Configuring Device Profiles and Policies

This chapter includes the following sections:

Device Configuration

Cisco VNMC provides the option to configure devices. You configure devices by adding policies to device profile. You can add DNS and NTP server policies, SNMP policies, and syslog, fault, core and log file policies. You can also enable policy engine logging for the device.

Device Profiles

Device profiles specify device configuration policies that are applied on a per device basis. You create and delete device profiles on the **Device Configurations** tab.

You create device profiles for the Cisco VSG. Policies that reside at the current level or higher are available for assignment to a profile. If an assigned policy does not exist, the default policy is automatically assigned. Policies can be assigned to a device profile under the **Policies** tab when creating the device profile. While creating or editing device profiles, you also have the option of creating policies in the same dialog boxes.

Device Policies

Device policies that can be created and assigned to a device profile are as follows:

- Core file policy
- Fault policy
- Logging policy
- SNMP policy
- Syslog policy

DNS server, NTP server and domain names can be assigned as inline policies. A time zone setting can also be assigned to the profile.

When the system boots up, the fault, logging, SNMP, and syslog policies already have existing default policies. The default policies cannot be deleted but may be modified. A device profile uses name resolution to resolve policy assignments. For details, see Name Resolution in a Multi-tenancy Environment

Device policies capture the device level configuration objects that can be applied to one of more VSGs. The following policies created under root only, in the Device Policies area, will be visible in the VNMC profile:

- Core file policy
- Fault policy
- Logging policy
- Syslog policy

Policies created under root are visible to both the VNMC profile and the Device profile.

Configuring Device Profiles

Adding a Firewall Device Profile

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.

Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.

Step 3 In the **Navigation** pane, expand **root** > **Device Profiles** node.

Note You can add the component at any organizational level.

Step 4 In the **Work** pane, click the **Add Firewall Device Profile** link.

Step 5 In the **Add Firewall Device Profile** dialog box, **General** tab area, complete the following fields:

Name	Description
Name field	The name of the profile. This name can be between 1 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.
Description field	A description of the profile. The description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.

Name	Description
Time Zone drop-down list	A list of time zones. Use the list to designate a time zone.

Step 6 In the **Add Firewall Device Profile** dialog box, click the **Policies** tab.

a) In the **DNS Servers** area, complete the following fields as appropriate:

Name	Description
Add DNS Server link	Opens a dialog box that allows you to specify a new DNS server.
Delete link	Deletes the DNS server IP address selected in the **IP Address** table.
Up and **Down** arrows	Changes the priority of the selected DNS Server IP address.
IP Address table	Contains the IP addresses for the DNS servers configured in the system. VNMC uses the DNS servers in the order they appear in the table.

b) In the **NTP Servers** area, complete the following fields as appropriate:

Name	Description
Add NTP Server link	Opens a dialog box that allows you to specify a new NTP server.
Delete link	Deletes the NTP server hostname selected in the **Hostname** table.
Up and **Down** arrows	Changes the priority of the selected NTP Server hostname.
Hostname table	Contains the NTP server hostnames configured in the system. VNMC uses the NTP server hostnames in the order they appear in the table.

c) In the **DNS Domains** area, complete the following fields as appropriate:

Name	Description
Add link	Opens a dialog box to specify a new DNS domain name.
Edit link	Edits the DNS domain name selected in the **DNS Domains** table. The **default** DNS name cannot be edited.
Delete link	Deletes the DNS domain name selected in the **DNS Domains** table.
DNS Domains table	Contains the default DNS domain name and domain in the system.

d) In the Policies area, complete the following fields as appropriate:

Name	Description
SNMP area	The SNMP policies associated with this profile can be selected, added, or edited. Contains the **Resolved Policy** field.
Syslog area	The syslog policies associated with this profile can be selected, added, or edited. Contains the **Resolved Policy** field.
Fault area	The fault policies associated with this profile can be selected, added, or edited. Contains the **Resolved Policy** field.
Core File area	The core file policies associated with this profile can be selected, added, or edited. Contains the **Resolved Policy** field.
Policy Agent Log File area	The policy agent log file policies associated with this profile can be selected, added, or edited. Contains the **Resolved Policy** field.
Policy Engine Logging area	• **enabled** radio button enables logging. • **disabled** radio button disables logging.

Step 7 In the **Add Firewall Device Profile** dialog box, click **OK**.

Editing a Firewall Device Profile

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.

Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.

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

Step 4 In the **Navigation** pane, click the **Device Profiles** node.

Step 5 In the **Work** pane, click the profile you want to edit.

Step 6 Click the **Edit** link.

Step 7 In the **Edit** dialog box **General** tab area, modify the following fields as appropriate:

Name	Description
Name field	The name of the profile. This name can be between 1 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.
Description field	A description of the profile. The description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.
Time Zone drop-down list	A list of time zones. Use the list to designate a time zone.

Step 8 In the **Add Firewall Device Profile** dialog box, click the **Policies** tab.

a) In the **DNS Servers** area, modify the following fields as appropriate:

Name	Description
Add DNS Server link	Opens a dialog box that allows you to specify a new DNS server.
Delete link	Deletes the DNS server IP address selected in the **IP Address** table.
Up and **Down** arrows	Changes the priority of the selected DNS Server IP address.

Name	Description
IP Address table	Contains the IP addresses for the DNS servers configured in the system. VNMC uses the DNS servers in the order they appear in the table.

b) In the **NTP Servers** area, modify the following fields as appropriate:

Name	Description
Add NTP Server link	Opens a dialog box that allows you to specify a new NTP server.
Delete link	Deletes the NTP server hostname selected in the **Hostname** table.
Up and **Down** arrows	Changes the priority of the selected NTP Server hostname.
Hostname table	Contains the NTP server hostnames configured in the system. VNMC uses the NTP server hostnames in the order they appear in the table.

c) In the **DNS Domains** area, modify the following fields as appropriate:

Name	Description
Add link	Opens a dialog box to specify a new DNS domain name.
Edit link	Edits the DNS domain name selected in the **DNS Domains** table. The **default** DNS name cannot be edited.
Delete link	Deletes the DNS domain name selected in the **DNS Domains** table.
DNS Domains table	Contains the default DNS domain name and domain in the system.

d) In the Policies area, modify the following fields as appropriate:

Name	Description
SNMP area	The SNMP policies associated with this profile can be selected, added, or edited. Contains the **Resolved Policy** field.
Syslog area	The syslog policies associated with this profile can be selected, added, or edited. Contains the **Resolved Policy** field.
Fault area	The fault policies associated with this profile can be selected, added, or edited. Contains the **Resolved Policy** field.
Core File area	The core file policies associated with this profile can be selected, added, or edited. Contains the **Resolved Policy** field.
Policy Agent Log File area	The policy agent log file policies associated with this profile can be selected, added, or edited. Contains the **Resolved Policy** field.
Policy Engine Logging area	• **enabled** radio button enables logging. • **disabled** radio button disables logging.

Step 9 Click **OK**.

Deleting a Firewall Device Profile

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Device Profiles**.
Step 4 In the **Navigation** pane, click the **Device Profiles** node.
Step 5 In the **Work** pane, click the device profile you want to delete.
Step 6 Click the **Delete** link.
Step 7 In the **Confirm** dialog box, click **OK**.

Configuring Device Policies

Configuring Core Policy

Adding a Core File Policy for a Device Profile

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.

Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.

Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies**.

Step 4 In the **Navigation** pane, click the **Core File** node.

Step 5 In the **Work** pane, click the **Add Core File Policy** link.

Note You can add the policy at any organizational level.

Step 6 In the **Add Core File Policy** dialog box, complete the following fields:

Name	Description
Name field	The name of the core file policy. This name can be between 1 and 511 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been created.
Description field	The description of the core file policy. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon. You cannot change this description after it is saved.
Admin State drop-down list	The state of the core file policy. It can be one of the following states: • **Enabled**—Enables the core file policy. TFTP is used. • **Disabled**—Disables the core file policy.
Hostname field	The hostname or IP address to connect using TFTP. **Note** If you use a hostname rather than an IP address, you must configure a DNS server in Cisco VNMC.

Name	Description
Port field	The port number to send the core dump file to.
Protocol field	The protocol used to export the core dump file. This field cannot be edited.
Path field	The path to use when storing the core dump file on a remote system. The default path is /tftpboot. An example path would be /tftpboot/test, where test is the sub-folder.

Step 7 Click **OK**.

Editing a Core File Policy for a Device Profile

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies**.
Step 4 In the **Navigation** pane, click the **Core File** node.
Step 5 In the **Work** pane, click the **General** tab.
Step 6 On the **General** tab, click the core file policy you want to edit.
Step 7 On the **General** tab click the **Edit** link.
Step 8 In the **Edit** dialog box, modify the following fields as appropriate:

Name	Description
Name field	The name of the core file policy.
Description field	A description of the core file policy.
Admin State drop-down list	A list of administrative states. This can be one of the following states: • **enabled**—Enables the core file policy. • **disabled**—Disables the core file policy.
Hostname field	The hostname or IP address. **Note** If you use a hostname rather than an IP address, you must configure a DNS server.

Name	Description
Port field	The port number used when exporting the core dump file. The default path is /tftpboot. To mention a sub folder under tftpboot, use, for example, /tftpboot/test.
Protocol field	The protocol used to export the core dump file.
Path check box	The path to use when storing the core dump file on the remote system.

Step 9 Click **OK**.

Deleting a Core File Policy for a Device Profile

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies**.
Step 4 In the **Navigation** pane, click the **Core File** node.
Step 5 In the **Work** pane, click on the core file you want to delete.
Step 6 Click the **Delete** link.
Step 7 In the **Confirm** dialog box, click **Yes**.

Configuring Fault Policies

Adding a Fault Policy for a Device Profile

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Device Policies**.
Step 4 In the **Work** pane, click the **Add Fault Policy** link.
Note You can add the policy at any organizational level.

Step 5 In the **Add Fault Policy** dialog box, complete the following fields:

Name	Description
Name field	A user-defined name for the fault policy. This name can be between 1 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.
Description field	A user-defined description of the fault policy.
Flapping Interval spinbox	Flapping occurs when a fault is raised and cleared several times in rapid succession. To prevent this, the system does not allow a fault to change its state until this amount of time has elapsed since the last state change. If the condition reoccurs during the flapping interval, the fault returns to the active state. If the condition does not reoccur during the flapping interval, the fault is cleared. What happens at that point depends on the setting in the **Clear Faults Retention Action** field. The number of hours, minutes, and seconds that should pass before the system allows a fault to change its state. The default flapping interval is 10 seconds.
Clear Faults Retention Action drop-down list	The state of the clear faults retention action. It can be one of the following states: • **retain**—Retains the cleared faults section. • **delete**—The system immediately deletes all fault messages as soon as they are marked as cleared.
Clear Faults Retention Interval radio-button	The state of the clear faults retention interval. It can be one of the following states: • **Forever**—The system leaves all cleared fault messages regardless of how long they have been in the system. • **Other**—The system displays the **dd:hh:mm:ss** spinbox for selection of the number of days, hours, minutes, and seconds that should pass before the system deletes a cleared fault message. The default retention interval is 1 hour.

Step 6 Click **OK**.

Editing a Fault Policy for a Device Profile

Note When the system boots up, a default policy already exists. The default policy cannot be deleted but may be modified.

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.

Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.

Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies.**.

Step 4 In the **Navigation** pane, click the **Fault** node.

Step 5 In the **Work** pane, click the fault policy you want to edit.

Step 6 Click the **Edit** link.

Step 7 In the **Edit** dialog box, modify the following fields as appropriate:

Name	Description
Name field	The name of the fault policy.
Description field	A description of the fault policy.
Flapping Interval spinbox	The spinbox that lists flapping intervals. Use the box to set the interval. Flapping occurs when a fault is raised and cleared several times in rapid succession. To prevent this, the system does not allow a fault to change its state until this amount of time has elapsed since the last state change. The interval is the number of hours, minutes, and seconds that should pass before the system allows a fault to change its state. If the condition reoccurs during the flapping interval, the fault returns to the active state. If the condition does not reoccur during the flapping interval, the fault is cleared. What happens at that point depends on the setting in the **Clear Faults Retention Action** field. The default flapping interval is 10 seconds.

Name	Description
Clear Faults Retention Action drop-down list	The list that contains fault retention actions. Use the list to set an action. This can be one of the following actions: • **retain**—The system retains fault messages. • **delete**—The system immediately deletes all fault messages as soon as they are marked as cleared.
Clear Faults Retention Interval radio-button	The control that sets the retention interval. Use the control to set the interval. This can be one of the following values: • **forever**—The system leaves all cleared fault messages regardless of how long they have been in the system. • **other**—The system displays the **dd:hh:mm:ss** spinbox for selection of the number of days, hours, minutes, and seconds that should pass before the system deletes a cleared fault message. The default retention interval is 1 hour.

Step 8 Click **OK**.

Deleting a Fault Policy for a Device Profile

Note When the system boots up, a default policy already exists. The default policy cannot be deleted but may be modified.

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies**.
Step 4 In the **Navigation** pane, click the **Fault** node.
Step 5 In the **Work** pane, click the fault you want to delete.
Step 6 Click the **Delete** link.
Step 7 In the **Confirm** dialog box, click **OK**.

Configuring Log File Policies

Adding a Logging Policy for a Device Profile

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies**.
Step 4 In the **Navigation** pane, click the **Log File** node.
Note You can add the policy at any organizational level.
Step 5 In the **Work** pane, click the **Add Logging Policy** link.
Step 6 In the **Add Logging Policy** dialog box, complete the following fields:

Name	Description
Name field	The name of the logging policy. This name can be between 1 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.
Description field	A description of the logging policy.

Name	Description
Log Level drop-down list	A list of logging severity levels. This can be one of the following levels: • **debug0** • **debug1** • **debug2** • **debug3** • **debug4** • **info** • **warn** • **minor** • **major** • **crit** The default log level is **info**.
Backup Files Count field	The number of backup files that are filled before they are overwritten. The range is 1 to 9 files. The default is 2 files.
File Size (bytes) field	The backup file size. The range is 1MB to 100MB. The default file size is 5MB.

Step 7 Click **OK**.

Editing a Logging Policy for a Device Profile

Note When the system boots up, a default policy already exists. The default policy cannot be deleted but may be modified.

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.

Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.

Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies**.

Step 4 In the **Navigation** pane, click the **Log File** node.

Step 5 On the **Work** pane, click the logging policy you want to edit.

Step 6 Click the **Edit** link.

Step 7 In the **Edit** dialog box, modify the appropriate fields:

Name	Description
Name field	The name of the logging policy. This field cannot be edited.
Description field	A description of the logging policy.
Log Level drop-down list	A list of logging levels. This can be one of the following levels: • **debug0** • **debug1** • **debug2** • **debug3** • **debug4** • **info** • **warn** • **minor** • **major** • **crit** The default log level is **info**.
Backup Files Count field	The number of backup files that are filled before they are overwritten. The range is 1 to 9 files. The default is 2 files.
File Size (bytes) field	The backup file size. The range is 1MB to 100MB. The default file size is 5MB.

Step 8 Click **OK**.

Deleting a Logging Policy for a Device Profile

Note When the system boots up, a default policy already exists. The default policy cannot be deleted but may be modified.

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.
Step 3 In the **Navigation** pane, expand the nodes **root** > **Advanced** > **Device Policies**.
Step 4 In the Navigation pane, click the **Log File** node.
Step 5 In the **Work** pane, click the logging policy you want to delete.
Step 6 Click the **Delete** link.
Step 7 In the **Confirm** dialog box, click **OK**.

Configuring SNMP Policies

Adding an SNMP Policy

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies**.
Step 4 In the **Navigation** pane, click the **SNMP** node.
Note You can add the policy at any organizational level.
Step 5 In the **Work** pane, click the **Add SNMP** link.
Step 6 In the **Add SNMP** dialog box, **General** tab area, complete the following fields as appropriate:

Table 1: General Tab

Name	Description
Name field	The name of the SNMP policy. This name can be between 1 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.
Description field	A description of the SNMP policy. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon. You cannot change this description after it is saved.
Admin State drop-down list	The administrative state of the policy. It can be one of the following states: • **enabled** • **disabled** The default state is enabled.
Location field	The physical location of the device.
Contact field	The contact person for the device.
SNMP Port field	The port where the SNMP agent is listening for requests. You cannot edit this field.

Step 7 In the **Add SNMP** dialog box, **Communities** tab area do the following:

a) Click the **Add SNMP Community** link.

b) In the **Add SNMP Community** dialog box, complete the following fields as appropriate:

Name	Description
Community field	The name of the community.
Role field	The role associated with the community string. You cannot edit this field.

c) Click **OK**.

Step 8 In the **Add SNMP** dialog box, click **OK**.

Editing an SNMP Policy

Note When the system boots up, a default policy already exists. The default policy cannot be deleted but may be modified.

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.

Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.

Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies**.

Step 4 Click the **SNMP** node where you want to edit an SNMP policy.

Step 5 In the **Work** pane, click the SNMP policy you want to edit.

Step 6 Click the **Edit** link.

a) In the **Edit SNMP** dialog box **General** tab area, edit the appropriate information:

Name	Description
Name field	The name of the SNMP policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been created.
Description field	A description of the SNMP policy.
Admin State drop-down list	The administrative state of the policy. It can be one of the following states: • **enabled** • **disabled** The default state is enabled.
Location field	The physical location of the device.
Contact field	The contact person for the device.
SNMP Port field	The port where the SNMP agent is listening for requests.

b) In the **Edit SNMP** dialog box **Communities** tab area, edit the information as appropriate:

Name	Description
Community column	The name of the community.
Role column	The role associated with the community string.

Note Depending upon the object you select in the table, different options will appear in the area above the table.

c) In the **Edit SNMP** dialog box **Trap** tab area, edit the information as appropriate:

Name	Description
Hostname field	The IP address of the SNMP host.
Port field	The port where the SNMP agent is listening for requests.
Community field	The name of the community.

d) In the **Edit SNMP Trap** dialog box, click **OK**.

Step 7 Click **OK**.

Deleting an SNMP Policy

Note When the system boots up, a default policy already exists. The default policy cannot be deleted but may be modified.

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies**.
Step 4 In the **Navigation** pane, click the **SNMP** node.
Step 5 In the **Work** pane, click the SNMP policy you want to delete.
Step 6 Click the **Delete** link.
Step 7 In the **Confirm** dialog box, click **Yes**.

Adding an SNMP Trap Receiver

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.

Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.

Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies**.

Step 4 In the **Navigation** pane, click the **SNMP** node.

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

Step 6 Click the **Traps** tab.

Step 7 In the **Add SNMP** dialog box, click the **Add SNMP Trap** link.

Step 8 In the **Add SNMP Trap** dialog box, complete the following fields:

Name	Description
Hostname field	The IP address of the SNMP host.
Port field	The port where the SNMP agent is listening for requests. The default port is 162.
Community field	The name of the community.

Step 9 Click **OK**.

Editing an SNMP Trap Receiver

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.

Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.

Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies**.

Step 4 Click the **SNMP** > ***SNMP Policy_name*** where you want to edit the SNMP trap.

Step 5 In the **Work** pane, **Traps** tab area, click the hostname to edit.

Step 6 Click the **Edit** link.

Step 7 In the **Edit SNMP Trap** dialog box, edit the appropriate fields:

Name	Description
Hostname field	The IP address of the SNMP host.

Name	Description
Port field	The port where the SNMP agent is listening for requests.
Community field	The name of the community.

Step 8 Click **OK**.

Deleting an SNMP Trap Receiver

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies** > **SNMP**.
Step 4 In the **Navigation** pane, click the SNMP policy that contains the trap you want to delete.
Step 5 In the **Work** pane, click the **Traps** tab.
Step 6 In the **Work** pane, click the trap you want to delete.
Step 7 Click the **Delete** link.
Step 8 In the **Confirm** dialog box, click **Yes**.

Configuring Syslog Policies

Adding a Syslog Policy for a Device Profile

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies**.
Step 4 In the **Navigation** pane, click the **Syslog** node.
Note You can add the policy at any organizational level.
Step 5 In the **Work** pane, click the **Add Syslog** link.
Step 6 In the **Add Syslog** dialog box, complete the following tasks:

a) In the **Add Syslog** dialog box, **General** tab area, complete the following fields:

Table 2: General Tab

Name	Description
Name field	The name of the syslog policy. This name can be between 1 and 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is saved.
Description field	The description of the syslog policy.
Port field	The TCP or UDP port where syslog messages are sent. You cannot edit this field.

b) In the **Add Syslog** dialog box, **Local Destinations** tab, complete the following fields:

Table 3: Console Area

Name	Description
Admin State radio button	The administrative state of the policy. It can be one of the following states: • **enabled** • **disabled**
Level radio button	The message level. It can be one of the following levels: • **alerts** • **critical** • **emergencies** If the **Admin State** is enabled, select the lowest message level that you want displayed. The system displays that level and above on the console.

Table 4: Monitor Area

Name	Description
Admin State radio button	The administrative state of the policy. It can be one of the following states: • **enabled** • **disabled**
Level drop-down list	The message levels. It can be one of the following levels: • **emergencies (0)** • **alerts (1)** • **critical (2)** • **errors (3)** • **warnings (4)** • **notifications (5)** • **information (6)** • **debugging (7)** If the **Admin State** is enabled, select the lowest message level that you want displayed. The system displays that level and above on the console.

Table 5: File Area

Name	Description
Admin State radio button	The administrative state of the policy. It can be one of the following states: • **enabled** • **disabled**

Name	Description
Level drop-down list	The message levels. It can be one of the following levels: • **emergencies (0)** • **alerts (1)** • **critical (2)** • **errors (3)** • **warnings (4)** • **notifications (5)** • **information (6)** • **debugging (7)** If the **Admin State** is enabled, select the lowest message level that you want displayed. The system displays that level and above on the console.
File Name field	The name of the file in which messages are logged.
Size (Bytes) field	The maximum size, in bytes, the file can be before the system begins to over-write messages.

Step 7 Click **OK**.

Editing a Syslog Policy for a Device Profile

Note When the system boots up, a default policy already exists. The default policy cannot be deleted but may be modified.

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.

Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.

Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies**.

Step 4 In the **Navigation** pane, click the **Syslog** node.

Step 5 In the **Work** pane, click the syslog policy you want to edit.

Step 6 Click the **Edit** link.

Step 7 In the **Edit Syslog** dialog box, modify the following fields as appropriate:

a) In the **Add Syslog** dialog box, **General** tab area, edit the following fields as appropriate:

Name	Description
Name field	The name of the syslog policy. This field cannot be edited.
Description field	The description of the syslog policy.
Port field	The TCP or UDP port where syslog messages are sent.

b) In the **Add Syslog** dialog box, **Local Destinations** tab, edit the following fields as appropriate:

Table 6: Console Area

Name	Description
Admin State radio button	The administrative state of the policy. It can be one of the following states: • **enabled** • **disabled**
Level radio button	The message level. It can be one of the following levels: • **alerts** • **critical** • **emergencies** If the **Admin State** is enabled, select the lowest message level that you want displayed. The system displays that level and above on the console.

Table 7: Monitor Area

Name	Description
Admin State radio button	The administrative state of the policy. It can be one of the following states: • **enabled** • **disabled**
Level drop-down list	The message levels. It can be one of the following levels: • **emergencies (0)** • **alerts (1)** • **critical (2)** • **errors (3)** • **warnings (4)** • **notifications (5)** • **information (6)** • **debugging (7)** If the **Admin State** is enabled, select the lowest message level that you want displayed. The system displays that level and above on the console.

Table 8: File Area

Name	Description
Admin State radio button	The administrative state of the policy. It can be one of the following states: • **enabled** • **disabled**

Name	Description
Level drop-down list	The message levels. It can be one of the following levels: • **emergencies (0)** • **alerts (1)** • **critical (2)** • **errors (3)** • **warnings (4)** • **notifications (5)** • **information (6)** • **debugging (7)** If the **Admin State** is enabled, select the lowest message level that you want displayed. The system displays that level and above on the console.
File Name field	The name of the file in which messages are logged.
Size (Bytes) field	The maximum size, in bytes, the file can be before the system begins to over-write messages.

Step 8 Click **OK**.

Deleting a Syslog Policy for a Device Profile

Note When the system boots up, a default policy already exists. The default policy cannot be deleted but may be modified.

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies**.
Step 4 In the **Navigation** pane, click the **Syslog** node.
Step 5 In the **Work** pane, click the syslog policy you want to delete.
Step 6 Click the **Delete** link.
Step 7 In the **Confirm** dialog box, click **Yes**.

Adding a Syslog Server for a Device Profile

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies** > **Syslog**.
Step 4 In the **Work** pane, click the syslog policy where you want to add the server.
Step 5 Click the **Add Syslog** link.
Step 6 In the Work pane, click the **Servers** tab.
Step 7 In the **Add Syslog** dialog box, click the **Add Syslog Server** link.
Step 8 In the **Add Syslog Server** dialog box, complete the following fields:

Name	Description
Server Type field	The type of server. It can be one of the following types: • **primary** • **secondary** • **tertiary**
Hostname/IP address field	The hostname or IP address where the syslog file resides.

Name	Description
Severity field	The severity level. It can be one of the following levels: • **emergencies (0)** • **alerts (1)** • **critical (2)** • **errors (3)** • **warnings (4)** • **notifications (5)** • **information (6)** • **debugging (7)**
Forwarding Facility field	The forwarding facility. It can be one of the following types: • **auth** • **authpriv** • **cron** • **daemon** • **ftp** • **kernel** • **local0** • **local1** • **local2** • **local3** • **local4** • **local5** • **local6** • **lpr** • **mail** • **news** • **syslog** • **user** • **uucp**

Name	Description
Admin State field	The administrative state of the policy. It can be one of the following states: • **enabled** • **disabled**

Step 9 Click **OK**.

Editing a Syslog Server for a Device Profile

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.

Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.

Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies** > **Syslog** node.

Step 4 In the **Work** pane, click the appropriate syslog where you want to edit a syslog server.

Step 5 Click the **Edit** link.

Step 6 In the **Edit Syslog** dialog box **Servers** tab area, click the syslog server you want to edit and click the **Edit** link.

Step 7 In the **Edit Syslog Server** dialog box modify the fields as appropriate.

Name	Description
Server Type field	The type of server. It can be one of the following types: • **primary** • **secondary** • **tertiary**
Hostname/IP address field	The hostname or IP address where the syslog file resides.

Name	Description
Severity field	The severity level. It can be one of the following levels: • **emergencies (0)** • **alerts (1)** • **critical (2)** • **errors (3)** • **warnings (4)** • **notifications (5)** • **information (6)** • **debugging (7)**
Forwarding Facility field	The forwarding facility. It can be one of the following types: • **auth** • **authpriv** • **cron** • **daemon** • **ftp** • **kernel** • **local0** • **local1** • **local2** • **local3** • **local4** • **local5** • **local6** • **lpr** • **mail** • **news** • **syslog** • **user** • **uucp**

Name	Description
Admin State field	The administrative state of the policy. It can be one of the following states: • **enabled** • **disabled**

Step 8 Click **OK**.

Deleting a Syslog Server for a Device Profile

Procedure

Step 1 In the **Navigation** pane, click the **Policy Management** tab.
Step 2 In the **Navigation** pane, click the **Device Configurations** subtab.
Step 3 In the **Navigation** pane, expand **root** > **Advanced** > **Device Policies** > **Syslog** node.
Step 4 In the **Work** pane, click the **Add Syslog** link.
Step 5 In the **Add Syslog** dialog box, click the **Servers** tab.
Step 6 Click the server you want to delete.
Step 7 Click the **Delete** link.
Step 8 In the **Confirm** dialog box, click **Yes**.