Event Analysis Using External Tools

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.

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.

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.

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 3.

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

- See Requirements for Custom Contextual Cross-Launch Resources, on page 2.
- 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.

About Sending Syslog Messages for Connection and Intrusion Events

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

These events may also be referred in this documentation to as "security events."

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

About Configuring the System to Send Connection and Intrusion 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, on page 5
- Configuration Locations for Security Event Syslogs, on page 9
- 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 version 6.3 or later	**1.** Configure FTD platform settings (**Devices** > **Platform Settings** > **Threat Defense Settings** > **Syslog**.) See also FTD Platform Settings That Apply to Security Event Syslog Messages. **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.) Overriding any of these settings is not recommended. For essential details, see Send Security Event Syslog Messages from FTD Devices, on page 6.
All other devices	**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. For complete details, see Send Security Event Syslog Messages from Classic Devices, on page 8.

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:

a) Click **Devices** > **Platform Settings**.

b) **Edit** the platform settings policy associated with your Firepower Threat Defense 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 Configure a Syslog Server.

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) Select whether or not to **Send syslogs in EMBLEM format**.

h) **Save** your settings.

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

a) Click **Policies** > **Access Control**.

b) Edit the applicable access control policy.

c) Click **Logging**.

d) Select **FTD 6.3 and later: Use the syslog settings configured in the FTD Platform Settings policy deployed on the device**.

e) (Optional) Select a **Syslog Severity**.

f) If you will send file and malware events, select **Send Syslog messages for File and Malware events**.

g) Click **Save**.

Step 3 Enable logging for Security-related connection events for the access control policy:

a) In the same access control policy, click the **Security Intelligence** tab.

b) 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**.

c) Click **Save**.

Step 4 Enable syslog logging for each rule in the access control policy:

a) In the same access control policy, click the **Rules** tab.

b) Click a rule to edit.

c) Click the **Logging** tab in the rule.

d) 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.)

e) If you will log file events, select **Log Files**.

f) Enable **Syslog Server**.

g) Verify that the rule is "**Using default syslog configuration in Access Control Logging**."

h) Click **Add**.

i) Repeat for each rule in the policy.

Step 5 If you will send intrusion events:

a) Navigate to the intrusion policy associated with your access control policy.

b) In your intrusion policy, click **Advanced Settings** > **Syslog Alerting** > **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. 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.

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 policies and rules.

  See the applicable table rows in Configuration Locations for Syslogs for Connection and Security Intelligence Events (All Devices), on page 9.

  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 8.

- 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**.
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, click **Advanced Settings** > **Syslog Alerting** > **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. See Syslog Alert Facilities.
Severity	This setting is applicable only if you specify a Logging Host on this page. See Syslog Severity Levels.

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 9. 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 6.

Configuration Locations for Security Event Syslogs

- Configuration Locations for Syslogs for Connection and Security Intelligence Events (All Devices), on page 9
- Configuration Locations for Syslogs for Intrusion Events (FTD Devices Version 6.3+), on page 11
- Configuration Locations for Syslogs for Intrusion Events (Devices Other than FTD and Versions Earlier than 6.3), on page 12

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**	This option applies only to Firepower Threat Defense devices running version 6.3 or later. 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. See FTD Platform Settings That Apply to Security Event Syslog Messages and About Syslog and subtopics.
Policies > **Access Control**, <each policy>, **Logging**	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. Recommended setting for FTD devices running 6.3 or later: Use FTD Platform Settings. For information, see FTD Platform Settings That Apply to Security Event Syslog Messages and About Syslog and subtopics. Required setting for all other devices: Use a syslog alert. If you specify a syslog alert, see Creating a Syslog Alert Response. For more information about the settings on the Logging tab, see Logging Settings for Access Control Policies.
Policies > **Access Control**, <each policy>, **Rules**, **Default Action** row, **Logging** (□)	Logging settings for the default action associated with an access control policy. See information about logging in the Access Control Rules chapter and Logging Connections with a Policy Default Action.
Policies > **Access Control**, <each policy>, **Rules**, <each rule>, **Logging**	Logging settings for a particular rule in an access control policy. See information about logging in the Access Control Rules chapter.
Policies > **Access Control**, <each policy>, **Security Intelligence**, **Logging** (□)	Logging settings for Security Intelligence Block lists. Click these buttons to configure: • DNS Block List Logging Options • URL Block List Logging Options • Network Block List Logging Options (for IP addresses on the blocked list) See Configure Security Intelligence, including the prerequisites section, and subtopics and links.
Policies > **SSL**, <each policy>, **Default Action** row, **Logging** (□)	Logging settings for the default action associated with an SSL policy. See Logging Connections with a Policy Default Action.

Configuration Location	Description and More Information
Policies > **SSL**, <each policy>, <each rule>, **Logging**	Logging settings for SSL rules. See TLS/SSL Rule Components.
Policies > **Prefilter**, <each policy>, **Default Action** row, **Logging** (□)	Logging settings for the default action associated with a prefilter policy. See Logging Connections with a Policy Default Action.
Policies > **Prefilter**, <each policy>, <each prefilter rule>, **Logging**	Logging settings for each prefilter rule in a prefilter policy. See Tunnel and Prefilter Rule Components
Policies > **Prefilter**, <each policy>, <each tunnel rule> , **Logging**	Logging settings for each tunnel rule in a prefilter policy. See Tunnel and Prefilter Rule Components
Additional syslog settings for FTD cluster configurations:	The Clustering for the Firepower Threat Defense chapter has multiple references to syslog; search the chapter for "syslog."

Configuration Locations for Syslogs for Intrusion Events (FTD Devices Version 6.3+)

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**	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. See FTD Platform Settings That Apply to Security Event Syslog Messages and About Syslog and subtopics.
Policies > **Access Control**, <each policy>, **Logging**	Default setting for syslog destination for intrusion events, if the intrusion policy does not specify other logging hosts. See Logging Settings for Access Control Policies.
Policies > **Intrusion**, <each policy>, **Advanced Settings**, enable **Syslog Alerting**, click **Edit**	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. 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.

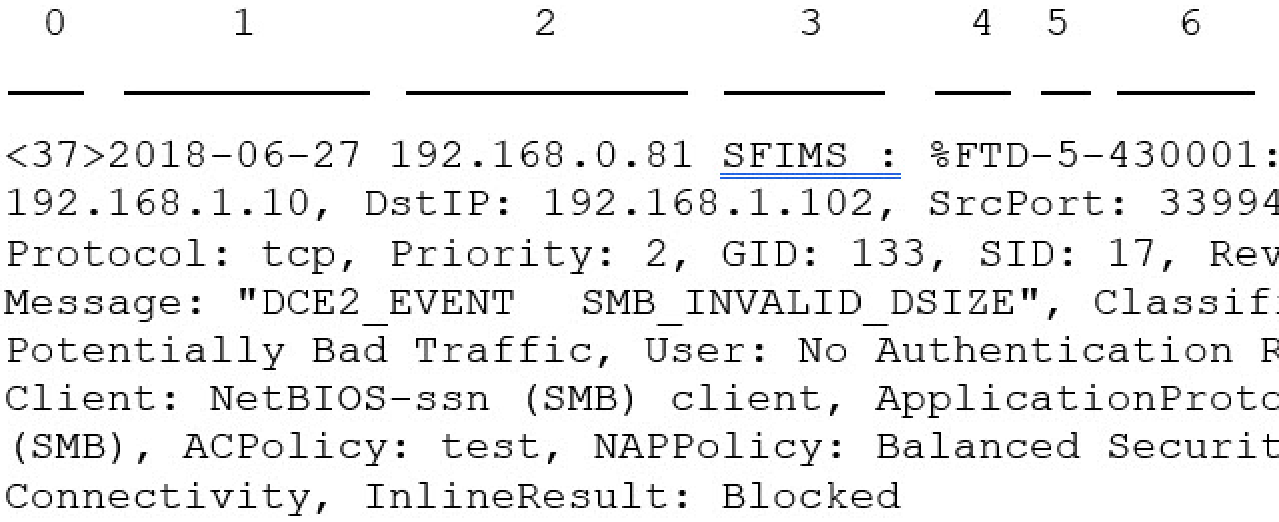
Configuration Locations for Syslogs for Intrusion Events (Devices Other than FTD and Versions Earlier than 6.3)

- (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 6.3 are not configured there, syslogs will not be sent for devices other than FTD 6.3 and no warning appears.

Anatomy of Connection and Intrusion Event Syslog Messages

Example security event message from FTD 6.3 and later (Intrusion Event)



```
<37>2018-06-27 192.168.0.81 SFIMS : %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, ApplicationProtc
(SMB), ACPolicy: test, NAPPolicy: Balanced Securit
Connectivity, InlineResult: Blocked
```

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 Enable Logging and Configure Basic Settings. For information on PRI, see RFC5424.

Item Number in Sample Message	Header Element	Description
1	Timestamp	Date and time the syslog message was sent from the device. • (Syslogs sent from FTD devices running version 6.3 or later) 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 running version 6.3 or later) 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. To configure the timestamp setting in FTD Platform Settings, see Configure Syslog Settings.
2	Device or interface from which the message was sent. This can be: • IP address of the interface • Device hostname • Custom device identifier	(For syslogs sent from FTD devices version 6.3 and later only) 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. Otherwise, this element is not present in the header. To configure this setting in FTD Platform Settings, see Configure Syslog Settings.
3	Custom value	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.) Otherwise, this element is not present in the header.
4	%FTD %NGIPS	Type of device that sent the message. • %FTD is Firepower Threat Defense running version 6.3 or later • %NGIPS is all other devices running version 6.3 or later • For messages sent from devices running version 6.2.3 or earlier, this element is not present.

Item Number in Sample Message	Header Element	Description
5	Severity	The severity specified in the syslog settings for the policy that triggered the message. For severity descriptions, see Severity Levels or Syslog Severity Levels.
6	Event type identifier	For messages sent from devices running version 6.3 or later: • 430001: Intrusion event • 430002: Connection event logged at beginning of connection • 430003: Connection event logged at end of connection For messages sent from devices running version 6.2.3 or earlier, an event type identifier is not present.
--	Facility	See Facility in Security Event Syslog Messages, on page 14.
--	Remainder of message	Fields and values separated by colons. Fields with empty or unknown values are omitted from messages. For field descriptions, see: • Connection and Security Intelligence Event Fields. • Intrusion Event Fields **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. 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.

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 6.3 and later	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. Enable syslog alerting and configure facility and severity on the intrusion policy. See Configuring Syslog Alerting for Intrusion Events.	Facility does not appear in the message header, but the syslog collector can derive the value based on RFC 5424, section 6.2.1.
Pre-6.3 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.	
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 (7000/8000 series, 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 Connection and Intrusion Event Data to Syslog, on page 5.

Syslog Data Type	See
Connection, security intelligence, and intrusion event logs from Classic devices	About Configuring the System to Send Connection and Intrusion Event Data to Syslog, on page 5

eStreamer Server Streaming

The Event Streamer (eStreamer) allows you to stream several kinds of event data from a Firepower Management Center or 7000 or 8000 Series device 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	Available on FMC	Available on 7000 & 8000 Series Devices
Intrusion Events	intrusion events generated by managed devices	yes	yes
Intrusion Event Packet Data	packets associated with intrusion events	yes	yes
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	yes	yes
Discovery Events	Network discovery events	yes	no
Correlation and White List Events	correlation and white list events	yes	no
Impact Flag Alerts	impact alerts generated by the FMC	yes	no
User Events	user events	yes	no
Malware Events	malware events	yes	no
File Events	file events	yes	no

Event Type	Description	Available on FMC	Available on 7000 & 8000 Series Devices
Connection Events	information about the session traffic between your monitored hosts and all other hosts.	yes	yes

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 connection events (including security intelligence events) and intrusion events.	Support for all event types listed in eStreamer Server Streaming, on page 16.
Some event data can be sent only from FMC. See Data Sent Only via eStreamer, Not via Syslog, on page 17.	Includes data that cannot be sent via syslog directly from devices. See Data Sent Only via eStreamer, Not via Syslog, on page 17.

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 16.
- Statistics and aggregate events
- Network Discovery events
- User activity and login events
- Correlation events
- File and malware events
- The following fields:

    - Impact and ImpactFlag fields

      For a description, see eStreamer Server Streaming, on page 16.

    - 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 and 7000 & 8000 Series devices.

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 16.

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 and 7000 & 8000 Series devices.

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 Investigation Using Cisco Security Packet Analyzer

If your organization has deployed Cisco Security Packet Analyzer (a separate product from your Firepower system), you can use Cisco Security Packet Analyzer to gather context, in the form of full packet captures, around incidents and suspicious events that your Firepower system detects.

You can instantly query multiple Cisco Security Packet Analyzer instances from events in the Firepower Management Center, then view and work with the results in Cisco Security Packet Analyzer, or download the results to perform timeline analysis using other tools such as Wireshark (TM).

The Cisco Security Packet Analyzer and the Firepower Management Center are deployed independently of each other, and the Cisco Security Packet Analyzer deployment is unaware of the Firepower system. Captured data is not moved between packet analyzers and the management center.

Requirements for the Packet Analyzer Deployment

When you deploy your Cisco Security Packet Analyzer instances, keep the following points in mind:

- You can register up to 500 Cisco Security Packet Analyzer instances to your Firepower Management Center. Each packet analyzer instance in a stack must be individually registered.
- For supported Cisco Security Packet Analyzer models and versions for this integration, see the *Cisco Firepower Compatibility Guide* at https://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html.
- Packet analyzer instances that you use with the Firepower system should generally be dedicated to this purpose, unless a single capture session can serve separate purposes simultaneously and queries will not overwhelm the deployment.
- Cisco Security Packet Analyzer must be able to capture the traffic you want to analyze, and the packet analyzer instances and your Firepower managed devices must see the same traffic.
- Your Firepower Management Center must be able to reach each packet analyzer on the network.
- To set up your packet analyzer instances and complete the prerequisites for this deployment, use the Cisco Security Packet Analyzer documentation at https://www.cisco.com/c/en/us/support/security/security-packet-analyzer/tsd-products-support-series-home.html and the online help in the packet analyzer.
- Each packet analyzer must synchronize time using the same NTP server as the Firepower Management Center and its managed devices.
- On each packet analyzer:
    - Web access to the packet analyzer must be enabled.
    - You need the following accounts with Capture Query privileges:
        - A user account that the Firepower Management Center will use when submitting queries to the packet analyzer.
        - User accounts for yourself and others who will view query results in the packet analyzer.

      See the Cisco Security Packet Analyzer documentation for restricted characters in Web User passwords.

      Tip: Test these account credentials on the packet analyzer to be sure they work.
    - You must be able to successfully run queries in the packet analyzer web interface.
    - Complete the capture session requirements described in Requirements and Recommendations for the Packet Analyzer Capture Session, on page 21.

  For instructions for these tasks, see the documentation for your packet analyzer.

Requirements and Recommendations for the Packet Analyzer Capture Session

- You must create a capture session on each Cisco Security Packet Analyzer instance.
- Each packet analyzer instance should have only one capture session configured.
- The default capture session name in the Firepower Management Center registration form is **`firepower_rolling_capture`**. For simplicity, use this capture session name on all packet analyzer instances unless you have reason to use a different name.
- Remaining values should be the following:

Option	Value
Packet Slice Size	Zero (0), to capture complete packets
Storage Type	File
Disk Utilization (%)	80
File Size (MB)	The maximum for your packet analyzer model, for best performance (either 2000 or 500)
Rotate Files	Selected, to enable a rolling capture
All others	Values that work in your deployment

- The capture session must be running before anyone can query against it. After you've saved the session, go to the **Capture Sessions** page, select the capture session and click **Start**.

Register Packet Analyzer Instances

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	Any	Any	Admin/Security Analyst

In a multidomain deployment, you can create, modify, or delete Cisco Security Packet Analyzer instances for the current domain only. You can run queries on, and view query results for, packet analyzer instances in the current domain and any descendant domains. A single packet analyzer instance can be registered to multiple domains.

Before you begin

- Your Cisco Security Packet Analyzer deployment must be installed, configured, and working properly to capture the packets you want to analyze, according to the guidelines in Requirements for the Packet Analyzer Deployment, on page 20.
- Each packet analyzer instance must have a single capture session that meets the guidelines in Requirements and Recommendations for the Packet Analyzer Capture Session, on page 21.
- For each packet analyzer that you will register, gather the following:
  - hostname or IP address

- port
- credentials for the user account that the Firepower Management Center will use to connect
- capture session name

Procedure

Step 1 Select **System** > **Integration**.

Step 2 Click **Packet Analyzers**.

Step 3 Click **New**.

Step 4 Complete the form with the values that you gathered in the prerequisites for this procedure.

The capture session name must match the name of the capture session configured on the packet analyzer.

If the packet analyzer does not present a CA-signed certificate, disable **Verify SSL/TLS certificate**.

Step 5 Click **Save**.

The system immediately tests the connection and validates the capture session.

Step 6 Repeat for each packet analyzer instance.

What to do next

If you have not yet done so, start the capture session on each packet analyzer instance.

Query Packet Analyzers

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	Any	Any	Admin/Any Security Analyst

You can query up to 500 Cisco Security Packet Analyzer instances at a time, using a single query with parameters that are automatically populated based on a specific event.

Tip To run a query that is not based on a specific event, select **Analysis** > **Advanced** > **Packet Analyzer Queries**, then click **New Query**.

Procedure

Step 1 Navigate to one of the following pages in the Firepower Management Center that shows events including data of a type included in packet captures:

- 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 an event and choose **Query Packet Analyzer**.

Available event data pre-populates the query form.

The time window on the event or dashboard page determines the default start and end times of the query.

Step 3 Enter a name for this query, such as the number of the ticket you are investigating.

Step 4 Edit the query parameters as desired.

For example, you might want to extend the time window by 30 seconds or a few minutes to capture more packets around the event.

Queries without both a start time and an end time will take a long time to complete.

Fields marked with an asterisk require a value.

If you increase the **Split Pcaps At** value, make sure the file size you enter is supported by all selected packet analyzer instances and by any other tools in which you will work with the query results. This option is the **Max PCAP File Size** option in the packet analyzer's own query dialog.

If you edit the query string in the Filter Preview, work carefully; syntax is not validated.

Step 5 Select the packet analyzer instances to query.

In a multidomain deployment, you can include Cisco Security Packet Analyzer instances from the current domain and from any descendant domains.

Step 6 Click **Query**.

What to do next

Check for status and results of your query. See View Packet Analyzer Query Status, on page 23 and View Packet Analyzer Query Results, on page 24.

View Packet Analyzer Query Status

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	Any	Any	Admin/Any Security Analyst

On the query status page, each table row summarizes the status of each query across all Cisco Security Packet Analyzer instances, and you can expand the row to see results for individual instances.

In a multidomain deployment, you can view packet analyzer query status and results only for the current domain and for any descendant domains.

Procedure

Step 1 Do one of the following:

- Click Message Center in the menu bar at the top of the window, then click **Tasks**. Look for a **Query Packet Analyzers** task, then click **View Details** or **View Results**.
- Select **Analysis** > **Advanced** > **Packet Analyzer Queries**.

Step 2 Determine the status of your query:

The **Status** column shows the number of packet analyzer instances on which the query succeeded and the number of instances on which it failed. Hover over the instances to see the specific status.

The **Duration** column shows how long it took for the query to complete or fail.

Duration is impacted by the specificity of the query, network conditions, and so on.

Step 3 Do one of the following:

- View query results. See View Packet Analyzer Query Results, on page 24.
- Determine which packet analyzer instances failed or took too long to complete the query: Click the caret to expand the query row, then look for failed instances or unusually long durations.
- Troubleshoot issues or an unexpected status. See Troubleshoot Packet Analyzer Queries, on page 25.
- Cancel a query that is in progress, or cancel a query on an individual packet analyzer instance. Cancelling also cancels the query on the packet analyzer.
- Delete a completed or failed query, or a query on an individual packet analyzer instance. Deleting a query does not delete the captured data on the packet analyzer.

Step 4 To update the results on this page, reload the page.

View Packet Analyzer Query Results

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	Any	Any	Admin/Any Security Analyst

You can view and analyze the packets that match your query in Cisco Security Packet Analyzer, or download the packets to view and analyze them in another tool.

In a multidomain deployment, you can view packet analyzer query results only for the current domain and for any descendant domains.

Before you begin

Make sure you have Cisco Security Packet Analyzer user account credentials that will allow you to access the packet analyzer instances that hold the query results you want to view.

Procedure

Step 1 Select **Analysis** > **Advanced** > **Packet Analyzer Queries**.

Step 2 Click the caret to expand the row that corresponds to your query.

Step 3 Look for one or more packet analyzer instances that show the following: **Download** (⬇) **Open Link**

No results indicates that there were no packets on that packet analyzer instance that matched the query.

If you don't see the results you expect, see Troubleshoot Packet Analyzer Queries, on page 25.

Step 4 Do one of the following:

a) To view and work with the captured packets in the Cisco Security Packet Analyzer, click the **Open Link**.

b) To download a PCAP file so you can view it in a third-party packet analysis tool, click **Download** (⬇).

The packet analyzer instance will open in a separate web browser window and request your credentials.

Step 5 Sign in to the packet analyzer.

Step 6 Return to the Firepower Management Center and click download or open link again.

Step 7 Work with the captured packets in your preferred application or tool. For example, in the Cisco Security Packet Analyzer, you might decode the captured packets and then perform tasks like private key decryption and file extraction to see what was transferred.

Troubleshoot Packet Analyzer Queries

No query results

Possible causes and solutions:

- The capture session is not running on the packet analyzer. If this is the cause of the problem, there is no data for the event you are querying. To enable packet collection for future events, start the capture session on the packet analyzer.
- The query time window is outside the time window of the captured files, or the capture session has been overwritten.
- The packet analyzer(s) are not capturing the right packets.
- The capture session file with the relevant data is still being written to the buffer. You cannot query a session until writing to the file is complete. Wait a few minutes and then try again.
- See also troubleshooting information in the *Cisco Security Packet Analyzer User Guide* at https://www.cisco.com/c/en/us/support/security/security-packet-analyzer/products-user-guide-list.html.

Queries are taking too long

- Only one query can run at a time on each packet analyzer; if there are several queries queued ahead of a particular query, the query will take longer to complete. If there is more than one source of queries, there is still a single queue.
- Queries that do not specify both start and end time take significantly longer to process.
- The greater the duration between the start and end times, the longer it will take for the system to complete the search.

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, on page 16.

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, on page 16.

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
Integration with IBM QRadar	6.0 and later	IBM QRadar users can use a new Firepower-specific app to analyze their event data. Available functionality is affected by your Firepower version. See Event Analysis in IBM QRadar, on page 26.
Integration with Splunk	Supports all 6.x versions	Splunk users can use a new, separate Splunk app, Cisco Secure Firewall (f.k.a. Firepower) app for Splunk, to analyze events. Available functionality is affected by your Firepower version. See Event Analysis in Splunk, on page 26.
Integration with Cisco Security Packet Analyzer	6.3	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. New screens: **System** > **Integration** > **Packet Analyzer** **Analysis** > **Advanced** > **Packet Analyzer Queries** 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. Supported platforms: Firepower Management Center

Feature	Version	Details
Contextual cross-launch	6.3	Feature introduced: Right-click an event to look up related information in predefined or custom URL-based external resources. New screens: **Analysis** > **Advanced** > **Contextual Cross-Launch** New menu options: Multiple options when right-clicking on an event on Dashboard pages and even tables on pages under the Analysis menu. Supported platforms: Firepower Management Center
Syslog messages for connection and intrusion events	6.3	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. Supported Platforms: • 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. For more information, see the topics under About Sending Syslog Messages for Connection and Intrusion Events, on page 4 and subtopics.
eStreamer	6.3	Moved eStreamer content from the Host Identity Sources chapter to this chapter and added a summar comparing eStreamer to syslog.