Device Management Basics

The following topics describe how to manage devices in the Firepower System:

- About Device Management, on page 1
- The Device Management Page, on page 5
- Remote Management Configuration, on page 6
- Add Devices to the Firepower Management Center, on page 6
- Deleting Devices from the Firepower Management Center, on page 8
- Device Configuration Settings, on page 9
- The Interfaces Table View, on page 18
- Device Group Management, on page 20

About Device Management

Use the Firepower Management Center to manage your devices.

About the Firepower Management Center

You can use the Firepower Management Center to manage the full range of devices that are a part of the Firepower System. When you manage a device, you set up a two-way, SSL-encrypted communication channel between the Firepower Management Center and the device. The Firepower Management Center uses this channel to send information to the device about how you want to analyze and manage your network traffic to the device. As the device evaluates the traffic, it generates events and sends them to the Firepower Management Center using the same channel.

By using the Firepower Management Center to manage devices, you can:

- configure policies for all your devices from a single location, making it easier to change configurations
- install various types of software updates on devices
- push health policies to your managed devices and monitor their health status from the Firepower Management Center

The Firepower Management Center aggregates and correlates intrusion events, network discovery information, and device performance data, allowing you to monitor the information that your devices are reporting in relation to one another, and to assess the overall activity occurring on your network.
You can use a Firepower Management Center to manage nearly every aspect of a device’s behavior.

**Note**

### What Can Be Managed by a Firepower Management Center?

You can use the Firepower Management Center as a central management point in a Firepower System deployment to manage the following devices:

- 7000 and 8000 Series devices
- ASA FirePOWER modules
- NGIPSv devices
- Firepower Threat Defense (physical hardware and virtual)

When you manage a device, information is transmitted between the Firepower Management Center and the device over a secure, SSL-encrypted TCP tunnel.

The following illustration lists what is transmitted between a Firepower Management Center and its managed devices. Note that the types of events and policies that are sent between the appliances are based on the device type.

![Diagram](image)

### Beyond Policies and Events

In addition to deploying policies to devices and receiving events from them, you can also perform other device-related tasks on the Firepower Management Center.

**Backing Up a Device**

You **cannot** create or restore backup files for NGIPSv devices or ASA FirePOWER modules.

When you perform a backup of a physical managed device from the device itself, you back up the device configuration **only**. To back up configuration data and, optionally, unified files, perform a backup of the device using the managing Firepower Management Center.

To back up event data, perform a backup of the managing Firepower Management Center.
Updating Devices

From time to time, Cisco releases updates to the Firepower System, including:

- intrusion rule updates, which may contain new and updated intrusion rules
- vulnerability database (VDB) updates
- geolocation updates
- software patches and updates

You can use the Firepower Management Center to install an update on the devices it manages.

NAT Environments

Network address translation (NAT) is a method of transmitting and receiving network traffic through a router that involves reassigning the source or destination IP address. The most common use for NAT is to allow private networks to communicate with the internet. Static NAT performs a 1:1 translation, which does not pose a problem for FMC communication with devices, but port address translation (PAT) is more common. PAT lets you use a single public IP address and unique ports to access the public network; these ports are dynamically assigned as needed, so you cannot initiate a connection to a device behind a PAT router.

Normally, you need both IP addresses (along with a registration key) for both routing purposes and for authentication: the FMC specifies the device IP address when you add a device (see Add Devices to the Firepower Management Center, on page 6), and the device specifies the FMC IP address (see the getting started guide for your model; or see Management Interfaces to change settings after initial setup). However, if you only know one of the IP addresses, which is the minimum requirement for routing purposes, then you must also specify a unique NAT ID on both sides of the connection to establish trust for the initial communication and to look up the correct registration key. The FMC and device use the registration key and NAT ID (instead of IP addresses) to authenticate and authorize for initial registration.

For example, you add a device to the FMC, and you do not know the device IP address (for example, the device is behind a PAT router), so you specify only the NAT ID and the registration key on the FMC; leave the IP address blank. On the device, you specify the FMC IP address, the same NAT ID, and the same registration key. The device registers to the FMC's IP address. At this point, the FMC uses the NAT ID instead of IP address to authenticate the device.

Although the use of a NAT ID is most common for NAT environments, you might choose to use the NAT ID to simplify adding many devices to the FMC. On the FMC, specify a unique NAT ID for each device you want to add while leaving the IP address blank, and then on each device, specify both the FMC IP address and the NAT ID. Note: The NAT ID must be unique per device.

The following example shows three devices behind a PAT IP address. In this case, specify a unique NAT ID per device on both the FMC and the devices, and specify the FMC IP address on the devices.
The following example shows the FMC behind a PAT IP address. In this case, specify a unique NAT ID per device on both the FMC and the devices, and specify the device IP addresses on the FMC.
The Device Management Page

The Device Management page provides you with a range of information and options that you can use to manage your registered devices, 7000 and 8000 Series device high availability pairs, and device groups. The page displays a list of all the devices currently registered on the Firepower Management Center.

You can use the View by drop-down list to sort and view the device list by any of the following categories: group, license, model, or access control policy. In a multidomain deployment, you can also sort and view by domain, which is the default display category in that deployment. Devices must belong to a leaf domain.

You can expand and collapse the list of devices in any of the device categories. By default, the device list is expanded.

See the following table for more information about the device list.

Table 1: Device List Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The display name used for the device in Firepower Management Center. The status icon to the left of the name indicates its current health status.</td>
</tr>
<tr>
<td>Group</td>
<td>The group to which you assigned the managed devices.</td>
</tr>
<tr>
<td>Model</td>
<td>The model of the managed devices.</td>
</tr>
<tr>
<td>License Type</td>
<td>The licenses that are enabled on the managed device.</td>
</tr>
<tr>
<td>Access Control Policy</td>
<td>A link to the currently deployed access control policy. If the system identifies the access control policy as out-of-date, it displays a warning icon (⚠️) next to the link.</td>
</tr>
</tbody>
</table>

Related Topics
- About Firepower Licenses
- About Health Monitoring
- Managing Access Control Policies

Filtering Managed Devices

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Leaf only</td>
<td>Admin/Network Admin</td>
</tr>
</tbody>
</table>

When your Firepower Management Center manages a large volume of devices, you can narrow the results on the Device Management page to make it easier find a particular device.
### Procedure

**Step 1** Choose Devices > Device Management.

**Step 2** In the Device Name field, enter a full or partial device name, host name or IP address to narrow the device list.

**Step 3** To clear the filter, clear the Device Name field.

### Remote Management Configuration

**All Devices Except 7000 and 8000 Series**

For information on configuring remote management, see the quick start guide for your device.

**7000 and 8000 Series Devices**

See Remote Management Configuration (Classic Devices).

### Add Devices to the Firepower Management Center

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin</td>
</tr>
</tbody>
</table>

Use this procedure to add a single device to the Firepower Management Center. If you plan to link devices for redundancy or performance, you must still use this procedure, keeping in mind the following points:

- **8000 Series stacks**—Use this procedure to add each device to the Firepower Management Center, then establish the stack; see Establishing Device Stacks.

- **7000 and 8000 Series high availability**—Use this procedure to add each device to the Firepower Management Center, then establish high availability; see Establishing Firepower 7000/8000 Series High Availability. For high availability stacks, first stack the devices, then establish high availability between the stacks.

- **FTD high availability**—Use this procedure to add each device to the Firepower Management Center, then establish high availability; see Add a Firepower Threat Defense High Availability Pair.

- **FTD clusters**—Make sure cluster units are in a successfully formed cluster on FXOS, then use this procedure to add each unit to the Firepower Management Center as a separate managed device. Finally, cluster the units on the Firepower Management Center. For more information, see FMC: Add a Cluster.
If you have established or will establish Firepower Management Center high availability, add devices only to the active (or intended active) Firepower Management Center. When you establish high availability, devices registered to the active Firepower Management Center are automatically registered to the standby.

**Before you begin**

- Set up the device to be managed by the Firepower Management Center. For 7000 and 8000 Series devices, see Configuring Remote Management on a Managed Device. For information on configuring remote management for other models, see the appropriate quick start guide.

- If you registered a Firepower Management Center and a device using IPv4 and want to convert them to IPv6, you must delete and reregister the device.

**Procedure**

**Step 1** Choose **Devices > Device Management**.

**Step 2** From the **Add** drop-down menu, choose **Add Device**.

**Step 3** In the **Host** field, enter the IP address or the hostname of the device you want to add.

The hostname of the device is the fully qualified domain name or the name that resolves through the local DNS to a valid IP address. Use a hostname rather than an IP address if your network uses DHCP to assign IP addresses.

In a NAT environment, you may not need to specify the IP address or hostname of the device, if you already specified the IP address or hostname of the Firepower Management Center when you configured the device to be managed by the Firepower Management Center. For more information, see **NAT Environments, on page 3**.

**Step 4** In the **Display Name** field, enter a name for the device as you want it to display in the Firepower Management Center.

**Step 5** In the **Registration Key** field, enter the same registration key that you used when you configured the device to be managed by the Firepower Management Center. The registration key is a one-time-use shared secret.

**Step 6** In a multidomain deployment, regardless of your current domain, assign the device to a leaf **Domain**.

If your current domain is a leaf domain, the device is automatically added to the current domain. If your current domain is not a leaf domain, post-registration, you must switch to the leaf domain to configure the device.

**Step 7** (Optional) Add the device to a device **Group**.

**Step 8** Choose an initial **Access Control Policy** to deploy to the device upon registration, or create a new policy.

If the device is incompatible with the policy you choose, deploying will fail. This incompatibility could occur for multiple reasons, including licensing mismatches, model restrictions, passive vs inline issues, and other misconfigurations. After you resolve the issue that caused the failure, manually deploy configurations to the device.

**Step 9** Choose licenses to apply to the device.

For Classic devices, note that:
• Control, Malware, and URL Filtering licenses require a Protection license.

• VPN licenses require a 7000 or 8000 Series device.

• Control licenses are supported on NGIPSv and ASA FirePOWER devices, but do not allow you to configure 8000 Series fastpath rules, switching, routing, stacking, or device high availability.

Step 10
If you used a NAT ID during device setup, expand the Advanced section and enter the same NAT ID in the Unique NAT ID field.

Step 11
Check the Transfer Packets check box to allow the device to transfer packets to the Firepower Management Center.

This option is enabled by default. When events like IPS or Snort are triggered with this option enabled, the device sends event metadata information and packet data to the Firepower Management Center for inspection. If you disable it, only event information will be sent to the Firepower Management Center but packet data is not sent.

Step 12
Click Register.

It may take up to two minutes for the Firepower Management Center to verify the device’s heartbeat and establish communication.

Related Topics
Creating a Basic Access Control Policy

Deleting Devices from the Firepower Management Center

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Network Admin</td>
</tr>
</tbody>
</table>

If you no longer want to manage a device, you can delete it from the Firepower Management Center. Deleting a device:

• Severs all communication between the Firepower Management Center and the device.

• Removes the device from the Device Management page.

• Returns the device to local time management if the device is configured via the platform settings policy to receive time from the Firepower Management Center via NTP.

To manage the device later, re-add it to the Firepower Management Center.

Note
When a device is deleted and then re-added, the Firepower Management Center web interface prompts you to re-apply your access control policies. However, there is no option to re-apply the NAT and VPN policies during registration. Any previously applied NAT or VPN configuration will be removed during registration and must be re-applied after registration is complete.
Procedure

**Step 1** Choose Devices > Device Management.

**Step 2** Next to the device you want to delete, click the delete icon (>Delete<).  

**Step 3** Confirm that you want to delete the device.

---

Device Configuration Settings

The Device page of the appliance editor displays detailed device configuration and information. It also allows you to make changes to some parts of device configuration, such as enabling and disabling licenses, shutting down and restarting a device, modifying management, and configuring advanced options.

General Device Settings

The General section of the **Device** tab displays the settings described in the table below.

**Table 2: General Section Table Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The display name of the device on the Firepower Management Center.</td>
</tr>
<tr>
<td>Transfer Packets</td>
<td>This displays whether or not the managed device sends packet data with the events to the Firepower Management Center.</td>
</tr>
<tr>
<td>Mode</td>
<td>The displays the mode of the management interface for the device: routed or transparent.</td>
</tr>
<tr>
<td>Compliance Mode</td>
<td>This displays the security certifications compliance for a device. Valid values are CC, UCAPL and None.</td>
</tr>
</tbody>
</table>

Note: The **Mode** field is displayed only for Firepower Threat Defense devices.

Device License Settings

The License section of the **Device** tab displays the licenses enabled for the device.

Related Topics

- About Firepower Licenses
Device System Settings

The System section of the Device tab displays a read-only table of system information, as described in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
<td>The model name and number for the managed device.</td>
</tr>
<tr>
<td>Serial</td>
<td>The serial number of the chassis of the managed device.</td>
</tr>
<tr>
<td>Time</td>
<td>The current system time of the device.</td>
</tr>
<tr>
<td>Version</td>
<td>The version of the software currently installed on the managed device.</td>
</tr>
<tr>
<td>Policy</td>
<td>A link to the platform settings policy currently deployed to the managed device.</td>
</tr>
</tbody>
</table>

You can also shut down or restart the device.

Device Health Settings

The Health section of the Device tab displays the information described in the table below.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>An icon that represents the current health status of the device. Clicking the icon displays the Health Monitor for the appliance.</td>
</tr>
<tr>
<td>Policy</td>
<td>A link to a read-only version of the health policy currently deployed at the device.</td>
</tr>
<tr>
<td>Blacklist</td>
<td>A link to the Health Blacklist page, where you can enable and disable health blacklist modules.</td>
</tr>
</tbody>
</table>

Related Topics

- Viewing Appliance Health Monitors
- Editing Health Policies
- Blacklisting Health Policy Modules

Device Management Settings

The Management section of the Device tab displays the fields described in the table below.
Table 5: Management Section Table Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>The IP address or host name of the device. The host name is fully qualified</td>
</tr>
<tr>
<td></td>
<td>domain name or the name that resolves through the local DNS to a valid IP</td>
</tr>
<tr>
<td></td>
<td>address (that is, the host name).</td>
</tr>
<tr>
<td>Status</td>
<td>An icon indicating the status of the communication channel between the</td>
</tr>
<tr>
<td></td>
<td>Firepower Management Center and the managed device. You can hover over the</td>
</tr>
<tr>
<td></td>
<td>status icon to view the last time the Firepower Management Center contacted</td>
</tr>
<tr>
<td></td>
<td>the device.</td>
</tr>
</tbody>
</table>

Advanced Device Settings

The Advanced section of the Device tab displays a table of advanced configuration settings, as described below. You can use the Advanced section to edit any of these settings.

Table 6: Advanced Section Table Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Supported Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Bypass</td>
<td>The state of Automatic Application Bypass on the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>device.</td>
<td>7000 &amp; 8000 Series NGIPSv</td>
</tr>
<tr>
<td>Bypass Threshold</td>
<td>The Automatic Application Bypass threshold, in</td>
<td></td>
</tr>
<tr>
<td></td>
<td>milliseconds.</td>
<td>ASA FirePOWER</td>
</tr>
<tr>
<td>Inspect Local Router</td>
<td>Whether the device inspects traffic received on</td>
<td></td>
</tr>
<tr>
<td>Traffic</td>
<td>routed interfaces that is destined for itself,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>such as ICMP, DHCP, and OSPF traffic.</td>
<td>7000 &amp; 8000 Series</td>
</tr>
<tr>
<td>Fast-Path Rules</td>
<td>The number of 8000 Series fastpath rules that</td>
<td></td>
</tr>
<tr>
<td></td>
<td>have been created on the device.</td>
<td>8000 Series</td>
</tr>
</tbody>
</table>

Viewing Device Information

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Admin/Network Admin</td>
</tr>
</tbody>
</table>

In a multidomain deployment, ancestor domains can view information about all devices in descendant domains. You must be in a leaf domain to edit a device.
Procedure

Step 1  Choose Devices > Device Management.
Step 2  Click the edit icon (✏️) next to the device you want to view.

In a multidomain deployment, if you are in an ancestor domain, you can click the view icon (🔍) to view a device from a descendant domain in read-only mode.

Step 3  Click the Device tab.
Step 4  You can view the following information:

- General — Displays general settings for the device; see General Device Settings, on page 9.
- License — Displays license information for the device; see Device License Settings, on page 9.
- System — Displays system information about the device; see Device System Settings, on page 10.
- Health — Displays information about the current health status of the device; see Device Health Settings, on page 10.
- Management — Displays information about the communication channel between the Firepower Management Center and the device; see Device Management Settings, on page 10.
- Advanced — Displays information about advanced feature configuration; see Advanced Device Settings, on page 11.

Editing Device Management Settings

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Leaf only</td>
<td>Admin/Network Admin</td>
</tr>
</tbody>
</table>

If you edit the hostname or IP address of a device after you added it to the FMC (using the device’s CLI, for example), you need to use the procedure below to manually update the hostname or IP address on the managing FMC.

Procedure

Step 1  Choose Devices > Device Management.
Step 2  Next to the device where you want to modify management options, click the edit icon (✏️).

In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

Step 3  Click the Device tab, and see the Management area.

Tip  For stacked devices, you modify management options on an individual device on the Device page of the appliance editor.

Step 4  Edit the Host IP address or hostname by clicking the edit icon (✏️).
In the **Management** dialog box, modify the name or IP address in the **Host** field, and click **Save**.

**Step 5**  
(Optional) Disable remote management.

Click the slider (✔️) to enable or disable management of the device. Disabling management blocks the connection between the Firepower Management Center and the device, but does **not** delete the device from the Firepower Management Center. If you no longer want to manage a device, see Deleting Devices from the Firepower Management Center, on page 8.

---

**What to do next**

- Deploy configuration changes; see Deploy Configuration Changes.

---

**Editing General Device Settings**

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Leaf only</td>
<td>Admin/N Network</td>
</tr>
</tbody>
</table>

**Procedure**

**Step 1**  
Choose **Devices > Device Management**.

**Step 2**  
Next to the device you want to modify, click the edit icon (🔍).

In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

**Step 3**  
Click **Device**.

**Step 4**  
In the **General** section, click the edit icon (✍️).

**Step 5**  
Enter a **Name** for the managed device.

**Tip**  
For stacked devices, you edit the assigned device name for the stack on the Stack page of the appliance editor. You can edit the assigned device name for an individual device on the Devices page of the appliance editor.

**Step 6**  
Change the **Transfer Packets** setting:

- Check the check box to allow packet data to be stored with events on the Firepower Management Center.
- Clear the check box to prevent the managed device from sending packet data with the events.

**Step 7**  
Click **Force Deploy** to force deployment of current policies and device configuration to the device.
Enabling and Disabling Device Licenses

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Leaf only</td>
<td>Admin/Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin</td>
</tr>
</tbody>
</table>

You can enable licenses on your device if you have available licenses on your Firepower Management Center.

Procedure

**Step 1** Choose Devices > Device Management.

**Step 2** Next to the device where you want to enable or disable licenses, click the edit icon.

In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

**Step 3** Click the Device tab.

**Tip** For stacked devices, you enable or disable the licenses for the stack on the Stack page of the appliance editor.

**Step 4** In the License section, click the edit icon.

**Step 5** Check or clear the check box next to the license you want to enable or disable for the managed device.

**Step 6** Click Save.

What to do next

• Deploy configuration changes; see Deploy Configuration Changes.

Related Topics

About Firepower Licenses

Editing Advanced Device Settings

You can configure Application Bypass, Local Router Traffic Inspection, and Fast-Path Rules.
Configuring Automatic Application Bypass

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>7000 &amp; 8000 Series</td>
<td>Leaf only</td>
<td>Admin Network Admin</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NGIPSv</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ASA FirePOWER</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The Automatic Application Bypass (AAB) feature limits the time allowed to process packets through an interface and allows packets to bypass detection if the time is exceeded. The feature functions with any deployment; however, it is most valuable in inline deployments.

You balance packet processing delays with your network’s tolerance for packet latency. When a malfunction within Snort or a device misconfiguration causes traffic processing time to exceed a specified threshold, AAB causes Snort to restart within ten minutes of the failure, and generates troubleshoot data that can be analyzed to investigate the cause of the excessive processing time.

Typically, you use Rule Latency Thresholding in the intrusion policy to fast-path packets after the latency threshold value is exceeded. Rule Latency Thresholding does not shut down the engine or generate troubleshoot data.

If detection is bypassed, the device generates a health monitoring alert.

By default the AAB is disabled; to enable AAB follow the steps described.

Caution

AAB activates when an excessive amount of time is spent processing a single packet. AAB activation partially restarts the Snort process, which temporarily interrupts the inspection of a few packets. Whether traffic drops during this interruption or passes without further inspection depends on how the target device handles traffic. See Snort® Restart Traffic Behavior for more information.

Procedure

Step 1 Choose Devices > Device Management.

Step 2 Next to the device where you want to edit advanced device settings, click the edit icon (-pencil).

In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

Step 3 Click the Device tab (or the Stack tab for stacked devices), then click the edit icon (-pencil) in the Advanced section.

Step 4 Check Automatic Application Bypass.

Step 5 Enter a Bypass Threshold from 250 ms to 60,000 ms. The default setting is 3000 milliseconds (ms).

Step 6 Click Save.

What to do next

- Deploy configuration changes; see Deploy Configuration Changes.
Inspecting Local Router Traffic

If locally-bound traffic matches a Monitor rule in a Layer 3 deployment, that traffic may bypass inspection. To ensure inspection of the traffic, enable Inspect Local Router Traffic.

**Procedure**

**Step 1** Choose Devices > Device Management.

**Step 2** Next to the device where you want to edit advanced device settings, click the edit icon (✏). In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

**Step 3** Click the Device tab (or the Stack tab for stacked devices), then click the edit icon (✏) in the Advanced section.

**Step 4** Check Inspect Local Router Traffic to inspect exception traffic when a 7000 or 8000 Series device is deployed as a router.

**Step 5** Click Save.

**What to do next**

- Deploy configuration changes; see Deploy Configuration Changes.

Configure Fastpath Rules (8000 Series)

As a form of early traffic handling, 8000 Series fastpath rules can send traffic directly through an 8000 Series device without further inspection or logging. (In a passive deployment, 8000 Series fastpath rules simply stop analysis.) Each 8000 Series fastpath rule applies to a specific security zone or inline interface set. Because 8000 Series fastpath rules function at the hardware level, you can use only the following simple, outer-header criteria to fastpath traffic:

- Initiator and responder IP address or address block
- Protocol, and for TCP and UDP, initiator and responder port
- VLAN ID

By default, 8000 Series fastpath rules affect connections from specified initiators to specified responders. To fastpath all connections that meets the rule's criteria, regardless of which host is the initiator and which is the responder, you can make the rule bidirectional.
Although they perform a similar function, 8000 Series fastpath rules are not related to the Fastpath tunnel or prefilter rules that you configure in prefilter policies.

**Note**
When you specify a port other than *Any* for TCP or UDP traffic, only the first fragment in matching fragmented traffic is fastpathed. All other fragments are forwarded for further inspection. This is because the 8000 Series only fastpaths fragmented traffic when the IP header in each fragment contains all the IP header information needed to match the fastpath rule, and subsequent fragments do not contain the field that identifies the port.

**Procedure**

**Step 1** Choose Devices > Device Management.

**Step 2** Next to the 8000 Series device where you want to configure the rule, click the edit icon (✏️).

In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

**Step 3** Click the Device tab (or the Stack tab for stacked devices), then click the edit icon (✏️) in the Advanced section.

**Step 4** Click New IPv4 Rule or New IPv6 Rule.

**Step 5** From the Domain drop-down list, choose an inline set or passive security zone.

**Step 6** Configure the traffic you want to fastpath. Traffic must meet all the conditions to be fastpathed.

- Initiator and Responder (required): Enter IP addresses or address blocks for initiators and responders.
- Protocol: Choose a protocol, or choose *All*.
- Initiator Port and Responder Port: For TCP and UDP traffic, enter initiator and responder ports. Leave the fields blank or enter *Any* to match all TCP or UDP traffic. You can enter a comma-separated list of ports, but you cannot enter port ranges.
- VLAN: Enter a VLAN ID. Leave the field blank or enter *Any* to match all traffic regardless of VLAN tag.

**Step 7** (Optional) Make the rule Bidirectional.

**Step 8** Click Save, then Save again.

**What to do next**

Deploy configuration changes; see Deploy Configuration Changes.

---

### Managing System Shut Down

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any except ASA</td>
<td>Leaf only</td>
<td>Admin/Network Admin</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FirePOWER</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---
You cannot shut down or restart the ASA FirePOWER with the Firepower System user interface. See the ASA documentation for more information on how to shut down the respective devices.

**Procedure**

**Step 1** Choose **Devices > Device Management**.

**Step 2** Next to the device that you want to restart, click the edit icon (🛠).

In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

**Step 3** Click the **Device** tab.

**Tip** For stacked devices, you shut down or restart an individual device on the Devices page of the appliance editor.

**Step 4** To shut down the device, click the shut down device icon (🛑) in the **System** section.

**Step 5** When prompted, confirm that you want to shut down the device.

**Step 6** To restart the device, click the restart device icon (🔄).

**Step 7** When prompted, confirm that you want to restart the device.

---

**The Interfaces Table View**

The interfaces table view is located below the hardware view and lists all the available interfaces you have on a device. The table includes an expandable navigation tree you can use to view all configured interfaces. You can click the arrow icon next to an interface to collapse or expand the interface to hide or view its subcomponents. The interfaces table view also provides summarized information about each interface.
Table 7: Classic Device Interfaces

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Name         | Each interface type is represented by a unique icon that indicates its type and link state (if applicable). You can hover your pointer over the name or the icon to view a tooltip with additional information. The interface icons are described in Interface Icons. The icons use a badging convention to indicate the current link state of the interface, which may be one of three states:  
  • Error (error icon)  
  • Fault (fault icon)  
  • Not available (not available icon)  
Logical interfaces have the same link state as their parent physical interface. ASA FirePOWER modules do not display link state. Note that disabled interfaces are represented by semi-transparent icons. Interface names, which appear to the right of the icons, are auto-generated with the exception of hybrid and ASA FirePOWER interfaces, which are user-defined. Note that for ASA FirePOWER interfaces, the system displays only interfaces that are enabled, named, and have link. Physical interfaces display the name of the physical interface. Logical interfaces display the name of the physical interface and the assigned VLAN tag. ASA FirePOWER interfaces display the name of the security context and the name of the interface if there are multiple security contexts. If there is only one security context, the system displays only the name of the interface. |
| Security Zone| The security zone where the interface is assigned. To add or edit a security zone, click the edit icon (edit icon).                                                                                      |
| Used by      | The inline set, virtual switch, or virtual router where the interface is assigned.                                                                                                                      |
| MAC Address  | The MAC address displayed for the interface when it is enabled for switched and routed features. For NGIPSv devices, the MAC address is displayed so that you can match the network adapters configured on your device to the interfaces that appear on the Interfaces page. |
| IP Addresses (7000/8000 series only) | IP addresses assigned to the interface. Hover your pointer over an IP address to view whether it is active. Inactive IP addresses are also grayed out. |

Table 8: FTD Interfaces

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The interface IDs. For the failover link or cluster control link interface, the interface settings are view-only.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Logical Name</td>
<td>The configured name of the interface.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of interface: Physical, SubInterface, EtherChannel, Redundant, or BridgeGroup (transparent firewall mode only).</td>
</tr>
<tr>
<td>Interface Object</td>
<td>The security zone or interface group where the interface is assigned.</td>
</tr>
<tr>
<td>MAC Address (Active/Standby)</td>
<td>The interface MAC address(es). For High Availability, this column shows both the active MAC address and the standby MAC address.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP addresses assigned to the interface. The type of address assignment shows in parentheses: Static, DHCP, or PPPoE.</td>
</tr>
</tbody>
</table>

**Device Group Management**

The Firepower Management Center allows you to group devices so you can easily deploy policies and install updates on multiple devices. You can expand and collapse the list of devices in the group. The list appears collapsed by default.

In a multidomain deployment, you can create device groups within a leaf domain only. When you configure a Firepower Management Center for multitenancy, existing device groups are removed; you can re-add them at the leaf domain level.

**Adding Device Groups**

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Leaf only</td>
<td>Admin/Network Admin</td>
</tr>
</tbody>
</table>

Device groups enable you to easily assign policies and install updates on multiple devices.

If you add the primary device in a stack or a high-availability pair to a group, both devices are added to the group. If you unstack the devices or break the high-availability pair, both devices remain in that group.

**Procedure**

- **Step 1** Choose Devices > Device Management.
- **Step 2** From the Add drop-down menu, choose Add Group.
- **Step 3** Enter a Name.
- **Step 4** Under Available Devices, choose one or more devices to add to the device group. Use Ctrl or Shift while clicking to choose multiple devices.
- **Step 5** Click Add to include the devices you chose in the device group.
- **Step 6** Click OK to add the device group.
Editing Device Groups

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Leaf only</td>
<td>Admin/Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Admin</td>
</tr>
</tbody>
</table>

You can change the set of devices that reside in any device group. You must remove an appliance from its current group before you can add it to a new group.

Moving an appliance to a new group does not change its policy to the policy previously assigned to the group. You must assign the group's policy to the new device.

If you add the primary device in a stack or a device high-availability pair to a group, both devices are added to the group. If you unstack the devices or break the high-availability pair, both devices remain in that group.

In a multidomain deployment, you can only edit device groups in the domain where they were created.

**Procedure**

**Step 1** Choose **Devices > Device Management**.

**Step 2** Next to the device group you want to edit, click the edit icon (✏).

**Step 3** Optionally, in the **Name** field, enter a new name for the group.

**Step 4** Under **Available Devices**, choose one or more devices to add to the device group. Use Ctrl or Shift while clicking to choose multiple devices.

**Step 5** Click **Add** to include the devices you chose in the device group.

**Step 6** Optionally, to remove a device from the device group, click the delete icon (🗑️) next to the device you want to remove.

**Step 7** Click **OK** to save the changes to the device group.