Configuring External Alerting

While the ASA FirePOWER module provides various views of events within the module interface, you may want to configure external event notification to facilitate constant monitoring of critical systems. You can configure the module to generate alerts that notify you using an SNMP trap or by writing to syslog when one of the following is generated:

- A network-based malware event or retrospective malware event
- A connection event, triggered by a specific access control rule

To have the ASA FirePOWER module send these alerts, you must first create an *alert response* , which is a set of configurations that allows the module to interact with the external system where you plan to send the alert. Those configurations may specify, for example, SNMP alerting parameters or syslog facilities and priorities.

After you create the alert response, you associate it with the event that you want to use to trigger the alert. Note that the process for associating alert responses with events is different depending on the type of event:

- You associate alert responses with malware events using their own configuration pages.
- You associate SNMP and syslog alert responses with logged connections using access control rules and policies.

There is another type of alerting you can perform in the ASA FirePOWER module, which is to configure SNMP and syslog intrusion event notifications for individual intrusion events. You configure these notifications in intrusion policies; see Configuring External Alerting for Intrusion Rules and Adding SNMP Alerts. The following table explains the licenses you must have to generate alerts.

Table 1: License Requirements for Generating Alerts

To generate an alert based on...	You need this license...
an intrusion event	Protection
a network-based malware event	Malware
a connection event	the license required to log the connection

Working with Alert Responses

License: Any

The first step in configuring external alerting is to create an alert response, which is a set of configurations that allows the ASA FirePOWER module to interact with the external system where you plan to send the alert. You can create alert responses to send alerts using an SNMP trap by writing to syslog.

The information you receive in an alert depends on the type of event that triggered the alert.

When you create an alert response, it is automatically enabled. Only enabled alert responses can generate alerts. To stop alerts from being generated, you can temporarily disable alert responses rather than deleting your configurations.

You manage alert responses on the Alerts page (**ASA FirePOWER Configuration** > **Policies** > **Actions Alerts**). The slider next to each alert response indicates whether it is active; only enabled alert responses can generate alerts. The page also indicates whether the alert response is being used in a configuration, for example, to log connections in an access control rule. You can sort alert responses by name, type, in use status, and enabled/disabled status by clicking the appropriate column header; click the column header again to reverse the sort.

Creating an SNMP Alert Response

License: Any

You can create SNMP alert responses using SNMPv1, SNMPv2, or SNMPv3.

Note If you want to monitor 64-bit values with SNMP, you must use SNMPv2 or SNMPv3. SNMPv1 does not support 64-bit monitoring.

To create an SNMP alert response:

Step 1 Select **Configuration** > **ASA FirePOWER Configuration** > **Policies** > **Actions Alerts**.

The **Alerts** page appears.

Step 2 From the **Create Alert** drop-down menu, select **Create SNMP Alert**.

The **Create SNMP Alert Configuration** pop-up window appears.

Step 3 In the **Name** field, type the name that you want to use to identify the SNMP response.

Step 4 In the **Trap Server** field, type the hostname or IP address of the SNMP trap server, using alphanumeric characters.

Note that the system does **not** warn you if you enter an invalid IPv4 address (such as 192.169.1.456) in this field. Instead, the invalid address is treated as a hostname.

Step 5 From the **Version** drop-down list, select the SNMP version you want to use.

SNMP v3 is the default. If you select SNMP v1 or SNMP v2, different options appear.

Step 6 Which version of SNMP did you select?

- For SNMP v1 or SNMP v2, type the SNMP community name, using alphanumeric characters or the special characters * or $, in the **Community String** field and skip to step 12.
- For SNMP v3, type the name of the user that you want to authenticate with the SNMP server in the **User Name** field and continue with the next step.

Step 7 From the **Authentication Protocol** drop-down list, select the protocol you want to use for authentication.

Step 8 In the **Authentication Password** field, type the password required for authentication with the SNMP server.

Step 9 From the **Privacy Protocol** list, select **None** to use no privacy protocol or **DES** to use Data Encryption Standard as the privacy protocol.

Step 10 In the **Privacy Password** field, type the privacy password required by the SNMP server.

Step 11 In the **Engine ID** field, type an identifier for the SNMP engine, in hexadecimal notation, using an even number of digits.

When you use SNMPv3, the system uses an Engine ID value to encode the message. Your SNMP server requires this value to decode the message.

Cisco recommends that you use the hexadecimal version of the ASA FirePOWER module's IP address. For example, if the ASA FirePOWER module has an IP address of 10.1.1.77 , use 0a01014D0 .

Step 12 Click **Store ASA FirePOWER Changes**.

The alert response is saved and is automatically enabled.

Creating a Syslog Alert Response

License: Any

When configuring a syslog alert response, you can specify the severity and facility associated with the syslog messages to ensure that they are processed properly by the syslog server. The facility indicates the subsystem that creates the message and the severity defines the severity of the message. Facilities and severities are not displayed in the actual message that appears in the syslog, but are instead used to tell the system that receives the syslog message how to categorize it.

Tip For more detailed information about how syslog works and how to configure it, refer to the documentation for your system. On UNIX systems, the man pages for syslog and syslog.conf provide conceptual information and configuration instructions.

Although you can select any type of facility when creating a syslog alert response, you should select one that makes sense based on your syslog server; not all syslog servers support all facilities. For UNIX syslog servers, the syslog.conf file should indicate which facilities are saved to which log files on the server.

The following table lists the syslog facilities you can select.

Table 2: Available Syslog Facilities

Facility	Description
ALERT	An alert message.

Facility	Description
AUDIT	A message generated by the audit subsystem.
AUTH	A message associated with security and authorization.
AUTHPRIV	A restricted access message associated with security and authorization. On many systems, these messages are forwarded to a secure file.
CLOCK	A message generated by the clock daemon. Note that syslog servers running a Windows operating system will use the CLOCK facility.
CRON	A message generated by the clock daemon. Note that syslog servers running a Linux operating system will use the CRON facility.
DAEMON	A message generated by a system daemon.
FTP	A message generated by the FTP daemon.
KERN	A message generated by the kernel. On many systems, these messages are printed to the console when they appear.
LOCAL0-LOCAL7	A message generated by an internal process.
LPR	A message generated by the printing subsystem.
MAIL	A message generated by a mail system.
NEWS	A message generated by the network news subsystem.
NTP	A message generated by the NTP daemon.
SYSLOG	A message generated by the syslog daemon.
USER	A message generated by a user-level process.
UUCP	A message generated by the UUCP subsystem.

The following table lists the standard syslog severity levels you can select.

Table 3: Syslog Severity Levels

Level	Description
ALERT	A condition that should be corrected immediately.
CRIT	A critical condition.
DEBUG	Messages that contain debugging information.
EMERG	A panic condition broadcast to all users.
ERR	An error condition.

Level	Description
INFO	Informational messages.
NOTICE	Conditions that are not error conditions, but require attention.
WARNING	Warning messages.

Before you start sending syslog alerts, make sure that the syslog server can accept remote messages.

To create a syslog alert:

Step 1 Select **Configuration** > **ASA FirePOWER Configuration** > **Policies** > **Actions Alerts**.

The **Alerts** page appears.From the **Create Alert** drop-down menu, select **Create Syslog Alert**.

The **Create Syslog Alert Configuration** pop-up window appears.

Step 2 In the **Name** field, type the name you want to use to identify the saved response.

Step 3 In the **Host** field, type the hostname or IP address of your syslog server.

Note that the system does **not** warn you if you enter an invalid IPv4 address (such as 192.168.1.456) in this field. Instead, the invalid address is treated as a hostname.

Step 4 In the **Port** field, type the port the server uses for syslog messages.

By default, this value is 514.

Step 5 From the **Facility** list, select a facility.

See the Available Syslog Facilities table for a list of the available facilities.

Step 6 From the **Severity** list, select a severity.

See the Syslog Severity Levels table for a list of the available severities.

Step 7 In the **Tag** field, type the tag name that you want to appear with the syslog message.

Use only alphanumeric characters in tag names. You **cannot** use spaces or underscores.

As an example, if you wanted all messages sent to the syslog to be preceded with From MC, type From MC in the field.

Step 8 Click **Store ASA FirePOWER Changes**.

The alert response is saved and is automatically enabled.

Modifying an Alert Response

License: Any

For most types of alerting, if an alert response is enabled and in use, changes to the alert response take effect immediately. However, for alert responses used in access control rules to log connection events, changes do not take effect until you reapply the access control policy.

To edit an alert response:

Step 1 Select **Configuration** > **ASA FirePOWER Configuration** > **Policies** > **Actions Alerts**.

The **Alerts** page appears.

Step 2 Next to the alert response you want to edit, click the **edit** icon.

A **configuration** pop-up window for that alert response appears.

Step 3 Make changes as needed.

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

The alert response is saved.

Deleting an Alert Response

License: Any

You can delete any alert response that is not in use.

To delete an alert response:

Step 1 Select **Configuration** > **ASA FirePOWER Configuration** > **Policies** > **Actions Alerts**.

The **Alerts** page appears.

Step 2 Next to the alert response you want to delete, click the **delete** icon.

Step 3 Confirm that you want to delete the alert response.

The alert response is deleted.

Enabling and Disabling Alert Responses

License: Any

Only enabled alert responses can generate alerts. To stop alerts from being generated, you can temporarily disable alert responses rather than deleting your configurations. Note that if an alert is in use when you disable it, it is still considered in use even though it is disabled.

To enable or disable an alert response:

Step 1 Select **Configuration** > **ASA FirePOWER Configuration** > **Policies** > **Actions Alerts**.

The **Alerts** page appears.

Step 2 Next to the alert response you want to enable or disable, click the **enable/disable** slider.

If the alert response was enabled, it is disabled. If it was disabled, it is enabled.