

Managing Device Configuration

The Device Management page allows you to manage the device and interface configurations for the ASA FirePOWER module.

Caution If you configure the ASA in a failover pair, the ASA FirePOWER configuration does not automatically synchronize with the ASA FirePOWER module on the secondary device. You must manually export the ASA FirePOWER configuration from the primary and import it into the secondary every time you make a change.

For more information, see the following sections:

- Editing Device Configuration, page 3-1
- Managing ASA FirePOWER Module Interfaces, page 3-4
- Applying Changes to Device Configuration, page 3-4
- Configuring Remote Management, page 3-5
- Configuring eStreamer on the eStreamer Server, page 3-7

Editing Device Configuration

The Device tab of the Device Management page displays detailed device configuration and information, as it applies to the ASA FirePOWER module. It also allows you to make changes to some parts of device configuration, such as changing the displayed module name and modifying management settings.

See the following sections for more information:

- Editing General Device Configuration, page 3-1
- Viewing Device System Settings, page 3-2
- Understanding Advanced Device Settings, page 3-2

Editing General Device Configuration

License: Any

The General section of the Device tab shows the module name, which you can change. Here, you can also specify whether or not the device can transfer packets to the ASA FirePOWER module.

To edit general device configuration:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Device Management > Device**.

The Device page appears.

Step 2 Next to the **General** section, click the edit icon ( ).

The General pop-up window appears.

Step 3 In the **Name** field, type a new assigned name for the module. You may enter alphanumeric characters and special characters, with the exception of the following characters, which are invalid: +, (,), {, }, #, &, \, <, >, ?, ‘, and “.

Step 4 Select the **Transfer Packets** check box to allow packet data to be stored in the ASA FirePOWER module with events. Clear the check box to prevent the device from sending packet data with the events.

Step 5 Click **Save**.

The changes are saved. Note that your changes do not take effect until you apply the device configuration; see Applying Changes to Device Configuration, page 3-4 for more information.

Viewing Device System Settings

License: Any

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

Table 3-1 System Section Table Fields

Field	Description
Model	The model name and number for the device.
Serial	The serial number of the chassis of the device.
Time	The current system time of the device.
Version	The version of the software currently installed on the ASA FirePOWER module.
Policy	A link to the system policy currently applied to the ASA FirePOWER module.

Understanding Advanced Device Settings

The Advanced section of the Device tab displays advanced configuration settings, as described in the following table.

Table 3-2 Advanced Section Table Fields

Field	Description
Application Bypass	The state of Automatic Application Bypass on the module.
Bypass Threshold	The Automatic Application Bypass threshold, in milliseconds.

You can use the Advanced section to edit any of these settings. See the following sections for more information:

- Automatic Application Bypass, page 3-3
- Editing Advanced Device Settings, page 3-3

Automatic Application Bypass

License: Any

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.

You can change the bypass threshold if the option is selected. The default setting is 3000 milliseconds (ms). The valid range is from 250 ms to 60,000 ms.

Note AAB is activated only when an excessive amount of time is spent processing a single packet. If AAB engages, the system kills all Snort processes.

For more information about enabling Automatic Application Bypass and setting the bypass threshold, see Editing Advanced Device Settings, page 3-3.

Editing Advanced Device Settings

You can use the Advanced section of the Devices tab to modify the Automatic Application Bypass.

To modify advanced device settings:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Device Management > Device**.

The Device page appears.

Step 2 Next to the **Advanced** section, click the edit icon ( ).

The Advanced pop-up window appears.

Step 3 Optionally, select **Automatic Application Bypass** if your network is sensitive to latency. Automatic Application Bypass is most useful in inline deployments. For more information, see Automatic Application Bypass, page 3-3.

Step 4 When you select the Automatic Application Bypass option, you can type a **Bypass Threshold** in milliseconds (ms). The default setting is 3000 ms and the valid range is from 250 ms to 60,000 ms.

Step 5 Click **Save**.

Your changes are saved. Note that your changes do not take effect until you apply the device configuration; see Applying Changes to Device Configuration, page 3-4 for more information.

Managing ASA FirePOWER Module Interfaces

License: Control, Protection

When editing an ASA FirePOWER interface, you can configure only the interface's security zone from the ASA FirePOWER module. See Working with Security Zones, page 2-33 for more information.

You configure interfaces using ASDM and CLI.

To edit an ASA FirePOWER Interface:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Device Management > Interfaces**.

The Interfaces page appears.

Step 2 Next to the interface you want to edit, click the edit icon ().

The Edit Interface pop-up window appears.

Step 3 From the **Security Zone** drop-down list, select an existing security zone or select **New** to add a new security zone.

Step 4 Click **Store ASA FirePOWER Changes**.

The security zone is configured. Note that your changes do not take effect until you apply the device configuration; see Applying Changes to Device Configuration, page 3-4 for more information.

Applying Changes to Device Configuration

License: Any

After you make changes to the ASA FirePOWER configuration of a device, you must apply the changes before they take effect throughout the module. Note that the device must have unapplied changes or this option remains disabled.

Note that if you edit interfaces and reapply a device policy, Snort restarts for all interface instances on the device, not just those that you edited.

To apply changes to the device:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Device Management > Device** or **Configuration > ASA FirePOWER Configuration > Device Management > Interfaces**.

The Device Management page appears.

Step 2 Click **Apply ASA FirePOWER Changes**.

Step 3 When prompted, click **Apply**.

The device changes are applied.

Tip Optionally, from the Apply Device Changes dialog box, click **View Changes**. The Device Management Revision Comparison Report page appears in a new window. For more information, see Using the Device Management Revision Comparison Report, page 3-5.

Step 4 Click **OK**.

You are returned to the Device Management page.

Using the Device Management Revision Comparison Report

License: Any

A device management comparison report allows you to view the changes you have made to an appliance before you apply them. The report displays all differences between the current appliance configuration and the proposed appliance configuration. This gives you an opportunity to discover any potential configuration errors.

To compare appliance changes before applying them:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Device Management > Device** or **Configuration > ASA FirePOWER Configuration > Device Management > Interfaces**.

The Device Management page appears.

Step 2 Click **Apply Changes**.

The Apply Device Changes pop-up window appears. Note that the appliance must have unapplied changes or the Apply Changes button remains disabled.

Step 3 Click **View Changes**.

The Device Management Revision Comparison Report page appears in a new window.

Step 4 Click **Previous** and **Next** to scroll through the differences between the current appliance configuration and the proposed appliance configuration.

Step 5 Optionally, click **Comparison Report** to produce a PDF version of the report.

Configuring Remote Management

License: Any

Before you can manage one FireSIGHT System appliance with another, you must set up a two-way, SSL-encrypted communication channel between the two appliances. The appliances use the channel to share configuration and event information. High availability peers also use the channel, which is by default on port 8305/tcp.

You must configure remote management on the appliance that will be managed, that is, on the device that you want to manage with a Defense Center. After you configure remote management, you can use the managing appliance's web interface to add the managed appliance to your deployment.

Note After you establish remote management and register the Cisco ASA with FirePOWER Services to a Defense Center, you must manage the ASA FirePOWER module from the Defense Center instead of ASDM.

To enable communications between two appliances, you must provide a way for the appliances to recognize each other. There are three criteria the FireSIGHT System uses when allowing communications:

- the hostname or IP address of the appliance with which you are trying to establish communication

  In NAT environments, even if the other appliance does not have a routable address, you must provide a hostname or an IP address either when you are configuring remote management, or when you are adding the managed appliance.
- a self-generated alphanumeric registration key up to 37 characters in length that identifies the connection
- an optional unique alphanumeric NAT ID that can help the FireSIGHT System establish communications in a NAT environment

  The NAT ID **must** be unique among all NAT IDs used to register managed appliances.

When you register a managed device to a Defense Center, the access control policy you select applies to the device. However, if you do not enable licenses for the device required by features used in the access control policy you select, the access control policy apply fails.

To configure remote management of the local appliance:

Access: Admin

Step 1 Select **Configuration > ASA FirePOWER Configuration > Local > Configuration > Registration**.

The Remote Management page appears.

Step 2 Click **Add Manager**.

The Add Remote Management page appears.

Step 3 In the **Management Host** field, type the IP address or the hostname of the appliance that you want to use to manage this appliance.

The hostname is the fully qualified domain name or the name that resolves through the local DNS to a valid IP address.

In a NAT environment, you do not need to specify an IP address or hostname here if you plan to specify it when you add the managed appliance. In this case, the FireSIGHT System uses the NAT ID you will provide later to identify the remote manager on the managed ASA FirePOWER module interface.

Caution Use a hostname rather than an IP address if your network uses DHCP to assign IP addresses.

Step 4 In the **Registration Key** field, type the registration key that you want to use to set up communications between appliances.

Step 5 For NAT environments, in the **Unique NAT ID** field, type a **unique** alphanumeric NAT ID that you want to use to set up communications between appliances.

Step 6 Click **Save**.

After the appliances confirm that they can communicate with each other, the Pending Registration status appears.

Step 7 Use the managing appliance's web user interface to add this appliance to your deployment.

Note When enabling remote management of a device, in some high availability deployments that use NAT, you may also need to add the secondary Defense Center as a manager. For more information, contact Support.

Editing Remote Management

License: Any

Use the following procedure to edit the hostname or IP address of the managing appliance. You can also change the display name of the managing appliance, which is a name only used within the context of the FireSIGHT System. Although you can use the hostname as the display name of the appliance, entering a different display name does not change the hostname.

To edit remote management:

Access: Admin

Step 1 Select **Configuration > ASA FirePOWER Configuration > Local > Configuration > Registration**.

The Remote Management page appears.

Step 2 Click the edit icon ( ) next to the manager for which you want to edit remote management settings.

The Edit Remote Management page appears.

Step 3 In the **Name** field, change the display name of the managing appliance.

Step 4 In the **Host** field, change the IP address or the hostname of the managing appliance.

The hostname is the fully qualified domain name or the name that resolves through the local DNS to a valid IP address.

Step 5 Click **Save**.

Your changes are saved.

Configuring eStreamer on the eStreamer Server

License: FireSIGHT + Protection

Before the appliance you want to use as an eStreamer server can begin streaming eStreamer events to an external client, you must configure the eStreamer server to send events to clients, provide information about the client, and generate a set of authentication credentials to use when establishing communication.

Configuring eStreamer Event Types

You can control which types of events the eStreamer server is able to transmit to clients that request them.

Available event types on either a managed device or a Defense Center are:

- Intrusion events
- Intrusion event packet data
- Intrusion event extra data

To configure the types of events transmitted by eStreamer:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Local > Configuration > Registration**.

The Registration page appears.

Step 2 Select the **eStreamer** tab.

The eStreamer page appears.

Step 3 Under **eStreamer Event Configuration**, select the check boxes next to the types of events you want eStreamer to forward to requesting clients.

You can select any or all of the following on a managed device or Defense Center:

- **Intrusion Events** to transmit intrusion events.
- **Intrusion Event Packet Data** to transmit packets associated with intrusion events.
- **Intrusion Event Extra Data** to transmit additional data associated with an intrusion event such as the originating IP addresses of a client connecting to a web server through an HTTP proxy or load balancer.

Note Note that this controls which events the eStreamer server can transmit. Your client must still specifically request the types of events you want it to receive in the request message it sends to the eStreamer server. For more information, see the *FireSIGHT System eStreamer Integration Guide*.

Step 4 Click **Save**.

Your settings are saved and the events you selected will be forwarded to eStreamer clients when requested.

Adding Authentication for eStreamer Clients

Before eStreamer can send eStreamer events to a client, you must add the client to the eStreamer server's peers database from the eStreamer page. You must also copy the authentication certificate generated by the eStreamer server to the client.

To add an eStreamer client:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Local > Configuration > Registration**.

The Registration page appears.

Step 2 Select the **eStreamer** tab.

The eStreamer page appears.

Step 3 Click **Create Client**.

The Create Client page appears.

Step 4 In the **Hostname** field, enter the host name or IP address of the host running the eStreamer client.

Note If you use a host name, the eStreamer server **must** be able to resolve the host to an IP address. If you have not configured DNS resolution, you should configure it first or use an IP address.

Step 5 If you want to encrypt the certificate file, enter a password in the **Password** field.

Step 6 Click **Save**.

The eStreamer server now allows the host to access port 8302 on the eStreamer server and creates an authentication certificate to use during client-server authentication. The eStreamer page reappears, with the new client listed under **Hostname**.

Step 7 Click the download icon ( ) next to the client hostname to download the certificate file.

Step 8 Save the certificate file to the appropriate directory used by your client for SSL authentication.

The client can now connect to the eStreamer server. You do not need to restart the eStreamer service.

Tip To revoke access for a client, click the delete icon ( ) next to the host you want to remove. Note that you do not need to restart the eStreamer service; access is revoked immediately.