



## Event Analysis Using External Tools

---

- [Integrate with Cisco SecureX, on page 1](#)
- [Event Analysis with Cisco Threat Response, on page 5](#)
- [Cisco Cloud Event Settings, on page 6](#)
- [Event Investigation Using Web-Based Resources, on page 9](#)
- [Configure Cross-Launch Links for Secure Network Analytics, on page 12](#)
- [About Sending Syslog Messages for Security Events, on page 13](#)
- [eStreamer Server Streaming, on page 26](#)
- [Event Analysis in Splunk, on page 30](#)
- [Event Analysis in IBM QRadar, on page 30](#)
- [History for Analyzing Event Data Using External Tools, on page 30](#)

## Integrate with Cisco SecureX

View and work with data from all of your Cisco security products and more through a single pane of glass, the SecureX cloud portal. Use the tools available via SecureX to enrich your threat hunts and investigations. SecureX can also provide useful appliance and device information such as whether each is running an optimal software version. For more information, see the [Cisco SecureX](#) page.

## Enable SecureX Integration

The Cisco SecureX platform connects the breadth of Cisco's integrated security portfolio and your infrastructure for a consistent experience that unifies visibility, enables automation, and strengthens your security across network, endpoints, cloud, and applications. For more information about SecureX, see the [Cisco SecureX product page](#).

Integrating SecureX with the FMC provides you a complete overview of all the data from the FMC. For more information about integrating the FMC with SecureX, see the [Cisco Secure Firewall Management Center \(Version 7.2 and later\) and SecureX Integration Guide](#).

### Before you begin

You need a SecureX account that belongs to an organization. If you don't have a SecureX account, create a SecureX account using your CDO tenant. See [Create a SecureX Account Using CDO](#) for more information.

## Procedure

**Step 1** In the FMC, choose **Integration > SecureX**.

**Step 2** (Optional) For the **Cloud Region**, choose your **Current Region**.

The region selected by default matches your Smart Licensing region, so you probably do not need to change the region.

**Step 3** In **SecureX Enablement**, perform the following steps.

a) Click **Enable SecureX**.

*Figure 1: Enable SecureX*

### SecureX Setup

This feature allows Secure Firewall Management Center to integrate with other SecureX services via SecureX ribbon. [Learn more](#)

1 Cloud Region

This setting determines where events are sent to, if configured to send to the cloud, as well as data generated by the Cisco Success Network and Cisco Support Diagnostics tools.

Current Region

2 SecureX Enablement

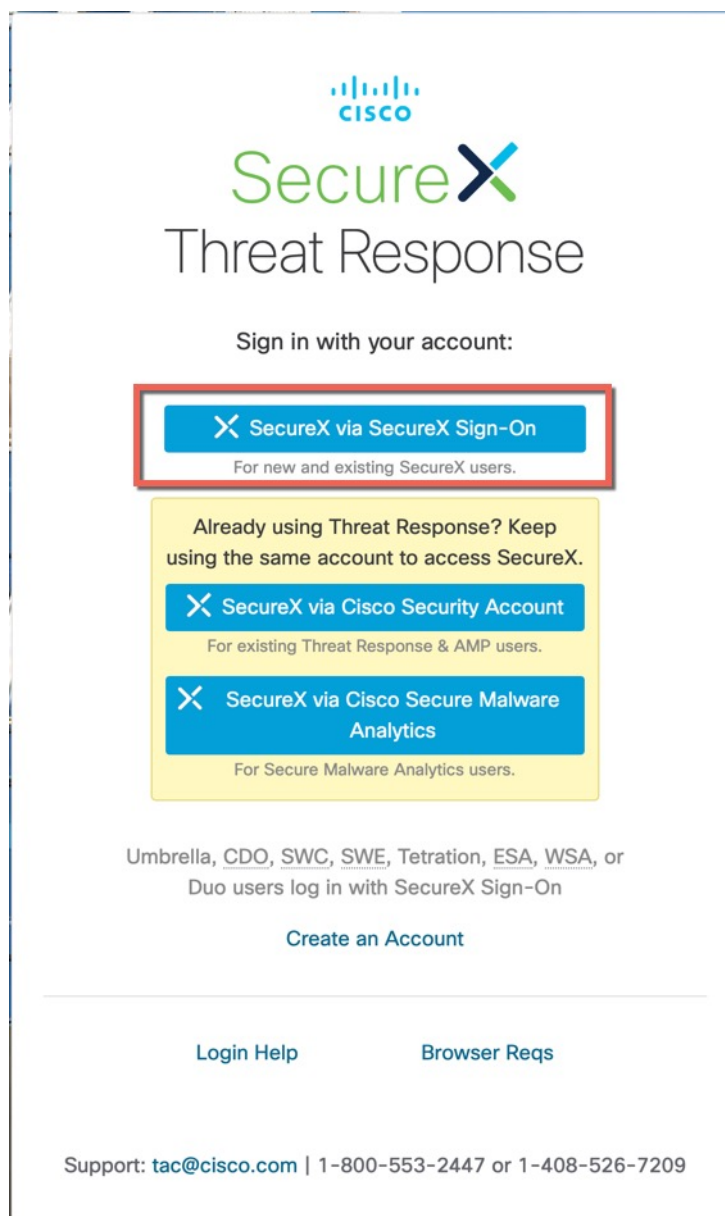
After completing this configuration, the SecureX ribbon will show up at the bottom of each page. [Learn more](#)

[Enable SecureX](#)

b) Log into SecureX.

A separate browser tab or window opens to log you into your SecureX account. Make sure this page is not blocked by a pop-up blocker.

Figure 2: SecureX Sign-In



The image shows the SecureX Threat Response sign-in page. At the top is the Cisco logo and the text "SecureX Threat Response". Below this is the instruction "Sign in with your account:". There are three main sign-in options, each with a blue button and a description below it. The first option, "SecureX via SecureX Sign-On", is highlighted with a red rectangular border. The second option is "SecureX via Cisco Security Account" for existing Threat Response & AMP users. The third option is "SecureX via Cisco Secure Malware Analytics" for Secure Malware Analytics users. Below these options, it states that users from Umbrella, CDO, SWC, SWE, Tetration, ESA, WSA, or Duo should log in with SecureX Sign-On. There is a "Create an Account" link. At the bottom, there are links for "Login Help" and "Browser Reqs", and a support contact line: "Support: tac@cisco.com | 1-800-553-2447 or 1-408-526-7209".

**SecureX**  
Threat Response

Sign in with your account:

**SecureX via SecureX Sign-On**  
For new and existing SecureX users.

Already using Threat Response? Keep using the same account to access SecureX.

**SecureX via Cisco Security Account**  
For existing Threat Response & AMP users.

**SecureX via Cisco Secure Malware Analytics**  
For Secure Malware Analytics users.

Umbrella, CDO, SWC, SWE, Tetration, ESA, WSA, or Duo users log in with SecureX Sign-On

[Create an Account](#)

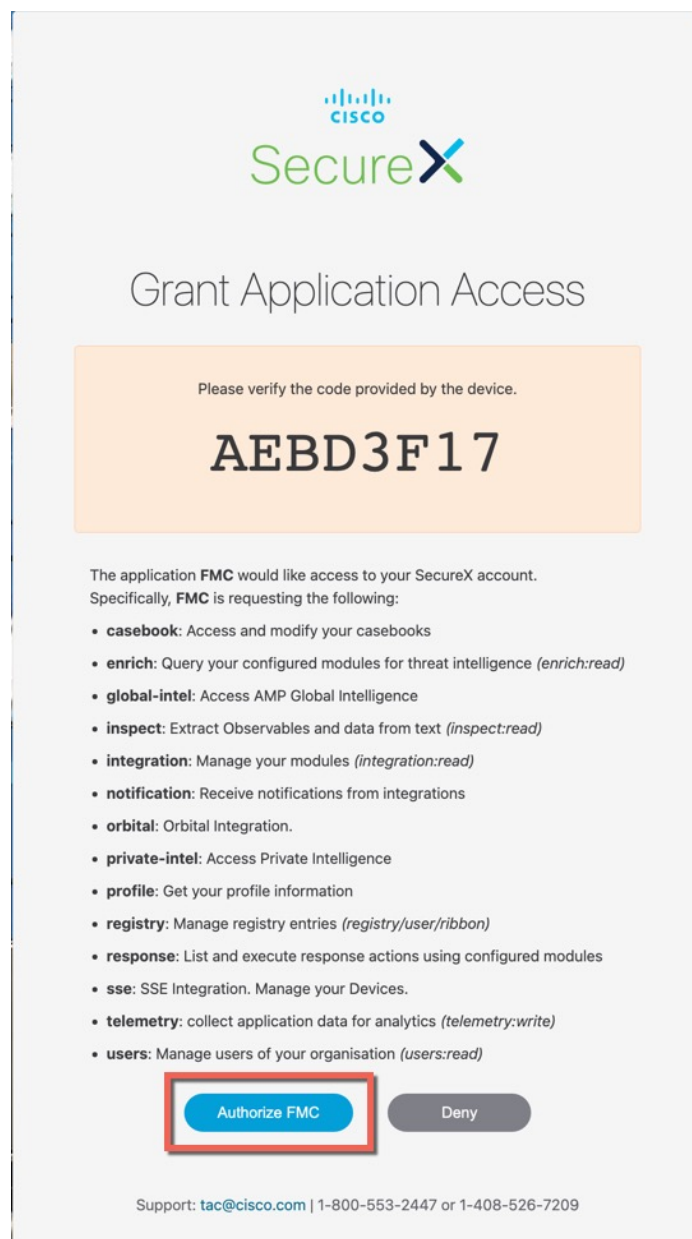
[Login Help](#) [Browser Reqs](#)

Support: [tac@cisco.com](mailto:tac@cisco.com) | 1-800-553-2447 or 1-408-526-7209

c) Click **Authorize FMC**.

You are shown a code that should match the code shown in the FMC.

Figure 3: Grant Application Access



d) After the FMC integrates with SecureX, you see a success message. Click **Save**.

**Figure 4: Success Message**

2 SecureX Enablement

After completing this configuration, the SecureX ribbon will show up at the bottom of each page.  
[Learn more](#)

▲ SecureX is enabled for US Region. You will need to save your configuration for this change to take effect.

[Enable SecureX](#)

## Access SecureX Using the Ribbon

The ribbon appears at the bottom of every page in the FMC web interface. You can use the ribbon to quickly pivot to other Cisco security products and work with threat data from multiple sources.

### Before you begin

- If you do not see the SecureX ribbon at the bottom of FMC web interface pages, do not use this procedure. Instead, see the [Cisco Secure Firewall Threat Defense and SecureX Integration Guide](#).
- If you don't already have a SecureX account, obtain one from your IT department.

### Procedure

- Step 1** In FMC, click the ribbon at the bottom of any FMC page.
- Step 2** Click **Get SecureX**.
- Step 3** Sign in to SecureX.
- Step 4** Click the link to authorize access.
- Step 5** Click the ribbon to expand and use it.

### What to do next

For information about ribbon features and how to use them, see the online help in SecureX.

## Event Analysis with Cisco Threat Response

Cisco Threat Response was formerly known as Cisco Threat Response (CTR.)

Rapidly detect, investigate, and respond to threats using Cisco Threat Response, the integration platform in the Cisco Cloud that lets you analyze incidents using data aggregated from multiple products, including Secure Firewall.

- For general information about Cisco Threat Response, see:  
[Cisco SecureX Threat Response product page](#).
- For detailed instructions for integrating Firepower with Cisco Threat Response, see:
- See [Cisco Secure Firewall Threat Defense and Cisco SecureX Threat Response Integration Guide](#).

## View Event Data in Cisco Threat Response

### Before you begin

- Set up the integration as described in the [Cisco Secure Firewall Threat Defense and Cisco SecureX Threat Response Integration Guide](#).
- Review the online help in Cisco Threat Response to learn how to find, investigate, and take action on threats.
- You will need your credentials to access Cisco Threat Response.

### Procedure

#### Step 1

In Firepower Management Center, do the following:

- To pivot to Cisco Threat Response from a specific event:
  - a. Navigate to a page under the **Analysis > Intrusions > Events** menu that lists a supported event.
  - b. Right-click a source or destination IP address and choose **View in SecureX**.
- To view event info generally:
  - a. Navigate to **Integration > Other Integrations > Cloud Services**.
  - b. Click the link to view events in Cisco Threat Response.

#### Step 2

Sign in to Cisco Threat Response as prompted.

## Cisco Cloud Event Settings

Sending firewall events to the cloud allows you to use external tools to investigate the firewall incidents. The devices send firewall events to the Security Services Exchange (SSE), from where they can be forwarded to various cloud services to unify visibility and enhance your threat investigations.

To allow your devices to send firewall events to Cisco Security Cloud, you must either register the FMC with the smart license (**System** (⚙️) > **Licenses** > **Smart Licenses**) or enable SecureX integration. Cisco Security Cloud integration associates the FMC with your CDO account and brings your secure firewall deployment onboard to the Cisco cloud tenancy, allowing it to connect to Cisco's integrated security cloud services.

For more information about integrating the FMC with Cisco Security Cloud, see [Enable SecureX Integration](#).

### Security Services Exchange Event Consolidation

The Security Services Exchange does not display the complete list of events from the FMC. Instead, it correlates and consolidates events, presenting only unique events. This approach reduces redundancy of events and enhances clarity. The current categorization parameters used for this consolidation are detailed as follows:

- For identifying duplication of intrusion events, the following elements are considered: Initiator IP, Initiator IP, SID, and GID.
- For identifying duplication of connection events and security-related connection events, the following elements are considered: Initiator IP, Initiator IP, and Security Intelligence Category.
- For identifying duplication of file and malware events, all elements except Event Second are considered.

## Enable Sending Events to the Cisco Security Cloud

Configure your FMC to enable the managed Firepower Threat Defense devices send events directly to Cisco Security Cloud. The cloud region and event types that you configure in the **SecureX Integration** page can be used for multiple integrations when applicable and enabled.

### Before you begin

- Ensure that you register the management center with Smart License (**System** ⚙️ > **Licenses** > **Smart Licenses**) or enable Cisco Security Cloud integration to allow your devices to send firewall events to Cisco cloud.
- In the FMC:
  - Go to the **System** ⚙️ > **Configuration** page and give your FMC a unique name to clearly identify it in the **Devices** list in the cloud.
  - Add your Firepower Threat Defense devices to the FMC, assign licenses to them, and ensure that the system is working correctly. Ensure that you have created the necessary policies and that the generated events are displayed as expected in the FMC UI under the **Analysis** menu.
- Ensure that you have your Security Cloud Sign-On credentials and can sign in to the regional cloud in which your account was created.

For more information on regional cloud URLs and supported device versions, see [Regional Clouds](#).

- If you are currently sending events to the cloud using syslog, disable it to avoid duplication.

### Procedure

- 
- Step 1** Determine the regional cloud that you want to use for sending firewall events. For more information about choosing a regional cloud, refer to [Cisco Secure Firewall Threat Defense and Cisco XDR Integration Guide](#).

#### Note

If SecureX integration is enabled and the FMC is registered to the selected regional cloud, changing the regional cloud disables SecureX integration. You can enable the SecureX integration again after changing the regional cloud.

- Step 2** In your FMC, choose **Integration > SecureX**.
- Step 3** Choose a regional cloud from the **Current Region** drop-down list.
- Step 4** Check the **Send events to the cloud** check box to enable the cloud event configuration.
- Step 5** Select the event types that you want to send to the cloud.

**Note**

Events that you send to the cloud can be used for multiple integrations, as shown in the this table.

| Integration                                       | Supported Event Options                                                                                                                                                          | Notes                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco Security Analytics and Logging (SaaS)       | All                                                                                                                                                                              | High-priority connection events include: <ul style="list-style-type: none"> <li>• Security Intelligence connection events</li> <li>• Connection events related to file and malware events</li> <li>• Connection events related to intrusion events</li> </ul>                                                                                |
| Cisco Extended Detection and Response (Cisco XDR) | Depending on your version: <ul style="list-style-type: none"> <li>• Security-related connection events</li> <li>• Intrusion events</li> <li>• File and malware events</li> </ul> | Even if you send all the connection events, Cisco XDR supports only security-related connection events.<br><b>Note</b><br>Cisco XDR is a separately licensed product. It requires an additional subscription beyond the licenses required for Cisco Secure Firewall products. For more information, see <a href="#">Cisco XDR Licenses</a> . |

**Note**

- When you enable **Intrusion Events**, the FTD device sends events along with the impact flag.
- If you enable **File and Malware Events**, in addition to the events sent from the Firepower Threat Defense devices, the FMC sends retrospective events.

- Step 6** Click **Save**.

## Analyze Events Using Cisco XDR

Cisco Extended Detection and Response (Cisco XDR) is a cloud-based solution that unifies visibility by correlating detections across multiple telemetry sources, and enables security teams to detect, prioritize, and respond to the most sophisticated threats. Integrate FTD with Cisco XDR to connect Cisco's integrated security portfolio and your firewall deployment for a consistent experience that unifies visibility, enables automation, and strengthens your security across network.

For more information about Cisco XDR, see [Cisco XDR Help Center](#).



**Important**

- Cisco XDR is a separately licensed product. It requires an additional subscription beyond the licenses required for Cisco Secure Firewall products. For more information, see [Cisco XDR Licenses](#).
- If you were already sending events to the Cisco Security Cloud using a SecureX subscription before Version 7.6, you can continue to send events to Cisco XDR. However, if you now register your FMC to the cloud tenancy using your CDO account to send firewall events to Cisco XDR, your CDO account must have a Security Analytics and Logging license to forward events to Cisco XDR.

To integrate FTD with Cisco XDR, see the [Cisco Secure Firewall Threat Defense and Cisco XDR Integration Guide](#).

**Note**

As of July 31, 2024, Cisco SecureX is phased out and no longer available. Cisco SecureX cannot be provisioned for users, and access to Cisco SecureX is not provided alongside Cisco Secure Firewall product purchases. Additionally, all existing Cisco SecureX environments are disabled, and all capabilities are made unavailable. If you are using Firefox, you should remove Cisco SecureX Ribbon browser extension. For more information, see the [Frequently Asked Questions](#).

## Event Investigation Using Web-Based Resources

Use the contextual cross-launch feature to quickly find more information about potential threats in web-based resources outside of the Firepower Management Center. For example, you might:

- Look up a suspicious source IP address in a Cisco or third-party cloud-hosted service that publishes information about known and suspected threats, or
- Look for past instances of a particular threat in your organization's historical logs, if your organization stores that data in a Security Information and Event Management (SIEM) application.
- Look for information about a particular file, including file trajectory information, if your organization has deployed Cisco AMP for Endpoints.

When investigating an event, you can click directly from an event in the event viewer or dashboard in the Firepower Management Center to the relevant information in the external resource. This lets you quickly gather context around a specific event based on its IP addresses, ports, protocol, domain, and/or SHA 256 hash.

For example, suppose you are looking at the Top Attackers dashboard widget and you want to find out more information about one of the source IP addresses listed. You want to see what information Talos publishes about this IP address, so you choose the "Talos IP" resource. The Talos web site opens to a page with information about this specific IP address.

You can choose from a set of pre-defined links to commonly used Cisco and third-party threat intelligence services, and add custom links to other web-based services, and to SIEMs or other products that have a web interface. Note that some resources may require an account or a product purchase.

## About Managing Contextual Cross-Launch Resources

Manage external web-based resources using the **Analysis > Advanced > Contextual Cross-Launch** page.

**Exception:** Manage cross-launch links to a Secure Network Analytics appliance following the procedure in [Configure Cross-Launch Links for Secure Network Analytics, on page 12](#).

Pre-defined resources offered by Cisco are marked with the Cisco logo. The remaining links are third-party resources.

You can disable or delete any resources that you do not need, or you can rename them, for example by prefixing a name with a lower-case "z" so the resource sorts to the bottom of the list. Disabling a cross-launch resource disables it for all users. You cannot reinstate deleted resources, but you can re-create them.

To add a resource, see [Add Contextual Cross-Launch Resources, on page 10](#).

## Requirements for Custom Contextual Cross-Launch Resources

When adding custom contextual cross-launch resources:

- Resources must be accessible via web browser.
- Only http and https protocols are supported.
- Only GET requests are supported; POST requests are not.
- Encoding of variables in URLs is not supported. While IPv6 addresses may require colon separators to be encoded, most services do not require this encoding.
- Up to 100 resources can be configured, including pre-defined resources.
- You must be an Admin or Security Analyst user to create a cross launch, but you can also be a read-only Security Analyst to use them.

## Add Contextual Cross-Launch Resources

You can add contextual cross-launch resources such as threat intelligence services and Security Information and Event Management (SIEM) tools.

In multidomain deployments, you can see and use resources in parent domains, but you can only create and edit resources in the current domain. The total number of resources across all domains is limited to 100.

### Before you begin

- If you are adding links to a Secure Network Analytics appliance, check to see if the links you want already exist; most links are automatically created for you when you configure Security Analytics and Logging (On Premises).
- See [Requirements for Custom Contextual Cross-Launch Resources, on page 10](#).
- If needed for the resource you will link to, create or obtain an account and the credentials needed for access. Optionally, assign and distribute credentials for each user who needs access.
- Determine the syntax of the query link for the resource that you will link to:

Access the resource via browser and, using the documentation for that resource as needed, formulate the query link needed to search for a specific sample of the type of information you want your query link to find, such as an IP address.

Run the query, then copy the resulting URL from the browser's location bar.

For example, you might have the query URL

`https://www.talosintelligence.com/reputation_center/lookup?search=10.10.10.10.`

### Procedure

**Step 1** Choose **Analysis > Advanced > Contextual Cross-Launch**.

**Step 2** Click **New Cross-launch**.

In the form that appears, all fields marked with an asterisk require a value.

**Step 3** Enter a unique resource name.

**Step 4** Paste the working URL string from your resource into the **URL Template** field.

**Step 5** Replace the specific data (such as an IP address) in the query string with an appropriate variable: Position your cursor, then click a variable (for example, **ip**) once to insert the variable.

In the example from the "Before You Begin" section above, the resulting URL might be

`https://www.talosintelligence.com/reputation_center/lookup?search={ip}`.

When the contextual cross-launch link is used, the {ip} variable in the URL will be replaced by the IP address that the user right-clicks on in the event viewer or dashboard.

For a description of each variable, hover over the variable.

You can create multiple contextual cross-launch links for a single tool or service, using different variables for each.

**Step 6** Click **Test with example data** (🔗) to test your link with example data.

**Step 7** Fix any problems.

**Step 8** Click **Save**.

## Investigate Events Using Contextual Cross-Launch

### Before you begin

If the resource you will access requires credentials, make sure you have those credentials.

### Procedure

**Step 1** Navigate to one of the following pages in the Firepower Management Center that shows events:

- A dashboard (**Overview > Dashboards heading > Dashboard**), or

- An event viewer page (any menu option under the **Analysis** menu that includes a table of events.)

**Step 2** Right-click the event of interest and choose the contextual cross-launch resource to use.

If necessary, scroll down in the context menu to see all available options.

The data type you right-click on determines the options you see; for example, if you right-click an IP address, you will only see contextual cross-launch options that are relevant to IP addresses.

For example, to get threat intelligence from Cisco Talos about a source IP address in the intrusion event, choose **Talos SrcIP** or **Talos IP**.

If a resource includes multiple variables, the option to choose that resource is available only for events that have a single possible value for each included variable.

The contextual cross-launch resource opens in a separate browser window.

It may take some time for the query to be processed, depending on the amount of data to be queried, speed of and demand on the resource, and so on.

**Step 3** Sign in to the resource if necessary.

## Configure Cross-Launch Links for Secure Network Analytics

You can cross-launch from event data in FTD to related data in your Secure Network Analytics appliance. For more information about the Secure Network Analytics product, visit the [Cisco Security Analytics and Logging](#) product page.

For general information about contextual cross-launching, see [Investigate Events Using Contextual Cross-Launch](#), on page 11.

Use this procedure to configure a set of cross-launch links to your Secure Network Analytics appliance.



### Note

- If you want to change these links later, return to this procedure; you cannot make changes directly on the contextual cross-launch listing page.
- You can manually create additional links to cross-launch into your Secure Network Analytics appliance using the procedure in [Add Contextual Cross-Launch Resources](#), on page 10, but those links remain independent of the auto-created resources and you must manage them manually.

### Before you begin

- Ensure that a Secure Network Analytics appliance is available for use
- If your device sends events directly to Secure Network Analytics, disable syslog for those devices or assign them an access control policy without syslog configurations. This avoids duplicate events on the remote volume.
- Ensure you have these items:
  - Hostname or IP address of your manager.

- Credentials for an account on your Secure Network Analytics appliance that has administrator privileges.

If you want to send FTD data to your Secure Network Analytics appliance using Security Analytics and Logging (On Premises), see [Remote Data Storage on a Secure Network Analytics Appliance](#).

## Procedure

---

**Step 1** Choose **Integration > Security Analytics & Logging**.

**Step 2** You have two options for Secure Network Analytics deployment:

- **Manager Only**—Deploy a standalone Manager to receive and store events, and from which you can review and query events.
- **Data Store**—Deploy a Cisco Secure Network Analytics Flow Collector to receive events, a Secure Network Analytics Data Store to store events, and a Manager from which you can review and query events.

Choose the deployment option and click **Start**.

**Step 3** Complete the wizard. For more information, see the FMC Configuration section of [Cisco Security Analytics and Logging Firewall Event Integration Guide](#).

**Step 4** Choose **Analysis > Advanced > Contextual Cross-Launch** to verify your new cross-launch links.

If you want to make changes, return to this procedure; you cannot make changes directly on the contextual cross-launch listing page.

---

## What to do next

Use your Secure Network Analytics credentials to cross-launch from an event into the Secure Network Analytics event viewer.

To cross launch from an event in the FMC event viewer or dashboard, right-click a relevant event's table cell and choose the appropriate option.

Processing queries may take some time, depending on the amount of data, data transfer speed on the Secure Network Analytics Manager, and other factors.

# About Sending Syslog Messages for Security Events

You can send data related to connection, security intelligence, intrusion, and file and malware events via syslog to a Security Information and Event Management (SIEM) tool or another external event storage and management solution.

These events are also sometimes referred to as Snort® events.

## About Configuring the System to Send Security Event Data to Syslog

To find more about the platform settings that apply to syslog messages for security events, refer to *Threat Defense Platform Settings that Apply to Security Event Syslog Messages* in the [Firepower Management Center Device Configuration Guide](#).

Note that if you make changes to syslog settings in any policy, you must redeploy for the changes to take effect.

### Best Practices for Configuring Security Event Syslog Messaging

| Device and Version       | Configuration Location                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| All                      | If you will use syslog or store events externally, avoid special characters in object names such as policy and rule names. Object names should not contain special characters, such as commas, that the receiving application may use as separators.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Firepower Threat Defense | <ol style="list-style-type: none"> <li>Do the following to configure syslog in FTD platform settings: <ol style="list-style-type: none"> <li>Click <b>Devices &gt; Platform Settings</b>.</li> <li>Edit the threat defense settings policy.</li> <li>In the left navigation pane, click <b>Syslog</b>.</li> </ol> <p>See also <i>Threat Defense Platform Settings That Apply to Security Event Syslog Messages</i> in the <a href="#">Firepower Management Center Device Configuration Guide</a>.</p> </li> <li>In your access control policy <b>Logging</b> tab, opt to use the FTD platform settings.</li> <li>(For intrusion events) Configure intrusion policies to use the settings in your access control policy <b>Logging</b> tab. (This is the default.)</li> </ol> <p>Overriding any of these settings is not recommended.</p> <p>For essential details, see <a href="#">Send Security Event Syslog Messages from FTD Devices, on page 14</a>.</p> |
| All other devices        | <ol style="list-style-type: none"> <li>Create an alert response.</li> <li>Configure access control policy <b>Logging</b> to use the alert response.</li> <li>(For intrusion events) Configure syslog settings in intrusion policies.</li> </ol> <p>For complete details, see <a href="#">Send Security Event Syslog Messages from Classic Devices, on page 17</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

### Send Security Event Syslog Messages from FTD Devices

This procedure documents the best practice configuration for sending syslog messages for security events (connection, Security Intelligence, intrusion, file, and malware events) from FTD devices.



**Note** Many FTD syslog settings are not applicable to security events. Configure only the options described in this procedure.

### Before you begin

- In Firepower Management Center, configure policies to generate security events and verify that the events you expect to see appear in the applicable tables under the Analysis menu.
- Gather the syslog server IP address, port, and protocol (UDP or TCP):
- Ensure that your devices can reach the syslog server(s).
- Confirm that the syslog server(s) can accept remote messages.
- For important information about connection logging, see the chapter on [Connection Logging](#).

### Procedure

**Step 1** Configure syslog settings for your FTD device:

- a) Click **Devices > Platform Settings**.
- b) **Edit** the platform settings policy associated with your FTD device.
- c) In the left navigation pane, click **Syslog**.
- d) Click **Syslog Servers** and click **Add (+)** to enter server, protocol, interface, and related information.  
If you have questions about options on this page, see [Firepower Management Center Device Configuration Guide](#).
- e) Click **Syslog Settings** and configure the following settings:
  - **Enable timestamp on syslog messages**
  - **Timestamp Format**
  - **Enable syslog device ID**
- f) Click **Logging Setup**.
- g) On the **Basic Logging Settings**, select whether or not to **Send syslogs in EMBLEM format**.
- h) Click **Save**, to save your settings.

**Step 2** Configure general logging settings for the access control policy (including file and malware logging):

- a) Click **Policies > Access Control heading > Access Control**.
- b) Edit the applicable access control policy.
- c) From the **More** drop-down, click **Logging**.
- d) FTD 6.3 and later: Select **Use the syslog settings configured in the Threat Defense Platform Settings policy deployed on the device**.
- e) (Optional) Select a **Syslog Severity**.
- f) If you want to send file and malware events, select **Send Syslog messages for File and Malware events**.
- g) Click **Save**.

- Step 3** Enable logging for Security Intelligence events for the access control policy:
- In the same access control policy, click the **Security Intelligence** tab.
  - In each of the following locations, click **Logging** (  ) and enable beginning and end of connections and **Syslog Server**:
    - Beside **DNS Policy**.
    - In the **Block List** box, for **Networks** and for **URLs**.
  - Click **Save**.

- Step 4** Enable syslog logging for each rule in the access control policy:
- In the same access control policy, click **Access Control**, and then choose **Add Rule**.
  - Select a rule to edit.
  - Click the **Logging** tab in the rule.
  - Choose whether to log the beginning or end of connections, or both.  
(Connection logging generates a lot of data; logging both beginning and end generates roughly double that much data. Not every connection can be logged both at beginning and end.)
  - If you want to log file events, select **Log Files**.
  - Enable **Syslog Server**.
  - Verify that the rule is "**Using default syslog configuration in Access Control Logging**."
  - Click **Confirm**.
  - Repeat for each rule in the policy.

- Step 5** If you send intrusion events:
- Navigate to the intrusion policy associated with your access control policy.
  - In your intrusion policy, from **Advanced Settings** drop-down menu, click **Syslog Alerting**, and then click **Enabled**.
  - If necessary, click **Edit**
  - Enter options:

| Option       | Value                                                                                                                                                                                       |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Logging Host | Unless you will send intrusion event syslog messages to a different syslog server than you will send other syslog messages, leave this blank to use the settings you have configured above. |
| Facility     | This setting is applicable only if you specify a Logging Host on this page.<br>For descriptions, see <a href="#">Syslog Alert Facilities</a> .                                              |
| Severity     | This setting is applicable only if you specify a Logging Host on this page.<br>For descriptions, see <a href="#">Syslog Severity Levels</a> .                                               |

- Click **Back**.
- Click **Policy Information** in the left navigation pane.
- Click **Commit Changes**.



### What to do next

- (Optional) Configure different logging settings for individual policies and rules.

See the applicable table rows in [Configuration Locations for Syslogs for Connection and Security Intelligence Events \(All Devices\)](#), on page 18.

These settings will require syslog alert responses, which are configured as described in [Creating a Syslog Alert Response](#). They do not use the platform settings you configured in this procedure.

- To configure security event syslog logging for Classic devices, see [Send Security Event Syslog Messages from Classic Devices](#), on page 17.
- If you are done making changes, deploy your changes to managed devices.

## Send Security Event Syslog Messages from Classic Devices

### Before you begin

- Configure policies to generate security events.
- Ensure that your devices can reach the syslog server(s).
- Confirm that the syslog server(s) can accept remote messages.
- For important information about connection logging, see the chapter on [Connection Logging](#).

### Procedure

- 
- Step 1** Configure an alert response for your Classic devices:  
See [Creating a Syslog Alert Response](#).
- Step 2** Configure syslog settings in the access control policy:
- a) Click **Policies > Access Control heading > Access Control**.
  - b) Edit the applicable access control policy.
  - c) Click **Logging**.
  - d) Select **Send using specific syslog alert**.
  - e) Select the **Syslog Alert** you created above.
  - f) Click **Save**.
- Step 3** If you will send file and malware events:
- a) Select **Send Syslog messages for File and Malware events**.
  - b) Click **Save**.
- Step 4** If you will send intrusion events:
- a) Navigate to the intrusion policy associated with your access control policy.
  - b) In your intrusion policy, from **Advanced Settings** drop-down menu, click **Syslog Alerting**, and then click **Enabled**.
  - c) If necessary, click **Edit**
  - d) Enter options:

| Option       | Value                                                                                                                                                                                       |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Logging Host | Unless you will send intrusion event syslog messages to a different syslog server than you will send other syslog messages, leave this blank to use the settings you have configured above. |
| Facility     | This setting is applicable only if you specify a Logging Host on this page.<br>See <a href="#">Syslog Alert Facilities</a> .                                                                |
| Severity     | This setting is applicable only if you specify a Logging Host on this page.<br>See <a href="#">Syslog Severity Levels</a> .                                                                 |

- e) Click **Back**.
- f) Click **Policy Information** in the left navigation pane.
- g) Click **Commit Changes**.

### What to do next

- (Optional) Configure different logging settings for individual access control rules. See the applicable table rows in [Configuration Locations for Syslogs for Connection and Security Intelligence Events \(All Devices\)](#), on page 18. These settings will require syslog alert responses, which are configured as described in [Creating a Syslog Alert Response](#). They do not use the settings you configured above.
- To configure security event syslog logging for FTD devices, see [Send Security Event Syslog Messages from FTD Devices](#), on page 14.

## Configuration Locations for Security Event Syslogs

These topics describe how to configure location for security event syslogs:

### Configuration Locations for Syslogs for Connection and Security Intelligence Events (All Devices)

There are many places to configure logging settings. Use the table below to ensure that you set the options you need.



#### Important

- Pay careful attention when configuring syslog settings, especially when using inherited defaults from other configurations. Some options may NOT be available to all managed device models and software versions, as noted in the table below.
- For important information when configuring connection logging, see the chapter on [Connection Logging](#).

| Configuration Location                                                                                                                                                                                             | Description and More Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Devices &gt; Platform Settings</b> , Threat Defense Settings policy, <b>Syslog</b>                                                                                                                              | <p>This option applies only to FTD devices.</p> <p>Settings you configure here can be specified in the Logging settings for an Access Control policy and then used or overridden in the remaining policies and rules in this table.</p> <p>See <a href="#">Firepower Management Center Device Configuration Guide</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Policies &gt; Access Control heading &gt; Access Control</b> , <each policy>, <b>Logging</b>                                                                                                                    | <p>Settings you configure here are the default settings for syslogs for all connection and security intelligence events, unless you override the defaults in descendant policies and rules at the locations specified in the remaining rows of this table.</p> <p>Recommended setting for FTD devices: Use Threat Defense Platform Settings. For information, see <a href="#">Firepower Management Center Device Configuration Guide</a>.</p> <p>Required setting for all other devices: Use a syslog alert.</p> <p>If you specify a syslog alert, see <a href="#">Creating a Syslog Alert Response</a>.</p> <p>For more information about the settings on the Logging tab, see <a href="#">Firepower Management Center Device Configuration Guide</a>.</p> |
| <b>Policies &gt; Access Control heading &gt; Access Control</b> , <each policy>, <b>Rules, Default Action row, Logging</b> (  ) | <p>Logging settings for the default action associated with an access control policy.</p> <p>See information about logging in <a href="#">Firepower Management Center Device Configuration Guide</a> and <a href="#">Logging Connections with a Policy Default Action</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Policies &gt; Access Control heading &gt; Access Control</b> , <each policy>, <b>Rules</b> , <each rule>, <b>Logging</b>                                                                                        | <p>Logging settings for a particular rule in an access control policy.</p> <p>See information about logging in <a href="#">Firepower Management Center Device Configuration Guide</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Policies &gt; Access Control heading &gt; Access Control</b> , <each policy>, <b>Security Intelligence, Logging</b> (  )     | <p>Logging settings for Security Intelligence Block lists.</p> <p>Click these buttons to configure:</p> <ul style="list-style-type: none"> <li>• DNS Block List Logging Options</li> <li>• URL Block List Logging Options</li> <li>• Network Block List Logging Options (for IP addresses on the blocked list)</li> </ul> <p>See <a href="#">Firepower Management Center Device Configuration Guide</a></p>                                                                                                                                                                                                                                                                                                                                                 |
| <b>Policies &gt; Access Control heading &gt; SSL</b> , <each policy>, <b>Default Action row, Logging</b> (  )                   | <p>Logging settings for the default action associated with an SSL policy.</p> <p>See <a href="#">Logging Connections with a Policy Default Action</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Policies &gt; Access Control heading &gt; SSL</b> , <each policy>, <each rule>, <b>Logging</b>                                                                                                                  | <p>Logging settings for SSL rules.</p> <p>See <a href="#">Firepower Management Center Device Configuration Guide</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

| Configuration Location                                                                                                                                                                                      | Description and More Information                                                                                                                      |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Policies &gt; Access Control heading &gt; Prefilter</b> , <each policy>, <b>Default Action</b> row, <b>Logging</b> (  ) | Logging settings for the default action associated with a prefilter policy.<br>See <a href="#">Logging Connections with a Policy Default Action</a> . |
| <b>Policies &gt; Access Control heading &gt; Prefilter</b> , <each policy>, <each prefilter rule>, <b>Logging</b>                                                                                           | Logging settings for each prefilter rule in a prefilter policy.<br>See <a href="#">Firepower Management Center Device Configuration Guide</a>         |
| <b>Policies &gt; Access Control heading &gt; Prefilter</b> , <each policy>, <each tunnel rule> , <b>Logging</b>                                                                                             | Logging settings for each tunnel rule in a prefilter policy.<br>See <a href="#">Firepower Management Center Device Configuration Guide</a>            |
| Additional syslog settings for FTD cluster configurations:                                                                                                                                                  | The <a href="#">Firepower Management Center Device Configuration Guide</a> has multiple references to syslog; search the chapter for "syslog."        |

### Configuration Locations for Syslogs for Intrusion Events (FTD Devices)

You can specify syslog settings for intrusion policies in various places and, optionally, inherit settings from the access control policy or the Threat Defense Platform Settings or both.

| Configuration Location                                                                                                                                   | Description and More Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Devices &gt; Platform Settings</b> , Threat Defense Settings policy, <b>Syslog</b>                                                                    | Syslog destinations that you configure here can be specified in the Logging tab of an access control policy which can be the default for an intrusion policy.<br><br>See <a href="#">Firepower Management Center Device Configuration Guide</a> .                                                                                                                                                                                                                                                                                                     |
| <b>Policies &gt; Access Control heading &gt; Access Control</b> , <each policy>, <b>Logging</b>                                                          | Default setting for syslog destination for intrusion events, if the intrusion policy does not specify other logging hosts.<br><br>See <a href="#">Firepower Management Center Device Configuration Guide</a> .                                                                                                                                                                                                                                                                                                                                        |
| <b>Policies &gt; Access Control heading &gt; Intrusion</b> , <each policy>, <b>Advanced Settings</b> , enable <b>Syslog Alerting</b> , click <b>Edit</b> | To specify syslog collectors other than the destinations specified in the access control policy Logging tab, and to specify facility and severity, see <a href="#">Configuring Syslog Alerting for Intrusion Events</a> .<br><br>If you want to use the <b>Severity</b> or <b>Facility</b> or both as configured in the intrusion policy, you must also configure the logging hosts in the policy. If you use the logging hosts specified in the access control policy, the severity and facility specified in the intrusion policy will not be used. |
| <b>Policies &gt; Access Control heading &gt; Intrusion &gt; Logging &gt; IPS settings</b>                                                                | If you want to send Syslog messages for IPS events. Default syslog settings configured are used for syslog destinations for IPS events.                                                                                                                                                                                                                                                                                                                                                                                                               |

### Configuration Locations for Syslogs for Intrusion Events (Devices Other than FTD)

- (Default) Access control policy [Firepower Management Center Device Configuration Guide](#), IF you specify a syslog alert (See [Creating a Syslog Alert Response](#).)
- Or see [Configuring Syslog Alerting for Intrusion Events](#).

By default, the intrusion policy uses the settings in the Logging tab of the access control policy. If settings applicable to devices other than FTD are not configured there, syslogs will not be sent for devices other than FTD and no warning appears.

### Configuration Locations for Syslogs for File and Malware Events

| Configuration Location                                                                                             | Description and More Information                                                                                                                                                                                                                                        |
|--------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| In an access control policy:<br><b>Policies &gt; Access Control</b> , <each policy>, <b>Logging</b>                | This is the main location for configuring the system to send syslogs for file and malware events.<br><br>If you do not use the syslog settings in FTD Platform Settings, you must also create an alert response. See <a href="#">Creating a Syslog Alert Response</a> . |
| In FTD Platform Settings:<br><b>Devices &gt; Platform Settings</b> , Threat Defense Settings policy, <b>Syslog</b> | These settings apply only to FTD devices running supported versions, and only if you configure the Logging tab in the access control policy to use FTD platform settings.<br><br>See <a href="#">Firepower Management Center Device Configuration Guide</a> .           |
| In an access control rule:<br><b>Policies &gt; Access Control</b> , <each policy>, <each rule>, <b>Logging</b>     | If you do not use the syslog settings in FTD Platform Settings, you must also create an alert response. See <a href="#">Creating a Syslog Alert Response</a> .                                                                                                          |

## Anatomy of Security Event Syslog Messages

### Example security event message from FTD (Intrusion Event)

| 0                                                                                                                                                                                                                                                                                                                                                                                                                               | 1 | 2 | 3 | 4 | 5 | 6 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|---|---|---|---|---|
| <pre>&lt;37&gt;2018-06-27 192.168.0.81 <u>SFIMS</u> : %FTD-5-430001: 192.168.1.10, DstIP: 192.168.1.102, SrcPort: 33994 Protocol: tcp, Priority: 2, GID: 133, SID: 17, Rev Message: "DCE2_EVENT SMB_INVALID_DSIZE", Classifi Potentially Bad Traffic, User: No Authentication R Client: NetBIOS-ssn (SMB) client, ApplicationProto (SMB), ACPolicy: test, NAPPolicy: Balanced Securit Connectivity, InlineResult: Blocked</pre> |   |   |   |   |   |   |

**Table 1: Components of Security Event Syslog Messages**

| Item Number in Sample Message | Header Element | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0                             | PRI            | The priority value that represents both Facility and Severity of the alert. The value appears in the syslog messages only when you enable logging in EMBLEM format using FMC platform settings. If you enable logging of intrusion events through access control policy Logging tab, the PRI value is automatically displayed in the syslog messages. For information on how to enable the EMBLEM format, see <a href="#">Firepower Management Center Device Configuration Guide</a> . For information on PRI, see <a href="#">RFC5424</a> . |

| Item Number in Sample Message | Header Element                                                                                                                                                                                                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1                             | Timestamp                                                                                                                                                                                                                      | <p>Date and time the syslog message was sent from the device.</p> <ul style="list-style-type: none"> <li>• (Syslogs sent from FTD devices) For syslogs sent using settings in the access control policy and its descendants, or if specified to use this format in the Threat Defense Platform Settings, the date format is the format defined in the ISO 8601 timestamp format as specified in RFC 5424 (yyyy-MM-ddTHH:mm:ssZ), where the letter Z indicates the UTC time zone.</li> <li>• (Syslogs sent from all other devices) For syslogs sent using settings in the access control policy and its descendants, the date format is the format defined in the ISO 8601 timestamp format as specified in RFC 5424 (yyyy-MM-ddTHH:mm:ssZ), where the letter Z indicates the UTC time zone.</li> <li>• Otherwise, it is the month, day, and time in UTC time zone, though the time zone is not indicated.</li> </ul> <p>To configure the timestamp setting in Threat Defense Platform Settings, see <a href="#">Firepower Management Center Device Configuration Guide</a>.</p> |
| 2                             | <p>Device or interface from which the message was sent.</p> <p>This can be:</p> <ul style="list-style-type: none"> <li>• IP address of the interface</li> <li>• Device hostname</li> <li>• Custom device identifier</li> </ul> | <p>(For syslogs sent from FTD devices)</p> <p>If the syslog message was sent using the Threat Defense Platform Settings, this is the value configured in <b>Syslog Settings</b> for the <b>Enable Syslog Device ID</b> option, if specified.</p> <p>Otherwise, this element is not present in the header.</p> <p>To configure this setting in Threat Defense Platform Settings, see <a href="#">Firepower Management Center Device Configuration Guide</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 3                             | Custom value                                                                                                                                                                                                                   | <p>If the message was sent using an alert response, this is the <b>Tag</b> value configured in the alert response that sent the message, if configured. (See <a href="#">Creating a Syslog Alert Response</a>.)</p> <p>Otherwise, this element is not present in the header.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 4                             | %FTD                                                                                                                                                                                                                           | Type of device that sent the message. %FTD is Firepower Threat Defense                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 5                             | Severity                                                                                                                                                                                                                       | <p>The severity specified in the syslog settings for the policy that triggered the message.</p> <p>For severity descriptions, see <i>Severity Levels</i> in the <a href="#">Firepower Management Center Device Configuration Guide</a> or <a href="#">Syslog Severity Levels</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Item Number in Sample Message | Header Element        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 6                             | Event type identifier | <ul style="list-style-type: none"> <li>• 430001: Intrusion event</li> <li>• 430002: Connection event logged at beginning of connection</li> <li>• 430003: Connection event logged at end of connection</li> <li>• 430004: File event</li> <li>• 430005: File malware event</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| --                            | Facility              | See <a href="#">Facility in Security Event Syslog Messages, on page 24</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| --                            | Remainder of message  | <p>Fields and values separated by colons.</p> <p>Fields with empty or unknown values are omitted from messages.</p> <p>For field descriptions, see:</p> <ul style="list-style-type: none"> <li>• <a href="#">Connection and Security Intelligence Event Fields</a>.</li> <li>• <a href="#">Intrusion Event Fields</a></li> <li>• <a href="#">File and Malware Event Fields</a></li> </ul> <p><b>Note</b></p> <p>Field description lists include both syslog fields and fields visible in the event viewer (menu options under the Analysis menu in the FMC web interface.) Fields available via syslog are labeled as such.</p> <p>Some fields visible in the event viewer are not available via syslog. Also, some syslog fields are not included in the event viewer (but may be available via search), and some fields are combined or separated.</p> |

## Facility in Security Event Syslog Messages

Facility values are not generally relevant in syslog messages for security events. However, if you require Facility, use the following table:



| Device                 | To Include Facility in Connection Events                                                                                                                                                     | To Include Facility in Intrusion Events                                                                                                                                                                                                                                                                                                                                                                       | Location in Syslog Message                                                                                                      |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| FTD                    | Use the EMBLEM option in Threat Defense Platform Settings.<br><br>Facility is always <b>ALERT</b> for connection events when sending syslog messages using Threat Defense Platform Settings. | Use the EMBLEM option in Threat Defense Platform Settings or configure logging using the syslog settings in the intrusion policy. If you use the intrusion policy, you must also specify the logging host in the intrusion policy settings.<br><br>Enable syslog alerting and configure facility and severity on the intrusion policy. See <a href="#">Configuring Syslog Alerting for Intrusion Events</a> . | Facility does not appear in the message header, but the syslog collector can derive the value based on RFC 5424, section 6.2.1. |
| Devices other than FTD | Use an alert response.                                                                                                                                                                       | Use the syslog setting in the intrusion policy advanced settings or an alert response identified in the access control policy Logging tab.                                                                                                                                                                                                                                                                    |                                                                                                                                 |

For more information, see [Facilities and Severities for Intrusion Syslog Alerts](#) and [Creating a Syslog Alert Response](#).

## Firepower Syslog Message Types

Firepower can send multiple syslog data types, as described in the following table:

| Syslog Data Type                                                                 | See                                                                                                                                      |
|----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Audit logs from FMC                                                              | <a href="#">Stream Audit Logs to Syslog</a> and the <a href="#">Audit and Syslog</a> chapter                                             |
| Device health and network-related logs from FTD devices                          | <a href="#">Firepower Management Center Device Configuration Guide</a>                                                                   |
| Connection, security intelligence, and intrusion event logs from FTD devices     | <a href="#">About Configuring the System to Send Security Event Data to Syslog</a> , on page 14.                                         |
| Connection, security intelligence, and intrusion event logs from Classic devices | <a href="#">About Configuring the System to Send Security Event Data to Syslog</a> , on page 14                                          |
| Logs for file and malware events                                                 | <a href="#">About Configuring the System to Send Security Event Data to Syslog</a> , on page 14                                          |
| IPS Settings                                                                     | Send Syslog messages for IPS events. <a href="#">Configuration Locations for Syslogs for Intrusion Events (FTD Devices)</a> , on page 20 |

## Limitations of Syslog for Security Events

- If you will use syslog or store events externally, avoid special characters in object names such as policy and rule names. Object names should not contain special characters, such as commas, that the receiving application may use as separators.
- It may take up to 15 minutes for events to appear on your syslog collector.
- Data for the following file and malware events is not available via syslog:
  - Retrospective events
  - Events generated by AMP for Endpoints

## eStreamer Server Streaming

The Event Streamer (eStreamer) allows you to stream several kinds of event data from a Firepower Management Center to a custom-developed client application. The event data can either be streamed as binary data, or as fully-qualified events in plaintext format. For more information, see *Firepower eStreamer Integration Guide*.



**Note** eStreamer Client has been deprioritized, and the eNcoreCLI is End of Life as of 7/1/2024.

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. You can perform all of these tasks from the appliance's user interface. Once your settings are saved, the events you selected will be forwarded to eStreamer clients when requested.

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

**Table 2: Event Types Transmittable by the eStreamer Server**

| Event Type                               | Description                                                                                                                                                           |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Intrusion Events</b>                  | intrusion events generated by managed devices                                                                                                                         |
| <b>Intrusion Event Packet Data</b>       | packets associated with intrusion events                                                                                                                              |
| <b>Intrusion Event Extra Data</b>        | 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 |
| <b>Discovery Events</b>                  | Network discovery events                                                                                                                                              |
| <b>Correlation and Allow List Events</b> | correlation and compliance allow list events                                                                                                                          |
| <b>Impact Flag Alerts</b>                | impact alerts generated by the FMC                                                                                                                                    |
| <b>User Events</b>                       | user events                                                                                                                                                           |
| <b>Malware Events</b>                    | malware events                                                                                                                                                        |

| Event Type        | Description                                                                             |
|-------------------|-----------------------------------------------------------------------------------------|
| File Events       | file events                                                                             |
| Connection Events | information about the session traffic between your monitored hosts and all other hosts. |

## Comparison of Syslog and eStreamer for Security Eventing

Generally, organizations that do not currently have significant existing investment in eStreamer should use syslog rather than eStreamer to manage security event data externally.

| Syslog                                                                                                                    | eStreamer                                                                                                                                          |
|---------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| No customization required                                                                                                 | Significant customization and ongoing maintenance required to accommodate changes in each release                                                  |
| Standard                                                                                                                  | Proprietary                                                                                                                                        |
| Syslog standard does not protect against data loss, especially when using UDP                                             | Protection against data loss                                                                                                                       |
| Sends directly from devices                                                                                               | Sends from FMC, adding processing overhead                                                                                                         |
| Support for file and malware events, connection events (including security intelligence events) and intrusion events.     | Support for all event types listed in <a href="#">eStreamer Server Streaming, on page 26</a> .                                                     |
| Some event data can be sent only from FMC. See <a href="#">Data Sent Only via eStreamer, Not via Syslog, on page 27</a> . | Includes data that cannot be sent via syslog directly from devices. See <a href="#">Data Sent Only via eStreamer, Not via Syslog, on page 27</a> . |

### Data Sent Only via eStreamer, Not via Syslog

The following data is available only from Firepower Management Center and thus cannot be sent via syslog from devices:

- Packet Logs
- Intrusion Event Extra Data events

For a description, see [eStreamer Server Streaming, on page 26](#).

- Statistics and aggregate events
- Network Discovery events
- User activity and login events
- Correlation events
- For malware events:
  - retrospective verdicts

- ThreatName and Disposition, unless information about the relevant SHAs has already been synchronized to the device
  - The following fields:
    - Impact and ImpactFlag fields  
For a description, see [eStreamer Server Streaming, on page 26](#).
    - the IOC\_Count field
  - Most raw IDs and UUIDs.  
Exceptions:
    - Syslogs for connection events do include the following: FirewallPolicyUUID, FirewallRuleID, TunnelRuleID, MonitorRuleID, SI\_CategoryID, SSL\_PolicyUUID, and SSL\_RuleID
    - Syslogs for intrusion events do include IntrusionPolicyUUID, GeneratorID, and SignatureID
  - Extended metadata, including but not limited to:
    - User details provided by LDAP, such as full name, department, phone number, etc.  
Syslog only provides usernames in the events.
    - Details for state-based information such as SSL Certificate details.  
Syslog provides basic information like the certificate fingerprint, but will not provide other certificate details like the cert CN.
    - Detailed application information, such as App Tags and Categories.  
Syslog provides only Application names.
- Some metadata messages also include extra information about the objects.
- Geolocation information

## Choosing eStreamer Event Types

The **eStreamer Event Configuration** check boxes control 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 *Firepower eStreamer Integration Guide*.

In a multidomain deployment, you can configure eStreamer Event Configuration at any domain level. However, if an ancestor domain has enabled a particular event type, you cannot disable that event type in the descendant domains.

You must be an Admin user to perform this task, for FMC.

### Procedure

- 
- Step 1** Choose **System** (⚙️) > **Integration**.

- Step 2** Click **eStreamer**.
- Step 3** Under **eStreamer Event Configuration**, check or clear the check boxes next to the types of events you want eStreamer to forward to requesting clients, described in [eStreamer Server Streaming, on page 26](#).
- Step 4** Click **Save**.
- 

## Configuring eStreamer Client Communications

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. After completing these steps you do not need to restart the eStreamer service to enable the client to connect to the eStreamer server.

In a multidomain deployment, you can create an eStreamer client in any domain. The authentication certificate allows the client to request events only from the client certificate's domain and any descendant domains. The eStreamer configuration page shows only clients associated with the current domain, so if you want to download or revoke a certificate, switch to the domain where the client was created.

You must be an Admin or Discovery Admin user to perform this task, for FMC.

### Procedure

---

- Step 1** Choose **System** (⚙) > **Integration**.
- Step 2** Click **eStreamer**.
- Step 3** Click **Create Client**.
- Step 4** In the **Hostname** field, enter the host name or IP address of the host running the eStreamer client.
- Note**  
If you have not configured DNS resolution, 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.
- Step 7** Click **Download** (↓) 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.
- Step 9** To revoke access for a client, click **Delete** (🗑) next to the host you want to remove.  
Note that you do not need to restart the eStreamer service; access is revoked immediately.
-

## Event Analysis in Splunk

You can use the Cisco Secure Firewall app for Splunk as an external tool to display and work with Firepower event data, to hunt and investigate threats on your network. To use the Splunk tool, eStreamer is required. This is an advanced functionality. See [eStreamer Server Streaming, on page 26](#). For more information, see [User Guide for Cisco Secure Firewall App for Splunk](#).

## Event Analysis in IBM QRadar

You can use the Cisco Firepower app for IBM QRadar as an alternate way to display event data and help you analyze, hunt for, and investigate threats to your network.

eStreamer is required. This is an advanced functionality. See [eStreamer Server Streaming, on page 26](#).

For more information, see <https://www.cisco.com/c/en/us/td/docs/security/firepower/integrations/QRadar/integration-guide-for-the-cisco-firepower-app-for-ibm-qradar.html>.

## History for Analyzing Event Data Using External Tools

| Feature                                                                                                                                | Minimum FMC | Minimum FTD | Details                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------------------------------------------------------------------------------------------|-------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Deprecated: SecureX Ribbon                                                                                                             | Any         | Any         | SecureX Ribbon is deprecated.<br><br>If you have installed the <b>Cisco SecureX Ribbon</b> browser extension in your Firefox browser and are experiencing compatibility errors while using FMC, remove the SecureX Ribbon extension.<br><br>To remove the extension, open Firefox, go to the browser's add-ons or extensions manager, locate the <b>Cisco SecureX Ribbon</b> extension, and remove or disable it. Restart Firefox to apply the changes.               |
| Register your firewall deployment to Cisco Security Cloud tenancy using your Cisco Security Cloud Sign-On account and your CDO tenant. | Any         | Any         | You can now register your FMC and its managed devices to the Cisco Security Cloud using your Cisco Security Cloud Sign-On account and your CDO tenant.<br><br>Cisco SecureX is phased out and no longer available. If you have an active Cisco SecureX environments, you will continue to receive support from the Cisco Technical Assistance Center (TAC) through the product end-of-support. For more information, see <a href="#">Frequently Asked Questions</a> . |
| SecureX ribbon                                                                                                                         | 7.0         | Any         | The SecureX ribbon pivots into SecureX for instant visibility into the threat landscape across your Cisco security products.<br><br>To display the SecureX ribbon in FMC, see the <i>Firepower and SecureX Integration Guide</i> at <a href="https://cisco.com/go/firepower-securex-documentation">https://cisco.com/go/firepower-securex-documentation</a> .<br><br>New/Modified screens: New page: <b>System &gt; SecureX</b> .                                     |

| Feature                                               | Minimum FMC   | Minimum FTD | Details                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------------------------|---------------|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Send all connection events to the Cisco cloud         | 7.0           | Any         | <p>You can now send all connection events to the Cisco cloud, rather than just sending high-priority connection events.</p> <p>New/Modified screens: New option on the <b>System &gt; Integration &gt; Cloud Services</b> page .</p>                                                                                                                                                                                                                                                                                                                                                                                 |
| Cross-launch to view data in Secure Network Analytics | 6.7           | Any         | <p>This feature introduces a quick way to create multiple entries for your Secure Network Analytics appliance on the Analysis &gt; Contextual Cross-Launch page.</p> <p>These entries allow you to right-click a relevant event to cross-launch Secure Network Analytics and display information related to the data point from which you cross-launched.</p> <p>New menu item: <b>System &gt; Logging &gt; Security Analytics and Logging</b>.</p> <p>New page to configure sending events to Secure Network Analytics.</p>                                                                                         |
| Contextual cross-launch from additional field types   | 6.7           | Any         | <p>You can now cross-launch into an external application using the following additional types of event data:</p> <ul style="list-style-type: none"> <li>• Access control policy</li> <li>• Intrusion policy</li> <li>• Application protocol</li> <li>• Client application</li> <li>• Web application</li> <li>• Username (including realm)</li> </ul> <p>New menu options: Contextual-cross launch options are now available when right-clicking the above data types for events in Dashboard widgets and event tables on pages under the Analysis menu.</p> <p>Supported platforms: Firepower Management Center</p> |
| Integration with IBM QRadar                           | 6.0 and later | Any         | <p>IBM QRadar users can use a new Firepower-specific app to analyze their event data.</p> <p>Available functionality is affected by your Firepower version.</p> <p>See <a href="#">Event Analysis in IBM QRadar, on page 30</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                 |

| Feature                                                | Minimum FMC                                               | Minimum FTD | Details                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------------------------|-----------------------------------------------------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enhancements to integration with Cisco Threat Response | 6.5                                                       | Any         | <ul style="list-style-type: none"> <li>• Support for regional clouds: <ul style="list-style-type: none"> <li>• United States (North America)</li> <li>• Europe</li> </ul> </li> <li>• Support for additional event types: <ul style="list-style-type: none"> <li>• File and malware events</li> <li>• High-priority connection events</li> </ul> <p>These are connection events related to the following:</p> <ul style="list-style-type: none"> <li>• Intrusion events</li> <li>• Security Intelligence events</li> <li>• File and malware events</li> </ul> </li> </ul> <p>Modified screens: New options on <b>System &gt; Integration &gt; Cloud Services</b>.</p> <p>Supported Platforms: All devices supported in this release, either via direct integration or syslog.</p> |
| Syslog                                                 | 6.5                                                       | Any         | The AccessControlRuleName field is now available in intrusion event syslog messages.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Integration with Cisco Security Packet Analyzer        | 6.5                                                       | Any         | Support for this feature was removed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Integration with Cisco Threat Response                 | 6.3 (via syslog, using a proxy collector)<br>6.4 (direct) | Any         | <p>Integrate Firepower intrusion event data with data from other sources for a unified view of threats on your network using the powerful analysis tools in Cisco Threat Response.</p> <p>Modified screens (version 6.4): New options on <b>System &gt; Integration &gt; Cloud Services</b>.</p> <p>Supported Platforms: Firepower Threat Defense devices running version 6.3 (via syslog) or 6.4.</p>                                                                                                                                                                                                                                                                                                                                                                            |
| Syslog support for File and Malware events             | 6.4                                                       | Any         | <p>Fully-qualified file and malware event data can now be sent from managed devices via syslog.</p> <p>Modified screens: <b>Policies &gt; Access Control &gt; Access Control &gt; Logging</b>.</p> <p>Supported Platforms: All managed devices running version 6.4.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Integration with Splunk                                | Supports all 6.x versions                                 | Any         | <p>Splunk users can use a new, separate Splunk app, Cisco Secure Firewall app for Splunk, to analyze events.</p> <p>Available functionality is affected by your Firepower version.</p> <p>See <a href="#">Event Analysis in Splunk, on page 30</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |



| Feature                                             | Minimum FMC | Minimum FTD | Details                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------------------|-------------|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Integration with Cisco Security Packet Analyzer     | 6.3         | Any         | <p>Feature introduced: Instantly query Cisco Security Packet Analyzer for packets related to an event, then click to examine the results in Cisco Security Packet Analyzer or download them for analysis in another external tool.</p> <p>New screens:</p> <p><b>System &gt; Integration &gt; Packet Analyzer</b></p> <p><b>Analysis &gt; Advanced &gt; Packet Analyzer Queries .</b></p> <p>New menu options: <b>Query &gt; Packet Analyzer</b> menu item when right-clicking on an event on Dashboard pages and event tables on pages under the Analysis menu.</p> <p>Supported platforms: Firepower Management Center</p>                                                                                                                                                 |
| Contextual cross-launch                             | 6.3         | Any         | <p>Feature introduced: Right-click an event to look up related information in predefined or custom URL-based external resources.</p> <p>New screens: <b>Analysis &gt; Advanced &gt; Contextual Cross-Launch.</b></p> <p>New menu options: Multiple options when right-clicking on an event on Dashboard pages and event tables on pages under the Analysis menu.</p> <p>Supported platforms: Firepower Management Center</p>                                                                                                                                                                                                                                                                                                                                                 |
| Syslog messages for connection and intrusion events | 6.3         | Any         | <p>Ability to send fully-qualified connection and intrusion events to external storage and tools via syslog, using new unified and simplified configurations. Message headers are now standardized and include event type identifiers, and messages are smaller because fields with unknown and empty values are omitted.</p> <p>Supported Platforms:</p> <ul style="list-style-type: none"> <li>• All new functionality: FTD devices running version 6.3.</li> <li>• Some new functionality: Non-FTD devices running version 6.3.</li> <li>• Less new functionality: All devices running versions older than 6.3.</li> </ul> <p>For more information, see the topics under <a href="#">About Sending Syslog Messages for Security Events, on page 13</a> and subtopics.</p> |
| eStreamer                                           | 6.3         | Any         | Moved eStreamer content from the Host Identity Sources chapter to this chapter and added a summary comparing eStreamer to syslog.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

