step 5   Depending on your requirement, click **Configure as Server Port** or **Configure as Uplink Port**.

Step 6   In the confirmation dialog box, click **OK**.

Cisco UCS Central communicates the configuration to the port through the registered Cisco UCS domain. Make sure to wait for the configuration to take effect before performing any actions on the port.

Configuring Scalability Port

You can configure the Scalability port only as a **Server Port**. When you configure the port, the port is automatically enabled. You can also **Disable** or **UnConfigure a port**.

Procedure

Step 1   From **Domains** tab, click **Equipment** > **UCS Domains**.

Step 2   In the **Navigation** pane, expand **Domain Groups** or **Ungrouped Domains** as applicable.

Step 3   In the **Navigation** pane, expand the UCS Domain name and expand **Fabric Interconnects** > **Fabric Interconnect A or B** > **Fixed Module 1 or 2** > **Ethernet Port** and click **Scalability Port**.
The **Work** pane displays a list of available Scalability ports in this module.

Step 4   Right click on one of the ports to display port configuration options.

Step 5   Click **Configure as Server Port**.

The option to **Configure as Uplink Port** is disabled because you cannot configure the scalability port as an uplink port.

Step 6 In the confirmation dialog box, click **OK**.

Cisco UCS Central communicates the configuration to the port through the registered Cisco UCS domain. Make sure to wait for the configuration to take effect before performing any actions on the port.