Configuring Communication Services

This chapter includes the following sections:

Remote Access Policies

Cisco UCS Central supports global remote access policies defining the interfaces monitoring policy, displaying SSH configuration status, and providing policy settings for HTTP, Telnet, web session limits and CIM XML.

Configuring HTTP

Configuring an HTTP Remote Access Policy

Before You Begin

Before configuring an HTTP remote access policy under a domain group, this policy must first be created. 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, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.

- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

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

Step 5 In the **Work** pane, click **Remote Access**.

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

Step 7 In the **Actions** area, click **Create** and complete all applicable fields.
For **Operational Policies** under the **Domain Group root** node, it is not necessary to click **Create** to 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**.
Admin State field	Whether Cisco UCS Central allows HTTP or HTTPS communication with the Cisco UCS domains included in the Cisco UCS Central domain group. This can be one fo the following: • **disabled**—Cisco UCS Central does not allow communication with any included Cisco UCS domain via HTTP or HTTPS. • **enabled**—Cisco UCS Central allows communication over HTTP if **Redirect HTTP to HTTPS** is set to **disabled**. All HTTP data is exchanged in clear text mode. If **Redirect HTTP to HTTPS** is set to **enabled**, Cisco UCS Central requires HTTPS communication for all included Cisco UCS domains.
Port field	The port to use for HTTP or HTTPS connections. Enter an integer between 1 and 65535. The default port is 80.
Redirect HTTP to HTTPS	If enabled, all attempts to communicate via HTTP are redirected to the equivalent HTTPS address. This option effectively disables HTTP access to all included Cisco UCS domains.

Step 8 Click **Save**.

What to Do Next

Optionally, configure the following remote access policies:

- Telnet
- Web Session Limits
- CIM XML
- Interfaces Monitoring Policy
- SSH Configuration

Deleting an HTTP Remote Access Policy

An HTTP remote access policy is deleted from a domain group under the domain group root. HTTP remote access policies under the domain groups root cannot be deleted.

Procedure

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

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

Step 3 Expand the node for a domain group containing the policy to delete.

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

Step 5 In the **Work** pane, click **Remote Access**.

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

Step 7 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 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Step 9 Click **Save**.

Configuring Telnet

Configuring a Telnet Remote Access Policy

Before You Begin

Before configuring a Telnet remote access policy under a domain group, this policy must first be created. 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, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

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

Step 5 In the **Work** pane, click **Remote Access**.

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

Step 7 In the **Actions** area, click **Create** and complete all applicable fields.
For **Operational Policies** under the **Domain Group root** node, it is not necessary to click **Create** to 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**.
Admin State field	If enabled, the Cisco UCS Manager CLI is available via Telnet in all Cisco UCS domains included in the Cisco UCS Central domain group.

Step 8 Click **Save**.

What to Do Next

Optionally, configure the following remote access policies:

- HTTP
- Web Session Limits

- CIM XML
- Interfaces Monitoring Policy
- SSH Configuration

Deleting a Telnet Remote Access Policy

A Telnet remote access policy is deleted from a domain group under the domain group root. Telnet remote access policies under the domain groups root cannot be deleted.

Procedure

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

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

Step 3 Expand the node for a domain group containing the policy to delete.

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

Step 5 In the **Work** pane, click **Remote Access**.

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

Step 7 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 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Step 9 Click **Save**.

Configuring Web Session Limits

Configuring a Web Session Limits Remote Access Policy

Before You Begin

Before configuring a web session limits remote access policy under a domain group, this policy must first be created. 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, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.

- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

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

Step 5 In the **Work** pane, click **Remote Access**.

Step 6 In the **Work** pane, click the **Web Session Limits** tab.

Step 7 In the **Actions** area, click **Create** and complete all applicable fields.
For **Operational Policies** under the **Domain Group root** node, it is not necessary to click **Create** to 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**.
Maximum Sessions Per User field	The maximum number of concurrent HTTP and HTTPS sessions allowed for each user in the Cisco UCS domains included in the Cisco UCS Central domain group. Enter an integer between 1 and 256.
Maximum Sessions field	The maximum number of concurrent HTTP and HTTPS sessions allowed for all users within the in the Cisco UCS domains included in the Cisco UCS Central domain group. Enter an integer between 1 and 256.

Step 8 Click **Save**.

What to Do Next

Optionally, configure the following remote access policies:

- HTTP
- Telnet
- CIM XML

- Interfaces Monitoring Policy

Deleting a Web Session Limits Remote Access Policy

A web session limits remote access policy is deleted from a domain group under the domain group root. Web session limits remote access policies under the domain groups root cannot be deleted.

Procedure

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

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

Step 3 Expand the node for a domain group containing the policy to delete.

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

Step 5 In the **Work** pane, click **Remote Access**.

Step 6 In the **Work** pane, click the **Web Session Limits** tab.

Step 7 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 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Step 9 Click **Save**.

Configuring CIM XML

Configuring a CIM XML Remote Access Policy

Before You Begin

Before configuring a CIM XML remote access policy under a domain group, this policy must first be created. 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, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.

- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

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

Step 5 In the **Work** pane, click **Remote Access**.

Step 6 In the **Work** pane, click the **CIM XML** tab.

Step 7 In the **Actions** area, click **Create** and complete all applicable fields.
For **Operational Policies** under the **Domain Group root** node, it is not necessary to click **Create** to 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**.
Admin State field	If enabled, the Cisco UCS domains included in the Cisco UCS Central domain group can send XML messages over HTTP.

Step 8 Click **Save**.

What to Do Next

Optionally, configure the following remote access policies:

- HTTP
- Telnet
- Web Session Limits
- Interfaces Monitoring Policy

Deleting a CIM XML Remote Access Policy

A CIM XML remote access policy is deleted from a domain group under the domain group root. CIM XML remote access policies under the domain groups root cannot be deleted.

Procedure

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

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

Step 3 Expand the node for a domain group containing the policy to delete.

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

Step 5 In the **Work** pane, click **Remote Access**.

Step 6 In the **Work** pane, click the **CIM XML** tab.

Step 7 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 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Step 9 Click **Save**.

Configuring Interfaces Monitoring

Configuring an Interfaces Monitoring Remote Access Policy

Before You Begin

Before configuring an interfaces monitoring remote access policy under a domain group, this policy must first be created. 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, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

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

Step 5 In the **Work** pane, click **Remote Access**.

Step 6 In the **Work** pane, click the **Interfaces Monitoring** tab.

Step 7 In the **Actions** area, click **Create** and complete all applicable fields.
For **Operational Policies** under the **Domain Group root** node, it is not necessary to click **Create** to 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**.
Admin State field	Whether the monitoring policy is enabled or disabled for the management interfaces in the Cisco UCS domains included in the Cisco UCS Central domain group.
Poll Interval field	The number of seconds Cisco UCS waits between data recordings. Enter an integer between 90 and 300.
Max Fail Report Count field	The maximum number of monitoring attempts that can fail before Cisco UCS assumes that the management interface is unavailable and generates a fault message. Enter an integer between 2 and 5.
Monitoring Mechanism field	The type of monitoring you want Cisco UCS to use. This can be one of the following: • **Mii Status**—Cisco UCS monitors the availability of the Media Independent Interface (MII). If you select this option, Cisco UCS Central GUI displays the **Media Independent Interface Monitoring** area. • **Ping Arp Targets**—Cisco UCS pings designated targets using the Address Resolution Protocol (ARP). If you select this option, Cisco UCS Central GUI displays the **ARP Target Monitoring** area. • **Ping Gateway**—Cisco UCS pings the default gateway address configured for each Cisco UCS domain included in the Cisco UCS Central domain group. If you select this option, Cisco UCS Central GUI displays the **Gateway Ping Monitoring** area.

a) In the **Monitoring Mechanism** area, select **Mii Status** to select Media Independent Interface Monitoring.

Name	Description
Retry Interval field	The number of seconds Cisco UCS waits before requesting another response from the MII if a previous attempt fails. Enter an integer between 3 and 10.
Max Retry Count field	The number of times Cisco UCS polls the MII until the system assumes the interface is unavailable. Enter an integer between 1 and 3.

b) In the **Monitoring Mechanism** area, select **Ping ARP Targets** to select ARP Target Monitoring.

Name	Description
Target IP 1 field	The first IP address Cisco UCS pings.
Target IP 2 field	The second IP address Cisco UCS pings.
Target IP 3 field	The third IP address Cisco UCS pings.
Number of ARP Requests field	The number of ARP requests Cisco UCS sends to the target IP addresses. Enter an integer between 1 and 5.
Max Deadline Timeout field	The number of seconds Cisco UCS waits for responses from the ARP targets until the system assumes they are unavailable. Enter an integer between 5 and 15.

c) In the **Monitoring Mechanism** area, select **Ping Gateway** to select Gateway Ping Monitoring.

Name	Description
Number of Ping Requests field	The number of times Cisco UCS pings the gateway. Enter an integer between 1 and 5.
Max Deadline Timeout field	The number of seconds Cisco UCS waits for a response from the gateway until Cisco UCS assumes the address is unavailable. Enter an integer between 5 and 15.

Step 8 Click **Save**.

What to Do Next

Optionally, configure the following remote access policies:

- HTTP
- Telnet
- Web Session Limits
- CIM XML

Deleting an Interfaces Monitoring Remote Access Policy

A interfaces monitoring remote access policy is deleted from a domain group under the domain group root. Interfaces monitoring remote access policies under the domain groups root cannot be deleted.

Procedure

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

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

Step 3 Expand the node for a domain group containing the policy to delete.

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

Step 5 In the **Work** pane, click **Remote Access**.

Step 6 In the **Work** pane, click the **Interfaces Monitoring** tab.

Step 7 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 8 If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Step 9 Click **Save**.

SNMP Policies

Cisco UCS Central supports global SNMP policies enabling or disabling, defining SNMP traps and SNMP users (with regular and privacy passwords, authentication types of md5 or sha, and option for AES-128). Registered Cisco UCS domains choosing to define security policies globally within that client's policy resolution control will defer all security policies to its registration with Cisco UCS Central.

Configuring an SNMP Policy

Before You Begin

Before configuring a SNMP policy under a domain group, this policy must first be created. 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, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

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

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

Step 6 In the **Actions** area, click **Create** and complete all applicable fields.
For **Operational Policies** under the **Domain Group root** node, it is not necessary to click **Create** to complete all applicable fields.

a) In the Actions area, click the **Enabled** state and complete the following:
The default state is **Disabled** with no fields displayed. Leaving the default state disables the SNMP policy.

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**.
Admin State field	If enabled, Cisco UCS uses SNMP in all Cisco UCS domains included in the Cisco UCS Central domain group and Cisco UCS Central GUI displays the rest of the fields in this area. You should only enable SNMP if all included Cisco UCS domains are integrated with an SNMP server.
Community/Username field	The default SNMP v1 or v2c community name or SNMP v3 username Cisco UCS includes on any trap messages it sends to the SNMP host. Enter an alphanumeric string between 1 and 32 characters. Do not use @ (at sign), \ (backslash), " (double quote), ? (question mark) or an empty space. The default is public.

Name	Description
System Contact field	The system contact person responsible for the SNMP implementation. Enter a string of up to 255 characters, such as an email address or a name and telephone number.
System Location field	The location of the host on which the SNMP agent (server) runs. Enter an alphanumeric string up to 510 characters.

b) In the **SNMP Traps** area, complete the following:

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)**.
Create SNMP Trap button	Allows you to create an SNMP trap.
Properties button	Displays detailed properties for the object selected in the table.
Delete button	Deletes the object selected in the table.
Name column	The IP address of the SNMP host to which Cisco UCS should send the trap.
Community/Username column	The SNMP v1 or v2c community name or the SNMP v3 username Cisco UCS includes when it sends the trap to the SNMP host. This must be the same as the community or username that is configured for the SNMP service.
Port column	The port on which Cisco UCS communicates with the SNMP host for the trap.
Version column	The SNMP version and model used for the trap.
v3 Privilege column	The type of trap to send, if applicable.
Type column	The privilege associated with the trap, if applicable. This can be one of the following: • **auth**—Authentication but no encryption • **noauth**—No authentication or encryption • **priv**—Authentication and encryption

c) In the **SNMP Users** area, complete the following:

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)**.
Create SNMP User button	Allows you to create an SNMP user.
Properties button	Displays detailed properties for the object selected in the table.
Delete button	Deletes the object selected in the table.
Name column	The SNMP user name.

Step 7 Click **Save**.

Deleting an SNMP Policy

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

Deleting an SNMP policy will remove all SNMP trap and SNMP User 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 Under the **Domain Groups root** node, do one of the following choices:

- To configure the policy in the domain group root, click **Operational Policies**.
- To configure the policy in a specific domain group, expand the node for that domain group and click **Operational Policies**.

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

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

Step 6 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 7 Click **Save**.

Creating an SNMP Trap

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 **SNMP**.

Step 5 In the **SNMP Traps** area, click **Create SNMP Trap** and complete all applicable fields.

a) In the **Create SNMP Trap** dialog, complete the following:

Name	Description
IP Address field	The IP address of the SNMP host to which Cisco UCS should send the trap.
Community/Username field	The SNMP v1 or v2c community name or the SNMP v3 username Cisco UCS includes when it sends the trap to the SNMP host. This must be the same as the community or username that is configured for the SNMP service. Enter an alphanumeric string between 1 and 32 characters. Do not use @ (at sign), \ (backslash), " (double quote), ? (question mark) or an empty space.
Port field	The port on which Cisco UCS communicates with the SNMP host for the trap. Enter an integer between 1 and 65535. The default port is 162.
Version field	The SNMP version and model used for the trap. This can be one of the following: • **v1** • **v2c** • **v3**
Type field	If you select **v2c** or **v3** for the version, the type of trap to send. This can be one of the following: • **informs** • **traps**

Name	Description
v3 Privilege field	If you select **v3** for the version, the privilege associated with the trap. This can be one of the following: • **auth**—Authentication but no encryption • **noauth**—No authentication or encryption • **priv**—Authentication and encryption

b) Click **OK**.

Step 6 Click **Save**.

Deleting an SNMP Trap

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 **SNMP**.

Step 5 In the **SNMP Traps** area, select the SNMP trap to delete and click **Delete**.
You can also right-click the SNMP trap to access that option.

Step 6 Click **Save**.

Creating an SNMP User

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 **SNMP**.

Step 5 In the **SNMP Users** area, click **Create SNMP User** and complete all applicable fields.

a) In the **Create SNMP User** dialog, complete the following:

Name	Description
Name field	The username assigned to the SNMP user. Enter up to 32 letters or numbers. The name must begin with a letter and you can also specify _ (underscore), . (period), @ (at sign), and - (hyphen). **Note** You cannot create an SNMP username that is identical to a locally authenticated username.
Auth Type field	The authorization type. This can be one of the following: • **MD5** • **SHA**
Use AES-128 check box	If checked, this user uses AES-128 encryption.
Password field	The password for this user.
Set field	Whether the password has been set for this SNMP user.
Confirm Password field	The password again for confirmation purposes.
Privacy Password field	The privacy password for this user.
Set field	Whether the privacy password has been set for this SNMP user.
Confirm Privacy Password field	The privacy password again for confirmation purposes.

b) Click **OK**.

Step 6 Click **Save**.

Deleting an SNMP User

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 **SNMP**.

Step 5 In the **SNMP Users** area, select the SNMP user to delete and click **Delete**.
You can also right-click the SNMP user to access that option.

Step 6 Click **Save**.