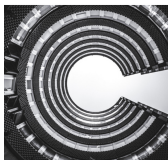




TECHNICAL  
DOCUMENTATION

# Illumio Core What's New and Release Notes 25.2.10, 25.2.11

---



Learn about new features and review the resolved and known issues for Illumio Core and other components.

- [25.2.11](#)
- [25.2.10](#)

## Table of Contents

Illumio Core Release Notes 25.2.10, 25.2.11 .....	6
Product Version .....	6
Security Information .....	6
Resolved Issues in 25.2.11 .....	6
Resolved Issues in 25.2.10 .....	7
What's New in 25.2.10 .....	9
What's New and Changed in Release 25.2.10 .....	9
Rule Search now supports Deny and Override Deny rules .....	9
Deny and Override Deny rules now support Intra- and Extra-Scopes .....	9
Rule IDs now included in Syslog .....	10
Label Exclusion now available for Deny and Override Deny rules .....	11
VEN Remote Restart .....	12
Conflicted Rules panel .....	12
Deny Rules created from a Template now appear in the Policies page .....	13
Support for searching App Groups by Deny and Override Deny rules .....	14
Support for checking policy by Deny and Override Deny rules .....	14
Support for Enhanced Data Collection in all enforcement modes .....	15
Alert when certificate is nearing expiration .....	16
Illumio Content Enhancements .....	16
New and Changed APIs in 25.2.10 .....	17
New APIs in 25.2.10 .....	17
<b>sec_policy_policy_check_get</b> .....	17
<b>vens_remote_action_put</b> .....	18
New Common Schemas .....	19
Changed APIs in 25.2.10 .....	26
What's New and Release Notes for LW-VEN 1.1 .....	30
What's New in LW-VEN Release 1.1.0 .....	30
Support for flow reporting for legacy Windows servers .....	30
Release Notes in LW-VEN 1.1 .....	30
Resolved Issues in 1.1.10 LW-VEN .....	30
Resolved Issues in 1.1.0 LW-VEN .....	31
Illumio Core for Kubernetes .....	32
Illumio Core for Kubernetes 5.4 .....	32
Illumio Core for Kubernetes What's New and Release Notes for 5.3 .....	32
What's New in Illumio Core for Kubernetes 5.3.2 .....	32
What's New in Illumio Core for Kubernetes 5.3.1 .....	33
Release Notes for 5.3.2 .....	34
Resolved Issues in 5.3.1 .....	35
Illumio Core for Kubernetes Release Notes 5.2 .....	36
About Illumio Core for Kubernetes 5.2 .....	36
Updates for Core for Kubernetes 5.2.3 .....	37
Updates for Core for Kubernetes 5.2.2 .....	37
What's New in Release 5.2.1 .....	38
Updates for Core for Kubernetes 5.2.1 .....	38
What's New in Release 5.2.0 .....	38
Updates for Core for Kubernetes 5.2.0 .....	43
Illumio Core for Kubernetes Release Notes 5.1 .....	44
Core for Kubernetes 5.1.10 .....	44
Limitations .....	45
Updates for Core for Kubernetes 5.1.10 .....	45
Updates for Core for Kubernetes 5.1.7 .....	46
Updates for Core for Kubernetes 5.1.3 .....	46
Updates for Core for Kubernetes 5.1.2 .....	47

Updates for Core for Kubernetes 5.1.0 .....	47
Security Information for Core for Kubernetes 5.1 .....	49
Illumio Core for Kubernetes Release Notes 5.0.0 .....	49
About Illumio Core for Kubernetes 5.0 .....	49
Product Version .....	50
What's New in C-VEN and Kubelink .....	50
NodePort Limitations .....	50
Updates for Core for Kubernetes 5.0.0-LA .....	51
Illumio Core for Kubernetes Release Notes 4.3.0 .....	52
What's New in Kubernetes 4.3.0 .....	52
Product Version .....	53
Updates for Core for Kubernetes 4.3.0 .....	54
Illumio Flowlink Release Notes for Release 1.4.0 .....	55
Product Version .....	55
New Features in Illumio Flowlink 1.4.0 .....	55
Resolved and Known Issues in Flowlink 1.4.0 .....	55
Resolved Issue .....	55
Known Issue .....	56
Illumio Flowlink Release Notes 1.3.0 .....	57
Product Version .....	57
New Feature in Flowlink 1.3.0 .....	57
Resolved Issue in Flowlink 1.3.0 .....	58
Illumio NEN Release Notes 2.6 .....	59
Product Version .....	59
Release Types and Numbering .....	59
What's New in NEN 2.6.x Releases .....	59
NEN 2.6.40 New Feature .....	59
NEN 2.6.30 New Features .....	61
NEN 2.6.20 New Features .....	61
NEN 2.6.10 New Features .....	62
NEN 2.6.1 New Features .....	62
NEN 2.6.0 New Features .....	62
Resolved Issues in NEN 2.6.40 .....	63
Known Issues in NEN 2.6.40 .....	64
Resolved Issues in NEN 2.6.30 .....	64
Known Issues in NEN 2.6.30 .....	64
Resolved Issue in NEN 2.6.20 .....	64
Known Issues in NEN 2.6.20 .....	64
Resolved Issues in NEN 2.6.10 .....	64
Known Issues in NEN 2.6.10 .....	65
2.6.10 Security Information .....	65
Resolved Issues in NEN 2.6.1 .....	65
Known Issues in NEN 2.6.1 .....	65
Resolved Issues in NEN 2.6.0 .....	65
Known Issues in NEN 2.6.0 .....	66
Illumio NEN Release Notes 2.5 .....	67
Product Version .....	67
Resolved Issue in NEN 2.5.2.A1 .....	67
Known Issues in NEN 2.5.2.A1 .....	67
Resolved Issues in NEN 2.5.2 .....	68
Known Issues in NEN 2.5.2 .....	68
Resolved Issue in NEN 2.5.1 .....	68
Known Issues in NEN 2.5.1 .....	68
Resolved Issues in NEN 2.5.0 .....	68
Known Issues in NEN 2.5.0 .....	69

Illumio CLI Release Notes 1.4.4 .....	70
What's New in CLI Tool 1.4.4 .....	70
Support for Proxy Communication .....	70
Illumio Core PCE CLI Tool Guide 1.4.3 .....	71
What's New and Changed in Release 1.4.3 .....	71
Illumio CLI Tool 1.4.3 .....	71
Support for Proxy .....	71
Connecting via a Proxy .....	72
Using API Keys and Secrets with a Proxy Server .....	73
Legal Notice .....	74

## Illumio Core Release Notes 25.2.10, 25.2.11

These release notes describe resolved issues in these releases:

- 25.2.11
- 25.2.10

Updated: May 12, 2025

### Product Version

PCE Version: 25.2.11 (Illumio SaaS and on-premise customers)

VEN Version: 25.2.10 (Illumio SaaS and on-premise customers)

These release notes provide a list of resolved issues for Illumio Core 25.2.11-PCE and 25.2.10-VEN.

Illumio Core release numbering uses the following format: “a.b.c-d+e”.

- “a.b”: Standard or LTS release number, for example, “2.2”
- “.c”: Maintenance release number, for example, “.1”
- “-d”: Optional descriptor for pre-release versions, for example, “preview2”

### Security Information

This section provides important security information for this release. For additional information about security issues, security advisories, and other security guidance about this release, go to the [Illumio Support portal](#). You must have a valid login and password.

- **cURL upgraded to v8.12.1**

cURL was upgraded to v8.12.1 to address CVE-2024-9681




### Resolved Issues in 25.2.11

The resolved issues in release 25.2.11-PCE are:

Issue	Fix Description
E-127181	<b>Fixed rule search that never loads</b>  Fixed an issue at the Rule Search page when clicking on Rule Search a query for all rules is immediately started, which could cause the page to become unresponsive when there are many rules and rulesets present.
E-126122	<b>Fixed public flows API queries</b>  Fixed occasional multiple failures of <code>async_query</code> API calls.
E-126121	<b>Improved performance by enhancing bulk operations</b>  Improved overall performance by enhancing bulk workload and event operations.
E-125150	<b>Resolved container cluster update issue that caused performance problems</b>  C-VEs and Kubelink updated their network interfaces (C-VE) and Kubernetes Workloads (Kubelink) against their corresponding cluster in sequential mode. Sequential mode was enforced to avoid race conditions between database data changes and data caching. This, however, produced problems for big clusters where C-VE and Kubelink queries started to stretch with big latencies -- basically, waiting for each other to finish. A solution has been implemented to avoid this race condition, removing the need to enforce sequential mode updates. Those API requests are no longer blocked, resulting in a much faster overall reporting process.

## Resolved Issues in 25.2.10

The resolved issues in release 25.2.10-PCE are:

Issue	Fix Description	Applies To
E-124971	<p><b>Flow log retrieval issue is fixed</b></p> <p>An issue with the <code>flow-analytics-monitor</code> prevented users from retrieving flow logs in some cases.</p>	
E-124817	<p><b>Vulnerabilities resolved in ruby-saml upgrade</b></p> <p>The <code>ruby_saml</code> upgrade from version 1.17.0 to 1.18.0 detected vulnerabilities. The latest testing verified that the upgrade to 1.18.0 was successful.</p> <div>  <p><b>NOTE</b> This issue applies to only on-premises deployments of 25.2.10-PCE.</p> </div>	On-premise deployments
E-123026	<p><b>Users no longer able to add duplicate filters</b></p> <p>Users were able to add the same filter manually and through the contextual menu. With this fix, users are no longer able to add duplicate filters.</p>	
E-121287	<p><b>Customer's pre-existing iptables no longer removed</b></p> <p>After switching the VEN from Idle mode to a different node, an organization's pre-existing iptables rules were removed (which in turn blocked the associated traffic), even though the Illumio Core non-primary coexistence mode was enabled. This issue was caused by using a dash instead of an underscore between "non" and "primary" in the coexistence mode setting. This is fixed. Pre-existing customer iptables are no longer removed.</p> <div>  <p><b>NOTE</b> This issue applies to only on-premises deployments of 25.2.10-PCE.</p> </div>	On-premise deployments
E-121096	<p><b>job_queue service running in Core nodes as expected</b></p> <p>The <code>data_job_queue_service</code> was not running on the Core nodes. This is fixed. The <code>data_job_queue_service</code> is running in Core nodes as expected.</p> <div>  <p><b>NOTE</b> This issue applies to only on-premises deployments of 25.2.10-PCE.</p> </div>	On-premise deployments



## What's New in 25.2.10

Learn about new features released in this version.

### What's New and Changed in Release 25.2.10

Before upgrading to Illumio Core 25.2.10, familiarize yourself with the new and modified features in this release for PCE, REST API, and the PCE web console.

#### Rule Search now supports Deny and Override Deny rules

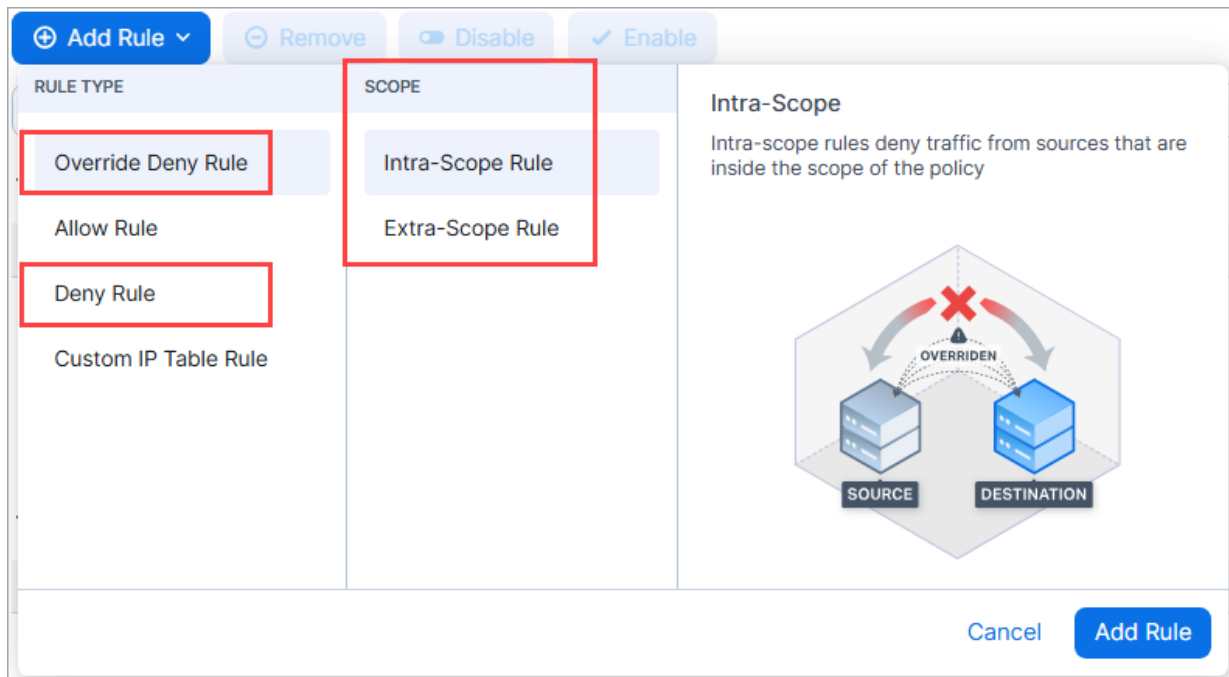
You can now search for any combination of Allow, Deny, and Override Deny rules from the **Policies > Rule Search** tab. Previously, Rule Search was limited to Allow rules. Also, the total number of each rule type is prominently displayed just below the search filter.

The screenshot shows the 'Policies' section with the 'Rule Search' tab selected. A search filter dropdown is set to 'Override Deny Rules \* or Allow Rules \* or Deny Rules \*'. Below the filter, three summary boxes are displayed, each with a red circle around the count: '1 Override Deny Rules' (1 Policy), '2 Allow Rules' (2 Policies), and '1 Deny Rules' (1 Policy). Below these, three expandable sections are shown, each with a red circle around the section header:

- Override Deny Rules**: Shows a table with columns: Provision Status, Status, Policy, Sources, Destinations, Destination Services, Scopes, and Scope Type. The table contains one row for 'Override Deny Rule example'.
- Allow Rules**: Shows a table with the same columns. It contains two rows: one for 'App59321 | Env59321 | Loc59321' and another for 'policy'.
- Deny Rules**: Shows a table with the same columns. It contains one row for 'Override Deny Rule example'.

#### Deny and Override Deny rules now support Intra- and Extra-Scopes

You can now specify an Intra-Scope or Extra-Scope scope when you add Deny and Override Deny rules. Previously, this was only possible for Allow rules.



## Rule IDs now included in Syslog

To help you trace and investigate traffic flows, each traffic flow entry in Syslog now includes the rule ID associated with the policy decision of the flow. This provides an explicit reference to the rule that affected the flow's policy state.



### CAUTION

For large customers with 10K+ messages per second, adding rule IDs to the syslog events will make the recorded data significantly larger.

To use this feature, perform these steps:

1. Enable Rule Hit Count on the PCE and the VEN.
  - [Enable Rule Hit Count on a VEN](#)
  - [Enable Rule Hit Count on a PCE](#)
2. Enable the Rule ID feature as described in [Showing Rule ID in Syslog](#) in the Illumio REST API Guide.
3. Find the rule IDs in your syslog.

Server: localhost - Database: syslog2 - Table: auditable\_events

Sort by key: None

+ Options

	facility	host	priority	level	tag	datetime	program	msg	seq
<input type="checkbox"/>	local6	core1-2x2testvc196	info	info	b6	2025-03-24 10:23:17	1	2025-03-24T10:23:17.000000-07:00 core1-2x2testvc196 illumio_pce/collector 24822 - [meta sequenceId="282"]	3939
<input type="checkbox"/>	local6	core1-2x2testvc196	info	info	b6	2025-03-24 10:23:17	1	id":2,"times	3938
<input type="checkbox"/>	local6	core1-2x2testvc196	info	info	b6	2025-03-24 10:23:17	1	4T17:21:32Z","st	3937
<input type="checkbox"/>	local6	core1-2x2testvc196	info	info	b6	2025-03-24 10:23:17	1	un":"ntp","src_ip":"1	3935
<input type="checkbox"/>	local6	core1-2x2testvc196	info	info	b6	2025-03-24 10:18:2	1	unt":1,"dir":"0","o	3266
<input type="checkbox"/>	local6	core1-2x2testvc196	info	info	b6	2025-03-24 10:18	1	alifier":0,"pd":0	3264
<input type="checkbox"/>	local6	core1-2x2testvc196	info	info	b6	2025-03-24 10:13	1	active/rule_sets	2218
<input type="checkbox"/>	local6	core1-2x2testvc196	info	info	b6	2025-03-24 10:13	1	stname":"beqa-	2217
<input type="checkbox"/>	local6	core1-2x2testvc196	info	info	b6	2025-03-24 10:13	1	as/21d2efd2-	2216
<input type="checkbox"/>	local6	core1-2x2testvc196	info	info	b6	2025-03-24 10:08:2	1	dev-regr-	1499
<input type="checkbox"/>	local6	core1-2x2testvc196	info	info	b6	2025-03-24 10:08:2	1	vm28","src_href":"/of	1495
<input type="checkbox"/>	local6	core1-2x2testvc196	info	info	b6	2025-03-24 10:03:19	1	2979-47e1-bdf9-	404
<input type="checkbox"/>	local6	core1-2x2testvc196	info	info	b6	2025-03-24 10:03:19	1	97e2fe9e1285","netv	395
<input type="checkbox"/>	local6	core1-2x2testvc196	info	info	b6	2025-03-24 10:03:19	1	"role":"role1"}	

With selected: ☐ Check All ☐ Change ☐ Delete ☐ Export

## Label Exclusion now available for Deny and Override Deny rules

The ability to use an "all labels except. ." approach when selecting labels for your rules is now available for Override Deny and Deny Rules. Previously, this feature was only available for Allow rules.

Scopes 1 Scope - Each scope must include **Application Labels**

app1

Select properties to filter view

**Override Deny Rules**

Provision Status	No.	Status	Scope Type	Sources	Destinations	Destination Services
<input type="checkbox"/> Pending	1	Enabled	Extra-Scope	All Environments except Production	All Workloads	S-RDP

**Allow Rules**

Provision Status	No.	Status	Scope Type	Sources	Source Process / Service	Destinations	Destination Services
There are no Allow Rules defined							

**Deny Rules**

Provision Status	No.	Status	Scope Type	Sources	Destinations	Destination Services
<input type="checkbox"/> Pending	1	Enabled	Extra-Scope	All Environments except Production	All Workloads	new service

## VEN Remote Restart

You can now restart a VEN directly from the PCE without physical access to the workload. Remote Restart is similar to other VEN operations that you can initiate from the PCE, such as unpairing and upgrading. For details, see [Restart the VEN Remotely](#).



### NOTE

The Restart button is grayed out if the VEN is Suspended or Offline.

[Home](#) > [Servers & Endpoints](#) > [VENs](#)

## workload-80

[Edit](#) [Unpair](#) [Upgrade](#) [Restart](#) [Generate Support Bundle](#) [Mark as Suspended](#)

### NODE

Name	workload-80
Description	
Hostname	workload-80
Enforcement Node Type	Server VEN
Version	23.3.0
Activation Type	Pairing Key





### STATUS

Status	Active
--------	--------

## Conflicted Rules panel

You are now alerted when rules are in conflict with one or more other rules in the same or another policy in your organization. Click the yellow icon to display a panel with the conflict details and use the information to perform housekeeping on your policy or troubleshoot unexpected policy behavior.

Rule Options

  Deny  

Rules are in conflict when:

- Traffic allowed by an Allow rule in your policy is overridden by an Override Deny rule in the same or another policy in your organization. Result: traffic is **denied**, which you may or may not have intended.

The screenshot shows a 'Conflicted Rules' dialog box. At the top, a rule is shown with status 'Enabled', scope 'Intra Scope', source 'envLabel-RuleSearch-Comb-4805852', destination 'locLabel-RuleSearch-Comb-4805853', and destination service 'All Services'. The action is 'Allow'. Below this, a message states: 'Your allow rule is being overridden by this override deny rule'. Underneath, a table lists rules. The first rule is 'RuleSet-Appgroup-3label' with status 'Enabled', scope type 'App-Lbl-219668', source 'All Workloads', destination 'API', and destination service 'All Services'. The action for this rule is 'Override Deny'.

- Traffic denied by a Deny rule in your policy is overridden by an Allow rule in the same or another policy in your organization. Result: traffic is **allowed**, which you may or may not have intended.

The screenshot shows a 'Conflicted Rules' dialog box. At the top, a rule is shown with status 'Enabled', source 'Any (0.0.0.0/0 and :::0)', destination 'Amazon', and destination service 'All Services'. The action is 'Deny'. Below this, a message states: 'Your deny rule is overriding these allow rules'. Underneath, a table lists rules. The first rule is 'Copy of test1' with status 'Enabled', scope type 'env1\_4515', source 'Any (0.0.0.0/0 and :::0)', destination 'Amazon', and destination service 'All Services'. The action for this rule is 'Allow'. Below this, another rule is shown with status 'Enabled', scope type 'Ruleset\_AppGroup82132-2label', source 'App82132', and destination 'Env82132'. The action for this rule is 'Allow'.

## Deny Rules created from a Template now appear in the Policies page

When you add a deny rule from a template, it's now placed in the Policies list page, not the Deny Rules page as before.



### NOTE

Although the stand-alone Deny Rules page still appears in the left navigation, Illumio plans to deprecate it in a future release. If your Core instance was upgraded to release 25.2.10 or later, Illumio recommends that you migrate your Deny rules from the Deny Rules page to the Policies page and add and manage Deny Rules from the Policies page from now on.

**Policies**

Home > Policy

Policies Rule Search

Add Start Policy Generator Provision Revert Remove Disable Enable

Select properties to filter view

Provision Status	Status	Name
Pending	Enabled	Example: Deny policy from template
Pending	Enabled	RS-OUT-LGA-RDP-PROTECT LGA-SSH-PROTECT
Pending	Enabled	Ransomware
Pending	Enabled	Ransomware 556
Pending	Enabled	Block Ransomware 555
Pending	Enabled	rule_set_2

## Support for searching App Groups by Deny and Override Deny rules

You can now search for Deny and Override Deny rules from an App Group's details page. Previously, you could only search for App Groups containing Allow rules from this page.

Home > Explore > App Groups

App82132 | Env82132 | Loc82132

Explore Members Rules Policy Generator Vulnerabilities Ransomware Protection PREVIEW

Override Deny Rules or Allow Rules or Deny Rules

Ruleset\_AppGroup82132 App82132 Env82132 Loc82132 Default Policy Generator Policy

Provision Status	Status	Sources	Destinations	Destination Services	Rule Type
Pending	Enabled	app2	All Workloads	new service	Override Deny
Enabled	Enabled	Any (0.0.0.0/0 and ::/0)	All Workloads	All Services	Allow
Enabled	Enabled	API	All Workloads	All Services	Deny

## Support for checking policy by Deny and Override Deny rules

Beginning with this release, the policy check feature (**Troubleshooting > Policy Check**) checks for policies that include Deny and Override Deny rules. Previously, this featured only checked policies containing Allow rules.

**Policy Check**

Destination: Workloads: beqa-dev-regi-vm31 x Source: Workloads: beqa-dev-regi-vm32 x Destination Port and Protocol: Corporate Check

Result: Connection is blocked by override deny rules

Match Rules: 9

- 1 Override Deny Rules 1 Policy
- 2 Allow Rules 2 Policies
- 1 Deny Rules 1 Policy

Override Deny Rules

Provision Status	Status	Policies	Destinations	Destination Services	Sources	Scopes	Scope Type
Pending	Enabled	rules_web_traffic	bound_service_in tcp/15000 udp/15000	Uses Virtual Services only	All Workloads	test_app.1 test_env.1 test_place.1	

Allow Rules

Provision Status	Status	Policies	Destinations	Destination Services	Sources	Scopes	Scope Type
Pending	Enabled	rule_set_svcnode_4	bound_service_in tcp/15000 udp/15000	Uses Virtual Services only	All Workloads	test_app.1 test_env.1 test_place.1	
Pending	Enabled	rules_web_traffic	test_place.1	Secure Shell Daemon (sshd)	All Workloads	test_app.1 test_env.1 test_place.1	

Deny Rules

Provision Status	Status	Policies	Destinations	Destination Services	Sources	Scopes	Scope Type
Pending	Enabled	rules_web_traffic	test_place.1	service_tcp_38700	Any (0.0.0.0 and ::0) All Workloads	test_app.1 test_env.1 test_place.1	

## Support for Enhanced Data Collection in all enforcement modes

You can now enable the [Enhanced Data Collection](#) option in any enforcement mode, not just Full Enforcement as before. Enhanced Data Collection allows the VEN to log byte counts and connection details for Allowed, Blocked, and Potentially Blocked traffic.

Home > Servers & Endpoints

## Workloads

Workloads Container Workloads VENS

Add Remove Edit Labels Enforcement Visibility

Select properties to filter view

Enhanced Data Collection

Show Vulnerability Exposure Score (V-E) Score in: Full Enforcement Visibility Only

1 Selected

	Connectivity	Full Enforcement V-E Score	Current V-E Score	Enforcement	Visibility	Policy Sync
<input type="checkbox"/>	Offline	0	885	Visibility Only	Blocked + Allowed	
<input checked="" type="checkbox"/>	Online	0	885	Visibility Only	Blocked + Allowed	

## Alert when certificate is nearing expiration



### NOTE

This feature is available only to on-premise deployments of 25.2.10-PCE.

On-premise PCE users are now alerted when a certificate on a PCE node is nearing expiration. A message is logged to syslog and displayed in the PCE health page.

```
2025-03-19T17:29:12.658437-07:00 level=notice host= program=illumio_pce/system_health| sec= src=certificate certificate=web_service expiration_days=47
```

## Illumio Content Enhancements

The 25.2.10 release introduces the following enhancements to the Illumio Documentation Portal:

TECHNICAL DOCUMENTATION

Platform Knowledge Base (Log in) Doc Archives (Log in) Security Advisories PDF Related Guides

Search

PCE Installation and Upgrade Guide

PCE Supercluster

VEN Install and Upgrade

Illumio Legacy Windows VEN

Kubernetes and OpenShift

NEN Installation and Usage Guide

Flowlink Configuration and Usage

Illumio Core PCE CLI Tool Guide 1.4.3

Illumio Core PCE CLI Tool Guide 1.4.2

Legal Notice

## Illumio Core 25.2.10 Install, Configure, Upgrade

In this Library	Description
PCE Installation and Upgrade Guide	Describes how to install and configure the Illumio Core Policy Compute Engine (PCE).
PCE Supercluster Deployment Guide	Describes how to deploy and administer a PCE Supercluster, a single administrative domain that spans two or more replicating PCEs.
VEN Installation Guide	Explains the two methods for installation: using the PCE web console to pair VENs with your hosts or to download the VEN software from the Illumio Support portal and install the software by using the VEN command line interface.
Illumio LW-VEN Installation Guide	Describes how to install and use the Legacy Windows VEN (LW-VEN) with the Illumio Core PCE to enforce security policies.
NEN Installation Guide	Describes how to install the Illumio Network Enforcement Node (NEN), to configure Server Load Balancers (SLBs) and switches to work with it, and to use the NEN to secure workloads attached to those network devices.
Illumio Core for Kubernetes and OpenShift Guide	Provides information about how to use Illumio Core with containerized applications running in clusters orchestrated by Kubernetes, and/or by other similar operators like OpenShift.
Flowlink Configuration and Usage Guide	Describes how to install, configure, and use Flowlink, an Illumio standalone application that can be used with the Illumio Core to collect network flow data from different types of network sources, such as switches, routers, F5 load balancers, cloud monitoring tools, and syslog exporters.

Was this helpful?

Yes No

Next

© 2025 Illumio Last modified: April 2, 2025

- A new Related Guides menu with links to other documents is available at the top of the page.



- PDFs of all guides are now available on the top navigation menu.
- Security Advisories are now available on the top navigation menu.

## New and Changed APIs in 25.2.10

This topic lists the new and updated REST APIs in 25.2.10.

### New APIs in 25.2.10

- [sec\\_policy\\_policy\\_check\\_get](#) [17]
- [vens\\_remote\\_action\\_put](#) [18]

### sec\_policy\_policy\_check\_get

This API is used to get all `sec_rules`, `deny_rules`, and `override_deny_rules` based on parameters. It was created to extend the response of the original **allow** endpoint and preserve compatibility with existing tools.

The request format is as follows:

```
GET api/v2/orgs/:xorg_id/sec_policy/:pversion/policy_check?<params>;
```

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "required": [
    "sec_rules",
    "deny_rules",
    "override_deny_rules"
  ],
  "properties": {
    "sec_rules": {
      "description": "Array of allow rules",
      "type": "array",
      "items": {
        "allOf": [
          {
            "$ref": "../common/sec_rules_get.schema.json"
          },
          {
            "rule_set": {
              "$ref": "../common/rule_set.schema.json"
            }
          }
        ]
      }
    },
    "deny_rules": {
      "description": "Array of deny rules",
```

```

    "type": "array",
    "items": {
      "allOf": [
        {
          "$ref": "../common/deny_rules_get.schema.json"
        },
        {
          "rule_set": {
            "$ref": "../common/rule_set.schema.json"
          }
        }
      ]
    }
  },
  "override_deny_rules": {
    "description": "Array of override deny rules",
    "type": "array",
    "items": {
      "allOf": [
        {
          "$ref": "../common/deny_rules_get.schema.json"
        },
        {
          "rule_set": {
            "$ref": "../common/rule_set.schema.json"
          }
        }
      ]
    }
  }
}

```

## vens\_remote\_action\_put

The new schema **vens\_remote\_action\_put** is sent by a user to execute a remote action on a VEN. Users authorized to use this method are global administrators, global organization owners, and workload managers.

The required properties include:

- **action** which describes the remote action type
- **vens** which describes an array of VENs to restart

```

{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "additionalProperties": false,
  "required": [
    "action",
    "vens"
  ],
  "properties": {

```

```

    "action": {
      "description": "Remote action type",
      "type": "string",
      "enum": [
        "restart"
      ]
    },
    "vens": {
      "description": "An array of VENS to restart",
      "type": "array",
      "minItems": 1,
      "maxItems": 1,
      "items": {
        "type": "object",
        "additionalProperties": false,
        "required": [
          "href"
        ],
        "properties": {
          "href": {
            "description": "VEN URI",
            "type": "string"
          }
        }
      }
    }
  }
}

```

## New Common Schemas

- **common deny\_rule\_actor**: The Enforcement Boundary Actor schema describes the actors as workloads and defines the exclusions.

```

{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "description": "Enforcement boundary actor",
  "type": "array",
  "minItems": 1,
  "items": {
    "type": "object",
    "additionalProperties": false,
    "properties": {
      "actors": {
        "description": "Rule actors are all workloads ('ams')",
        "type": "string",
        "enum": ["ams"]
      },
      "exclusion": {
        "description": "Boolean to specify whether or not the actor is an  
exclusion - only for labels and label groups",
        "type": "boolean",
        "expose_to": ["end_user_experimental"],
        "default": false
      }
    }
  }
}

```

```

    "label": {
      "$ref": "href_object.schema.json"
    },
    "label_group": {
      "$ref": "href_object.schema.json"
    },
    "ip_list": {
      "$ref": "href_object.schema.json"
    },
    "workload": {
      "expose_to": ["end_user_private_perm"],
      "$ref": "href_object.schema.json"
    }
  }
}

```

- **common deny\_rules\_get:** For deny\_rules, this gets the timestamps when the Enforcement Boundary was created, updated, and deleted. It also defines the users who originally created, updated, and deleted the boundary.

```

{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "description": "Enforcement boundary",
  "type": "object",
  "required": ["href", "providers", "consumers", "ingress_services"],
  "expose_to": ["end_user_private_perm"],
  "_comment": "Don't set additionalProperties:false here as it collides
with usage in allOf, set that in the schema that references this one
instead.",
  "properties": {
    "created_at": {
      "description": "Timestamp when this Enforcement Boundary was first
created",
      "type": "string",
      "format": "date-time"
    },
    "updated_at": {
      "description": "Timestamp when this Enforcement Boundary was last
updated",
      "type": "string",
      "format": "date-time"
    },
    "deleted_at": {
      "description": "Timestamp when this Enforcement Boundary was
deleted",
      "type": ["string", "null"],
      "format": "date-time"
    },
    "created_by": {
      "type": ["object", "null"],
      "required": ["href"],
      "properties": {
        "href": {
          "description": "User who originally created this Enforcement
Boundary",
          "type": "string"

```

```

    }
  },
  "updated_by": {
    "type": ["object", "null"],
    "required": ["href"],
    "properties": {
      "href": {
        "description": "User who last updated this Enforcement
Boundary",
        "type": "string"
      }
    }
  },
  "deleted_by": {
    "type": ["object", "null"],
    "required": ["href"],
    "properties": {
      "href": {
        "description": "User who deleted this Enforcement Boundary",
        "type": "string"
      }
    }
  },
  "update_type": {
    "$ref": "../common/sec_policy_update_type.schema.json"
  },
  "href": {
    "description": "The job URI.",
    "type": "string"
  },
  "providers": { "$ref": "deny_rule_actor.schema.json" },
  "consumers": { "$ref": "deny_rule_actor.schema.json" },
  "ingress_services": {
    "$ref": "sec_rule_ingress_services.schema.json"
  },
  "egress_services": {
    "$ref": "sec_rule_egress_services.schema.json"
  },
  "caps": {
    "$ref": "../common/entity_caps.schema.json"
  },
  "enabled": {
    "description": "Enabled flag",
    "type": "boolean"
  },
  "description": {
    "description": "Description",
    "type": ["string", "null"]
  },
  "network_type": {
    "$ref": "../common/rule_network_type.schema.json"
  },
  "override": {
    "description": "When true, the deny rule will override and take

```

```
precedence over other user defined allow rules.",
  "default": false,
  "type": "boolean"
},
"unscoped_consumers": {
  "description": "Set the scope for rule consumers to All",
  "type": "boolean"
}
}
}
```

- **common\_rule\_set**: Parent Rule Set of a Rule.

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "description": "Enforcement boundary",
  "type": "object",
  "required": ["href", "providers", "consumers", "ingress_services"],
  "expose_to": ["end_user_private_perm"],
  "_comment": "Don't set additionalProperties:false here as it collides
with usage in allOf, set that in the schema that references this one
instead.",
  "properties": {
    "created_at": {
      "description": "Timestamp when this Enforcement Boundary was first
created",
      "type": "string",
      "format": "date-time"
    },
    "updated_at": {
      "description": "Timestamp when this Enforcement Boundary was last
updated",
      "type": "string",
      "format": "date-time"
    },
    "deleted_at": {
      "description": "Timestamp when this Enforcement Boundary was
deleted",
      "type": ["string", "null"],
      "format": "date-time"
    },
    "created_by": {
      "type": ["object", "null"],
      "required": ["href"],
      "properties": {
        "href": {
          "description": "User who originally created this Enforcement
Boundary",
          "type": "string"
        }
      }
    },
    "updated_by": {
      "type": ["object", "null"],
      "required": ["href"],
      "properties": {
        "href": {
```

```

        "description": "User who last updated this Enforcement
Boundary",
        "type": "string"
    }
},
"deleted_by": {
    "type": ["object", "null"],
    "required": ["href"],
    "properties": {
        "href": {
            "description": "User who deleted this Enforcement Boundary",
            "type": "string"
        }
    }
},
"update_type": {
    "$ref": "../common/sec_policy_update_type.schema.json"
},
"href": {
    "description": "The job URI.",
    "type": "string"
},
"providers": { "$ref": "deny_rule_actor.schema.json" },
"consumers": { "$ref": "deny_rule_actor.schema.json" },
"ingress_services": {
    "$ref": "sec_rule_ingress_services.schema.json"
},
"egress_services": {
    "$ref": "sec_rule_egress_services.schema.json"
},
"caps": {
    "$ref": "../common/entity_caps.schema.json"
},
"enabled": {
    "description": "Enabled flag",
    "type": "boolean"
},
"description": {
    "description": "Description",
    "type": ["string", "null"]
},
"network_type": {
    "$ref": "../common/rule_network_type.schema.json"
},
"override": {
    "description": "When true, the deny rule will override and take
precedence over other user defined allow rules.",
    "default": false,
    "type": "boolean"
},
"unscoped_consumers": {
    "description": "Set the scope for rule consumers to All",
    "type": "boolean"
}

```

- ```

    }
  }

```
- **common sec\_rule\_egress\_services:** Array of objects.

```

{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "description": "Array of objects",
  "type": "array",
  "items": {
    "type": "object",
    "$ref": "../common/href_object.schema.json"
  }
}

```

- **common sec\_rules\_get:** For sec\_rules, this gets the timestamps when the Enforcement Boundary was created, updated, and deleted. It also defines the users who originally created, updated, and deleted the boundary.

```

{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "description": "Enforcement boundary",
  "type": "object",
  "required": ["href", "providers", "consumers", "ingress_services"],
  "expose_to": ["end_user_private_perm"],
  "_comment": "Don't set additionalProperties:false here as it collides with usage in allOf, set that in the schema that references this one instead.",
  "properties": {
    "created_at": {
      "description": "Timestamp when record was first created",
      "type": "string",
      "format": "date-time"
    },
    "updated_at": {
      "description": "Timestamp when record was last updated",
      "type": "string",
      "format": "date-time"
    },
    "deleted_at": {
      "description": "Timestamp when record was deleted",
      "type": ["string", "null"],
      "format": "date-time"
    },
    "created_by": {
      "type": "object",
      "properties": {
        "username": {
          "description": "The username which created this record",
          "type": "string"
        }
      }
    },
    "updated_by": {
      "type": "object",
      "properties": {
        "username": {
          "description": "The username which last updated this record",

```



```

        "type": "string"
    }
}
},
"deleted_by": {
    "type": ["object", "null" ],
    "properties": {
        "username": {
            "description": "The username which deleted this record",
            "type": "string"
        }
    }
},
"update_type": {
    "description": "Type of update",
    "oneOf": [
        {
            "type": "null"
        },
        {
            "type": "string",
            "enum": ["create", "update", "delete"]
        }
    ]
},
"update_label": {
    "description": "Type of update",
    "oneOf": [
        {
            "type": "null"
        },
        {
            "type": "string",
            "enum": ["create", "update", "delete"]
        }
    ]
},
"href": {
    "description": "URI of object",
    "type": "string"
},
"enabled": {
    "description": "Enabled flag",
    "type": "boolean"
},
"description": {
    "description": "Description",
    "type": ["string", "null"]
},
"ingress_services": { "$ref":
"sec_rule_ingress_services.schema.json" },
    "egress_services": { "$ref": "sec_rule_egress_services.schema.json" },
    "resolve_labels_as": { "$ref":
"sec_rule_resolve_labels_as.schema.json" },
    "sec_connect": {

```

```

    "description": "Whether a secure connection is established",
    "type": "boolean"
  },
  "stateless": {
    "expose_to": ["end_user_experimental"],
    "description": "Whether packet filtering is stateless for the rule",
    "type": "boolean"
  },
  "machine_auth": {
    "expose_to": ["end_user_experimental"],
    "description": "Whether machine authentication is enabled",
    "type": "boolean"
  },
  "providers": { "$ref":
"sec_policy_rule_sets_sec_rules_providers_get.schema.json" },
  "consumers": { "$ref":
"sec_policy_rule_sets_sec_rules_consumers_get.schema.json" },
  "consuming_security_principals": { "$ref":
"consuming_security_principals_get.schema.json" },
  "unscoped_consumers": {
    "description": "Set the scope for rule consumers to All",
    "type": "boolean"
  },
  "use_workload_subnets": {
    "$ref": "sec_rule_use_workload_subnets.schema.json"
  },
  "rule_set": { "$ref": "../common/rule_set.schema.json" },
  "log_flow": {
    "description": "If false, the VEN will not log any traffic that
matches this flow.",
    "type": "boolean",
    "expose_to": ["end_user_private_transitional"]
  },
  "network_type": { "$ref": "../common/rule_network_type.schema.json" }
}

```

## Changed APIs in 25.2.10

The following public APIs have changed in 25.2.10.

### Simplified schema by using a reference for

- **sec\_policy\_allow\_get**

```

{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "array",
  "items": {
    "allOf": [
      {
        "$ref": "sec_policy_rule_sets_sec_rules_get.schema.json"
      }
    ]
  }
}

```

```

    }
  }
}

```

The initial schema, which contained the required objects "enabled", "providers", "consumers", and "ub\_service", has been simplified to use a reference to the `sec_policy_rule_sets_sec_rules_get` schema.

### **Additional properties `container_workload` and `kubernetes_workload` were added to**

- `sec_policy_rule_search_consumers`
- `sec_policy_rule_search_providers`

```

{
  "items": {
    "properties": {
      "container_workload__added": {
        "type": "object",
        "additionalProperties": false,
        "required": [
          "href"
        ],
        "properties": {
          "href": {
            "description": "Container workload URI",
            "type": "string"
          }
        }
      },
      "kubernetes_workload__added": {
        "type": "object",
        "additionalProperties": false,
        "required": [
          "href"
        ],
        "properties": {
          "href": {
            "description": "Kubernetes workload URI",
            "type": "string"
          }
        }
      }
    }
  }
}

```

In the initial API `sec_policy_rule_search_consumers`, in addition to properties "actors", "label", "label\_group", "workload", "virtual\_service", and "ip\_list", two new ones have been added:

### **Additional properties:**

- `kubernetes_workload`: href of `kubernetes_workload` to which the searched rule should apply to
- `container_workload`: href of `container_workload` to which the searched rule should apply to

**Property rule\_types added to****• sec\_policy\_rule\_search\_post**

```
{
  "properties": {
    "rule_types": {
      "description": "List of rule types",
      "type": "array",
      "items": {
        "type": "string",
        "enum": [
          "sec_rules",
          "deny_rules",
          "override_deny_rules",
          "ip_tables_rules"
        ]
      }
    }
  }
}
```

A new property rule\_types was added, which lists the rule types: sec\_rules, deny\_rules, override\_deny\_rules, and ip\_tables\_rules. Request rule\_types that should be searched for.

**Simplified schema****• sec\_policy\_rule\_search\_post\_response**

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "additionalProperties": false,
  "properties": {
    "sec_rules": {
      "description": "Array of allow rules",
      "type": "array",
      "items": {
        "allOf": [
          {
            "$ref": "../common/sec_rules_get.schema.json"
          },
          {
            "rule_set": {
              "$ref": "../common/rule_set.schema.json"
            }
          }
        ]
      }
    },
    "deny_rules": {
      "description": "Array of deny rules",
      "type": "array",
      "items": {
        "allOf": [
```

```

    {
      "$ref": "../common/deny_rules_get.schema.json"
    },
    {
      "rule_set": {
        "$ref": "../common/rule_set.schema.json"
      }
    }
  ]
},
"override_deny_rules": {
  "description": "Array of override deny rules",
  "type": "array",
  "items": {
    "allOf": [
      {
        "$ref": "../common/deny_rules_get.schema.json"
      },
      {
        "rule_set": {
          "$ref": "../common/rule_set.schema.json"
        }
      }
    ]
  }
},
"ip_tables_rules": {
  "type": "array",
  "items": {
    "allOf": [
      {
        "$ref": "../common/ip_tables_rules_get.schema.json"
      },
      {
        "rule_set": {
          "$ref": "../common/rule_set.schema.json"
        }
      }
    ]
  }
}
}

```

This schema was simplified using `allOf` and a reference to the two existing schemas.

# What's New and Release Notes for LW-VEN 1.1

## What's New in LW-VEN Release 1.1.0

The following new feature is added in this release:

### Support for flow reporting for legacy Windows servers

Beginning with release 1.1.0, the LW-VEN can enable the native Windows Firewall log on your legacy Windows server, which allows the LW-VEN to generate and log traffic flow information for ingestion by the PCE. After ingesting the log information, the PCE displays it in its Map and Traffic views to help you gain insights about and create policy for your business applications. See [Enable Flow Reporting](#).

## Release Notes in LW-VEN 1.1

Review these release notes for a list of resolved and known issues.

### Resolved Issues in 1.1.10 LW-VEN

| Issue    | Description                                                                                                                                                                                                                                                                                                                                           | Status   |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| E-120840 | <b>ICMP rule generation created empty command</b><br><br>When the LW-VEN generated a rule to add/modify/delete an ICMP rule, it also generated an empty command which caused the LW-VEN to fail when it tried to apply policy to that empty command.                                                                                                  | Resolved |
| E-120184 | <b>Excessive time needed for Windows firewall to apply Illumio rules</b><br><br>Policy application failed when the Windows firewall took longer than expected to apply PCE-generated rules. This issue is fixed. Policy is now applied in the background. Note that applying firewall commands on a low-powered server can take longer than expected. | Resolved |
| E-120119 | <b>Policy conflict lead to policy sync failure and LW-VEN crash</b><br><br>A conflict occurred when merging the default Illumio policy with the customer's Illumio-generated policy. This caused an Illumio policy sync failure and crashed the LW-VEN service.                                                                                       | Resolved |

## Resolved Issues in 1.1.0 LW-VEN

| Issue     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Status   |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|
| E-119190  | <p><b>LW-VEN activation failed on non-UTF-8 legacy Windows workloads</b></p> <p>LW-VEN activation failed on workloads configured for non-US languages. This happened because LW-VEN version 1.0.1 doesn't support non-UTF-8 strings. This issue is fixed. Support for non-UTF-8 was added in LW-VEN 1.1.0.</p>                                                                                                                                                                                                                                                                                                | Resolved |
| E-118952  | <p><b>Activate option appeared during "non-fresh" LW-VEN installation</b></p> <p>When installing an LW-VEN on a supported legacy Windows machine on which an LW-VEN is already activated, the option Start + Activate appeared, which was unexpected. As this wasn't a fresh installation, only the Start option should've appeared, not Start+Activate. This issue is resolved. Now, only Start appears during non-fresh installations.</p>                                                                                                                                                                  | Resolved |
| (E-118764 | <p><b>Users weren't prompted during LW-VEN activation if activation command was run without options</b></p> <p>Attempting to activate LW-VEN failed if users issued the illumio-lwven-ctl activate command without options. A command prompt appeared but no prompts displayed and the activation hung. This issue is fixed.</p>                                                                                                                                                                                                                                                                              | Resolved |
| E-118600  | <p><b>LW-VEN 1.0.1 failed to apply 2008 firewall policy that contained very large port range</b></p> <p>The Windows Firewall rejected Illumio security policy rules that specified extremely large port ranges, resulting in policy not being applied. This issue is resolved. Rules exceeding 1000 ports are now split into multiple rules, and rules with large port ranges are no longer rejected. Caveat: Customers should keep in mind that applying a policy with a large port range may cause the Windows firewall to become unresponsive and take a long time to respond to any firewall command.</p> | Resolved |

# Illumio Core for Kubernetes

This document provides an overview of how you can use Illumio Core with Kubernetes or OpenShift.

Published: 2025

## Illumio Core for Kubernetes 5.4

## Illumio Core for Kubernetes What's New and Release Notes for 5.3

This document describes the new features, enhancements, resolved issues, and known issues for the 5.3.x releases of Illumio Core for Kubernetes, also known as Illumio Kubernetes Operator. This product was formerly known as Illumio Containerized VEN, or C-VEN. Illumio Core for Kubernetes also includes the related required component Kubelink. Because of this heritage, some references to this product as "C-VEN" occur throughout the documentation.

### What's New in Illumio Core for Kubernetes 5.3.2

Learn what's new in the 5.3.2 release of Illumio Core for Kubernetes, also known as Illumio Kubernetes Operator.

#### Product Version

**Compatible PCE Versions:** 23.5.31 and later

**Current Illumio Core for Kubernetes Version:** 5.3.2, which includes:

- **C-VEN version:** 23.4.4
- **Kubelink version:** 5.3.2
- **Helm Chart version:** 5.3.2

#### Release Types and Numbering

Illumio Core release numbering uses the following format: "a.b.c-d+e".

- "a.b": Standard or LTS release number, for example, "2.2"
- ".c": Maintenance release number, for example, ".1"
- "-d": Optional descriptor for pre-release versions, for example, "preview2"

### What's New in Release 5.3.2

Illumio Core for Kubernetes release 5.3.2 consists of several resolved issues and bug fixes described here:[Release Notes for 5.3.2 \[34\]](#).



## What's New in Illumio Core for Kubernetes 5.3.1

The following describes what is new in the 5.3.1 release of Illumio Core for Kubernetes, also known as Illumio Kubernetes Operator.

### Product Version

**Compatible PCE Versions:** 23.5.31 and later

**Current Illumio Core for Kubernetes Version:** 5.3.1, which includes:

- **C-VEN version:** 23.4.3
- **Kubelink version:** 5.3.1
- **Helm Chart version:** 5.3.1

### Release Types and Numbering

Illumio Core release numbering uses the following format: "a.b.c-d+e".

- "a.b": Standard or LTS release number, for example, "2.2"
- ".c": Maintenance release number, for example, ".1"
- "-d": Optional descriptor for pre-release versions, for example, "preview2"

## What's New in Release 5.3.1

Here's a summary of the new features in this release:

- **Support installation of Illumio Core for Kubernetes into a custom namespace**

You can now install Illumio Core for Kubernetes into a custom namespace instead of into the default namespace of `illumio-system`. The default namespace is overridden for backward compatibility by using the variable `namespaceOverride: illumio-system`.

For example, to install into the `ilo` namespace, specify the namespace with the `--namespace` option and the `--set` option specifying `namespaceOverride` to `null`:

```
helm install illumio -f illumio-values.yaml oci://quay.io/illumio/illumio --version 5.3.1 --namespace ilo --create-namespace --set namespaceOverride=null
```

Alternatively, specify the namespace with the `--namespace` option but also use `--set` to explicitly set `namespaceOverride` to `ilo`:

```
helm install illumio -f illumio-values.yaml oci://quay.io/illumio/illumio --version 5.3.1 --namespace ilo --create-namespace --set namespaceOverride=ilo
```

- **"Enforce NAT Mode 1:1" option creates public workload interface**

Workloads now have a new optional feature "Enforced NAT mode 1:1" that, when enabled, ensures that pseudo-public IP addresses are detected and are then saved as workload interfaces even when the C-VEN (or VEN) cannot identify the datacenter or service provider. If this option remains disabled, the PCE either relies on the C-VEN to report the public IP address or derives it based on a datacenter match. When this option is enabled on a Container Cluster, the feature applies to all host workloads on all of its cluster nodes.

- **Map Kubernetes Workload labels to Illumio labels**

You can now map labels on Kubernetes Workloads to corresponding Illumio labels by using a `workloadLabelMap` section in a label mapping Custom Resource Definition (CRD) within

a YAML, in a `kind: LabelMap` declaration. This Kubernetes Workload label mapping is otherwise defined like the existing feature for mapping Kubernetes node (or host workloads) labels to Illumio labels. See [Map Kubernetes Node or Workload Labels to Illumio Labels](#).



### CAUTION

Mapping labels for Kubernetes Workloads only works in CLAS-enabled deployments, and requires PCE release 24.5.0.

- **Added Support for hostPort**

Traffic enforcement of Kubernetes Workloads, which have Pods exposed via hostPort, is now available.



### CAUTION

The support for hostPort is available only on deployments running PCE 24.5.0.

- **Added support for Google Kubernetes Engine (GKE)**

The Google Kubernetes Engine (GKE) is now a supported orchestration platform on Illumio Core for Kubernetes CLAS-enabled deployments that use PCE release 24.5.0 or later. For complete requirements for GKE support, see the Illumio Support Portal page on "Kubernetes Operator OS Support and Dependencies."

- **Kubernetes Workloads Show Label Source**

A new `com.illumio.result.*` annotation on a PCE label for a Kubernetes Workload now shows the source of that label with a code appended to the annotation: where the code `cwp` means from a Container Workload Profile, `map` means from a LabelMap, and `annotations` means from a Kubernetes annotation. These values are shown in the PCE UI on the workload details page (under the Kubernetes Attributes section), and at the command-line as part of the `kubectl get deploy` command output.

## Limitations

- You cannot change an existing deployment in the `illumio-system` namespace to a custom namespace through an upgrade.
- Mapping labels for Kubernetes Workloads is available only in CLAS-enabled deployments, and currently requires PCE release 24.5.0.

## Base Image Upgraded

The C-VEN base OS image has been upgraded to address several vulnerabilities, including CVE-2024-45337 and CVE-2024-45338. Customers are advised to upgrade to Core for Kubernetes 5.3.1 for these security fixes.

## Release Notes for 5.3.2

These release notes describe the resolved issues for this release.

## Resolved Issues in Release 5.3.2

| Issue                 | Description                                                                                                                                                                                                                 |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| E-125731,<br>E-125362 | <b>C-VEN - Improve performance by adjusting retry handling</b><br><br>Retry logic has been adjusted to reduce latency times, and improve performance.                                                                       |
| E-125661              | <b>Kubelink: Improved PCE load handling</b><br><br>Several PCE timeout values have been adjusted to improve PCE performance and resilience when under load, and to more appropriately enter degraded mode when appropriate. |

## Resolved Issues in 5.3.1

This section provides a list of resolved issues in Release 5.3.1.

## Resolved Issues

| Issue    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| E-123084 | <p><b>Kubelink: wrong LabelMap feature flag for older 24.x PCE versions</b></p> <p>Kubelink incorrectly interpreted some older PCE versions as higher (more recent) than 24.5, which enabled the LabelMap feature for PCE versions that do not support it. This caused Kubelink 5.3.0 to be incompatible with many older 24.x PCE versions.</p>                                                                                                                                                                                                   |
| E-123080 | <p><b>Kubelink: labels defined by Container Workload Profile are ignored when Kubelink restarts</b></p> <p>Kubelink was not receiving accurate data for workloads using managed Container Workload Profiles. So when Kubelink restarted, it might use out-of-date Container Workload Profile data and improperly remove or mislabel some workloads, causing incorrect policies.</p>                                                                                                                                                               |
| E-122830 | <p><b>Kubelink: skip of ACK of unknown workload causes repeated policy calculations and sets ACK</b></p> <p>Part of the policy Kubelink received from the PCE for disconnected C-VEs was not being acknowledged back to the PCE, which caused unnecessary policy calculations and high PCE load.</p>                                                                                                                                                                                                                                              |
| E-122553 | <p><b>C-VEN 23.4.x fw_tampering_revert_failure after upgrade</b></p> <p>False-positive firewall tamper alerts ("VEN firewall tampered") appeared after upgrading to C-VEN 23.x, because of the old and unused Illumio iptables chain.</p>                                                                                                                                                                                                                                                                                                         |
| E-122422 | <p><b>C-VEN activation failing</b></p> <p>In some cases, attempts to bring onboard and pair a second Kubernetes AWS EKS cluster were failing to activate the C-VEs.</p>                                                                                                                                                                                                                                                                                                                                                                           |
| E-122306 | <p><b>Kubelink: One service appears multiple times in service update</b></p> <p>Kubelink was sending one service multiple times in an update request to PCE, which caused multiple duplicates of Service Backends, and slowed PCE responsiveness. Older Kubelink 3.1.x and 4.x also have this issue and should be upgraded to Kubelink 5.3.0, either using Helm chart 5.3.0, or by using YAML files generated from this Helm chart version. Kubelink 5.3.0 in non-CLAS mode is backward compatible with all currently supported PCE versions.</p> |
| E-121122 | <p><b>C-VEN: False positive vulnerability detection on Quay</b></p> <p>The Quay vulnerability scanner falsely detected C-VEN as having high severity vulnerabilities.</p>                                                                                                                                                                                                                                                                                                                                                                         |
| E-120773 | <p><b>Increasing memory use and "out of memory errors" occur on 22.5.14 C-VEN nodes</b></p> <p>Resolved intermittent "out of memory" occurrences in C-VEN 22.5.14.</p>                                                                                                                                                                                                                                                                                                                                                                            |

## Illumio Core for Kubernetes Release Notes 5.2

January 2025

### About Illumio Core for Kubernetes 5.2

These release notes describe the resolved issues, known issues, and related information for the 5.2.x releases of Illumio Core for Kubernetes, formerly known as Illumio Containerized VEN, or C-VEN. Illumio Core for Kubernetes also includes the related required component,

Kubelink. Because of this heritage, many references to this product as "C-VEN" are still used throughout the documentation.

**Document Last Revised:** January 2025

## Product Version

**Compatible PCE Versions:** 23.5.10 and later releases

**Current Illumio Core for Kubernetes Version:** 5.2.3, which includes:

- C-VEN version: 23.4.2
- Kubelink version: 5.2.1
- Helm Chart version: 5.2.3

## Updates for Core for Kubernetes 5.2.3

### Kubelink

#### Resolved Issue

- **One service appears multiple times in service update** (E-122306)  
Kubelink was sending one service multiple times in an update request to PCE, which caused multiple duplicates of Service Backends, and slowed PCE responsiveness. Older Kubelink 3.1.x and 4.x also have this issue and should be upgraded to Kubelink 5.2.1, either using Helm chart 5.2.3, or by using yaml files generated from this Helm chart version. Kubelink 5.2.1 in non-CLAS mode is backward compatible with all currently supported PCE versions.

## Updates for Core for Kubernetes 5.2.2

### C-VEN

#### Resolved Issues

- **Multiple C-VEs not syncing policy** (E-122102)  
In larger CLAS-enabled clusters with very big policies, even though C-VEs initially appeared to be properly synced, the policy was not updated.
- **C-VEN on PCE UI has "-dev" in version but image pulled from helm does not** (E-120423)  
After upgrading to release 5.2.0, the C-VEN version was reported with a "-dev" string appended (for example, "23.4.0-8-dev") in the PCE UI (at the VEN details page) and other locations like in `/etc/agent_version`, but the image specified in the C-VEN daemonset resource did not.
- **C-VEN: unable to send flows if there is a lot of data** (E-119110)

When C-VEN attempted to send a large amount of flow data at once, the transmission would fail, and after a few retries the AgentMgr process would crash, causing C-VEN to stop sending flow records.

## What's New in Release 5.2.1

- **Helm Chart option to Disable NodePort Forwarding**

A new option was added to Helm Chart for C-VEN that disables NodePort forwarding on host workloads. After setting `enforceNodePortTraffic: never` in the Helm values file, C-VEN behaves like before in its 22.5 version-- that is, the forward chain on Node is open, and custom iptables rules must be used to enforce traffic in this chain.

## Updates for Core for Kubernetes 5.2.1

### Kubelink

#### Resolved Issues

- **Kubelink can't start on OpenShift because of fsGroup 1001** (E-120425)

When using Helm Chart 5.2.0 on OpenShift, Kubelink would not start because of fsGroup 1001.

### C-VEN

#### Resolved Issues

In an early version of these Release Notes issues E-119682 and E-119110 were incorrectly listed as being resolved.

- **NodePort access is working when it should be blocked** (E-120655)

NodePort traffic was being always allowed, with or without a rule allowing the traffic from an external resource to the NodePort service. This issue was fixed by adding missing legacy iptables command line utilities to the UBI9-based C-VEN.

- **Move C-VEN base image to a smaller image** (E-118492)

C-VEN now uses a UBI9-micro image as its base image, using the current latest version 9.4-15.

## What's New in Release 5.2.0

- **"Wait for Policy" Feature**

With a new Wait For Policy feature, CLAS-enabled Kubelink can be configured to automatically and transparently delay the start of an application container in a pod until a policy is properly applied to the pod. This feature replaces the local policy convergence controller, the Illumio readiness gate. A readiness gate required adding the `readinessGates.conditionType` into the spec YAML file of the Kubernetes Workload. Instead, Wait For Policy uses an automatically injected init container, with no change of the user application needed. When enabled, Wait For Policy synchronizes the benefit of Kubernetes automatic container creation with the protection of proper policy convergence into the new container. For more information, see ["Wait For Policy" Feature \[42\]](#).

- **CLAS Flat Network Support**

Starting in version 5.2.0, the Kubelink Operator supports flat network CNIs in CLAS mode, a feature that was previously only available in non-CLAS mode. This update includes compatibility with flat network types such as [Azure CNI Pod Subnet](#) and [Amazon VPC CNI](#). To enable a flat network CNI, set the `networkType` parameter to `flat` in the Helm Chart's `illumio-values.yaml` file during installation.

Also note that in CLAS-enabled flat networks, if a pod communicates with a virtual machine outside the cluster using private IP addresses, you must enable the annotation `meta.illumio.podIPObservability`. This is a scenario in which the virtual machine is in a private network and has an IP address from the same range as cluster nodes and pods. In this case, the PCE needs to know the private IP address of the pod to be able to open a connection on the virtual machine. The main benefit of CLAS is that the PCE no longer directly manages individual pods, so the implementation expects a specific annotation on such pods. Traffic between such private IPs will be blocked without this annotation, and will appear in the UI as blocked.

In this case, when the application communicates through private IPs, add the following annotation so that Kubelink can then report the private IPs of Kubernetes Workloads to the PCE:

```
metadata:
  annotations:
    meta.illumio.podIPObservability: "true"
```

- **Kubelink Support Bundle**

To assist the Illumio Support team with more details for troubleshooting, Kubelink now provides a support bundle that collects up to 2 GB of logs, metrics, and other data inside its pod. Future versions will add the option to upload these support bundles to the PCE. Currently, you must copy this support bundle by running the script `/support_bundle.sh` inside the Kubelink pod. The script generates debug data, creates a gzipped tar archive using `stdout` as output, and encodes this data using Base64.

Use the following command to generate and transfer the Kubelink support bundle from its pod:

```
kubectl --namespace illumio-system exec deploy/illumio-kubelink
-- /support_bundle.sh | base64 --decode > /tmp/kubelink_support.tgz
```

Send the resulting compressed archive file to Illumio Support when requested.

- **Base OS Upgraded to UBI9**

The base OS has been upgraded to Red Hat Universal Base Image 9 (micro UBI9 for Kubelink, mini UBI9 for C-VEN).



### IMPORTANT

**Important Notice:** With the base image upgrade for both Kubelink and C-VEN, you must adjust resource allocations according to the guidance described below in the "[Resource Allocation Guidelines \[40\]](#)" section. You must ensure that resources are updated prior to the upgrade to achieve optimal performance, and to avoid any potential degradation in product performance.

- **Enhanced Pod Stability for Kubelink and C-VEN**

To address the challenge of pod eviction during Kubernetes cluster issues or space shortages, Kubelink was previously the first pod to be evicted, which led to failures in policy enforcement. Recognizing the critical need for stability, Helm Chart version 5.2.0 introduces default priority classes for both Kubelink and C-VEN. Kubelink is now assigned the priority class of `system-cluster-critical`, while C-VEs receive `system-node-critical`. This

implementation significantly enhances the resilience of your deployments, ensuring that key components remain operational even under resource constraints.

- **Changes to Supported Orchestration Platforms and Components in 5.2.0**

The 5.2.0 release contains several changes to supported platforms and components. For full details, see [Kubernetes Operator OS Support and Dependencies](#) on the Illumio Support portal (log in required).

## Resource Allocation Guidelines

New resource allocation guidelines have been developed to help configure deployments to achieve optimal performance and cost-efficiency.

These guidelines are grouped into the following general deployment sizes:

- **Small-scale:** Customers with limited Kubernetes deployments and moderate workloads.
- **Medium-scale:** Customers with moderate-sized Kubernetes environments and growing workloads.
- **Large-scale:** Customers with extensive Kubernetes deployments and high-performance requirements.

The following variables determine the deployment sizes listed above:

- Number of nodes per cluster
- Total number of workloads per cluster
- Total policy size per cluster

Set the `resources` values in the appropriate pod spec (Kubelink or C-VEN) `yaml` file under the `storage` section, as shown in the following example:

```
storage:
  sizeGi: 1
  resources:
    limits:
      memory: 600Mi
    requests:
      memory: 500Mi
      cpu: 500m
```

If you have two parameters that match one category, and a third parameter that matches another, it's important to select the category based on the highest value among them.

For instance, if the number of nodes per cluster is 8, and the total number of Kubernetes workloads is 500, but the average size of the policy is 1 Gi, the resource allocation should align with the large-scale resource allocation. This ensures that your resources are appropriately scaled to meet the demands of your workloads, optimizing performance and stability.

In practice, monitor these resources, and if usage is at 80% of these limits, then consider increasing.

**NOTE** that amounts are expressed in mebibytes (Mi) and gibibytes (Gi) and not in megabytes (MB) or gigabytes (GB).



**Small-scale resource allocation**

| Customer Category | Nodes per Cluster | Total K8s Workloads | Total Policy Size |                |
|-------------------|-------------------|---------------------|-------------------|----------------|
| Small-scale       | 1 - 10            | 0 - 1000            | 0 - 1.5 Mi        |                |
| <b>Resources</b>  |                   | <b>C-VEN</b>        | <b>Kubelink</b>   | <b>Storage</b> |
| Requests          | CPU               | 0.5                 | 0.5               | 0.5            |
| Requests          | memory            | 600 Mi              | 500 Mi            | 500 Mi         |
| Limits            | CPU               | 1                   | 1                 | 1              |
| Limits            | memory            | 700 Mi              | 600 Mi            | 600 Mi         |
| Volumes           | size limits       | n/a                 | n/a               | 1 Gi           |

**Medium-scale resource allocation**

| Customer Category | Nodes per Cluster | Total K8s Workloads | Total Policy Size |                |
|-------------------|-------------------|---------------------|-------------------|----------------|
| Medium-scale      | 10 - 20           | 1000 - 5000         | 1.5 Mi - 500 Mi   |                |
| <b>Resources</b>  |                   | <b>C-VEN</b>        | <b>Kubelink</b>   | <b>Storage</b> |
| Requests          | CPU               | 2                   | 2                 | 1              |
| Requests          | memory            | 3 Gi                | 5 Gi              | 5 Gi           |
| Limits            | CPU               | 3                   | 2                 | 2              |
| Limits            | memory            | 5 Gi                | 7 Gi              | 7 Gi           |
| Volumes           | size limits       | n/a                 | n/a               | 5 Gi           |

## Large-scale resource allocation

| Customer Category | Nodes per Cluster | Total K8s Workloads | Total Policy Size |         |
|-------------------|-------------------|---------------------|-------------------|---------|
| Large-scale       | 20+               | 5000 - 8000         | 500 Mi - 1.5 Gi   |         |
| Resources         |                   | C-VEN               | Kubelink          | Storage |
| Requests          | CPU               | 2                   | 3                 | 1       |
| Requests          | memory            | 6 Gi                | 10 Gi             | 10 Gi   |
| Limits            | CPU               | 3                   | 4                 | 2       |
| Limits            | memory            | 8 Gi                | 12 Gi             | 12 Gi   |
| Volumes           | size limits       | n/a                 | n/a               | 10 Gi   |

## "Wait For Policy" Feature

With a new *Wait For Policy* feature, CLAS-enabled Kubelink can be configured to automatically and transparently delay the start of an application container in a pod until a policy is properly applied to that container. This synchronizes the benefit of automatic container creation with the protection of proper policy convergence into the new container.

This Wait For Policy feature replaces the existing local policy convergence controller, also known as a readiness gate. A readiness gate required manually adding the `readinessGate` condition into the spec of the Kubernetes Workload. Instead, Wait For Policy uses an automatically injected init container, which requires no change to the user application.

## Behavior

When Wait For Policy is enabled, Kubelink creates a new `MutatingWebhookConfiguration`. This webhook injects an Illumio init container into every new pod. Now a new pod lifecycle consists of the following sequence of actions:

1. Kubernetes creates a pod.
2. The pod creation request is intercepted by a mutating webhook.
3. Kubernetes requests MutatingAdmissionWebhook Controller running in Kubelink.
4. Controller returns with a new pod patched with an Illumio init container.
5. Init container starts in the pod, and periodically checks the policy status of the pod using the Kubelink status server.
6. At the same time, Kubelink is preparing a policy for the new pod, and is sending the policy to the pod's C-VEN.
7. The C-VEN applies policy to the pod, and sends an acknowledgment to Kubelink.
8. Kubelink reports that the policy is now applied to the init container.
9. The Init container exits, and allows the original container to start.
- 10 If a policy is not applied within the configured time (see [Configuration \[43\]](#) section for Helm Chart `waitForPolicy.timeout` parameter), the init container exits anyway, and allows the original container to start.

The Illumio init container must be accessible from all namespaces that use Wait for Policy. An easy way to ensure this accessibility is to make init available from a public repository.

However, a private repository can be used if you manage the secret deployment properly, such as by deploying init from the same repository as all other containers, or by using a secret management tool.

## Configuration

The Wait For Policy feature is disabled by default. To enable it, change the `waitForPolicy: enabled` value to `true` in the Helm Chart `illumio-values.yaml` file. The following is the default Helm Chart configuration for Wait For Policy:

```
## Wait for Policy - Illumio delays the start of Pods until policy is
## applied
waitForPolicy:
  ## @param waitForPolicy.enabled Enable Wait for Policy feature
  enabled: false
  ## @param waitForPolicy.ignoredNamespaces List of namespaces where
  ## Illumio
  ## doesn't delay start of Pods. kube-system and
  ## illumio-system name are ignored by Kubelink for this feature by
  ## default,
  ## even if not specified in this list.
  ignoredNamespaces:
    - kube-system
    - illumio-system
  ## @param waitForPolicy.timeout How long will pods wait for policy, in
  ## seconds
  timeout: 130
```

Pods starting in namespaces listed in `ignoredNamespaces` start immediately, without an Illumio init container injected into them. The namespaces `kube-system` and `illumio-system` are always ignored by the MutatingAdmissionWebhook Controller running in Kubelink, even if those are not specified in the configuration. The default value of `ignoredNamespaces` contains `kube-system` and `illumio-system` for reference, and can be extended with custom namespaces.

The `timeout` value is a total allowed run time of the init container. After this time elapses, the init container exits even if policy is not applied, and allows the original container to start.

## Updates for Core for Kubernetes 5.2.0

### Kubelink

#### Resolved Issues

- **Helm: pull secret to quay gets created even if no credentials are set** (E-119659)  
Helm chart now creates Illumio pull secret only if credentials are specified and also externally passed secret names are included.
- **Kubelink: error concurrent map read and map write** (E-119626)  
Kubelink was restarted because previous container exited with the message "fatal error concurrent map read and map write."
- **Kubelink: Update base image to address vulnerabilities** (E-119429)  
The Unified Base Image was upgraded to address CVE-2023-45288.

- **Kubelink needs to have higher priority assigned to avoid going to evicted state** (E-113920)

If the Kubernetes cluster encounters problems or runs out of space, Kubelink was the first pod to be put into the evicted state, which caused policy enforcement to fail. To prevent permanent eviction, in Helm chart version 5.2.0 the Kubelink Deployment and C-VEN DaemonSets are assigned priority classes by default -- `system-cluster-critical` for Kubelink and `system-node-critical` for C-VEs.

## C-VEN

### Resolved Issues

- **CVEN: Update base image to address vulnerabilities** (E-119428)

The 23.4 C-VEN Unified Base Image was upgraded to the latest UBI9 to address vulnerabilities described in CVE-2014-3566, CVE-2014-3566, CVE-2014-3566, CVE-2022-3358, and CVE-2023-27533.

- **Cannot deploy C-VEN to GKE when using default OS** (E-116506)

For GKE clusters, when using the default cluster OS (Container-Optimized OS from Google), the node filesystems are read-only. This prevented C-VEN from mounting `/opt/illumio_ven_data` and writing into it for persistent storage.

To resolve this issue, a new variable `cven.hostBasePath` was added to the 5.2.0 Helm Chart to specify where the C-VEN DaemonSet mounts its data directory. The default value is `/opt`. Use this variable to specify where the C-VEN DaemonSet mounts its data directory. If using a Container-Optimized OS, you can set the directory to `/var`.

- **[CVEN]: Failed to load policy** (E-115231)

The log message "Error: Failed to load policy" was appearing during scenarios that were obvious or expected. The log level for this message has been changed from Error to Info.

- **Re-adding node does not re-pair it** (E-98120)

When deleting and then re-adding the same node, the node would not reappear, and its policy disappeared.

## Illumio Core for Kubernetes Release Notes 5.1

Published: September 4, 2024

### Core for Kubernetes 5.1.10

**Compatible PCE Versions:** 23.5.10 and most later releases

**Current Illumio Core for Kubernetes Version:** 5.1.10, which includes:

- C-VEN version: 23.3.1
- Kubelink version: 5.1.10
- Helm Chart version: 5.1.10

Before deploying any Illumio Core for Kubernetes 5.1.x version, confirm your PCE version supports it. For example, currently Illumio Core for Kubernetes versions 5.1.0 and 5.1.2 are supported **only** with PCE versions 23.5.10 (for On Premises customers) or 24.1.x (for SaaS customers), but NOT on PCE versions 23.5.1 or 23.6.0, or any lower versions. For complete

compatibility details, see the [Kubernetes Operator OS Support and Dependencies](#) page on the Illumio Support Portal.

Illumio Core release numbering uses the following format: "a.b.c-d+e".

- "a.b": Standard or LTS release number, for example, "2.2"
- ".c": Maintenance release number, for example, ".1"
- "-d": Optional descriptor for pre-release versions, for example, "preview2"

## Limitations

### • NodePort

The following limitations exist regarding NodePort policy enforcement and flows:

- Only NodePort Services with `externalTrafficPolicy` set to "cluster" are supported. (This is the default and most frequently used value for this setting.)
- When writing rules to allow traffic to flow from external (to the cluster) entities and NodePort Service, the source side of the rule must contain all nodes in the cluster.

For example, given the following setup:

- Worker nodes in the cluster are labeled as Role: Worker Node
- Clients accessing the Service running in the Kubernetes cluster are labeled Role: Client
- The NodePort Service is labeled Role: Ingress

Normally, the rule would be written as Role: Client -> Role: Ingress. However, for this release the rule must also include all nodes in the cluster to work correctly: Role: Client + Role: Worker Node -> Role: Ingress.

### • Flat Network support in CLAS mode

Using EKS or AKS in a flat network topology, such as EKS with AWS VPC CNI or AKS with Azure CNI, is not supported in CLAS-enabled clusters.

## Updates for Core for Kubernetes 5.1.10

### Kubelink

### Resolved Issues

- **Last updated policy timestamp for C-VEs reflects Kubernetes Workload policy changes** (E-118372)

The last updated policy timestamp on C-VEs now updates after a C-VE successfully updates the policy for its pods.

- **Unexpected Potentially Blocked traffic in Explorer (CLAS mode)** (E-116105)

In CLAS environments, some allowed traffic flows were wrongly reported as Potentially Blocked because of missing IP sets in the firewall test database.

## Updates for Core for Kubernetes 5.1.7

### Kubelink

#### Resolved Issues

- **Kubelink: policy service blocked when agent disconnects while receiving policy message** (E-117099)  
In some situations, policies stopped being sent due to a policy channel lock after C-VEN disconnected while receiving a policy update.
- **Kubelink: policy service blocked if one agent is not reading policy message** (E-116967)  
In some situations, policies stopped being sent after a C-VEN became unresponsive.
- **Kubelink can't save sets because of message size limit** (E-116825)  
Policy updates were being interrupted when large policy sets were being sent. The message size has been increased to permit larger policy transmissions .
- **Kubelink: workload events processing is slowed down by policy updates** (E-116706)  
The processing of workload events from Kubernetes sometimes became slow when handling thousands of Kubernetes Workloads, or the policy PCE requests were taking too long, or if there was no previous policy version in storage.
- **Kubelink sends wrong workload href in policy ACK request** (E-116640)  
In some CLAS-enabled clusters that host large numbers of workloads, the Kubernetes Workloads page showed an old policy apply date. Kubelink incorrectly sent a policy ACK for some Kubernetes Workloads with the host workload URI. The PCE responded with a 406 error, and a "no policy" ACK was stored.

## Updates for Core for Kubernetes 5.1.3

### Kubelink

#### Resolved Issues

- **Kubelink can't save policy to storage** (E-116539)  
Kubelink could not store cluster policy due to storage size limitations. To permit increased storage sizes, the Helm chart now includes new `resources` values under the `storage` component, as well as under `cven` and `kubelink` (note that amounts are in MiB not MB, and GiB not GB):

```
kubelink:
  resources:
    limits:
      memory: 500Mi
    requests:
      memory: 200Mi
      cpu: 200m

cven:
  resources:
    limits:
      memory: 300Mi
    requests:
      memory: 100Mi
      cpu: 250m
```

```
storage:
  resources:
    limits:
      memory: 500Mi
    requests:
      memory: 200Mi
      cpu: 100m
```

- **Pod to pod flows and pod labels are missing from Explorer search results** (E-116271, E-116272)

In CLAS-enabled clusters, Explorer was not showing pod labels, only workload labels. In addition, Explorer did not return some traffic flows, even when trying with label-based search, or port-based search, or even searching using workload labels + pod labels. Also, pod traffic was being mapped to workloads.

## Updates for Core for Kubernetes 5.1.2

### Kubelink

#### Resolved Issues

- **Helm Chart: etcd storage size limit** (E-115417)  
Kubelink in CLAS mode uses etcd as a local cache for policy and runtime data. The Helm Chart now accepts a new variable called `storage.sizeGi` to set the size (in GiB not GB) of ephemeral storage. The default value is 1.
- **Kubelink - Unable to process policy with custom iptables rules** (E-115250)  
Kubelink in CLAS mode failed to process policy received from the PCE when custom iptables rules were present, producing the error message "json: cannot unmarshal object into Go struct field."
- **Kubelink to PCE connectivity issues - connection reset by peer** (E-115049)  
CLAS-enabled Kubelink was entering degraded mode too soon because of PCE connectivity problems. Now Kubelink also retries requests after network and OS errors, which avoids premature degraded mode entry.
- **C-VEN reporting potentially blocked traffic between worker nodes** (E-114691)  
CLAS processing of outbound rules to a ClusterIP Service replaced the "All Services" destination in the rule with actual ports from the Kubernetes Service. If a destination label included a Kubernetes Service, this caused a missing iptables rule between nodes.
- **Max policy message size between Kubelink and C-VEN is too small** (E-113714)  
The default gRPC message size was set to too small of a value, which caused C-VEs to reject policy messages that were larger than this value. The default gRPC message size is now larger, to avoid this problem.

## Updates for Core for Kubernetes 5.1.0

### What's New in the 5.1.0 Release

The following are new and changed items in the 5.1.0 release from the previous releases of C-VEN and Kubelink:

- **New CLAS architecture option**  
Kubelink now can be deployed with a Cluster Local Actor Store (CLAS) module, which manages flows from C-VEs to PCE, and policies from PCE to C-VEs. The CLAS-enabled

Kubelink tracks individual pods, and when they are created or destroyed, instead of this being communicated directly to the PCE. To migrate from an existing (non-CLAS) environment to a CLAS-enabled one, set the `clusterMode` parameter to `migrateLegacyToClas` in your deployment YAML file (typically named `illumio-values.yaml`). See the `README.md` file accompanying the Helm Chart for full details on this and other Helm Chart parameters.

- **Workloads more closely match Kubernetes architecture**

In CLAS-enabled environments, workloads are now conceptually tied to their containers, instead of being referred to in context of their pods, which more closely matches Kubernetes practice. To reflect this change, such workloads in CLAS environments are called *Kubernetes Workloads*, regardless of what containers have been spun up or destroyed to run the applications. In non-CLAS environments, the existing term *Container Workloads* is still used as in prior releases, corresponding to Pods. In mixed environments (with both non-CLAS and CLAS-enabled clusters), the PCE UI shows both Container Workloads and Kubernetes Workloads, as appropriate.

- **Degraded mode for CLAS-enabled Kubelink**

If a CLAS-enabled Kubelink detects that its connection with the PCE becomes unavailable (for example, due to connectivity problems or an upgrade), Kubelink by default enters a *degraded mode*. In this degraded mode, new Pods of existing Kubernetes Workloads get the latest policy version cached in CLAS storage. When Kubelink detects a new Kubernetes Workload with exactly the same label sets and in the same namespace as an existing Kubernetes Workload, Kubelink delivers the existing, cached policy to Pods to this new Workload. If Kubelink cannot find a cached policy (that is, when labels of a new Workload do not match those of any existing Workload in the same namespace), Kubelink delivers a “fail open” or “fail closed” policy based on the Helm Chart parameter `degradedModePolicyFail`. The degraded mode can also be turned on or off by the Helm Chart parameter `disableDegradedMode`.

- **Illumio annotations in CLAS mode specified on the workload and not on Pod's template**

Illumio annotations when in CLAS mode are now specified on the Kubernetes Workload and not on the pod's template.

- **Docker support dropped**

The Docker CRI is no longer supported as of the 5.0.0 release of Illumio Core for Kubernetes.

## C-VEN

### Resolved Issue

- **Permanently delete Kubernetes Workloads after certain period when they are unpaired** (E-112362)

Kubernetes Workloads (from a CLAS environment) are pruned from the PCE one day (by default) after they are unpaired. The length of time that elapses (in seconds) before this pruning occurs is configurable with the `vacuum_entities_wait_before_vacuum_seconds` parameter, which is set in the PCE `agent.yaml` file. The default value for this parameter is 86400 (24 hours).

### Known Issues

- **When C-VEN starts first, a 404 from PCE when getting CLAS token** (E-109259)

When C-VEN is started first, it tries to contact the PCE in order to obtain CLAS token, but receives a 404 error. This is expected behavior for this scenario, which is only momentary. Kubelink eventually starts normally, and C-VEN obtains the CLAS tokens as expected.

- **Helm install fails with Helm version 3.12.2 but works with 3.10** (E-108128)

When installing with Helm version 3.12.2, the installation fails with a YAML parse error. Workaround: Use Helm version 3.10, or version 3.12.3 or later.



- **Re-adding node does not re-pair it** (E-98120)

After deleting a node and re-adding the same node, the node does not reappear, and previously established policy disappears from the node.

Workaround: Uninstall and re-install Illumio Core for Kubernetes from scratch with the node present.

## Kubelink

### Resolved Issues

- **CLAS: NodePort - pod rules are not removed after disabling rule** (E-111689)

After disabling a NodePort rule that opens it to outside VMs, iptable entries for pods with a virtual service's targetPort were not being removed as expected. Now the pod no longer remains opened. Host iptables are removed, so traffic does not go through, and the pod ports are properly closed.

- **CLAS - The etcd pod crashes when node reboots** (E-106236)

The etcd pod would crash if one of the nodes in the cluster was rebooted.

### Known Issues

- **CLAS-mode Kubelink pod gets restarted once when deploying Illumio Core for Kubernetes** (E-109284)

The Kubelink pod is restarted after deploying Illumio Core for Kubernetes in CLAS mode. There is no workaround. Kubelink runs properly after this single restart.

- **CLAS: Container Workload Profile label change is not applied to Kubernetes Workloads, only to Virtual Services** (E-109168)

When removing labels in a Container Workload Profile, existing Kubernetes Workloads that are managed by that profile do not have their labels changed automatically to labels based on annotations. These existing Kubernetes Workloads must be updated with the `kubect1 apply` command for the labels change to take effect. New Kubernetes Workloads created after the profile label change will have the new labels.

This works as designed.

## Security Information for Core for Kubernetes 5.1

For information about security issues, security advisories, and other security guidance pertaining to this release, see Illumio's Knowledge Base in Illumio's Support portal.

## Illumio Core for Kubernetes Release Notes 5.0.0

### About Illumio Core for Kubernetes 5.0

These release notes describe the resolved issues, known issues, and related information for the 5.0.0 release of Illumio Core for Kubernetes, formerly known as Illumio Containerized VEN, or C-VEN. Illumio Core for Kubernetes also includes the related required component, Kubelink. Because of this heritage, many references to this product as "C-VEN" are still used throughout the documentation.

**Document Last Revised:** January 2024

## Product Version

**Compatible PCE Versions:** 23.5.10 and later releases

**Current Illumio Core for Kubernetes Version:** 5.2.3, which includes:

- C-VEN version: 23.4.2
- Kubelink version: 5.2.1
- Helm Chart version: 5.0.0

Illumio Core release numbering uses the following format: “a.b.c-d+e”.

- “a.b”: Standard or LTS release number, for example, “2.2”
- “.c”: Maintenance release number, for example, “.1”
- “-d”: Optional descriptor for pre-release versions, for example, “preview2”

## What's New in C-VEN and Kubelink

The following are new and changed items in this release from the previous releases of C-VEN and Kubelink:

- **New CLAS architecture option**

Kubelink now can be deployed with a Cluster Local Actor Store (CLAS) module, which manages flows from C-VEs to PCE, and policies from PCE to C-VEs. The CLAS-enabled Kubelink tracks individual pods, and when they are created or destroyed, instead of this being communicated directly to the PCE. To migrate from an existing (non-CLAS) environment to a CLAS-enabled one, set the `clusterMode` parameter to `migrateLegacyToClas` in your deployment YAML file (typically named `illumio-values.yaml`). See the `README.md` file accompanying the Helm Chart for full details on this and other Helm Chart parameters.

- **Workloads more closely match Kubernetes architecture**

In CLAS-enabled environments, workloads are now conceptually tied to their containers, instead of being referred to in context of their pods, which more closely matches Kubernetes practice. To reflect this change, such workloads in CLAS environments are called *Kubernetes Workloads*, regardless of what containers have been spun up or destroyed to run the applications. In non-CLAS environments, the existing term *Container Workloads* is still used as in prior releases, corresponding to Pods. In mixed environments (with both non-CLAS and CLAS-enabled clusters), the PCE UI shows both Container Workloads and Kubernetes Workloads, as appropriate.

- **Illumio annotations in CLAS mode specified on the workload and not on Pod's template**

Illumio annotations when in CLAS mode are now specified on the Kubernetes Workload and not on the pod's template.

- **Docker support dropped**

The Docker CRI is no longer supported as of this 5.0.0 release of Illumio Core for Kubernetes.

## NodePort Limitations

- **NodePort**

Here are some limitations around NodePort policy enforcement and flows:

- Only NodePort Services with `externalTrafficPolicy` set to "cluster" are supported. (This is the default and most frequently used value for this setting.)
- When writing rules to allow traffic to flow from external (to the cluster) entities and NodePort Service, the source side of the rule must contain all nodes in the cluster.  
For example, given the following setup:
  - Worker nodes in the cluster are labeled as Role: Worker Node
  - Clients accessing the Service running in the Kubernetes cluster are labeled Role: Client
  - The NodePort Service is labeled Role: Ingress
- Normally, the rule would be written as Role: Client -> Role: Ingress. However, for this beta1 release the rule must also include all nodes in the cluster to work correctly: Role: Client + Role: Worker Node -> Role: Ingress.

## Updates for Core for Kubernetes 5.0.0-LA

- [C-VEN \[51\]](#)
- [Kubelink \[51\]](#)
- [Security Information for Core for Kubernetes 5.0.0-LA \[52\]](#)

## C-VEN

### Resolved Issues

- **Scaling a Deployment with changed labels was not being updated on PCE** (E-107274)  
After deploying a workload with a non-existing label, create labels on the PCE and wait a few minutes before updating and applying the YAML to change the number of replicas. The deployment was not properly updated on the PCE. This issue is resolved.

### Known Issues

- **When C-VEN starts first, a 404 from PCE when getting CLAS token** (E-109259)  
When C-VEN is started first, it tries to contact the PCE in order to obtain CLAS token, but receives a 404 error. This is expected behavior for this scenario, which is only momentary. Kubelink eventually starts normally, and C-VEN obtains the CLAS tokens as expected.
- **Helm install fails with Helm version 3.12.2 but works with 3.10** (E-108128)  
When installing with Helm version 3.12.2, the installation fails with a YAML parse error.  
Workaround: Use Helm version 3.10, or version 3.12.3 or later.
- **Re-adding node does not re-pair it** (E-98120)  
After deleting a node and re-adding the same node, the node does not reappear, and previously established policy disappears from the node.  
Workaround: Uninstall and re-install Illumio Core for Kubernetes from scratch with the node present.

## Kubelink

### Resolved Issues

- **CLAS on IKS with Calico, the flow of ClusterIP is not displayed correctly** (E-109238)  
In a CLAS environment on IKS with Calico, when running traffic to a clusterIP service from a pod, flows were being displayed incorrectly. Sometimes flows were incorrectly shown as Allowed. Other times, flows that should not be present were being shown as Blocked. This issue is resolved.
- **Kubernetes cluster falsely detected as an OpenShift cluster** (E-107910)

After deployment, Kubelink falsely detected a Kubernetes cluster as an OpenShift cluster based on misinterpretations of installed VolumeReplicationClass and VolumeReplications APIs on the cluster. This issue is resolved.

- **Problem when label from PCE was deleted after Kubelink starts** (E-107779)

When creating a new workload on PCE, Kubelink uses cached or preloaded labels to label a workload. However, if the label was deleted before the workload was actually created, the PCE responded with a 406 status error. This issue is resolved.

- **Kubelink did not properly apply label mappings with PCE using two-sided management ports** (E-105391)

Label mappings were not properly applied when using the LabelMap CRD if the PCE used two-sided management ports. This issue is resolved.

## Known Issues

- **CLAS: NodePort - pod rules are not removed after disabling rule** (E-111689)

After disabling a NodePort rule that opens it to outside VMs, iptables entries for pods with a virtual service's targetPort are not removed as expected. The pod is still opened. Host iptables are removed, so traffic does not go through, but the pod ports stay opened towards original IPs.

There is no workaround available.

- **Non-CLAS mode: Failed to clean up the pods** (E-109687)

After deleting a non-CLAS container cluster, the cluster gets deleted but Container Workloads are not deleted, and remain present.

- **CLAS-mode Kubelink pod gets restarted once when deploying Illumio Core for Kubernetes** (E-109284)

The Kubelink pod is restarted after deploying Illumio Core for Kubernetes in CLAS mode.

There is no workaround. Kubelink runs properly after this single restart.

- **CLAS: Container Workload Profile label change is not applied to Kubernetes Workloads, only to Virtual Services** (E-109168)

In CLAS environments, after changing a label in a Container Workload Profile, the Kubernetes Workloads that are managed by that Profile do not have their labels changed as expected. No changes to these Kubernetes Workloads occur even when the Profile is changed to "No Label Allowed;" the original labels remain in the Kubernetes Workloads. However, Virtual Services managed by that profile do successfully have their labels changed properly.

No workaround is available.

- **CLAS - The etcd pod crashes when node reboots** (E-106236)

The etcd pod crashes if one of the nodes in the cluster is rebooted.

There is no workaround available.

## Security Information for Core for Kubernetes 5.0.0-LA

For information about security issues, security advisories, and other security guidance pertaining to this release, see Illumio's Knowledge Base in Illumio's Support portal.

## Illumio Core for Kubernetes Release Notes 4.3.0

### What's New in Kubernetes 4.3.0

These release notes describe the resolved issues and related information for the 4.3.0 release of Illumio Core for Kubernetes, formerly known as Illumio Containerized VEN, or C-VEN.

Illumio Core for Kubernetes also includes the related required component, Kubelink. Because of this heritage, many references to this product as "C-VEN" are still used throughout the documentation.

Here are the new and changed items in this release:

- **New Kubelink 3.3.1**

This Kubernetes 4.3.0 release includes an upgraded Kubelink component, version 3.3.1 .

- **New C-VEN 22.5.14**

This Kubernetes 4.3.0 release includes an upgraded C-VEN component, version 22.5.14.

**NOTE**

C-VEN 22.5.14 requires PCE version 22.5.0 or later, and supports PCE 23.3.0 or later.

## Security Information

For information about security issues, security advisories, and other security guidance pertaining to this release, see Illumio's Knowledge Base in Illumio's Support portal.

## Base Image Upgraded

The C-VEN base OS image is upgraded to minimal UBI for Red Hat Linux 7.9-979.1679306063, which is available at <https://catalog.redhat.com/software/containers/ubi7/ubi-minimal/5c3594f7dd19c775cddfa777>.

Customers are advised to upgrade to Core for Kubernetes 4.1.0 or higher for these security fixes.

## Product Version

**Compatible PCE Versions:** 22.5.0 and later releases

**Current Illumio Core for Kubernetes Version:** 4.3.0, which includes:

- C-VEN version: 22.5.14
- Kubelink version: 3.3.1
- Helm Chart version: 4.3.0

Illumio Core release numbering uses the following format: "a.b.c-d+e".

- "a.b": Standard or LTS release number, for example, "2.2"
- ".c": Maintenance release number, for example, ".1"
- "-d": Optional descriptor for pre-release versions, for example, "preview2"

## Updates for Core for Kubernetes 4.3.0

### C-VEN

#### Resolved Issues

- **C-VEN support report does not contain container workload firewalls** (E-106932)  
VEN support reports for C-VEs were missing the active firewall information for all container workloads. This issue is resolved. Support reports now include full firewalls from each network namespace, as gathered by `iptables-save` and `ipset list` output.
- **Conntrack tear-down for containers with policy updates** (E-44832)  
Although policy was changed to block a container workload from talking to another, traffic was still passing between the workloads, due to a conntrack connection remaining incorrectly active. This issue is resolved. Conntrack connections on sessions affected by a policy change are now properly torn down.

#### Known Issue

- **C-VEs not automatically cleaned up after AKS upgrade** (E-103895)  
After upgrading an AKS cluster, sometimes a few duplicate C-VEs might not be automatically removed as part of the normal upgrade process, and remain in the PCE as "non-active." Note there is no compromise to the security or other functionality of the product.  
Workaround: Manually prune the extra unmigrated C-VEs from the PCE by clicking the **Unpair** button for each of them.

### Kubelink

#### Resolved Issue

- **Kubelink does not pair with PCE when a separate management port is used** (E-107001)  
Kubelink would crash after start when the PCE had `front_end_management_https_port` set to 9443 instead of 8443, because of a missing `label_map` URL. This issue is resolved.

#### Known Issue

- **Kubelink does not properly apply label mappings with PCE using two-sided management ports** (E-105391)  
Label mappings are not properly applied when using the LabelMap CRD if the PCE uses two-sided management ports.  
Workaround: Use the label map feature only with a PCE that uses only one management port.

# Illumio Flowlink Release Notes for Release 1.4.0

December 2024

## Product Version

**Flowlink Version:** 1.4.0

**Compatible PCE Version:** PCE 19.3.0 and later releases

## Standard versus LTS Releases

For information about Standard versus Long Term Support (LTS) releases, see [Versions and Compatibility](#) in the Illumio Support portal (log in required).

Illumio Core release numbering uses the following format: "a.b.c-d+e".

- "a.b": Standard or LTS release number, for example, "2.2"
- ".c": Maintenance release number, for example, ".1"
- "-d": Optional descriptor for pre-release versions, for example, "preview2"

## New Features in Illumio Flowlink 1.4.0

The following new features were added in Illumio Flowlink 1.4.0.

- **Support for FIPS compliance on RHEL 9**

Beginning with this release, Flowlink now supports FIPS compliance on RHEL 9. For more information, see [FIPS Compliance for Flowlink](#).

- **Increased buffer size**

Flowlink buffer size is increased to 65kb. This was done to address an issue where Flowlink failed to process large UDP packets.

- **Support for ingesting multiple flow types**

Beginning with this release, the Flowlink text flow collector supports flows with any IP protocol number, not just UDP, TCP and ICMP.

## Resolved and Known Issues in Flowlink 1.4.0

### Resolved Issue

**Flowlink became non-responsive** (E-114431)

A parsing issue with the IPFIX packet caused Flowlink 1.3.0 to become non-responsive, requiring a manual restart. This issue is fixed with this release.

## **Known Issue**

### **No Automatic Restart Following Reboot** (E-15146)

Flowlink is not installed as a service, nor does it support a High Availability (HA) configuration. As such, it doesn't restart automatically if the host fails or is rebooted. In those cases, you need to restart Flowlink manually.



# Illumio Flowlink Release Notes 1.3.0

## Product Version

**Flowlink Version:** 1.3.0

**Compatible PCE Version:** PCE 19.3.0 and later releases

### Standard versus LTS Releases

For information about Standard versus Long Term Support (LTS) releases, see [Versions and Compatibility](#) in the Illumio Support portal (log in required).

Illumio Core release numbering uses the following format: “a.b.c-d+e”.

- “a.b”: Standard or LTS release number, for example, “2.2”
- “.c”: Maintenance release number, for example, “.1”
- “-d”: Optional descriptor for pre-release versions, for example, “preview2”

## New Feature in Flowlink 1.3.0

### Support for HTTP/HTTPS Proxy

Beginning with this release, Flowlink now supports HTTP/HTTPS proxy. When Flowlink is running behind a proxy or in a corporate network and the PCE is in the cloud, Flowlink can now access the PCE via HTTP/HTTPS proxy configurations.

The following configuration parameter is available to define an HTTP/HTTPS proxy:

```
proxy_config:
  https_proxy: <HTTPS_PROXY>
  http_proxy: {} <HTTPS_PROXY>{}
```

See the following example of Flowlink YAML configuration file:

```
proxy_config:
  https_proxy: http://proxy.corporate.com:3128
  http_proxy: http://proxy.corporate.com:3128
```

In the above example, the HTTP/HTTPS proxy is running on FQDN `proxy.corporate.com`{`port: 3128`}.

## Resolved Issue in Flowlink 1.3.0

The following security issue was resolved in this release:

**go-lang upgraded to 1.19.11** (E-107998)

The go-lang package was upgraded to 1.19.11 to address CVE-2023-29406.

## Illumio NEN Release Notes 2.6

### Product Version

**NEN Version:** 2.6.40

**Compatible PCE Versions:** NEN 2.6.40 is compatible with any PCE release.

**NEN Version:** 2.6.30

**Compatible PCE Versions:** 21.5.1 – 24.4

### Standard versus LTS Releases

For information about Standard versus Long Term Support (LTS) releases, see [Versions and Compatibility](#) in the Illumio Support portal (log in required).

Illumio Core release numbering uses the following format: “a.b.c-d+e”.

- “a.b”: Standard or LTS release number, for example, “2.2”
- “.c”: Maintenance release number, for example, “.1”
- “-d”: Optional descriptor for pre-release versions, for example, “preview2”

### Release Types and Numbering

Illumio Core release numbering uses the following format: “a.b.c-d+e”

- “a.b”: Standard or LTS release number, for example “2.2”
- “.c”: Maintenance release number, for example “.1”
- “-d”: Optional descriptor for pre-release versions, for example “preview2”

## What's New in NEN 2.6.x Releases

This section describes new features introduced in the following NEN releases.

### NEN 2.6.40 New Feature

#### JSON Format Change

Beginning with this release, generic workload JSON files are uploaded as a single, parseable object. This new format allows a program to use the JSON file to apply policy to a device customers want to protect.

```

1 [
2   {
3     "$schema": "http://json-schema.org/draft-04/schema#",
4     "definitions": {
5       "rules": {
6         "description": "Array of rule objects",
7         "type": "array",
8         "items": {
9           "description": "A single rule",
10          "type": "object",
11          "required": ["action", "port", "protocol", "ips"],
12          "properties": {
13            "action": {
14              "description": "Action for the rule either permit or deny",
15              "type": "string",
16              "enum": ["permit", "deny"]
17            },
18            "port": {
19              "description": "Inbound or Outbound port(s) bound to rule. Either a port, port range or *",
20              "type": "string"
21            },
22            "protocol": {
23              "description": "Protocol for rule. Either a protocol number or *",
24              "type": "string"
25            },
26            "ips": {
27              "description": "An array of inbound or outbound IP addresses bound to rule",
28              "type": "array",
29              "items": {
30                "description": "IP address associated to rule. Either IP address, CIDR block, IP address range or *",
31                "type": "string"
32              }
33            }
34          }
35        }
36      },
37      "description": "An array of objects, one per workload",
38      "type": "array",
39      "items": {
40        "type": "object",
41        "required": ["name", "href", "rules"],
42        "properties": {
43          "name": {
44            "description": "Name of workload",
45            "type": "string"
46          },
47          "href": {
48            "description": "href of workload",
49            "type": "string"
50          },
51          "rules": {
52            "description": "Object containing Inbound and Outbound rules",
53            "type": "object",
54            "properties": {
55              "Inbound": {
56                "description": "Array of Inbound rule objects",
57                "$ref": "#/definitions/rules"
58              },
59              "Outbound": {
60                "description": "Array of Outbound rule objects",
61                "$ref": "#/definitions/rules"
62              }
63            }
64          }
65        }
66      }
67    }
68  ]
69 ]
70

```

## NEN 2.6.30 New Features



### IMPORTANT

#### Before installing NEN release 2.6.30

Installing this release upgrades the existing database on the NEN to a newer version of the database software. Illumio recommends that you back up the existing NEN database before you install NEN 2.6.30 so that you can revert the installation if necessary.

To back up the existing NEN database, issue the following commands on the NEN primary node:

```
illumio-nen-ctl set-runlevel 1 -svw
```

```
illumio-nen-db-management dump --file <outputfile-name>
```

```
illumio-nen-ctl stop
```

## Support for CentOS Stream 9

This release includes support for installing NENs on nodes running CentOS Stream 9.

## Switch ACL generation now supports all protocols

With this release, the NEN now recognizes all PCE-supported protocols, ensuring that the NEN can translate switch policy into ACLs when such policy references any PCE-supported protocol.

## Support for VMware NSX Advanced Load Balancer AVI 22.1.6

With this release, the NEN now supports VMware NSX Advanced Load Balancer AVI version 22.1.6.

## NEN 2.6.20 New Features

### Support for RHEL 9

This release includes support for running standalone NENs on Red Hat Enterprise Linux (RHEL) 9 where the version of **openssl-lib** is **3.1 or earlier**.

To determine the openssl-lib version, issue `rpm -qa | grep openssl-lib`.

## NEN 2.6.10 New Features

### Support for Verifying NEN RPM Signature

Beginning with NEN release 2.6.10, you can verify the signature of the NEN RPM package before installation. This allows you to ensure that the package hasn't been modified since it was signed. For details, see [Verify the NEN RPM digital signature](#).

### Support for NEN Proxy Communication

Beginning with NEN release 2.6.10, there is now `runtime_env` support for defining an HTTP/HTTPS proxy for communication between the NEN and the PCE or between the NEN and managed devices (such as Server Load Balancers (SLBs)). You can also specify a list of IP address that are not allowed to communicate via a proxy server. For details, see [Configure Proxy Support for NENs](#).

### Ruby updated to version 3.1.2

Ruby was upgraded from version 2.7.1 to 3.1.2.

## NEN 2.6.1 New Features

### Support for all Citrix ADC (Netscaler) Load Balancer-supported protocols

With this release, the NEN now supports all the protocols that Citrix (NetScaler) 13.1 lists in the **Load Balancing > Virtual Servers > Add > Protocol** menu.

## NEN 2.6.0 New Features

### Support for Citrix ADC (Netscaler) Load Balancer

With this release, the NEN now supports Citrix ADC (Netscaler) Load Balancers and their associated virtual servers that have only a single IPv4 address.

To add a Citrix Software Load Balancer, see the section *Configure Load Balancers* in the "Load Balancers and Virtual Servers for the NEN" topic.

### Support for allowing customers to specify whether disabled VIPs are reported to the PCE

Prior to the release of NEN 2.6.0, if VIP filtering was disabled, all VIPs – including disabled VIPs – were reported to the PCE. You can now disable this reporting using the following new option in the `illumio-nen-ctl slb-enable` command:

```
--disabled-virtual-server-reporting enabled|disabled
```

To ensure backwards compatibility, the default value is `enabled`.

## PCE-provided rule IP addresses and ports now combined into CIDR blocks

NENs now combine rule IP addresses and ports provided by the PCE into CIDR blocks and port ranges. This reduces the number of ACLs that NENs need to generate for switches.

Benefits include:

- Fewer ACLs that the NEN generates for switches.
- Fewer ACLs generated for the IBM iSeries integration with Precisely (current limit: 10k ACLs) allows for optimization of IP addresses into ranges larger than can be covered by a single CIDR block.
- Lower demand on switch TCAM where ACLs are stored.

## Support for Rocky Linux 8.7

This release includes support for running standalone NENs on Rocky Linux 8.7.

## Support for configuring a PCE policy request timeout

Beginning with NEN 2.5.2.A1, you can configure a PCE policy request timeout. This may be needed if your NEN SLB implementation will involve large policy calculations. The timeout ensures that the NEN doesn't wait too long for the PCE to respond to policy requests in scenarios involving large policy calculations.

To configure the timeout, use the following runtime environment variable:

`pce_policy_request_timeout_minutes`

- Default value: 10 minutes
- Minimum value: 3 minutes

## Resolved Issues in NEN 2.6.40

| Issue    | Description                                                                                                                                                                                                                                                                                                                                      |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| E-119690 | <p><b>NEN setup command failed and 'unknown property' error thrown</b></p> <p>After the user configured the <code>proxy_config</code> entry in the <code>runtime_env</code>, the <code>illumio-nen-env setup</code> command failed with an 'unknown property' error.</p>                                                                         |
| E-119644 | <p><b>NEN activation failed and SSL error thrown</b></p> <p>When the user activated the NEN using the <code>proxy_config</code> settings in the <code>runtime_env</code>, the NEN ignored the specified values and failed with an SSL error.</p>                                                                                                 |
| E-122961 | <p><b>Not all Virtual IPs appeared on the PCE</b></p> <p>When using a VMware NSX Advanced Load Balancer greater than version 21.0, the NEN did not honor the "next" field in the <code>vsvip</code> API response and didn't read all entries that define the virtual server IP values. Therefore, it skipped related virtual server entries.</p> |

## Known Issues in NEN 2.6.40

There are no known issues in this release.

## Resolved Issues in NEN 2.6.30

- **ACL Generation Hangs if Switch Policy Includes Multicast Addresses** (E-117247)  
If a PCE switch policy includes a multicast address, the NEN became inoperative when trying to generate ACLs for that policy. This issue is fixed.
- **Rules referencing some protocols didn't appear in ACLs** (E-117013)  
PCE policy rules referencing certain protocols didn't appear in NEN-generated switch ACLs. This issue is fixed. With this release, the NEN now supports all PCE-supported protocols.

## Known Issues in NEN 2.6.30

There are no known issues in this release.

## Resolved Issue in NEN 2.6.20

- **Potential unexpected denial of some traffic flows** (E-114782)  
In NEN releases 2.6.10 and earlier, while in Selective Enforcement the NEN applied ACL deny rules before allow rules, which could inadvertently deny flows that you want to allow. This issue is fixed. Beginning with this release, NENs now apply ACL allow rules before deny rules.

## Known Issues in NEN 2.6.20

There are no known issues in this release.

## Resolved Issues in NEN 2.6.10

- **In NEN HA pair SLB jobs aborted in some circumstances** (E-112912)  
In a NEN HA pair, after the Secondary Node served temporarily as the Primary Node and then returned to its normal Secondary role, an issue occurred where SLB policy jobs on the Secondary Node were aborted and the database wasn't being reset to allow other SLB policy jobs to run on those SLBs. The issue stems from the timeout behavior being too aggressive. This issue is resolved: the Secondary Node now gracefully returns to its normal role.
- **Unnecessary word prevented some rules from being applied in IBM AS400 integration** (E-111870)  
In an IBM AS400 integration, the ACL files generated by the NEN contained the word `permit` at the end on each rule line, which prevented Precisely from ingesting the rules. This issue is resolved: `permit` is no longer appended at the end of rules.



## Known Issues in NEN 2.6.10

There are no known issues in this release.

## 2.6.10 Security Information

- Upgraded netaddr-1.5.0.gem to 2.0.4 or higher to address CVE-2019-17383
- Upgraded tzinfo-1.2.7.gem to 0.3.61,1.2.10 or higher to address CVE-2022-31163
- Upgraded json-1.8.6.gem to 2.3.0 or higher to address CVE-2020-10663
- Upgraded activesupport-5.2.4.2.gem to 5.2.4.3,6.0.3.1 or higher to address CVE-2020-8165 CVE-2023-22796
- Upgraded addressable-2.7.0.gem to 2.8.0 or higher to address CVE-2021-32740
- Upgraded cURL to v7.87.0 on the Illumio NEN to address CVE-2019-5443 & CVE-2019-3882

## Resolved Issues in NEN 2.6.1

- **Timeout issue prevented NEN from updating SLB Policy** (E-107324)  
Due to the shortness of the default connect timeout in the CURL library (5 minutes), the NEN was susceptible to timing out when trying to connect to the PCE. This in turn prevented the NEN from updating policy on the SLB. The issue was resolved by adding the following configurable PCE runtime\_env parameter:  
`pce_policy_connect_timeout_minutes`
  - Default value: 10 minutes
  - Minimum value: 3 minutes
- **Handling of SLB empty data response led to erroneous "deletion pending" state** (E-106930)  
An issue caused an F5 SLB to return an empty data response when the NEN queried it for virtual servers, even though managed virtual servers actually existed on the SLB. This occurred at a time when the NEN was programming the SLB. This in turn caused the PCE to put these existing virtual servers in a 'deletion pending' state. After the NEN was restarted, all the virtual servers were discovered and available on the PCE Web Console. This issue is resolved. The NEN will now ignore empty data responses if the SLB has managed virtual servers or is currently being programmed with policy.
- **Route domain length prevented virtual server discovery** (E-106800)  
F5 SLB virtual servers with route domains longer than two digits weren't discovered by the NEN and consequently weren't displayed on the PCE Web Console. This issue is resolved. The NEN now recognizes route domains up to five digits in length.

## Known Issues in NEN 2.6.1

There are no known issues in this release.

## Resolved Issues in NEN 2.6.0

- **Unable to deactivate the NEN** (E-104053)  
In a certain circumstance (described below), after using the PCE Web Console to remove all the SLBs and associated virtual servers from the NEN, users were unable to deactivate the NEN. Details are as follows:

1. The user removed SLBs through the PCE Web Console.
2. As the SLBs no longer existed on the PCE, the NEN couldn't inform the PCE of their state.
3. This prevented the NEN from removing the SLBs correctly from its database.
4. This caused the NEN to think it was still managing the SLBs.
5. This in turn prevented the user from deactivating the NEN.

*Circumstance:* At the time the user removed the SLBs through the PCE Web Console, the associated virtual servers were unmanaged.

This issue is resolved. The NEN now recognizes when the SLB is being removed and no longer tries to inform the PCE of changes in SLB state. This allows the NEN to remove SLBs from its database correctly.

- **NEN 2.5.2 Failed to Update SLB Policy** (E-103432)

An issue caused the NEN policy process to hang while sending an SLB policy request to the PCE. The NEN issue was resolved by adding a configurable PCE policy request timeout to the NEN's code. To configure the optional timeout, use the following runtime environment variable:

`pce_policy_request_timeout_minutes`

- Default value: 10 minutes
- Minimum value: 3 minutes

- **Extraneous API call to the load balancer** (E-96324)

The NEN made an extraneous GET API call to the AVI Advantage Load Balancer for programming the virtual server. This issue is resolved. The NEN no longer makes this extraneous API call.

## Known Issues in NEN 2.6.0

There are no known issues in this release.

# Illumio NEN Release Notes 2.5

## Product Version

**NEN Version:** 2.5.2

**Compatible PCE Versions:** 21.5.1 – 24.4

### Standard versus LTS Releases

For information about Standard versus Long Term Support (LTS) releases, see [Versions and Compatibility](#) in the Illumio Support portal (log in required).

Illumio Core release numbering uses the following format: “a.b.c-d+e”.

- “a.b”: Standard or LTS release number, for example, “2.2”
- “.c”: Maintenance release number, for example, “.1”
- “-d”: Optional descriptor for pre-release versions, for example, “preview2”

## Resolved Issue in NEN 2.5.2.A1

### NEN 2.5.2 Failed to Update SLB Policy (E-103432)

An issue caused the NEN policy process to hang while sending an SLB policy request to the PCE. The NEN issue was resolved by adding a configurable PCE policy request timeout to the NEN's code. To configure the optional timeout, use the following runtime environment variable:

```
pce_policy_request_timeout_minutes
```

```
pce_policy_request_timeout_minutes
```

- Default value: 10 minutes
- Minimum value: 3 minutes

## Known Issues in NEN 2.5.2.A1

There are no known issues in this release.

## Resolved Issues in NEN 2.5.2

- **Tamper checking was prevented on the SLB** (E-98697)

In some circumstances, the PCE may inform the NEN that there is a policy update for an SLB when there isn't actually an update. This may prevent the NEN from running tamper checking on the SLB. To help resolve this condition going forward, if the NEN is told about a non-existent policy update for the SLB and the time for performing a tamper check has lapsed, the NEN will now perform a full policy check for the SLB.

- **Problems caused when deleting a VS before unmanaging it on the PCE** (E-97909)

Deleting an enforced VS from an SLB without first unmanaging the VS on the PCE interfered with the NEN's attempt to remove policy from the SLB, which prevented the NEN from correctly handling error responses from the SLB. This caused the NEN to:

- Retry removing policy multiple times, which put a load on the SLB.
- Run multiple simultaneous SLB programming jobs.

This issue is resolved. Now, the NEN no longer retries sending APIs requests when 4xx API response codes are returned during the removal of policy from a VS and only runs one programming job per SLB at a time.

## Known Issues in NEN 2.5.2

There are no known issues in this release.

## Resolved Issue in NEN 2.5.1

- **Excessive NEN API GET calls to F5 prevented policy programming** (E-96989)

When trying to unmanage F5 Virtual Servers, NEN API GET requests to the F5 encountered slower than expected response times, which lead to the following sequence of events:

1. Responses from the F5 timed out.
2. Which in turn caused the NEN to retry its requests repeatedly.
3. Lacking timely F5 responses, the NEN ran multiple simultaneous unmanage jobs for VSs.
4. This caused the NEN to DDOS the F5 with `GET /mgmt/tm/security/firewall/policy?expandSubcollections=true` API calls.
5. **Result:** This overloaded the F5 and caused policy programming to fail due to API timeouts.

This issue is resolved. The NEN now serializes unmanage VS jobs for server load balancers.

## Known Issues in NEN 2.5.1

There are no known issues in this release.

## Resolved Issues in NEN 2.5.0

- **When processing multi-paged AVI API responses, policy programming failed** (E-95740)

While processing multiple-paged AVI `networksecuritypolicy` API responses during policy programming, the NEN incorrectly stored the policy ID to associate the policy to its rules. This caused the NEN to point to an invalid memory location, which in turn caused `network_enforcement_policymgr` to crash and policy programming to fail. This issue is resolved.

- **Problem when tamper checking AVI SLBs in multi-page AVI API responses** (E-95546)

An invalid check of the returned API response occurred when the NEN performed tamper checking of multiple-paged AVI `networksecuritypolicy` API responses. This issue could have caused the NEN to miss some Illumio `networksecuritypolicies`. The NEN could then have interpreted the missed policy as policy tampering, triggering a check on the SLB for those missing policies, resulting in no errors found. The issue was resolved by fixing the API response checks to make sure the NEN retrieved all `networksecuritypolicies` from the AVI SLB.

- **Generating switch policy failed in a HA configuration** (E-94344)

Generating policy by running the `switch policy generate` command on the primary node of an High Availability (HA)-configured NEN (from either the UI or from the CLI) could cause policy generation to fail and return the following error message: *This command can only be run on the node running the primary Network Enforcement Service*. This issue is resolved. The command can now be run on any NEN node – primary or secondary – that is running the `network_enforcement` service.

- **Policy update failed when new Illumio iRules weren't applied correctly** (E-93921)

An error occurred when trying to create a policy that applied a new Illumio iRule to block an existing non-Illumio iRule. The error prevented policy from being updated. This issue is resolved. New Illumio iRules are now applied before non-Illumio iRules.

- **PCE sent multiple unnecessary policy updates to the NEN** (E-93851)

Illumio updated the NEN 2.5.0 to address this issue in the PCE. In previous releases, the PCE sent policy updates to the NEN even when the SLB virtual services address list hadn't changed. This issue occurred because pods frequently go down and come back up and that triggered a policy job with "no address list changes" in the PCE. In this release, this issue is resolved for the NEN. The issue will be resolved in the PCE in a future release. In this release, the NEN optimizes the addresses in the address list and stores the SHA of the sorted address list for comparison between policies. The PCE ignores policy updates that don't contain changes in the overall address list by comparing the SHA of new address list with the previous one.

- **F5 AM policy deletion for a deleted VS failed** (E-92008)

When a NEN tried to delete a policy from an F5 BIG-IP Advanced Firewall Manager (F5 AFM) for a virtual server (VS) that had been deleted, the NEN defaulted to treating the VS like a non-AS3 managed VS. This resulted in the policy remaining on the F5 AFM. This issue is resolved and the NEN now makes sure (as originally intended) that no artifact of a policy remains on the SLB for the deleted VS.

## Known Issues in NEN 2.5.0

There are no known issues in this release.

## Illumio CLI Release Notes 1.4.4

### What's New in CLI Tool 1.4.4

Here's a summary of the new and enhanced features in this release.

The CLI Tool 1.4.4 is compatible with these versions of the PCE:

- 25.2.10 and earlier versions



#### NOTE

See the [Compatibility Matrix](#) for the complete list of compatible versions.

You must log into Illumio Support.

### Support for Proxy Communication

The new CLI version includes support for enabling or disabling the proxy for communication between Tenable or Qualis and the PCE CLI tool.

**Table 1. New in CLI 1.4.4**

| Command                     | Description                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>--enable-proxy</code> | <p>Use this to enable the proxy between tenable and CLI.</p> <p>Use this command to enable the proxy:</p> <pre>ilo upload_vulnerability_report --source-scanner tenable-sc --format api --severities=3 --enable-proxy -v --debug</pre> <p>Use this command if you do not want to enable the proxy:</p> <pre>ilo upload_vulnerability_report --source-scanner tenable-sc --format api --severities=3 -v --debug</pre> |

## **Illumio Core PCE CLI Tool Guide 1.4.3**

### **What's New and Changed in Release 1.4.3**

#### **Illumio CLI Tool 1.4.3**

Illumio CLI Tool 1.4.3 includes an updated version of the CLI Tool software which now includes proxy support.

Illumio provides regular maintenance updates for reported bugs and security issues and adds support for new operating system versions.

For the new commands for authenticated and unauthenticated proxies, `ilo login` and `ilo_use_api_key`, see PCE CLI Tool Guide, "Support for Proxy".

This release of the CLI Tool has no Release Notes issues.

### **Support for Proxy**

Release CLI 1.4.3 includes support for authenticated and unauthenticated proxies.

Type the `ilo login --help` command to see proxy-related options.

**Table 2. ilo login --help**

| Command Options                                            | Description                                                                              |
|------------------------------------------------------------|------------------------------------------------------------------------------------------|
| <code>-v, --verbose</code>                                 | Verbose logging mode                                                                     |
| <code>--trace</code>                                       | Enable API Trace Mode                                                                    |
| <code>--server SERVER_NAME</code>                          | Illumio API Access gateway server name                                                   |
| <code>--login-server LOGIN_SERVER</code>                   | Illumio login server name                                                                |
| <code>--kerberos-spn KERBEROS_SPN</code>                   | Illumio Kerberos SPN Kerberos authentication is only applicable to --login-server option |
| <code>--proxy-server PROXY_SERVER</code>                   | proxy server                                                                             |
| <code>--proxy-port PROXY_PORT</code>                       | proxy port                                                                               |
| <code>--proxy-server-username PROXY_SERVER_USERNAME</code> | proxy server username                                                                    |
| <code>--proxy-server-password PROXY_SERVER_PASSWORD</code> | proxy server password                                                                    |
| <code>--logout</code>                                      | Logout                                                                                   |
| <code>--username USER</code>                               | User Name                                                                                |
| <code>--username USER</code>                               | User Name                                                                                |
| <code>--auth-token AUTH_TOKEN</code>                       | authorization token                                                                      |

## Connecting via a Proxy

The command for connecting via an unauthenticated proxy:

```
ilo login --server <fqdn:port> --proxy-server <proxy_ip> --proxy-port
<proxy_port> --user-name selfserve@illumio.com
```

An example of connecting via an unauthenticated proxy:

```
ilo login --server 2x2testvc308.ilabs.io:8443 --proxy-server 10.2.184.62 --
proxy-port 3128 --user-name selfserve@illumio.com
```

An example of connecting via an authenticated proxy:

```
ilo login --server 2x2testvc308.ilabs.io:8443 --proxy-server
devtest30.ilabs.io --proxy-port 3128 --user-name selfserve@illumio.com --
proxy-server-username proxy_user --proxy-server-password proxy_124
```

After the command is executed, users are prompted to enter the PCE user's password, and then a session will be created in the context of the proxy server.

From this point on, all connections/traffic will use the proxy to send traffic.



## Using API Keys and Secrets with a Proxy Server

With the command `ilo use_api_key`, you can use an API Key and a secret with a proxy server:

**Table 3. ilo use\_api\_key --help**

| Command options                                            | Description                            |
|------------------------------------------------------------|----------------------------------------|
| <code>--key-id</code>                                      | API Key ID                             |
| <code>--key-secret</code>                                  | API Key Secret                         |
| <code>--org-id</code>                                      | Illumio Org ID                         |
| <code>--user-id Illumio</code>                             | User ID                                |
| <code>-v, --verbose</code>                                 | Verbose logging mode                   |
| <code>--trace</code>                                       | Enable API Trace Mode                  |
| <code>--server SERVER_NAME</code>                          | Illumio API Access gateway server name |
| <code>--login-server LOGIN_SERVER</code>                   | Illumio login server name              |
| <code>--kerberos-spn KERBEROS_SPN</code>                   | proxy server                           |
| <code>--proxy-port PROXY_PORT</code>                       | proxy port                             |
| <code>--proxy-server-username PROXY_SERVER_USERNAME</code> | proxy server username                  |
| <code>--proxy-server-password PROXY_SERVER_PASSWORD</code> | proxy server password                  |

The command for using an API Key with an unauthenticated proxy:

```
ilo use_api_key --key-id <key_id> --key-secret <secret> --server
<pce_fqdn> --org-id <orgid> --proxy-server <proxy_server> --proxy-port
<proxy_port>
```

The command for using an API Key with an authenticated proxy:

```
ilo use_api_key --key-id <key_id> --key-secret <secret> --server
<pce_fqdn> --org-id <orgid> --proxy-server <proxy_server> --proxy-port
<proxy_port> --proxy-server-username <proxy_username> --proxy-server-
password <proxy_password>
```

After a command is executed, all connections/traffic from this point on will use the proxy.

## Legal Notice

Copyright © 2025 Illumio 920 De Guigne Drive, Sunnyvale, CA 94085. All rights reserved.

The content in this documentation is provided for informational purposes only and is provided "as is," without warranty of any kind, expressed or implied, of Illumio. The content in this documentation is subject to change without notice.

### Resources

- [Legal information](#)
- [Trademarks statements](#)
- [Patent statements](#)
- [License statements](#)

### Contact Information

- [Contact Illumio](#)
- [Contact Illumio Legal](#)
- [Contact Illumio Documentation](#)