Configuring Device Policies and Profiles

This section includes the following topics:

Device Policies and Profiles

Prime Network Services Controller enables you to create device profiles and policies at any organizational level.

Device Profiles

A Prime Network Services Controller device profile is a set of custom security attributes and device policies. For Nexus 1000V VSMs, the device profile is added to the port profile. The port profile is assigned to the Nexus 1000V VSM vNIC, making the device profile part of the virtual machine (VM). Adding a device profile to the VM allows the addition of custom attributes to the VM. Firewall rules can be written using custom attributes such that traffic between VMs can be allowed to pass or be dropped.

You apply device profiles to compute and edge firewalls by choosing Resource Management > Managed Resources and then navigating to the required compute or edge firewall at the root or tenant level. The Firewall Settings area of the firewall pane includes the Device Profile option.

Prime Network Services Controller includes a default device profile at root level. The default device profile can be edited but cannot be deleted.

Policies

Prime Network Services Controller supports the following objects related to policies:

- Policy set—Contains policies. After a policy set is created, it can be assigned to a profile. An existing default policy set is automatically assigned at system boot up.
- Policy—Contains rules that can be ordered. An existing default policy is automatically assigned at system boot up. The default policy contains a rule with an action of **drop**.
- Rule—Contains conditions for regulating traffic. The default policy contains a rule with an action of **drop**. Conditions for a rule can be set using the network, custom, and virtual machine attributes.
- Object group—Can be created under an organization node. An object group defines a collection of condition expressions on a system-defined or user-defined attribute. An object group can be referred to in a policy rule condition when the member or not-member operator is selected. A rule condition that refers to an object group resolves to true if any of the expressions in the object group are true.
- Security Profile Dictionary—Logical collection of security attributes. You define dictionary attributes for use in a security profile. A security profile dictionary is created at the root or tenant node. You can create only one dictionary for a tenant and one for root. The security profile dictionary allows the user to define names of custom attributes. Custom attribute values are specified on security profile objects. Custom attributes can be used to define policy rule conditions. Attributes configured in a root level dictionary can be used by any tenant. You cannot create a dictionary below the tenant level.
- Zone—Set of VMs based on conditions. The zone name is used in the authoring rules.

Security policies are created and then pushed to the Cisco VSG or ASA 1000V.

Device Configuration

Prime Network Services Controller enables you to configure devices by adding policies to a device profile and then applying that profile to a device. To create a root device profile, choose **Policy Management > Device Configurations > root** and click **Add Device Profile**. Device profiles contain options for the following policies and settings:

- DNS server and domain
- NTP server
- SNMP policy
- Syslog policy
- Fault policy
- Core policy
- Log file policy
- Policy engine logging
- Authentication policy

Device Policies

Prime Network Services Controller enables you to create the following policies and assign them to device profiles for application to service devices:

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

Prime Network Services Controller provides default polices for fault, logging, SNMP, and syslog. The default policies cannot be deleted but can be modified. A device profile uses name resolution to resolve policy assignments. For details, see Name Resolution in a Multi-Tenant Environment.

Policies created under root are visible to both the Prime Network Services Controller profile and the Device profile.

Configuring Device Policies

Prime Network Services Controller enables you to configure and manage the following types of device policies:

- AAA
- Core File
- Fault
- Log File
- SNMP
- Syslog

Configuring AAA Policies

Authentication, authorization, and accounting (AAA) policies verify users before they are allowed access to a network and network services. By creating AAA policies in Prime Network Services Controller and associating the policies with objects through device profiles, you can ensure that only authenticated users can access the objects.

Prime Network Services Controller supports authentication and authorization for edge firewalls and server groups using the following protocols:

- Kerberos
- Lightweight Directory Access Protocol (LDAP)
- Windows NT

- RADIUS
- RSA SecurID (SDI)
- TACACS+

You can use Prime Network Services Controller to configure an AAA policy on ASA 1000V. Prime Network Services Controller does not support AAA policies on VSG, VPX, or CSR 1000V.

Procedure

Step 1 Choose **Policy Management** > **Device Configurations** > **root** > **Policies** > **AAA** > **Auth Policies**.

Step 2 In the General tab, click **Add Auth Policy**.

Step 3 In the Add Auth Policy dialog box, enter the information as described in Add Auth Policy Dialog Box, on page 4, then click **OK**.

Note If you add a remote server group with a new server group with a new server host, the information that you must provide for the host depends on the protocol used. For example, the information required for a RADIUS server host is different from the information required for an LDAP server host. See the online help for the information required for the selected protocol.

Field Descriptions

Add Auth Policy Dialog Box

Field	Description
Name	Policy name.
Description	Brief policy description.
Authorization	Check the Enable check box to enable authorization via server authentication.
Remote Access Methods	
Add Remote Access Method	Adds a remote access method to the policy. For more information, see Remote Access Method Dialog Box, on page 5.
Access Method	One of the following access methods: • Enable Mode • HTTP • Serial • SSH • Telnet

Field	Description
Admin State	Whether the administrative state of the policy is enabled or disabled.
Remote Server Group	Remote server group name.
Local Auth	This column is not used.

Remote Access Method Dialog Box

Field	Description
Access Method	One of the following access methods: • Enable Mode • HTTP • Serial • SSH • Telnet
Admin State	Whether the administrative state of the access method is enabled or disabled.
Server Group	Indicate the server group to use: **1** In the Protocol for Creation field, choose the required protocol. **2** In the Server Group fields, do one of the following: • From the drop-down list, choose an available remote server group. • Click **Add Remote Server Group - *protocol*** to add a new remote server group. **Note** If you add a new remote server group, the information that you must provide for the server group and host depends on the protocol used. For example, the information required for a RADIUS server group and host is different from the information required for an LDAP server group and host.

Configuring Core File Policies

Adding a Core File Policy for a Device

You can add a core file policy at any organizational level.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Core File**.

Step 2 In the General tab, click **Add Core File Policy**.

Step 3 In the Add Core File Policy dialog box, add the information as described in the following table, then click **OK**:

Field	Description
Name	Core file policy name, containing 1 to 32 characters. You can use alphanumeric characters, hyphen (-), underscore (_), and period (.). You cannot change the name after the policy has been saved.
Description	Brief policy description, containing 1 to 256 characters. You can use alphanumeric characters, hyphen (-), underscore (_), and period (.).
Admin State	Indicate whether the administrative state of the policy is to be enabled or disabled.
Hostname/IP Address	Hostname or IP address to use for this policy. If you use a hostname rather than an IP address, you must configure a DNS server in Prime Network Services Controller.
Port	Port number for sending the core dump file. This field is read-only for InterCloud policies.
Protocol	Protocol for exporting the core dump file (tftp only).
Path	Path to use when storing the core dump file on a remote system. The default path is /tftpboot; for example, /tftpboot/*test*, where *test* is the subfolder.

Editing a Core File Policy for a Device Profile

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Core File**.

Step 2 In the General tab, select the core file policy you want to edit, then click **Edit**.

Step 3 In the Edit Core File Policy dialog box, edit the fields as required, using the information in the following table, then click **OK**.

Field	Description
Name	Name of the core file policy (read-only).
Description	Brief policy description.
Admin State	Administrative status of the policy: enabled or disabled.
Hostname	Hostname or IP address. **Note** If you use a hostname, you must configure a DNS server.
Port	Port number to use when exporting the core dump file. This field is read-only for InterCloud policies.
Protocol	Protocol used to export the core dump file (tftp only).
Path	Path to use when storing the core dump file on the remote system. The default path is /tftpboot. To specify a subfolder under tftpboot, use the format /tftpboot/*folder* where *folder* is the subfolder.

Deleting a Core File Policy from a Device Profile

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Core File**.

Step 2 In the General tab, select the core file policy you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.

Configuring Fault Policies

Adding a Fault Policy for a Device Profile

You can add a fault policy at any organizational level.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Fault**.

Step 2 In the General tab, click **Add Fault Policy**.

Step 3 In the Add Fault Policy dialog box, enter the information as described in the following table, then click **OK**.

Field	Description
Name	Fault policy name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created.
Description	Brief policy description.
Flapping Interval	Length of time (in hours, minutes, and seconds) that must elapse before the system allows a fault to change its state. 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 default flapping interval is ten seconds.
Clear Faults Retention Action	Action to be taken when faults are cleared: • retain—Retain the cleared faults. • delete—Delete fault messages as soon as they are marked as cleared.

Field	Description
Clear Faults Retention Interval	How long the system is to retain cleared fault messages: • Forever—The system retains all cleared fault messages regardless of their age. • Other—The system retains cleared fault message for a specified the length of time. In the spinbox that is displayed when you select this option, enter the length of time (in days, hours, minutes, and seconds) that the system is to retain cleared fault messages.

Editing a Fault Policy for a Device Profile

Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Fault**.

Step 2 In the General tab, select the fault policy you want to edit, then click **Edit**.

Step 3 In the Edit Fault Policy dialog box, modify the following fields as required, then click **OK**.

Field	Description
Name	Policy name (read-only).
Description	Brief policy description.

Field	Description
Flapping Interval	Length of time (in hours, minutes, and seconds) that must elapse before the system allows a fault to change its state. 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 recurs during the flapping interval, the fault returns to the active state. If the condition does not recur during the flapping interval, the fault is cleared. The next action depends on the setting in the Clear Faults Retention Action field. The default flapping interval is ten seconds.
Clear Faults Retention Action	Available fault retention actions: • retain—The system retains fault messages. • delete—The system deletes fault messages when they are marked as cleared.
Clear Faults Retention Interval	How long the system is to retain cleared fault messages: • Forever—The system retains all cleared fault messages regardless of their age. • Other—The system retains cleared fault message for a specified the length of time. In the spinbox that is displayed when you select this option, enter the length of time (in days, hours, minutes, and seconds) that the system is to retain cleared fault messages.

Deleting a Fault Policy for a Device Profile

Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Fault**.

Step 2 In the General tab, select the fault policy that you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.

Configuring Log File Policies

Adding a Logging Policy for a Device Profile

You can add a logging policy for a device at any organizational level.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Log File**.

Step 2 In the General tab, click **Add Logging Policy**.

Step 3 In the Add Logging Policy dialog box, complete the following fields, then click **OK**.

Field	Description
Name	Logging policy name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created.
Description	Brief policy description.

Field	Description
Log Level	One of the following logging severity levels: • debug0 • debug1 • debug2 • debug3 • debug4 • info • warning • minor • major • critical The default log level is info.
Backup Files Count	Number of backup files that are filled before they are overwritten. The range is 1 to 9 files, with a default of 2 files.
File Size (bytes)	Backup file size. The range is 1 MB to 100 MB with a default of 5 MB.

Editing a Logging Policy for a Device Profile

Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Log File**.

Step 2 In the General tab, select the log file policy that you want to edit, then click **Edit**.

Step 3 In the Edit Log File Policy dialog box, edit the fields as required by using the information in the following table, then click **OK**.

Field	Description
Name	Logging policy name (read-only).
Description	Brief policy description.
Log Level	One of the following logging levels: • debug0 • debug1 • debug2 • debug3 • debug4 • info • warning • minor • major • critical The default log level is info.
Backup Files Count	Number of backup files that are filled before they are overwritten. The range is 1 to 9 files, with a default of 2 files.
File Size (bytes)	Backup file size. The range is 1 MB to 100 MB with a default of 5 MB.

Deleting a Logging Policy for a Device Profile

Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Log File**.

Step 2 In the General tab, select the logging policy you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.

Configuring SNMP Policies

Adding an SNMP Policy

You can add an SNMP policy at any organizational level.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > SNMP**.

Step 2 In the General tab, click **Add SNMP Policy**.

Step 3 In the Add SNMP dialog box, complete the following fields as appropriate:

Table 1: General Tab

Field	Description
Name	SNMP policy name. This name can contain 1 to 32 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon. You cannot change this name after it is created.
Description	SNMP policy description. This description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphens, underscore, dot, and colon.
Admin State	Indicate whether the administrative status of the policy is enabled or disabled.
Location	Physical location of the device.
Contact	Contact person for the device.
SNMP Port	Port that the SNMP agent listens to for requests. You cannot edit this field.

Step 4 Click the **Communities** tab, then complete the following steps:

a) Click **Add SNMP Community**.

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

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

Step 5 In the Add SNMP dialog box, click **OK**.

Editing an SNMP Policy

Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > SNMP**.

Step 2 In the General tab, select the SNMP policy that you want to edit, then click **Edit**.

Step 3 In the Edit SNMP Policy dialog box, edit the information in the General tab as required, using the information in the following table:

Field	Description
Name	SNMP policy name (read-only).
Description	Brief policy description.
Admin State	Administrative state of the policy: enabled (default) or disabled.
Location	Physical location of the device.
Contact	Contact person for the device.
SNMP Port	Port that the SNMP agent listens to for requests (read-only).

Step 4 In the Communities tab, edit the information as required:

Field	Description
Add SNMP Community	Adds an SNMP community.
Delete	Deletes the selected SNMP community.
Filter	Enter the string or value that you want to filter the table contents by.
Community	SNMP community name.
Role	Role associated with the SNMP community.

Step 5 In the Traps tab, edit the information as required:

Field	Description
Add SNMP Trap	Adds an SNMP trap.
Edit	Enables you to edit the selected SNMP trap.
Delete	Deletes the selected SNMP trap.
Filter	Enter the string or value that you want to filter the table contents by.
Hostname/IP Address	IP address of the SNMP host.
Port	Port where the SNMP agents listens for requests.
Community	SNMP community name.

Step 6 Click **OK**.

Deleting an SNMP Policy

Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > SNMP**.

Step 2 In the General tab, select the SNMP policy that you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.

Adding an SNMP Trap Receiver

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > SNMP**.

Step 2 In the General tab, click **Add SNMP Policy > Traps > Add SNMP Trap.**.

Step 3 In the Add SNMP Trap dialog box, enter the following information, then click **OK**:

Field	Description
Hostname/ IP Address	Hostname or IP address of the SNMP host.
Port	Port that the SNMP agent listens to for requests. The default port is 162.
Community	SNMP community name.

Editing an SNMP Trap Receiver

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > SNMP**.

Step 2 In the General tab, select the SNMP policy with the SNMP trap that you want to edit, then click **Edit**.

Step 3 In the Edit SNMP Policy dialog box, click the **Traps** tab.

Step 4 In the Traps tab, select the entry that you want to edit, then click **Edit**.

Step 5 In the Edit SNMP Trap dialog box, edit the information in the General tab as required, using the following information:

Field	Description
Hostname/IP Address	Hostname or IP address of the SNMP host (read-only).

Field	Description
Port	Port that the SNMP agent listens to for requests.
Community	SNMP community name.

Step 6 Click **OK** in the open dialog boxes.

Deleting an SNMP Trap Receiver

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > SNMP**.
Step 2 In the General tab, select the SNMP policy with the SNMP trap that you want to delete, then click **Edit**.
Step 3 In the Edit SNMP Policy dialog box, click the **Traps** tab.
Step 4 In the Traps tab, select the entry that you want to delete, then click **Delete**.
Step 5 When prompted, confirm the deletion.

Configuring Syslog Policies

Adding a Syslog Policy for a Device

Prime Network Services Controller enables you to configure syslog policies for syslog messages and then attach a created syslog policy to a device profile for implementation on all devices using that profile.

You can create syslog policies for logging syslog messages to a remote syslog server or to a local buffer for later review.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Syslog**.
Step 2 In the General tab, click **Add Syslog Policy**.
Step 3 In the Add Syslog dialog box, provide the information as described in Add Syslog Policy Dialog Box, on page 19, then click **OK**.

Field Descriptions

Add Syslog Policy Dialog Box

Field	Description
General Tab	
Name	Policy name.
Description	Brief policy description.
Use Emblem Format	Check the check box to use the EMBLEM format for syslog messages. This option appears only on supported devices.
Continue if Host is Down	Check the check box to continue logging if the syslog server is down. This option only appears on supported devices.
Servers Tab	
Add Syslog Server	Click to add a new syslog server.
Syslog Servers table	List of configured syslog servers.
Local Destinations Tab	
Console	• Admin State—Administrative state of the policy: disabled or enabled. • Level—Message level: alert, critical, or emergency. If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency.

Field	Description
Monitor	• Admin State—Administrative state of the policy: disabled or enabled. • Level—Message level: emergency, alert, critical, error, warning, notification, information, or debugging. If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency.
File	• Admin State—Administrative state of the policy: disabled or enabled. • Level—Message level: emergency, alert, critical, error, warning, notification, information, or debugging. If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency. • File Name—Name of the file to which messages are logged. • Size (bytes)—Maximum size, in bytes, that the file can reach before the system begins to overwrite the messages.

Field	Description
Buffer	Buffer options are not available for InterCloud policies. • Admin State—Administrative state of the policy: disabled or enabled. • Level—Message level: emergency, alert, critical, error, warning, notification, information, or debugging. If the Admin State is enabled, select the message level that you want displayed. The system displays that level and above on the console. For example, if you choose critical, the system also displays messages with the severities alert and emergency. • Buffer Size (Bytes)—In bytes, the size of the buffer for syslog messages. • Wrap to Flash—Indicates whether or not the buffer contents are saved to flash memory when the buffer wraps (becomes full). Check the check box to save the contents to flash memory if the buffer wraps. • Max File Size in Flash (KB)—Maximum size, in kilobytes, that can be used by the syslog buffer. This option is enabled if the Wrap to Flash option is enabled. • Min Free Flash Size (KB)—Minimum size, in kilobytes, that is allocated for the syslog buffer. This option is enabled if the Wrap to Flash option is enabled.
Time Stamp	Check the check box for each of the following options that you want to enable for timestamp display: • Enable Timestamp • Include Year • Include Milliseconds • Show Time Zone • Use Local Time Zone

Editing a Syslog Policy for a Device Profile

Prime Network Services Controller enables you to edit existing syslog policies as described in this procedure.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Syslog**.

Step 2 In the General tab, select the policy you want to edit, then click **Edit**.

Step 3 In the Edit Syslog Policy dialog box, in the General tab, edit the information as required, using the following information:

Field	Description
Name	Policy name (read-only).
Description	Brief policy description.
Use Emblem Format	Check the check box to use the EMBLEM format for syslog messages. This option is supported for ASA 1000Vs. It is not supported for VSGs.
Continue if Host is Down	Check the check box to continue logging if the syslog server is down. This option is supported for ASA 1000Vs. It is not supported for VSGs.

Step 4 In the Servers tab, click **Add Syslog Server** to add a new syslog server, or select an existing server and click **Edit** to edit it.

Step 5 In the Local Destinations tab, edit the information as required, using the following information:

Field	Description
Console	• Admin State—Administrative state of the policy: enabled or disabled. • Level—Message level: alerts, critical, or 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.

Field	Description
Monitor	• Admin State—Administrative state of the policy: enabled or disabled. • Level—Message level: alert, critical, emergency, error, warning, notification, information, or debugging. 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	• Admin State—Administrative state of the policy: enabled or disabled. • Level—Message level: alert, critical, emergency, error, warning, notification, information, or debugging. 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—Name of the file to which messages are logged. • Size (bytes)—Maximum size, in bytes, that the file can reach before the system begins to overwrite the messages.

Field	Description
Buffer	• Admin State—Administrative state of the policy: enabled or disabled. • Level—Message level: alert, critical, emergency, error, warning, notification, information, or debugging. 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. • Buffer Size (Bytes)—In bytes, the size of the buffer for syslog messages. • Wrap to Flash—Indicates whether or not the buffer contents are saved to flash memory with the buffer wraps (becomes full). Check the check box to save the contents to flash memory if the buffer wraps. • Max File Size in Flash (KB)—Maximum size, in kilobytes, that can be used by the syslog buffer. This option is enabled if the Wrap to Flash option is enabled. • Min Free Flash Size (KB)—Minimum size, in kilobytes, that is allocated for the syslog buffer. This option is enabled if the Wrap to Flash option is enabled.
Time Stamp	Check the check box for each of the following options that you want to enable for displaying timestamps: • Enable Timestamp • Include Year • Include Milliseconds • Show Time Zone • Use Local Time Zone

Step 6 Click **OK**.

Deleting a Syslog Policy for a Device Profile

Note When the system boots up, a default policy already exists. You can modify the default policy, but you cannot delete it.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Syslog**.

Step 2 In the General tab, select the syslog policy that you want to delete, then click **Delete**.

Step 3 When prompted, confirm the deletion.

Adding a Syslog Server for a Device Profile

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Syslog**.

Step 2 In the General tab, click **Add Syslog Policy**.

Step 3 In the Add Syslog Policy dialog box, click the **Servers** tab, then click **Add Syslog Server**.

Step 4 In the Add Syslog Server dialog box, provide the information as described in Add Syslog Server Dialog Box, on page 25, then click **OK** in the open dialog boxes.

Field Descriptions

Add Syslog Server Dialog Box

Field	Description
Server Type	One of the following server types: • primary • secondary • tertiary
Hostname/IP Address	Hostname or IP address where the syslog file resides. **Note** If you use a hostname, you must configure a DNS server.

Field	Description
Severity	One of the following severity levels: • emergencies (0) • alerts (1) • critical (2) • errors (3) • warnings (4) • notifications (5) • information (6) • debugging (7)
Forwarding Facility	One of the following forwarding facilities: • auth • authpriv • cron • daemon • ftp • kernel • local0 • local1 • local2 • local3 • local4 • local5 • local6 • local7 • lpr • mail • news • syslog • user • uucp

Field	Description
Admin State	Administrative state of the server: disabled or enabled.
Port	Port to use to send data to the syslog server. The default port selection is 514 for UDP. This option is not available for InterCloud policies.
Protocol	Protocol to use: TCP or UDP (default). This option is not available for InterCloud policies.
Use Transport Layer Security	Check the check box to use Transport Layer Security. This option is available only for TCP. This option is not available for InterCloud policies.
Server Interface	Interface to use to access the syslog server.

Editing a Syslog Server for a Device Profile

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Syslog**.

Step 2 In the General tab, select the required syslog policy, then choose **Edit**.

Step 3 In the Edit Syslog Policy dialog box, from the **Servers** tab, select the syslog server you want to edit, then click **Edit**

Step 4 In the Edit Syslog Server dialog box, edit the fields as required, using the information in the following table.

Field	Description
Server Type	One of the following server types: primary, secondary, or tertiary (read-only).
Hostname/IP Address	Hostname or IP address where the syslog file resides.

Field	Description
Severity	One of the following severity levels: • emergencies (0) • alerts (1) • critical (2) • errors (3) • warnings (4) • notifications (5) • information (6) • debugging (7)
Forwarding Facility	One of the following forwarding facilities: • auth • authpriv • cron • daemon • ftp • kernel • local0 • local1 • local2 • local3 • local4 • local5 • local6 • local7 • lpr • mail • news • syslog • user • uucp

Field	Description
Admin State	Administrative state of the policy: enabled or disabled.
Port	Port to use to send data to the syslog server. Valid port values are 1025 through 65535 for both TCP and UDP. The default TCP port is 1470. The default UDP port is 514.
Protocol	Protocol to use: TCP or UDP.
Use Transport Layer Security	Check the check box to use Transport Layer Security. This option is available only for TCP.
Server Interface	Interface to use to access the syslog server. This option applies to ASA 1000V only. Enter the data interface name specify in the edge firewall. Use the device CLI to configure a route through the management interface.

Step 5 Click **OK** in the open dialog boxes to save your changes.

Deleting a Syslog Server for a Device Profile

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Policies > Syslog**.
Step 2 In the General tab, select the syslog policy with the server you want to delete, then click **Edit**.
Step 3 In the Edit Syslog Policy dialog box, click the **Servers** tab.
Step 4 In the Servers tab, select the syslog server that you want to delete, then click **Delete**.
Step 5 When prompted, confirm the deletion.
Step 6 Click **OK** to save the policy.

Configuring Device Profiles

Adding a Firewall Device Profile

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Device Profiles**.

Step 2 In the General tab, click **Add Device Profile**.

Step 3 In the New Device Profile dialog box, enter the required information in the General and Policies tabs, then click **OK**:

Field	Description
DNS Servers	You can: • Add a new server. • Select an existing server and edit or delete it. • Use the arrows to change priority.
DNS Domains	You can: • Add a new domain. • Select an existing domain and edit or delete it.
NTP Servers	You can: • Add a new server. • Select an existing server and edit or delete it. • Use the arrows to change priority.
SNMP	You can: • Choose a policy from the drop-down list. • Add a new policy. • Click the Resolved Policy link to review or modify the policy currently assigned. This option is not available for InterCloud Management device profiles.

Field	Description
Syslog	You can: • Choose a policy from the drop-down list. • Add a new policy. • Click the Resolved Policy link to review or modify the policy currently assigned.
Fault	You can: • Choose a policy from the drop-down list. • Add a new policy. • Click the Resolved Policy link to review or modify the policy currently assigned. This option is not available for InterCloud Management device profiles.
Core File	You can: • Choose a policy from the drop-down list. • Add a new policy. • Click the Resolved Policy link to review or modify the policy currently assigned.
Policy Agent Log File	You can: • Choose a policy from the drop-down list. • Add a new policy. • Click the Resolved Policy link to review or modify the policy currently assigned.
Policy Engine Logging	Select the appropriate radio button to enable or disable logging. This option is not available for InterCloud Management device profiles.

Field	Description
Auth Policy	You can: • Choose a policy from the drop-down list. • Add a new policy. • Click the Resolved Policy link to review or modify the policy currently assigned. This option is not available for InterCloud Management device profiles.

Editing a Firewall Device Profile

After you create a firewall device profile, you can edit it as needed.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Device Profiles**.

Step 2 In the Device Profiles pane, select the profile you want to edit, then click **Edit**.

Step 3 In the Edit Firewall Device Policy dialog box, update the information in the General tab as described in the following table:

Field	Description
Name	Profile name. 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	Brief profile description. The description can be between 1 and 256 identifier characters. You can use alphanumeric characters including hyphen, underscore, dot, and colon.
Time Zone	Select the required time zone from the drop-down list.

Step 4 In the Policies tab, update the information as described in the following table, then click **OK**:

Field	Description
DNS Servers	
Add DNS Server	Adds a DNS server.
Edit	Enables you to edit the selected DNS server.
Delete	Deletes the selected DNS server.
Up and down arrows	Change the priority of the selected DNS server. Prime Network Services Controller uses the DNS servers in the order in which they appear in the table.
DNS Servers Table	
IP Address	IP addresses for the DNS servers configured in the system.
Server Interface	Interface to use to access the DNS server.
NTP Servers	
Add NTP Server	Click to add an NTP server.
Edit	Enables you to edit the selected NTP server.
Delete	Deletes the selected NTP server.
Up and down arrows	Change the priority of the selected NTP Server hostname. Prime Network Services Controller uses the NTP servers in the order in which they appear in the table.
NTP Servers Table	
Hostname / IP Address	Hostnames or IP addresses for NTP servers configured in the system.
Interface Name	Interface to use to access the NTP server.
DNS Domains	
Add	Click to add a DNS domain name.
Edit	Click to edit the DNS domain name selected in the DNS Domains table. The default DNS name cannot be edited.

Field	Description
Delete	Click to delete the DNS domain name selected in the DNS Domains table.
DNS Domains table	Default DNS domain name and domain in the system.
Other Options	
SNMP	Select, add, or edit SNMP policies as needed.
Syslog	Select, add, or edit syslog policies as needed.
Fault	Select, add, or edit fault policies as needed.
Core File	Select, add, or edit core file policies as needed.
Policy Agent Log File	Select, add, or edit the policy agent log file policies as needed.
Policy Engine Logging	Select the appropriate radio button to enable or disable logging.
Auth Policy	Select an available authentication policy, or click **Add Auth Policy** to add a new authentication policy.

Deleting a Firewall Device Profile

Procedure

Step 1 Choose **Policy Management > Device Configurations > root** > **Device Profiles**.

Step 2 In the **Work** pane, click the device profile you want to delete.

Step 3 Click **Delete.**

Step 4 In the Confirm dialog box, click **OK**.

Configuring NTP

Network Time Protocol (NTP) is a networking protocol used to synchronize the time on a network of machines. An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server.

Prime Network Services Controller enables you to configure NTP for compute firewalls, edge firewalls, and Prime Network Services Controller itself.

Configuring NTP for a compute or edge firewall requires the following steps:

1. Configuring a device profile with NTP.
2. Applying the device profile to a compute or edge firewall

The following topics describe how to perform these steps.

For information on configuring NTP on Prime Network Services Controller, see Adding an NTP Server.

Creating a Device Profile with NTP

This procedure describes how to create a device profile with NTP that you can apply to an edge or compute firewall.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Device Profiles**.

Step 2 In the General tab, click **Add Device Profile**.

Step 3 In the New Device Profile dialog box, provide the following information:

- Name—Profile name.
- Description—Brief profile description.
- Time Zone—From the drop-down list, choose the time zone.

Step 4 Click the **Policies** tab.

Step 5 In the NTP servers area, click **Add NTP Server**.

Step 6 In the Add NTP Server dialog box, enter the information as described in Add NTP Server Dialog Box, on page 36, then click **OK**.

Step 7 Click **OK**.

What to Do Next

After you have configured the device profile, you can apply it to a firewall as described in the following topics:

- Applying Device Profiles to Edge Firewalls, on page 36
- Applying Device Profiles to Compute Firewalls, on page 36

Field Descriptions

Add NTP Server Dialog Box

Add NTP Server Dialog Box

Field	Description
Hostname/IP Address	NTP server name or IP address. For Prime Network Services Controller andVSGs, you can enter either a hostname or IP address. For ASA 1000Vs, you must enter an IP address.
Interface Name	(Policy Management Device Profiles only) Device interface to reach the NTP server. Only ASA 1000Vs support interface names. • If you specify an interface, use the interface name specified by the edge firewall. • To use the management interface, you must configure the route by using the CLI.
Authentication Key	(Policy Management Device Profiles only) Authentication key to access the NTP server. Only ASA 1000Vs support authentication keys.

Applying Device Profiles to Compute Firewalls

After you have created a device profile, you can apply the profile to a compute firewall.

Procedure

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant* **> Compute Firewalls >** *compute-firewall*.

Step 2 In the General tab, click **Select** in the Device Profile field.

Step 3 In the Select Device Profile dialog box, select the desired profile, then click **OK**.

Step 4 Click **Save**.

Applying Device Profiles to Edge Firewalls

After you have created a device profile, you can apply the profile to an edge firewall.

Procedure

Step 1 Choose **Resource Management > Managed Resources > root >** *tenant* **> Edge Firewalls >** *edge-firewall*.

Step 2 In the General tab, click **Select** in the Device Profile field.

Step 3 In the Select Device Profile dialog box, select the desired profile, then click **OK**.

Step 4 Click **Save**.

Associating Device Policies with Profiles

After you create a device policy, you can associate it with a device profile. By doing so, you can ensure that all devices associated with the device profile use the same policy.

Procedure

Step 1 Choose **Policy Management > Device Configurations > root > Device Profiles >** *profile* where *profile* is the device profile that you want to add the device policy to.

Step 2 Click the **Policies** tab.

Step 3 In the Policies tab, locate the drop-down list for the type of policy you want to associate, such as Syslog or Auth Policy.

Step 4 From the drop-down list, choose the policy to add to the profile, then click **Save**.
The policy is automatically applied to all devices using the selected profile.