

Cisco Event Analysis Using External Tools User Guide

Contents

- [1 Cisco Event Analysis Using External Tools](#)
- [2 Product Information](#)
- [3 Product Usage Instructions](#)
- [4 View Event Data in Cisco SecureX Threat Response](#)
- [5 Integrate with Cisco SecureX](#)
- [6 Event Analysis with Cisco SecureX threat response](#)
- [7 Configure Cross-Launch Links for Secure Network Analytics](#)
- [8 About Configuring the System to Send Security Event Data to Syslog](#)
- [9 eStreamer Server Streaming](#)
 - [9.1 Comparison of Syslog and eStreamer for Security Eventing](#)
- [10 Event Analysis in Splunk](#)
- [11 Event Analysis in IBM QRadar](#)
- [12 History for Analyzing Event Data Using External Tools](#)
- [13 Documents / Resources](#)
 - [13.1 References](#)
- [14 Related Posts](#)



Cisco Event Analysis Using External Tools

Product Information

The product allows users to integrate with Cisco SecureX and access it using the ribbon feature in the FMC web interface.

Specifications

- **Integration:** Cisco SecureX
- **Interface:** FMC web interface
- **Ribbon Feature:** Bottom of every page

Product Usage Instructions

Accessing SecureX Using the Ribbon

To access SecureX using the ribbon feature, follow these steps:

1. In FMC, click the ribbon at the bottom of any FMC page.

2. Click "Get SecureX".
3. Sign in to SecureX.
4. Click the link to authorize access.
5. Click the ribbon to expand and use it.

Event Analysis Using External Tools

To perform event analysis using external tools, follow these steps:

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

Event Analysis with Cisco SecureX Threat Response

Cisco SecureX Threat Response (formerly known as Cisco Threat Response) allows users to rapidly detect, investigate, and respond to threats. To perform event analysis with Cisco SecureX Threat Response, follow these steps:

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

View Event Data in Cisco SecureX Threat Response

To view event data in Cisco SecureX Threat Response, follow these steps:

1. Sign in to Cisco SecureX Threat Response as prompted.

Event Investigation Using Web-Based Resources

To investigate events using web-based resources, follow these steps:

1. Sign in to Cisco SecureX Threat Response as prompted.
2. Use the contextual cross-launch feature to find more information about potential threats in web-based resources outside of the Firepower Management Center.
3. Click directly from an event in the event viewer or dashboard in the Firepower Management Center to the relevant information in the external resource.

About Managing Contextual Cross-Launch Resources

To manage external web-based resources, follow these steps:

1. Go to Analysis > Advanced > Contextual Cross-Launch.
2. Manage the pre-defined and third-party resources offered by Cisco.

3. You can disable, delete, or rename resources as needed.

FAQs

- **Q: What is SecureX?**

A: SecureX is an integration platform in the Cisco Cloud that allows users to analyze incidents using data aggregated from multiple products, including Firepower.

- **Q: How can I access SecureX using the ribbon feature?**

A: To access SecureX using the ribbon feature, click the ribbon at the bottom of any FMC page and follow the provided steps.

- **Q: Can I view event data in Cisco SecureX Threat Response?**

A: Yes, you can view event data in Cisco SecureX Threat Response by signing in as prompted.

- **Q: How can I investigate events using web-based resources?**

A: To investigate events using web-based resources, sign in to Cisco SecureX Threat Response and use the contextual cross-launch feature to find relevant information.

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 about SecureX, see <http://www.cisco.com/c/en/us/products/security/securex.html>.
- To integrate Firepower with SecureX, see the Firepower and SecureX Integration Guide at <https://cisco.com/go/firepower-securex-documentation>.

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 Firepower and SecureX Integration Guide at <https://cisco.com/go/firepower-securex-documentation>.
- 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 SecureX threat response

Cisco SecureX threat response was formerly known as Cisco Threat Response (CTR.) Rapidly detect, investigate, and respond to threats using Cisco SecureX threat response, the integration platform in the Cisco Cloud that lets you analyze incidents using data aggregated from multiple products, including Firepower.

- For general information about Cisco SecureX threat response, see:
<https://www.cisco.com/c/en/us/products/security/threat-response.html>.
- For detailed instructions for integrating Firepower with Cisco SecureX threat response, see:
- The Firepower and Cisco SecureX threat response Integration Guide at <https://cisco.com/go/firepower-ctr-integration-docs>.

View Event Data in Cisco SecureX threat response

Before you begin

- Set up the integration as described in the Firepower and Cisco SecureX threat response Integration Guide at <https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html>.
- Review the online help in Cisco SecureX threat response to learn how to find, investigate, and take action on threats.
- You will need your credentials to access Cisco SecureX threat response.

Procedure

Step 1

In Firepower Management Center, do one of the following:

- To pivot to Cisco SecureX threat response from a specific event:
 - Navigate to a page under the Analysis > Intrusions menu that lists a supported event.
 - Right-click a source or destination IP address and select View in SecureX.
- To view event info generally:
 - Navigate to System > Integrations > Cloud Services.
 - Click the link to view events in Cisco SecureX threat response.

Step 2

Sign in to Cisco SecureX threat response as prompted.

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.

- 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.

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 Cisco Security Analytics and Logging (On Premises).
- See Requirements for Custom Contextual Cross-Launch Resources.
- 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), 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.
 - So, for example, to get threat intelligence from Cisco Talos about a source IP address in the Top Attackers dashboard widget, 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 Firepower to related data in your Secure Network Analytics appliance.
- For more information about the Secure Network Analytics product, see <https://www.cisco.com/c/en/us/products/security/security-analytics-logging/index.html>.
- For general information about contextual cross-launching, see Investigate Events Using Contextual Cross-Launch.
- Use this procedure to quickly configure a set of cross-launch links to your Secure Network Analytics appliance.

Note

- If you need to make changes to 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, but those links would be independent of the auto-created resources and would thus need to be manually managed (deleted, updated, etc.)

Before you begin

- You must have a deployed and running Secure Network Analytics appliance.
- If you want to send Firepower data to your Secure Network Analytics appliance using Cisco Security Analytics and Logging (On Premises), see Remote Data Storage on a Secure Network Analytics Appliance.

Procedure

- Step 1 Select System > Logging > Security Analytics & Logging.

- Step 2 Enable the feature.
- Step 3 Enter the hostname or IP address, and port, of your Secure Network Analytics appliance. The default port is 443.
- Step 4 Click Save.
- Step 5 Verify your new cross-launch links: Select Analysis > Advanced > Contextual Cross-launch. If you need to make changes, return to this procedure; you cannot make changes directly on the contextual cross-launch listing page.

What to do next

- To cross-launch from an event into the Secure Network Analytics event viewer, you will need your Secure Network Analytics credentials.
- 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.
- 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 Stealthwatch Management Console, etc.

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

In order to configure the system to send security event syslogs, you will need to know the following:

- Best Practices for Configuring Security Event Syslog Messaging
- Configuration Locations for Security Event Syslogs
- FTD Platform Settings That Apply to Security Event Syslog Messages
- If you make changes to syslog settings in any policy, you must redeploy for 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"> 1. Configure FTD platform settings (Devices > Platform Settings > Threat Defense Settings > Syslog.) <p>See also FTD Platform Settings That Apply to Security Event Syslog Messages.</p> <ol style="list-style-type: none"> 2. In your access control policy Logging tab, opt to use the FTD platform settings. 3. (For intrusion events) Configure intrusion policies to use the settings in your access control policy Logging tab. (This is the default.) <p>Overriding any of these settings is not recommended.</p> <p>For essential details, see Send Security Event Syslog Messages from FTD Devices.</p>
All other devices	<ol style="list-style-type: none"> 1. Create an alert response. 2. Configure access control policy Logging to use the alert response. 3. (For intrusion events) Configure syslog settings in intrusion policies. <p>For complete details, see Send Security Event Syslog Messages from Classic Devices.</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-related connection, intrusion, file, and malware events) from Firepower Threat Defense devices.

Note


Many Firepower Threat Defense syslog settings are not applicable to security events. Configure only the options described in this procedure.

Before you begin

- In FMC, 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 Firepower Threat Defense device:
 - Click **Devices > Platform Settings**.
 - Edit the platform settings policy associated with your Firepower Threat Defense device.

- In the left navigation pane, click Syslog.
- Click Syslog Servers and click Add to enter server, protocol, interface, and related information. If you have questions about options on this page, see Configure a Syslog Server.
- Click Syslog Settings and configure the following settings:
 - Enable Timestamp on Syslog Messages
 - Timestamp Format
 - Enable Syslog Device ID
- Click Logging Setup.
- Select whether or not to Send syslogs in EMBLEM format.
- Save your settings.
- Step 2 Configure general logging settings for the access control policy (including file and malware logging):
 - Click Policies > Access Control.
 - Edit the applicable access control policy.
 - Click Logging.
 - Select FTD 6.3 and later: Use the syslog settings configured in the FTD Platform Settings policy deployed on the device.
 - (Optional) Select a Syslog Severity.
 - If you will send file and malware events, select Send Syslog messages for File and Malware events.
 - Click Save.
- Step 3 Enable logging for Security-related connection 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 the Rules tab.
 - Click 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 will log file events, select Log Files.
 - Enable Syslog Server.
 - Verify that the rule is “Using default syslog configuration in Access Control Logging.”
 - Click Add.
 - Repeat for each rule in the policy.
- Step 5 If you will send intrusion events:
 - Navigate to the intrusion policy associated with your access control policy.
 - In your intrusion policy, click Advanced Settings > Syslog Alerting > 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. For descriptions, see Syslog Alert Facilities.
Severity	This setting is applicable only if you specify a Logging Host on this page. For descriptions, see Syslog Severity Levels.

- 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).
 - 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.
- 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:
 - Click Policies > Access Control.
 - Edit the applicable access control policy.
 - Click Logging.
 - Select Send using specific syslog alert.

- Select the Syslog Alert you created above.
- Click Save.
- Step 3 If you will send file and malware events:
 - Select Send Syslog messages for File and Malware events.
 - Click Save.
- Step 4 If you will send intrusion events:
 - Navigate to the intrusion policy associated with your access control policy.
 - In your intrusion policy, click Advanced Settings > Syslog Alerting > 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. See Syslog Alert Facilities.
Severity	This setting is applicable only if you specify a Logging Host on this page. See Syslog Severity Levels.

- Click Back.
- Click Policy Information in the left navigation pane.
- 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). 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.

Configuration Locations for Security Event Syslogs

- Configuration Locations for Syslogs for Connection and Security Intelligence Events (All Devices)¹²
- Configuration Locations for Syslogs for Intrusion Events (FTD Devices)
- Configuration Locations for Syslogs for Intrusion Events (Devices Other than FTD)
- Configuration Locations for Syslogs for File and Malware Events





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
Devices > Platform Settings , Threat Defense Settings policy, Syslog	<p>This option applies only to Firepower Threat Defense 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 FTD Platform Settings That Apply to Security Event Syslog Messages and About Syslog and subtopics.</p>
Policies > Access Control , <each policy>, Logging	<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 FTD Platform Settings. For information, see FTD Platform Settings That Apply to Security Event Syslog Messages and About Syslog and subtopics.</p> <p>Required setting for all other devices: Use a syslog alert.</p> <p>If you specify a syslog alert, see Creating a Syslog Alert Response.</p> <p>For more information about the settings on the Logging tab, see Logging Settings for Access Control Policies.</p>

Policies > Access Control , <each policy>, Rules , Default Action row, Logging ()	<p>Logging settings for the default action associated with an access control policy.</p> <p>See information about logging in the Access Control Rules chapter and Logging Connections with a Policy Default Action.</p>
Policies > Access Control , <each policy>, Rules , <each rule>, Logging	<p>Logging settings for a particular rule in an access control policy.</p> <p>See information about logging in the Access Control Rules chapter.</p>
Policies > Access Control , <each policy>, Security Intelligence , Logging ()	<p>Logging settings for Security Intelligence Block lists. Click these buttons to configure:</p> <ul style="list-style-type: none"> • DNS Block List Logging Options • URL Block List Logging Options • Network Block List Logging Options (for IP addresses on the blocked list) <p>See Configure Security Intelligence, including the prerequisites section, and subtopics and links.</p>
Policies > SSL , <each policy>, Default Action row, Logging ()	<p>Logging settings for the default action associated with an SSL policy.</p> <p>See Logging Connections with a Policy Default Action.</p>
Policies > SSL , <each policy>, <each rule>, Logging	<p>Logging settings for SSL rules.</p> <p>See TLS/SSL Rule Components.</p>
Policies > Prefilter , <each policy>, Default Action row, Logging ()	<p>Logging settings for the default action associated with a prefilter policy.</p> <p>See Logging Connections with a Policy Default Action.</p>
Policies > Prefilter , <each policy>, <each prefilter rule>, Logging	<p>Logging settings for each prefilter rule in a prefilter policy.</p> <p>See Tunnel and Prefilter Rule Components</p>
Policies > Prefilter , <each policy>, <each tunnel rule> , Logging	<p>Logging settings for each tunnel rule in a prefilter policy.</p> <p>See Tunnel and Prefilter Rule Components</p>
Additional syslog settings for FTD cluster configurations:	<p>The Clustering for the Firepower Threat Defense chapter has multiple references to syslog; search the chapter for “syslog.”</p>

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 FTD Platform Settings or both.

Configuration Location	Description and More Information
Devices > Platform Settings , Threat Defense Settings policy, Syslog	<p>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.</p> <p>See FTD Platform Settings That Apply to Security Event Syslog Messages and About Syslog and subtopics.</p>
Policies > Access Control , <each policy>, Logging	<p>Default setting for syslog destination for intrusion events, if the intrusion policy does not specify other logging hosts.</p> <p>See Logging Settings for Access Control Policies.</p>
Policies > Intrusion , <each policy>, Advanced Settings , enable Syslog Alerting , click Edit	<p>To specify syslog collectors other than the destinations specified in the access control policy Logging tab, and to specify facility and severity, see Configuring Syslog Alerting for Intrusion Events.</p> <p>If you want to use the Severity or Facility 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.</p>

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

- (Default) Access control policy Logging Settings for Access Control Policies, 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
<p>In an access control policy:</p> <p>Policies > Access Control, <each policy>, Logging</p>	<p>This is the main location for configuring the system to send syslogs for file and malware events.</p> <p>If you do not use the syslog settings in FTD Platform Settings, you must also create an alert response. See Creating a Syslog Alert Response.</p>

Configuration Location	Description and More Information
<p>In Firepower Threat Defense Platform Settings:</p> <p>Devices > Platform Settings, Threat Defense Settings policy, Syslog</p>	<p>These settings apply only to Firepower Threat Defense devices running supported versions, and only if you configure the Logging tab in the access control policy to use FTD platform settings.</p> <p>See FTD Platform Settings That Apply to Security Event Syslog Messages and About Syslog and subtopics.</p>
<p>In an access control rule:</p> <p>Policies > Access Control, <each policy>, <each rule>, Logging</p>	<p>If you do not use the syslog settings in FTD Platform Settings, you must also create an alert response. See Creating a Syslog Alert Response.</p>

Anatomy of Security Event Syslog Messages

Example security event message from FTD (Intrusion Event)

0	1	2	3	4	5	6
<pre> <37>2018-06-27 192.168.0.81 <u>SFIMS</u> : %FTD-5-43000 192.168.1.10, DstIP: 192.168.1.102, SrcPort: 339 Protocol: tcp, Priority: 2, GID: 133, SID: 17, R Message: "DCE2_EVENT SMB_INVALID_DSIZE", Classi Potentially Bad Traffic, User: No Authentication Client: NetBIOS-ssn (SMB) client, ApplicationPro (SMB), ACPolicy: test, NAPPolicy: Balanced Secur Connectivity, InlineResult: Blocked </pre>						

Table 1: Components of Security Event Syslog Messages

Item Number in Sample Message	Header Element	Description
0	PRI	<p>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</p> <p>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 Enable Logging and Configure Basic Settings. For information on PRI, see RFC 5424.</p>
1	Timestamp	<p>Date and time the syslog message was sent from the device.</p> <ul style="list-style-type: none"> (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 FTD 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. (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. Otherwise, it is the month, day, and time in UTC time zone, though the time zone is not indicated. <p>To configure the timestamp setting in FTD Platform Settings, see Configure Syslog Settings.</p>
2	<p>Device or interface from which the message was sent.</p> <p>This can be:</p> <ul style="list-style-type: none"> IP address of the interface Device hostname Custom device identifier 	<p>(For syslogs sent from FTD devices)</p> <p>If the syslog message was sent using the FTD Platform Settings, this is the value configured in Syslog Settings for the Enable Syslog Device ID option, if specified.</p> <p>Otherwise, this element is not present in the header.</p> <p>To configure this setting in FTD Platform Settings, see Configure Syslog Settings.</p>

3	Custom value	<p>If the message was sent using an alert response, this is the Tag value configured in the alert response that sent the message, if configured. (See Creating a Syslog Alert Response.)</p> <p>Otherwise, this element is not present in the header.</p>
4	%FTD %NGIPS	<p>Type of device that sent the message.</p> <ul style="list-style-type: none"> • %FTD is Firepower Threat Defense • %NGIPS is all other devices
5	Severity	<p>The severity specified in the syslog settings for the policy that triggered the message.</p> <p>For severity descriptions, see Severity Levels or Syslog Severity Levels.</p>
6	Event type identifier	<ul style="list-style-type: none"> • 430001: Intrusion event • 430002: Connection event logged at beginning of connection • 430003: Connection event logged at end of connection • 430004: File event • 430005: File malware event
—	Facility	See Facility in Security Event Syslog Messages
—	Remainder of message	<p>Fields and values separated by colons.</p> <p>Fields with empty or unknown values are omitted from messages. For field descriptions, see:</p> <ul style="list-style-type: none"> • Connection and Security Intelligence Event Fields. • Intrusion Event Fields • File and Malware Event Fields <p>Note Field description lists include both syslog fields and fields visible in the event viewer (menu options under the Analysis menu in the Firepower Management Center 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 FTD Platform Settings. Facility is always ALERT for connection events when sending syslog messages using FTD Platform Settings.	Use the EMBLEM option in FTD 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.	Facility does not appear in the message header, but the syslog collector can derive the value based on RFC 5424, section 6.2.1.
		Enable syslog alerting and configure facility and severity on the intrusion policy. See Configuring Syslog Alerting for Intrusion Events.	
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	Stream Audit Logs to Syslog and the Auditing the System chapter
Audit logs from Classic devices (ASA FirePOWER, NGIPSv)	Stream Audit Logs from Classic Devices and the Auditing the System chapter CLI command: syslog
Device health and network-related logs from FTD devices	About Syslog and subtopics
Connection, security intelligence, and intrusion event logs from FTD devices	About Configuring the System to Send Security Event Data to Syslog.
Connection, security intelligence, and intrusion event logs from Classic devices	About Configuring the System to Send Security Event Data to Syslog
Logs for file and malware events	About Configuring the System to Send Security Event Data to Syslog

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. For more information, see Firepower System Event Streamer Integration Guide.
- 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
Intrusion Events	intrusion events generated by managed devices
Intrusion Event Packet Data	packets associated with intrusion events
Intrusion Event Extra Data	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
Discovery Events	Network discovery events
Correlation and Allow List Events	correlation and compliance allow list events
Impact Flag Alerts	impact alerts generated by the FMC
User Events	user events

Event Type	Description
Malware Events	malware events
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 eStreamer Server Streaming.
Some event data can be sent only from FMC. See Data Sent Only via eStreamer, Not via Syslog.	Includes data that cannot be sent via syslog directly from devices. See Data Sent Only via eStreamer, Not via Syslog.

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.
- 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.
 - 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 System Event Streamer 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.
- 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 (f.k.a. Firepower) app for Splunk (formerly known as the Cisco Firepower App for Splunk) as an external tool to display and work with Firepower event data, to hunt and investigate threats on your network.
- eStreamer is required. This is an advanced functionality. See eStreamer Server Streaming.
- For more information, see <https://cisco.com/go/firepower-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.
- 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	Version	Details
SecureX ribbon	7.0	<p>The SecureX ribbon pivots into SecureX for instant visibility into the threat landscape across your Cisco security products.</p> <p>To display the SecureX ribbon in FMC, see the Firepower and SecureX Integration Guide at https://cisco.com/go/firepower-securex-documentation.</p> <p>New/Modified screens: New page: System > SecureX</p>
Send all connection events to the Cisco cloud	7.0	<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 System > Integration > Cloud Services page</p>
Cross-launch to view data in Secure Network Analytics	6.7	<p>This feature introduces a quick way to create multiple entries for your Secure Network Analytics appliance on the Analysis > 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: System > Logging > Security Analytics and Logging New page to configure sending events to Secure Network Analytics.</p>


Contextual cross-launch from additional field types	6.7	<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"> • Access control policy • Intrusion policy • Application protocol • Client application • Web application • Username (including realm) <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	<p>IBM QRadar users can use a new Firepower-specific app to analyze their event data. Available functionality is affected by your Firepower version.</p> <p>See Event Analysis in IBM QRadar.</p>

Enhancements to integration with Cisco SecureX threat response	6.5	<ul style="list-style-type: none"> • Support for regional clouds: • United States (North America) • Europe <ul style="list-style-type: none"> • Support for additional event types: • File and malware events • High-priority connection events <p>These are connection events related to the following:</p> <ul style="list-style-type: none"> • Intrusion events • Security Intelligence events • File and malware events <p>Modified screens: New options on System > Integration > Cloud Services.</p> <p>Supported Platforms: All devices supported in this release, either via direct integration or syslog.</p>
Syslog	6.5	The AccessControlRuleName field is now available in intrusion event syslog messages.
Integration with Cisco Security Packet Analyzer	6.5	Support for this feature was removed.

Integration with Cisco SecureX threat response	6.3 (via syslog, using a proxy collector) 6.4 (direct)	<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 SecureX threat response.</p> <p>Modified screens (version 6.4): New options on System > Integration > Cloud Services. 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	<p>Fully-qualified file and malware event data can now be sent from managed devices via syslog. Modified screens: Policies > Access Control > Access Control > Logging.</p> <p>Supported Platforms: All managed devices running version 6.4.</p>
Integration with Splunk	Supports all 6.x versions	<p>Splunk users can use a new, separate Splunk app, Cisco Secure Firewall (f.k.a. Firepower) app for Splunk, to analyze events.</p> <p>Available functionality is affected by your Firepower version. See Event Analysis in Splunk.</p>
Integration with Cisco Security Packet Analyzer	6.3	<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>System > Integration > Packet Analyzer Analysis > Advanced > Packet Analyzer Queries</p> <p>New menu options: Query Packet Analyzer 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	<p>Feature introduced: Right-click an event to look up related information in predefined or custom URL-based external resources.</p> <p>New screens: Analysis > Advanced > Contextual Cross-Launch</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 f or connection and intrusion events	6.3	<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"> • All new functionality: FTD devices running version 6.3. • Some new functionality: Non-FTD devices running version 6.3. • Less new functionality: All devices running versions older than 6.3. <p>For more information, see the topics under About Sending Syslog Messages for Security Events.</p>
eStreamer	6.3	Moved eStreamer content from the Host Identity Sources chapter to this chapter and added a summary comparing eStreamer to syslog.

Documents / Resources

	<p>Cisco Event Analysis Using External Tools [pdf] User Guide</p> <p>Event Analysis Using External Tools, Event, Analysis Using External Tools, Using External Tools, External Tools</p>
-------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

References

- [User Manual](#)