TECHNICAL
DOCUMENTATION

Check Point Integration Guide

This guide explains how to set up the Illumio and Check Point integration. It explains how to connect to Check Point Log Exporters for firewall log ingestion and connect to the Check Point Infinity Portal for API integration.

What's New and Overview

Onboarding and Integration

Using the Integration

Reference

Table of Contents

What's New in the Illumio and Check Point Integration

May 7, 2026

New Firewall Orchestrator

There is now a Firewall Orchestrator for onboarding the Check Point integration for your on-premises data centers.

October 2025

Log Exporter Enhancements

The Check Point Connector now supports onboarding multiple Check Point Log Exporters, enabling organizations to forward logs from several Check Point Management Servers to Illumio. This enhancement allows Illumio Insights to receive a centralized and comprehensive view of network flow information regardless of how many Log Exporters you have deployed. By aggregating telemetry from multiple gateways into one management source, you can simplify your integration, maintain full visibility, and ensure that data is consistently ingested into Illumio Insights even in distributed or large-scale environments where separate Log Exporters are required.

The certificate-signing request process is now automated, eliminating the need to exchange emails when establishing an mTLS connection between Illumio Insights and the Illumio syslog server. With this enhancement, certificate signing occurs automatically during setup, which ensures that secure connections are established consistently with minimal administrative effort. This automation not only streamlines deployments, but it also enhances security by reducing the risk of configuration errors or certificate tampering. The redesigned integration provides stronger end-to-end encryption and assures the integrity of all of the data that is transmitted between components.

New API Connector

The API Connector allows Illumio Insights to query Check Point firewall metadata and firewall policies to augment Insights findings for firewall policy coverage.

About the Illumio and Check Point Integration

The Illumio integration with Check Point allows organizations to collect and analyze firewall logs to enhance visibility, drive segmentation decisions, and improve their security posture. This integration combines Check Point's native log export capabilities and Illumio's real-time traffic visibility to allow security teams to make data-driven policy decisions. While firewall logs provide valuable telemetry, the benefit comes from making Illumio and Check Point work through a direct API integration. By using the API, Illumio can collect policy information automatically from Check Point, removing the need for manual policy queries. This means that security teams can operate faster and with more accuracy and confidence.

Benefits of Using Check Point with Illumio Insights

If you're already using Check Point as your firewall, you can view Check Point firewall data with Illumio Insights. Firewall logs contain extensive telemetry data, but in many environments they are underused and often stored in isolated systems, left unanalyzed, or accessed only after a security incident.

Illumio Insights transforms these logs into an active part of your security strategy. By ingesting Check Point firewall telemetry, Illumio Insights provides these benefits:

- Real-time visibility into traffic behavior across your environment
- A thorough understanding of risks that can help you identify suspicious patterns before they occur
- A more informed investigation context so that security teams can connect events rapidly, prioritize threats, and respond faster

With this integration, your Check Point firewall logs go beyond compliance or record-keeping and become an engine for visibility and detection. Check Point and Illumio Insights allow teams to discover hidden risks and strengthen their ability to detect and respond to threats.

Prerequisites for the Illumio and Check Point Integration

To onboard Check Point, you must take the following actions to make sure that logs are properly formatted, aggregated, enriched, and securely transmitted.

IMPORTANT

Note the following about the Log Exporter and the API Connector:

- Onboarding the Check Point Connector using the Log Exporter and adding the API Connector are two separate procedures.

Prerequisites for the Log Exporter

- ☐ All Check Point clients must enable the Check Point Log Exporter feature to allow logs to be forwarded from the gateway or log server. Set the log format for the Check Point Log Exporter to Common Event Format (CEF) and aggregate all logs to the Check Point Management Server. Configure each Security Gateway to forward its logs to the Check Point Management Server so that it can process them. Doing so makes sure that the Illumio application receives a unified and complete view of Check Point data and confirms that the Check Point Management Server acts as a central point for sending logs to the Illumio application.

  See Log Exporter and Configuring the Security Management Server and Security Gateways.

- ☐ To onboard Check Point, you must have access to the Check Point Management Server CLI in Expert Mode.

- ☐ You must enable mTLS between the Check Point Management Server and the Illumio syslog server to secure log transmission. The Illumio and Check Point integration uses mTLS secure connectivity. When you onboard, you will generate a client certificate that Illumio will sign and return to you.

- ☐ To ensure that Illumio associates each log to the correct tenant, the onboarding process injects the Tenant ID value into the CEF logs using an automated script.

Prerequisites for the Infinity Portal API Connector

Review these prerequisites before you use the Infinity Portal API Connector.

- ☐ Activate Remote API Access. See Enable Remote API Access in Check Point [11].
- ☐ Create a Security Management API Key. See Create an API Key for Quantum Security Management [12].

> **NOTE**
> As long as your API key is valid and has not expired, you can use it to run APIs on your Management Server.

- ☐ Create an administrator type user with read only, read and write, or super user permissions to allow Illumio to make API calls. See Create an Administrator User to Make API Calls [11].
- ☐ Integrate the Check Point SmartConsole with the Check Point Infinity Portal.

> **NOTE**
> You do not need to enable log sharing as Illumio ingests logs directly from the management server.

Prerequisites for the Firewall Orchestrator API Connector

Illumio Prerequisites

- ☐ The Illumio Firewall Connector instance name. You can have multiple instances, but each must have a unique name.
- ☐ A PCE Service Account with administrator or higher privileges, the username and the client secret.

Check Point Prerequisites

- ☐ The connector must be installed on a host with network connectivity to the Check Point Management Server as well as the PCE.
- ☐ You must have permission to run `sudo` commands.
- ☐ You must have permission to run the connector binary.
- ☐ You must add the data center server object for Illumio.
- ☐ You must have Check Point credentials for the Check Point Smart Console.

About the Check Point Infinity Portal

The Check Point Infinity Portal is Check Point's unified, cloud-based platform for managing security services. It provides a single point of access for security policies, threat intelligence, and API integrations across Check Point products.

Using the portal, you can streamline management tasks, enable automation, and integrate with third-party solutions like Illumio. The portal allows Illumio to securely communicate with Check Point to exchange data and extend visibility and control.

To use the Infinity Portal, you must create an account on portal.checkpoint.com and assign your environment to the account. See Create a Check Point Infinity Portal Account [10].

Your Check Point Onboarding Journey

1. Create a Check Point Infinity Portal Account. [10]
   a. Integrate the Check Point Management Server with the Infinity Portal. [11]
   b. Create an Administrator User. [11]
   c. Enable Remote API Access in Check Point. [11]
   d. Create an API Key for Quantum Security Management. [12]
   e. Generate an Infinity Portal Token [12].
2. Onboard the Check Point Connector. [13]
3. Add the API Connector. [16]

Create a Check Point Infinity Portal Account

1. Navigate to portal.checkpoint.com and click the **Don't have an account? Register here** link.
2. Fill out the following fields on the **Create Your Infinity Account** page:
   - Account Name
   - First and Last Name
   - Email
   - Country
3. Click the drop-down arrow next to the **Select storage location** field and select your storage region.

4. Select **Customer** from the drop-down list.
5. Accept the **Terms of Service** and **Privacy Policy**, check the **I'm not a robot** check box, perform the required verification for reCaptcha, and click **Next**.
6. Follow the instructions in the email to activate your account.

Integrate the Check Point Management Server with the Infinity Portal

IMPORTANT
You must have created an account on portal.checkpoint.com before you perform this procedure.

To share management configurations, you must connect your on-premises management server to the Check Point Infinity Portal.

See Connecting On-Premises Management Servers and Security Gateways to the Infinity Portal.

Create an Administrator User to Make API Calls

You must have a user account with the permission to make API calls. If this user does not already exist, you must create it.

See Creating an Administrator Account with API Key Authentication.

Enable Remote API Access in Check Point

You must enable Remote API Access to allow Check Point Infinity Portal to run APIs on your management server.

1. On the **Connected Managements** page, select the management server and click the three-dot menu next to the management server name.

2. In the **Activate Remote APIs Access** pane, toggle the **Activate Remote APIs Access** setting to ON.

Create an API Key for Quantum Security Management

To use APIs with the Check Point Management Server, you must have an API key for Security Management.

1. Log into Check Point Infinity Portal and select your self-hosted account.
2. Navigate to **API Key** and click **New**.
3. Select **New account API key** from the **New** drop-down list.
4. In the **Create New Account API Key** dialog box, do the following:
   a. Select **Security Management** from the **Service** drop-down list.
   b. Select a date from the **Expiration** field.
   c. (Optional) Enter a description.
   d. Click **Create**.

> **IMPORTANT**
> Be sure to save the API Key information in a secure location.

Generate an Infinity Portal Token for Running APIs on the Check Point Management Server

Next, generate an Infinity Portal token using your API key to run APIs on the Check Point Management Server.

See Connecting On-Premises Management Servers and Security Gateways to the Infinity Portal.

Onboard the Check Point Connector with the Log Exporter

To ingest Check Point firewall logs, you must first onboard the Check Point Connector using the Log Exporter.

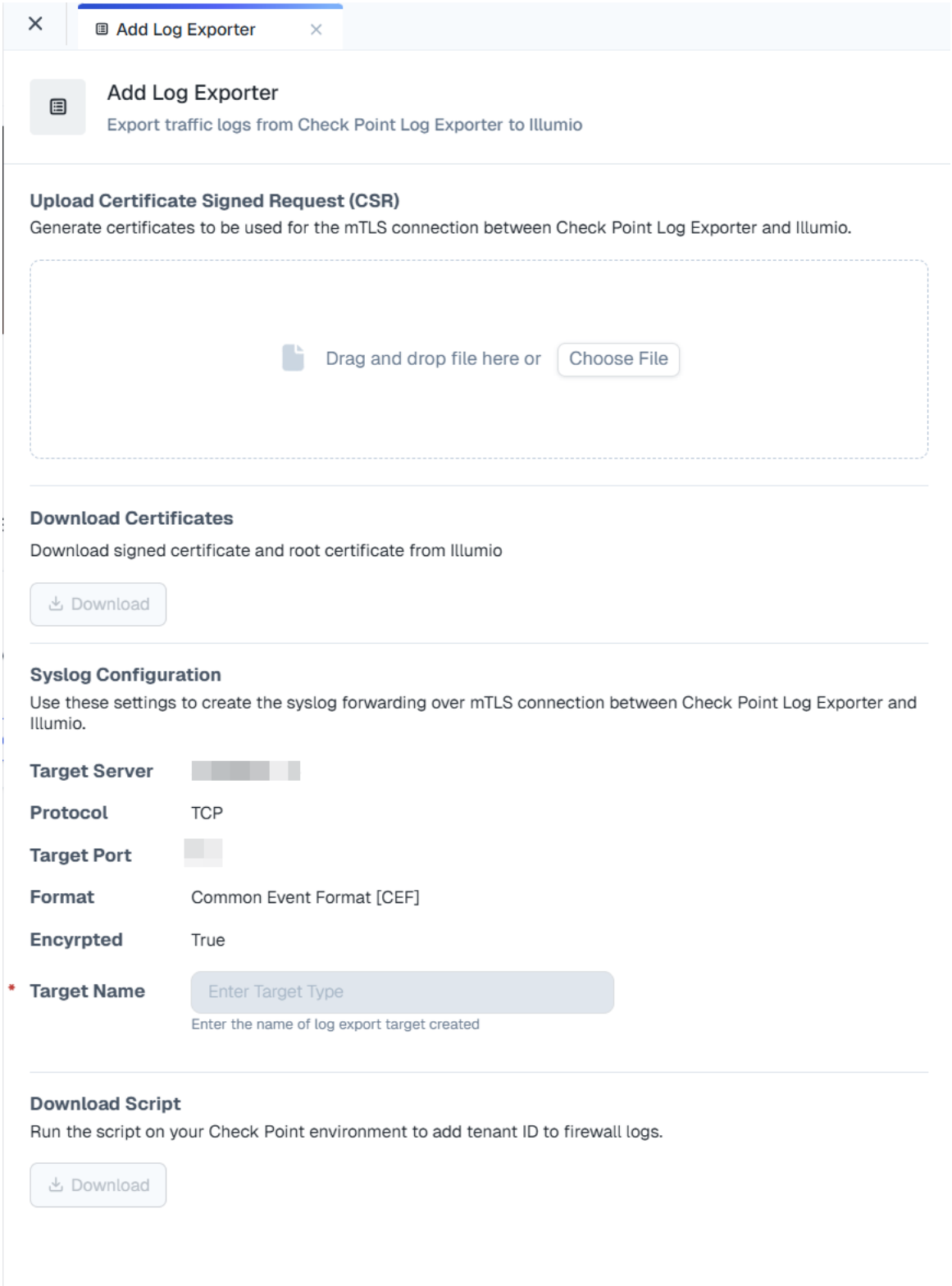
IMPORTANT

Do not add the API Connector until after you have successfully onboarded the Check Point integration using the Log Exporter.

1. Navigate to the **Connectors** page and click **+ Add** on the **Check Point Connector** tile.
2. On the **Check Point Connector** page, click **+ Add Log Exporter**.
3. On the **Add Log Exporter** page, under **Upload Certificate Signing Request (CSR)**, upload your CSR file.

IMPORTANT

You must have uploaded your CSR file to the Check Point Management Server to allow the mTLS connection. See Prerequisites for the Illumio and Check Point Integration [7] and Utilizing Mutual TLS Authentication with Log Exporter.



4. After the CSR has been successfully uploaded, click **Download** to download the signed client certificate and the CA root certificate.
5. Under **Syslog Configuration**, enter the target name in the **Target Name** field.
6. **Under Download Script**, click **Download** and run the script in your Check Point environment. This script adds the tenant ID to your firewall logs.

7. 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 that are managed in different domains, because it allows each firewall to establish a connection to Illumio Insights.

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.
- You can upload a different CSR if you need to. If you upload a new CSR, you'll get a new certificate to download.

Adding the API Connector

The API connection to Check Point allows Illumio to retrieve additional details that enrich the collected traffic logs and the ability to sync Illumio policies to Check Point and analyze firewall impact.

Use the API Connector to allow the Illumio application to collect policy information automatically from Check Point and to make sure that Illumio Segmentation policies are reflected in the Check Point firewall.

IMPORTANT

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

1. Navigate to the **Connectors** page and click **+ Add** on the **Check Point Connector** tile.
2. On the **Check Point Connector** page, click **+ Add API Connector**.
3. In the **API Connector** pane, enter values in the following fields:
   - Infinity Portal Client ID
   - Infinity Portal Client Secret
   - Quantum Smart Management API URL
   - Quantum Smart Management Auth URL
   - Quantum Smart Management API Key
   - Quantum Security Management Service Identifier
4. Click **Save**.

NOTE

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

Check Point Firewall Rule Writing Overview

Firewall Insights provides agentless visibility across data centers and clouds by enriching firewall logs with policy data, asset information, and risk assessments. It supports all Insights widgets without requiring additional agents or applications. For complete policy context, you can optionally connect the API. These integrations are currently supported: Check Point, Palo Alto Networks, and Fortinet.

Visibility and Policy Enforcement with Firewalls

- Connect to CheckPoint and Fortinet firewalls
  APIs are used to sync the list of firewalls and firewall policies. Firewall logs are imported through syslog.
- Export Illumio labels to firewalls
  Continuously sync labels and label to IP mapping to firewalls and enable label based rules in firewalls.
- View firewall traffic on the Unified Map
  Firewall traffic logs are aggregated as traffic in the Unified Map.
- Write automated firewall rules
  Illumio writes firewall rules upon policy provision. Single and multiple labels are supported for source and destination.

Firewall Integration User Flow

Step 1: Download the Illumio Firewall Orchestrator

As an administrator, enable the API connector and install the downloaded firewall orchestrator on-premises.

NOTE
Only one orchestrator is permitted for each firewall management server.

Result: Connection is Initiated with the Illumio Connector

The firewall orchestrator initiates a connection with the Illumio common connector, allowing on-premises deployment with no changes to your existing firewall policies.

Step 2: Forward firewall flow logs to Illumio

As an administrator, configure the firewall management server to forward firewall flow logs to Illumio.

Step 3: Configure the firewall management server to fetch labels

As an administrator, configure the firewall management server to fetch Illumio labels and labels to IP mappings, and then create firewall objects.

Firewall Orchestrator Post Configuration Actions

As a result of configuring the firewall orchestrator, policy updates are calculated and applied to the appropriate firewalls.

Policy Update Calculated

Whenever a policy is provisioned, Illumio calculates the policy update and identifies the firewalls impacted by this policy. It then pushes these updates to the relevant firewall orchestrator.

Firewall Rules Programmed to Each Management Server

The firewall orchestrator sends firewall rules to each management server, which then deploys the policy to the appropriate firewalls.

Onboard the Firewall Orchestrator

NOTE

Use this option if you want to install a connector in your Data Center to allow the Illumio Core to sync policies to Check Point.

1. Log in to the Illumio Console, navigate to **Settings** > **Connectors**, and click the Check Point tile.
2. On the Check Point Connector page, select **API Connector**.
3. Within the API Connector pane, select **Illumio Firewall Orchestrator (On-Prem)**.
4. Enter a unique name for your connector instance in the **Name the Connector Instance** field.
5. Under **Enter PCE Service Account Credentials**, create the API connection to the Illumio PCE:
   a. Service Account User
   b. Service Account Secret
6. Under **Enter Check Point Smart Console Credentials**, enter the following:
   a. Check Point Management Server URL
   b. Username
   c. Password
   d. Illumio Data Center Server Name
7. Under **Download Firewall Orchestrator**, click **Download**.
8. Identify a host on which you will run the Orchestrator.

   This server must be able to connect with the Check Point Management Server.
9. Transfer the .tar file to the server that you will run the Orchestrator on.
10. Run the following command to deploy the Orchestrator:

- `tar -xvf <archive-name>.tar.gz`

11. Execute the Orchestrator binary included in the .tar file.

    Illumio recommends that you run the binary on a non-terminating session (such as by using tmux).
12. Navigate to the Check Point tile on the Connectors page to view the status.

    Confirm that the orchestrator shows a Health status of **Connected**.
13. Next, go to the Firewalls page to see the Illumio policies and the associated firewalls that have been applied to it.

View the Label-Based Policies Applied to the Firewalls

After you have onboarded the API connector, you can view the Illumio label-based policies that are applied to the firewalls. You can see the policies on the Check Point Management Server and the Illumio added rules.

1. Go to the Firewalls page.
2. View the list of firewalls.
3. Click the Subnets Enforced column to open the slide-out and specify the subnets that the firewall is able to enforce on.
4. Click the Firewall Rules tab to view the Illumio label-based policies that are applied to the firewalls.

View the Policy Impact

View the policy impact where it takes into account the subnets that a firewall enforces.

1. Go to Policies > Show Impact to see the firewall that is impacted.
2. View the number of protected resources that fall within this firewall's IP range in the Impact of Policy page.

Policy Sync

After you've evaluated and provisioned your policy, Illumio will sync the policy to your Check Point firewalls.

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	Yes
deviceExternalId	The external identifier for the device	Yes
cs1Label	Custom string 1 label (tenant identification)	Yes
act	The action taken by the device or application	Yes
src	Source IP address of the connection	Yes
dst	Destination IP address of the connection	Yes
proto	Protocol number used	Yes
spt	Source port number	Yes
dpt	Destination port number	Yes
out	Bytes sent from source to destination	Yes
in	Bytes received at destination	Yes
conn_direction	Direction of the connection	Yes
outzone	Network security zone of the destination	Yes
inzone	Network security zone of the source	Yes
rule_uid	Primary key for rule metadata lookup	Yes
cs2Label	Rule Name indicator Use cs2Label and cs2 for Rule Name	Yes
cs2	Rule Name Use cs2 for Rule Name	Yes
cs3Label	Policy Name indicator Use c3Label and cs3 for Policy Name	Yes
cs3	Actual Policy Name Use cs3 for Policy Name	Yes

For more information about the fields available for Check Point, Fortinet, or Palo Alto Networks, see the following documentation:

- Check Point: Check Point
- Fortinet: Fortinet
- Palo Alto Networks: Common Event Format (CEF) Configuration Guides