TECHNICAL
DOCUMENTATION

Illumio and Palo Alto Networks Integration Guide

This guide describes how to implement the Illumio and Palo Alto Networks integration.

Table of Contents

About the Illumio and Palo Alto Networks Next-Generation Firewall (NGFW) Integration

The Illumio integration with Palo Alto Networks NGFW allows organizations to collect and analyze firewall logs to enhance visibility, drive segmentation decisions, and improve their security posture. This integration combines Palo Alto Networks' native log-export capabilities and Illumio's real-time traffic visibility to allow security teams to make data-driven policy decisions.

There are two supported methods to send Palo Alto Networks logs to Illumio: directly from Palo Alto Networks or from Cribl.

NOTE

You must enable syslog monitoring for both methods of sending Palo Alto Networks logs.

Forward logs directly from the Palo Alto Networks Panorama instance to the Illumio Syslog Service using mTLS and then onboard these logs using the Log Exporter.

For customers who are using Cribl, you have the option to send logs directly from Cribl to the Illumio-hosted Azure Event Hub. The Cribl method is supported for only select customers, so contact Illumio Support if you want to use this method. See Enable Cribl to Send Palo Alto Networks Firewall Logs to Azure Event Hub [9].

Prerequisites for the Illumio and Palo Alto Networks NGFW Integration

To onboard Palo Alto networks, take the following actions to make sure that logs are properly formatted, aggregated, enriched, and securely transmitted:

- ☐ You must have a Palo Alto Networks Panorama account with administrator credentials to be able to log into Panorama to configure the syslog server.
- ☐ You must configure each individual firewall to send logs to Panorama and you must ensure that the necessary network connectivity exists to successfully integrate with the Illumio HAProxy service. To generate and export Common Event Format (CEF) logs from Palo Alto Networks Panorama to a syslog server, you must configure a log-forwarding profile and a syslog server profile.

NOTE

As part of the onboarding process, Illumio provides a CEF configuration format that includes the Tenant ID.

Performing all of these tasks makes sure that the Palo Alto Networks logs flow into the Illumio application in a secure and structured manner so that you can view the log data and create enforcement policies.

Configure Syslog Monitoring

For information about how to configure syslog monitoring, see the Palo Alto Networks documentation: Configure Syslog Monitoring.

Onboard the Palo Alto Networks Connector with the Log Exporter

To ingest Palo Alto Networks firewall logs, you must first onboard the Palo Alto Networks Connector using the Log Exporter.

IMPORTANT
Do not add the API Connector until after you have successfully onboarded the Palo Alto Networks integration using the Log Exporter.

1. Navigate to the **Connectors** page and click **+ Add** on the **Palo Alto Networks Connector** tile.
2. On the **Palo Alto Networks Connector** page, click **+ Add Log Exporter**.
3. On the **Add Log Exporter** page, under **Download Certificates**, click **Download** to download the signed certificate and root certificate from Illumio.
4. Within Panorama, select **Certificate Management** > **Certificates** from the left navigation pane, and then click **Import** in the banner at the bottom of the page.
5. In the **Import Certificate** dialog box, enter the certificate name, select the certificate file to upload, and click **OK**.
6. Under **Syslog Configuration**, enter the target name in the **Target Name** field. This value is used to describe your connection and it does not affect your configuration.

   NOTE
   The other values under Syslog Configuration are prepopulated.

7. Under **Copy CEF Traffic Log Format**, click the copy icon to copy the CEF format. You must paste this into Palo Alto Networks Panorama: Format Syslog Messages in Common Event Format (CEF) [10].
8. Click **Save**.

   The **Log Exporter Added** status message displays and the Log Exporter appears as Active in the **Log Exporter** table.

Add Multiple Log Exporters

You can add multiple log exporters. This can be useful when you have multiple firewalls because a firewall can only be managed by one Panorama instance at a time, but organizations often use multiple Panorama instances for different groups of firewalls. It is usually done for scalability, to separate different regions or business units, to meet compliance requirements, or during migrations or mergers. Using multiple Panorama instances provides better management isolation, performance, and operational flexiblity.

Edit the Log Exporter

To edit Log Exporter information, on the Log Exporter page, click the edit icon at the end of the row for the Log Exporter whose information you want to edit.

Enable Cribl to Send Palo Alto Networks Firewall Logs to Azure Event Hub

Use the following procedures to allow Cribl Stream to send Palo Alto Networks firewall logs to the Illumio-hosted Azure Event Hub.

NOTE

For Cribl, use the default Palo Alto Networks log format instead of Common Event Format (CEF).

1. In Cribl Stream, add a Data Destination with the following values to the Azure Event Hub that you use for Illumio Insights:
   a. **Output ID:** Enter a unique name to identify the Azure Event Hubs definition.
   b. **Brokers:** arch-eventhub.servicebus.windows.net:9093
   c. **Event Hub Name:** rsyslog-logs
   d. **TLS:** Enabled
   e. **Authentication:** Enabled
   f. **SASL Mechanism:** PLAIN
   g. **Username:** $ConnectionString
   h. **Password:** Will be provided in a separate email. It is the full Event Hub connection string (usually starts with Endpoint=sb.//...;SharedAccessKeyName=...;SharedAccessKey=...).
2. Add a Data Route with the following values to the Data Destination that you created:
   a. **Route Name:** Enter a unique name for the route.
   b. **Pipeline:** Select a value.
   c. **Destination:** Select the Destination Name (Output ID) that you created in Step 1.a.

Format Syslog Messages in Common Event Format (CEF)

To be able to send syslogs in CEF format from Palo Alto Networks firewalls, you must create a custom Syslog Server Profile and define CEF field mappings for each log type.

NOTE

Perform the following procedures in the Palo Alto Networks Panorama application.

Step 1: Create a Syslog Server Profile:

1. Log into Panorama with admin privileges and navigate to **Device** > **Server Profiles** > **Syslog**.
2. Click **Add**, and do the following:
   a. In the **Name** field, enter a descriptive name, such as Illumio-CEF-Logs.
   b. In the **Server** field, set the server value to your syslog receiver's IP address.
   c. Set the value of the **Transport** value to TCP.
   d. Set the value of the **Port** field to 514.

Step 2: Define the Syslog Format:

1. Under the **Format** section, select **Custom Format**.
2. Paste in the **CEF Format** text that you copied from the **Add Log Exporter** pane within Illumio Console.

NOTE

Note the following about the CEF Format text:

- The CEF header value (`CEF:0|...|` defines the vendor, product, and version.
- The fields following the header (such as `src=, dst=` and so forth) map PAN-OS variables to CEF fields.

Step 3: Apply the Custom Profile to Log Forwarding:

1. Navigate to **Objects** > **Log Forwarding** and click **Add**.
2. Select the new **Syslog Server Profile** that you created.
3. Set **Traffic** as the log type to send in CEF format.
4. Click **Commit** to save the configuration and start forwarding logs in CEF format.

Note the following information:

- CEF format is not preconfigured for Palo Alto Networks, so you must configure it manually. See Configure Syslog Monitoring [6].
- Each log type (Traffic, Threat, URL, System, and so on) might require a different mapping depending on the use case. This integration only uses the **Traffic** log type.
- Custom tokens, such as %SRC%, %DST%, and %THREATNAME%, are used to populate CEF fields dynamically.
- If you copy and paste, the format might include unintended characters.

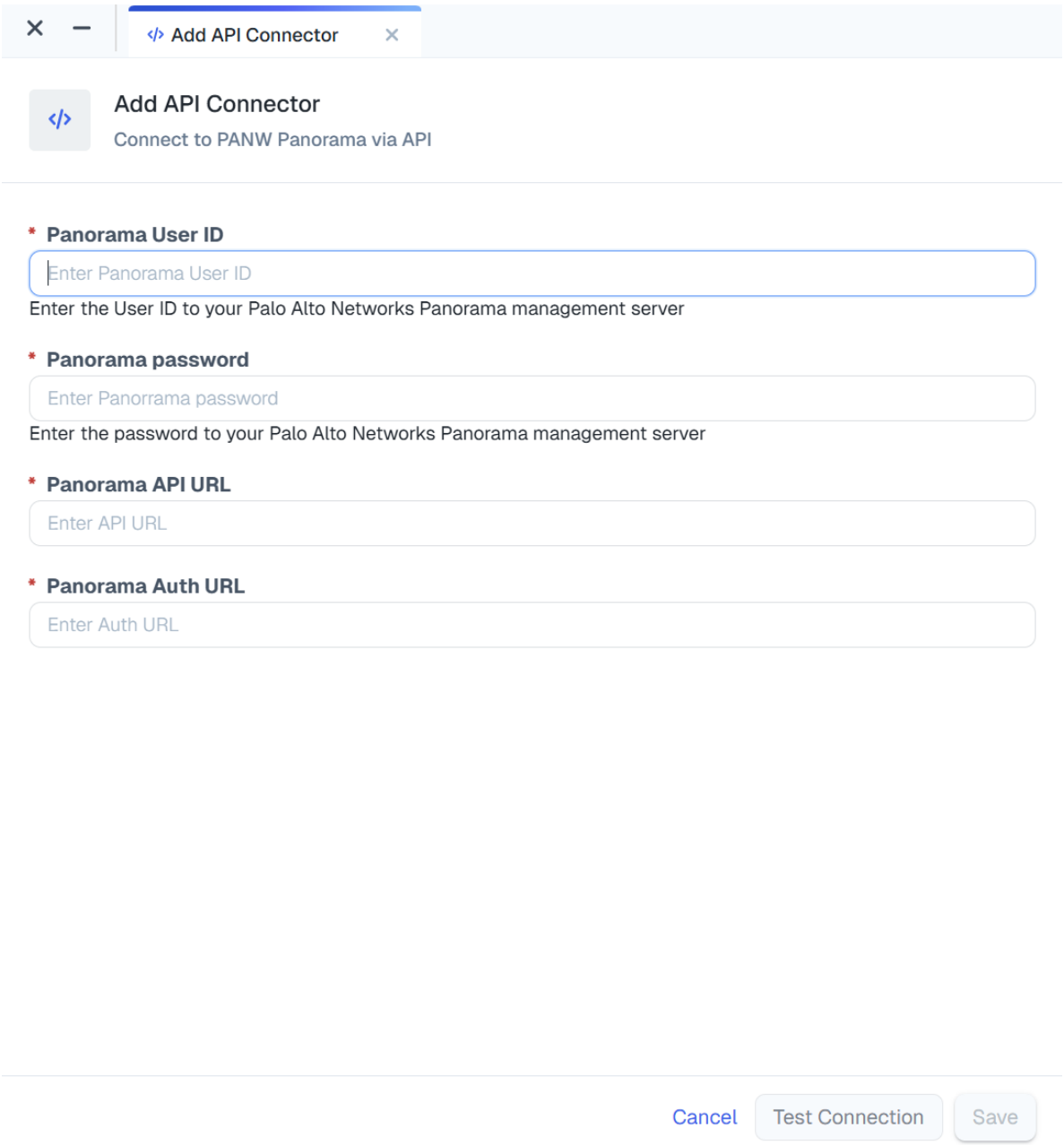
Adding the API Connector

IMPORTANT

You must have onboarded using the Log Exporter before you can add the API Connector.

Use the API Connector to allow the Illumio application to collect policy information automatically from Palo Alto Networks and to make sure that the intelligence that the Illumio application generates is reflected in the Palo Alto Networks firewall.

1. Navigate to the **Connectors** page and click **+ Add** on the **Palo Alto Networks** tile.
2. On the **Palo Alto Networks Connector** page, click **+ Add API Connector**.



3. In the **Add API Connector** pane, do the following:
   a. Enter your Panorama username and password in the **Panorama User ID** and **Panorama Password** fields.
   b. Enter the URL of your Panorama instance in the **Panorama API URL** field.
   c. Enter the auth URL in the **Auth URL** field. This value is your API URL, followed by `?type=keygen`.

> **IMPORTANT**
> These values are encrypted and stored in a secure vault.

4. Click **Save**.
   The values that you entered display in the **API Connector** pane.

NOTE

To test the connection, click **Test Connection.**

If you need to edit any of the API information, click **Edit API Connector**.

Reference: CEF Fields Required by Illumio Insights

Firewall traffic logs that are sent to Illumio Insights must be in CEF format.

Field Name	Description	Required
deviceVendor	The vendor of the device that is generating the log	Y
deviceExternalId	The external identifier for the device	Y, for future firewall Insights
cs1Label	Custom string 1 label (tenant identification)	Y
act	The action taken by the device or application	Y
src	Source IP address of the connection	Y
dst	Destination IP address of the connection	Y
proto	Protocol number used	Y
spt	Source port number	Y
dpt	Destination port number	Y
out	Bytes sent from source to destination	Y
in	Bytes received at destination	Y
conn_direction	Direction of the connection	Y
outzone	Network security zone of the destination	Y
inzone	Network security zone of the source	Y
rule_uid	Primary key for rule metadata lookup	Y, for future firewall Insights
cs2Label	Rule Name indicator Use cs2Label and cs2 for Rule Name	Y, for future firewall Insights
cs2	Rule Name Use cs2 for Rule Name	Y, for future firewall Insights
cs3Label	Policy Name indicator Use c3Label and cs3 for Policy Name	Y
cs3	Actual Policy Name Use cs3 for Policy Name	Y
app	Application or service identified	Y, for future firewall Insights

For more information about the fields available for Check Point, Palo Alto Networks, see the Check Point documentation: Check Point SupportConfiguration CEF Fields.