

External Alerting with Alert Responses

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

- Configuring external alerts with alert responses, on page 1
- Prerequisites for external alerting with alert responses, on page 2
- Guidelines for notifying external systems with alert responses, on page 2
- Alert responses, on page 3
- External alerts, on page 8
- Troubleshoot external alerts and alert response configuration, on page 10
- History for external alerting with alert responses, on page 11

Configuring external alerts with alert responses

An alert response is a configuration that defines a connection to external servers or services, such as email servers, Simple Network Management Protocol (SNMP) servers, syslog servers, or webhook endpoints. Alert response in Firewall Management Center enables you to send notifications about security events from Firewall Management Center to external monitoring servers or designated recipients. These configurations are called "responses" because they send alerts in response to events detected by the Firewall Threat Defense device.

Alert response configuration process

To send external alerts from Firewall Management Center:

1. Create alert responses for supported protocols (SNMP, syslog, email, webhooks). Specify required parameters such as server addresses, ports, credentials, and message formats.
2. Assign alert responses to specific alert types or event categories to send alerts based on event characteristics.

You can configure multiple alert responses to send different types of alerts to different monitoring servers or personnel (recipients).

Firewall Management Center sends alerts to the external systems using alert responses. By contrast, SNMP and syslog alerts triggered by individual intrusion rules are sent directly by the managed devices. For more information, see External Alerting for Intrusion Events. Firewall Management Center also sends intrusion email alerts, which do not use alert responses.

External alert types

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

Table 1: External alert configurations supporting alert responses

Event and alert type	For more information, refer to
Intrusion events, by impact flag	Configure impact flag alerts, on page 8
Discovery events, by type	Configure discovery event alerts, on page 9
Malware and retrospective malware events detected by Malware Defense ("network-based")	Configure Malware defense alerts, on page 9
Correlation events, by correlation policy violation	Add responses to rules and allow lists
Connection events, by the logging rule or default action (email alerts not supported)	Other Connections You Can Log
Health events, by health module and severity level	Create a health monitor alert

Prerequisites for external alerting with alert responses

Ensure that you meet these requirements before creating external alerting with alert responses in Firewall Management Center.

Model support

Any

Supported domains

Any

User roles

- Administrator

Guidelines for notifying external systems with alert responses

Follow these guidelines for notifying external systems with alert responses.

- Depending on your Firewall Threat Defense version and device model, alert responses may not be the best way to send syslog messages. For more information, see *About Syslog* in *Cisco Secure Firewall Management Center Device Configuration Guide* and Best practices for configuring security event syslog messaging.
- When you create a new alert response, it gets enabled automatically. If you want to temporarily stop alert generation, disable the alert response instead of deleting it.

- When you modify an alert response, your changes take effect immediately. However, if you are using an alert response to send connection logs to an SNMP trap or syslog server, deploy the configuration to ensure that your changes are applied.

Alert responses

Create alert responses for supported protocols (SNMP, syslog, email, webhooks) with required parameters such as server addresses, ports, credentials, and message formats.

Create an SNMP alert response

Configure an SNMP alert response in Firewall Management Center using SNMP versions SNPMv1, SNPMv2, or SNMPv3 to monitor network events.



Note When you select an SNMP version for the SNMP protocol, note that:

- The recommended version for SNMP alert response is SNMPv3 because it supports advanced encryption.
- SNMPv2 supports only read-only communities. SNMPv3 supports only read-only users and provides encryption with AES128.
- To monitor 64-bit values using SNMP, you must use either 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 list, 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.



Attention Firewall Management Center does not warn you if you enter an invalid IPv4 address (such as 192.169.1.456) in this field. Instead, Firewall Management Center treats the invalid address as a hostname.

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

These protocols are available:

- **SNMPv1** or **SNMPv2**: Enter a read-only SNMP community name in the **Community String** field, and then skip to the final step of this task.



Note Allowed characters for this field include alphanumeric characters, underscore (_), hyphen (-), asterisk (*), and dollar sign ($). The maximum length allowed is 128 characters.

- 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. Specifying a private password enables privacy and requires you to 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.

We recommend 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

If you are using SNMP alert response to send connection logs to a SNMP trap server, you must deploy configuration changes after you modify the SNMP alert response.

Syslog alert responses

A syslog alert response is a connection to an external syslog server. It enables you to send alerts triggered by various events detected by Firewall Management Center.

For more information about syslog and configuration steps, see the documentation for your system. If you use UNIX, review the **man** pages for **syslog** and **syslog.conf** for conceptual and configuration information.

Facility and severity

When configuring a syslog alert response, you can specify the facility and severity associated with the syslog messages to ensure that they are processed properly by the syslog server:

- Facility specifies the subsystem that creates the syslog message. Severity defines the severity of the syslog message.
- The actual syslog message does not display facility and severity. The system that receives the syslog message uses these values to categorize the message.
- You can choose any type of facility when creating a syslog alert response. However, you should choose one that is compatible with your syslog server, since 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 in the server.

Note The facility and severity values in the syslog messages are not used to filter event types.

SYSLOG alert facilities

This table lists the SYSLOG facilities that you can select.

Table 2: 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. SYSLOG servers that run a Linux operating system use the **CRON** facility.
DAEMON	A message generated by a system DAEMON.
FTP	A message generated by the File Transfer Protocol (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.

Facility	Description
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 Network Time Protocol (NTP) DAEMON.
SECURITY	A message generated by the audit subsystem.
SOLARIS-CRON	A message generated by the CLOCK DAEMON. SYSLOG servers that run a Windows operating system use the **CLOCK** facility.
SYSLOG	A message generated by the SYSLOG DAEMON.
USER	A message generated by a USER-level process.
UUCP	A message generated by the Unix-to-Unix Copy Program (UUCP) subsystem.

Syslog severity levels

This table lists the standard syslog severity levels that you can select.

Table 3: Syslog severity levels

Severity 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.

Create a syslog alert response

Create a syslog alert response to connect to an external syslog server. This enables you to send event alerts to an external syslog server with customizable severity and facility settings.

This procedure is not the recommended way to send syslog messages in many cases. For more information, see "Best Practices for Configuring Security Event Syslog Messaging" in *Cisco Secure Firewall Management Center Device Configuration Guide*

Before you begin

Confirm that your 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** that you want to use for the alert. In the **Host** field, enter the hostname or IP address of your syslog server.

Note If you enter an invalid IPv4 address (such as 192.168.1.456), Firewall Management Center treats it as a hostname and does not display a warning.

Step 4 In the **Port** field, enter the port the server uses for syslog messages. By default, this value is 514.

Step 5 From the **Facility** list, choose a facility. For more information, see SYSLOG alert facilities, on page 5.

Step 6 From the **Severity** list, choose a severity. For more information, see Syslog severity levels, on page 6.

Step 7 In the **Tag** field, enter the tag name that you want to be displayed with the syslog message.

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

Step 8 Click **Save**.

What to do next

- If you are using syslog alert responses to send connection logs to a syslog server, you must deploy configuration changes after you modify the syslog alert responses.
- To use a syslog alert response for security events, you must specify the alert response in a policy and configure location for security event syslogs. For more information, see Configuration locations for security event syslogs.

Create an email alert response

Email alert response configuration enables you to send email alerts about critical system events through configured mail relay hosts.

Before you begin

- Configure your mail relay host, as described in Configure a mail relay host and notification address.

Note You cannot use email alerting to log connections.

- Ensure that Firewall Management Center can reverse-resolve its own IP address. Some email servers use reverse DNS lookups to confirm the sender's identity and prevent spam and unauthorized access.

Follow these steps to create an email alert response:

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 to which you want to send alerts, separated by commas.

Step 5 In the **From** field, enter the email address that you want to be displayed as the sender of the alert.

Step 6 Next to **Relay Host**, verify that the listed mail server is the one that you want to use to send the alert.

If you want to change the email server, click **Edit** ( ).

Step 7 Click **Save**.

External alerts

Firewall Management Center supports sending external alerts to various systems using its alert response functionality. Assign alert responses to specific alert types or event categories, such as intrusion impact flags, discovery events, or malware detections. This assignment ensures that relevant alerts are sent to the appropriate external systems based on event characteristics.

Configure impact flag alerts

Configuring impact flag alerting allows you to receive notifications when intrusion events with specific impact flags are detected in your network.

Impact flags help you assess the impact an intrusion has on your network by correlating intrusion data, network discovery data, and vulnerability information. Firewall Management Center provides options to select alert responses for different impact types, and you can customize which impact flags will trigger alerts.

For more information about impact flags, see Intrusion event impact levels.

Before you begin

You must have the IPS Smart License or Protection Classic License to configure impact flag alerts.

Procedure

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

Step 2 Click **Impact Flag Alerts**.

Step 3 In the **Alerts** section, choose the alert response that you want to use for impact flag alerting.

To create a new alert response, choose **New** from the drop-down list.

Step 4 In the **Impact Flag Configuration** section, check the appropriate check boxes to specify the alerts you want to receive for each impact flag.

Check the check box next to the name of the notification to select all the impact flags.

Step 5 Click **Save**.

Configure discovery event alerts

Configuring discovery event alerting allows you to receive notifications whenever a specific type of discovery event occurs in your network. Firewall Management Center provides options to select alert responses for different discovery event types, and you can customize which discovery event will trigger alerts.

Before you begin

Configure your network discovery policy to log the discovery event types for which you want to receive alerts. For more information, see the Network Discovery Policies chapter in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

Procedure

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

Step 2 Click **Discovery Event Alerts**.

Step 3 In the **Alerts** section, choose the alert response that you want to use for discovery event alerting.

To create a new alert response, choose **New** from the drop-down list.

Step 4 In the **Events Configuration** section, check the check boxes that correspond to the discovery event type for which you want to receive alerts.

Tip Check the check box next to the name of the notification to select all the discovery event types.

Step 5 Click **Save**.

Configure Malware defense alerts

Configuring Malware defense alerting allows you to receive notifications whenever any malware event, including a retrospective event, is generated by Malware defense (network-based malware event). You cannot receive alerts for malware events generated by Secure Endpoint (endpoint-based malware events).

Before you begin

- You must have the Malware Defense license to configure Malware defense alerts.

- Configure a file policy to perform malware cloud lookups and associate that policy with an access control rule.

Procedure

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

Step 2 Click **Advanced Malware Protections Alerts**.

Step 3 In the **Alerts** section, choose the alert response you want to use for each alert type.

To create a new alert response, choose **New** from the drop-down list.

Step 4 In the **Event Configuration** section, check the check boxes that correspond to the alerts you want to receive for each malware event type.

Keep in mind that **All network-based malware events** includes **Retrospective Events**.

Network-based malware events do not include events generated by Secure Endpoint.

Step 5 Click **Save**.

Troubleshoot external alerts and alert response configuration

Use these troubleshooting steps for external alerting and alert response configurations in Firewall Management Center when external notifications are not working as expected.

Alerts are not being sent from Firewall Management Center

1. Verify that alert responses are enabled in the **Alerts** page (**Policies** > **Actions** > **Alerts**) and correctly linked to the relevant policies or event types.
2. Check that SNMP trap servers, syslog servers, email addresses, or webhook URLs are accurate.
3. Ensure that you deploy the configuration after making changes.

Connection logs are not sent to the syslog server

1. Ensure that connection log forwarding to the remote syslog server is enabled by configuring the access control policy to include logging options and selecting the appropriate syslog server. For more information, see Logging connections with access control rules.
2. Connection logs may not get sent to syslog server if you have not deployed configuration changes after editing alert responses and access control rules. Save and deploy all the changes to apply the updated settings.

Email alerts are not delivered or are rejected by the mail server

Email alerts can be rejected because of mail server policies or reverse DNS lookup failures.

1. Verify the mail relay host configuration. For more information, see Configure a mail relay host and notification address.

   You can also check the error messages for mail relay host configuration from the Firewall Management Center CLI. Navigate to **expert** and enter the command **cat /var/log/messages | grep -i "email\|smtp"** to view mail relay host configuration error messages:

   ```
   > expert
   admin@firepower:~$ cat /var/log/messages | grep -i "email\|smtp"
   Oct 16 17:57:38 firepower msmtp: host=example.host.com tls=on auth=off
   from=alertfmc760@****.com recipients=example@org.com mailsize=286 smtpstatus=250
   smtpmsg='250 2.0.0 Ok: queued as ****' exitcode=EX_OK
   ```

2. Verify that your DNS servers are reachable, and they can resolve the email relay hostname:

   ```
   admin@firepower:~$ ping example.host.com
   ping: example.host.com: Name or service not known
   ```

3. Verify that the Firewall Management Center can reverse-resolve its own IP address.

History for external alerting with alert responses

This table summarizes the introduction and evolution of the external alerting with alert responses in Cisco Secure Firewall Management Center across releases.

Table 4: Feature history

Feature	Minimum Firewall Management Center version	Minimum Firewall Threat Defense version	Details
Send alerts about security events from Firewall Management Center to external monitoring servers.	6.4.0	Any	This release introduces the alert response configuration and external alerting feature, enabling Firewall Management Center to send alerts to external monitoring systems. Alert responses can be configured to send notifications through email, syslog, or SNMP when specific events occur. These alerting options allow integration with monitoring and management tools for timely external notifications. New/modified screen: Choose **Policies** > **Alerts**.