



External Alerting with Alert Responses

The following topics describe how to send external event alerts from the Secure Firewall Management Center using alert responses:

- [Secure Firewall Management Center Alert Responses, on page 1](#)
- [Requirements and Prerequisites for Alert Responses, on page 2](#)
- [Creating an SNMP Alert Response, on page 2](#)
- [Creating a Syslog Alert Response, on page 4](#)
- [Creating an Email Alert Response, on page 6](#)

Secure Firewall Management Center Alert Responses

External event notification via SNMP, syslog, or email can help with critical-system monitoring. The Secure Firewall Management Center uses configurable *alert responses* to interact with external servers. An *alert response* is a configuration that represents a connection to an email, SNMP, or syslog server. They are called *responses* because you can use them to send alerts in response to events detected by Secure Firewall. You can configure multiple alert responses to send different types of alerts to different monitoring servers and/or people.



Note

Depending on your device and Secure Firewall version, alert responses may not be the best way to send syslog messages. See the *About Syslog* chapter in the [Cisco Secure Firewall Management Center Device Configuration Guide](#).



Note

Alerts that use alert responses are sent by the Secure Firewall Management Center. Intrusion email alerts, which do not use alert responses, are also sent by the Secure Firewall Management Center. By contrast, SNMP and syslog alerts that are based on individual intrusion rules triggering are sent directly by managed devices.

In most cases, the information in an external alert is the same as the information in any associated event you logged to the database. However, for correlation event alerts where the correlation rule contains a connection tracker, the information you receive is the same as for an alert on a traffic profile change, regardless of the base event type.

You create and manage alert responses on the Alerts page (**Policies** > **Actions** > **Alerts**). New alert responses are automatically enabled. To temporarily stop alert generation, you can disable alert responses rather than deleting them.

Changes to alert responses take effect immediately, except when sending connection logs to an SNMP trap or syslog server.

Configurations Supporting Alert Responses

After you create an alert response, you can use it to send the following external alerts from the Secure Firewall Management Center.

Alert/Event Type	For More Information
Health events, by health module and severity level	Creating Health Monitor Alerts

Requirements and Prerequisites for Alert Responses

Model Support

Any.

Supported Domains

Any

User Roles

- Admin

Creating an SNMP Alert Response

You can create SNMP alert responses using SNMPv1, SNMPv2, or SNMPv3 for Firewall Threat Defense devices.



Note When selecting SNMP versions for the SNMP protocol, note that SNMPv2 only supports read-only communities and SNMPv3 only supports read-only users. SNMPv3 also supports encryption with AES128.

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

Before you begin

- If your network management system requires the Firewall Management Center's management information base (MIB) file, obtain it at `/etc/sf/DCEALERT.MIB`.

Procedure

Step 1 Choose **Policies > Actions > Alerts**.

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

Step 3 Edit the SNMP Alert Configuration fields:

- a) **Name**—Enter a name to identify the SNMP response.
- b) **Trap Server**—Enter the hostname or IP address of the SNMP trap server.

Note

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.

- c) **Version**—Choose the SNMP version you want to use from the drop-down list. SNMPv3 is the default.

Choose from:

- **SNMPv1** or **SNMPv2**: Enter a read-only SNMP community name in the **Community String** field, then skip to the end of the procedure.

Note

Do not include special characters (<> / % # & ? ', etc.) in the SNMP community string name.

- For **SNMPv3**: Enter the name of the user that you want to authenticate with the SNMP server in the **User Name** field and continue to the next step.

- d) **Authentication Protocol**—Choose the protocol you want to use to encrypt authentication from the drop-down list.

Choose from:

- **MD5**—Message Digest 5 (MD5) hash function.
- **SHA**—Secure Hash Algorithm (SHA) hash function.

- e) **Authentication Password**—Enter the password to enable authentication.

- f) **Privacy Protocol**—Choose the protocol you want to use to encrypt a private password from the drop-down list.

Choose from:

- **DES**—Data Encryption Standard (DES) using 56-bit keys in a symmetric secret-key block algorithm.
- **AES**—Advanced Encryption Standard (AES) using 56-bit keys in a symmetric cipher algorithm.
- **AES128**—AES using 128-bit keys in a symmetric cipher algorithm. A longer key provides higher security but a reduction in performance.

- g) **Privacy Password**—Enter the privacy password required by the SNMP server. If you specify a private password, privacy is enabled, and you must also specify an authentication password.

- h) **Engine ID**—Enter 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 Firewall Management Center's IP address. For example, if the Firewall Management Center has an IP address of 10.1.1.77, use 0a01014D0.

Step 4 Click **Save**.

What to do next

Changes take effect immediately, except if you are using alert responses to send connection logs, you must deploy configuration changes after you edit those alert responses.

Creating a Syslog Alert Response

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. These fields allow you to set the severity and facility in the syslog events configured from the Management Center web interface but these fields are not meant for filtering event types.



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 choose any type of facility when creating a syslog alert response, you should choose 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.

Syslog messages are transmitted over either UDP or TCP, depending on the configuration of the syslog server.

Before you begin

- This procedure is not the recommended way to send syslog messages in many cases.
- Confirm that the syslog server can accept remote messages.

Procedure

- Step 1** Choose **Policies > Actions > Alerts**.
- Step 2** From the **Create Alert** drop-down menu, choose **Create Syslog Alert**.
- Step 3** Enter a **Name** for the alert.
- Step 4** In the **Host** field, enter the hostname or IP address of your syslog server.

Note

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 5 In the **Port** field, enter the port the server uses for syslog messages. By default, this value is 514.

Step 6 From the **Facility** list, choose a facility described in [Syslog Alert Facilities, on page 5](#).

Step 7 From the **Severity** list, choose a severity described in [Syslog Severity Levels, on page 6](#).

Step 8 In the **Tag** field, enter the tag name that you want to appear with the syslog message.

For example, if you wanted all messages sent to the syslog to be preceded with `FromMC`, enter `FromMC` in the field.

Step 9 Click **Save**.

What to do next

Changes take effect immediately, EXCEPT:

If you are using alert responses to send connection logs to a syslog server, you must deploy configuration changes after you edit those alert responses.

Syslog Alert Facilities

The following table lists the syslog facilities you can select.

Table 1: Available Syslog Facilities

Facility	Description
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.
CONSOLE	An alert message.
CRON	A message generated by the clock daemon. Note that syslog servers running a Linux operating system will use the <code>CRON</code> 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.

Facility	Description
NEWS	A message generated by the network news subsystem.
NTP	A message generated by the NTP daemon.
SECURITY	A message generated by the audit subsystem.
SYSLOG	A message generated by the syslog daemon.
SOLARIS-CRON	A message generated by the clock daemon. Note that syslog servers running a Windows operating system will use the <code>CLOCK</code> facility.
USER	A message generated by a user-level process.
UUCP	A message generated by the UUCP subsystem.

Syslog Severity Levels

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

Table 2: 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.
INFO	Informational messages.
NOTICE	Conditions that are not error conditions, but require attention.
WARNING	Warning messages.

Creating an Email Alert Response

Before you begin

- Ensure that the Secure Firewall Management Center can reverse-resolve its own IP address. Some mail servers may perform reverse DNS lookups to verify the sender's identity as a measure to prevent spam and unauthorized access.

Procedure

- Step 1** Choose **Policies** > **Actions** > **Alerts**.
- Step 2** From the **Create Alert** drop-down menu, choose **Create Email Alert**.
- Step 3** Enter a **Name** for the alert response.
- Step 4** In the **To** field, enter the email addresses where you want to send alerts, separated by commas.
- Step 5** In the **From** field, enter the email address that you want to appear as the sender of the alert.
- Step 6** Next to **Relay Host**, verify the listed mail server is the one that you want to use to send the alert.

Tip

To change the email server, click **Edit** ()

- Step 7** Click **Save**.
-

