



Learn about new features and review the resolved and known issues for Illumio PCE, VEN, LW-VEN, and Kubernetes releases.



**IMPORTANT**

Review the updated license information for PCE UI visualization components.

Release	What's New in 24.2.x	Release Notes for 24.2.x
24.2.30	<a href="#">What's New in 24.2.30-PCE [8]</a>	<a href="#">Release Notes for 24.2.30 PCE [27]</a>
	<a href="#">What's New in 24.2.30- VEN [8]</a>	<a href="#">Known Issues in Release 24.2.30 [36]</a>
24.2.20	<a href="#">What's New in 24.2.20 VEN [10]</a>	<a href="#">Release Notes for 24.2.30 VEN [28]</a>
	<a href="#">What's New in 24.2.20 PCE [9]</a>	<a href="#">Release Notes for 24.2.20 PCE [31]</a>
24.2.11	<a href="#">What's New in 24.2.11 [10]</a>	<a href="#">Resolved Issues for 24.2.20 VEN [32]</a>
24.2.10	<a href="#">What's New in 24.2.10 [11]</a>	<a href="#">Resolved Issues in 24.2.10 [34]</a>
24.2.0	<a href="#">What's New in 24.2.0 [14]</a>	<a href="#">Resolved Issues in 24.2.0 [39]</a>

## Table of Contents

Licenses for PCE UI Visualization Components .....	7
License Expired Watermark Message .....	7
Download and Apply the Patch .....	7
What's New in 24.2 .....	8
What's New and Changed in Release 24.2.30-PCE .....	8
24.2.30-PCE Maintenance Release .....	8
What's New and Changed in Release 24.2.30-VEN .....	8
Enhanced VEN resiliency .....	8
Drop pre-existing open connections not covered by Illumio policy .....	8
Illumio IPFilter Update .....	9
What's New and Changed in Release 24.2.21-PCE .....	9
Illumio Core 24.2.21-PCE LTS Maintenance Release .....	9
What's New and Changed in Release 24.2.21-VEN .....	9
Illumio Core 24.2.21-VEN Maintenance Release .....	9
What's New and Changed in Release 24.2.20-PCE .....	9
Illumio Core 24.2.20-PCE Maintenance Release .....	10
Whats New and Changed in Release 24.2.20-VEN .....	10
Support for Windows Server 2025 .....	10
Support for Endpoint VENs on macOS Sequoia 15 and 15.1 .....	10
Support for Endpoint VENs in Microsoft Global Secure Access environ- ments .....	10
What's New and Changed in Release 24.2.11 .....	10
Illumio Core 24.2.11-VEN Maintenance Release .....	10
What's New and Changed in Release 24.2.10 .....	11
Compare V-E scores by Enforcement Type .....	11
New icon indicates vulnerability severity level .....	12
Support for Endpoint VENs on macOS Sonoma 14.4 .....	12
Easier Identification of Public IP Addresses for Endpoint VENs .....	12
Enhanced VEN Platform Resiliency .....	13
Discontinued Dependency on PowerShell .....	13
Illumio IPFilter Update .....	14
What's New and Changed in Release 24.2 .....	14
Rule Hit Count for Illumio Core SaaS .....	14
Policy is a new section in the left navigation .....	15
Override Deny Rules .....	16
UI Updates for Extra-Scope and Intra-Scope rules .....	19
Only Allow Rules are listed on some pages .....	19
Get faster query results by turning off Aggregate Explorer Results .....	19
Illumio Core REST API in 24.2 .....	20
Illumio Core Release Notes for 24.2 .....	26
Product Versions 24.2.x .....	26
24.2.30-PCE .....	26
24.2.30-VEN .....	26
24.2.21-VEN .....	26
24.2.21+A1-PCE .....	26
24.2.21-PCE .....	26
24.2.20-PCE .....	26
24.2.20-VEN .....	26
24.2.11-VEN .....	26
24.2.10-PCE and VEN .....	27
24.2.0+UI2-PCE .....	27
24.2.0-PCE .....	27
Resolved Issues in Release 24.2.30-PCE .....	27

Resolved Issues .....	28
Resolved Issues in Release 24.2.30-VEN .....	28
Resolved Issues .....	29
Resolved Issue in Release 24.2.21-VEN .....	29
Resolved Issues in Release 24.2.21+A1-PCE .....	30
Resolved Issues in Release 24.2.20-PCE .....	31
Resolved Issues in Release 24.2.20-VEN .....	32
Resolved Issues in Release 24.2.11-VEN .....	33
Resolved Issues in Release 24.2.10 .....	34
Resolved Security Issue in Release 24.2.10-PCE .....	34
Resolved Issues in Release 24.2.10-PCE .....	34
Resolved Issues in Release 24.2.10-VEN .....	35
Known Issues in Release 24.2.30 .....	36
Known Issues .....	37
Known Issue in Release 24.2.20-PCE .....	37
Known Issues in Release 24.2.20-VEN .....	38
Known Issue in Release 24.2.10-VEN .....	38
UI improvements in Release 24.2.0+UI2 .....	38
Resolved Issues in Release 24.2.0 .....	39
Enterprise Server .....	39
Containers .....	40
Known Issues in Release 24.2.0 .....	41
Enterprise Server .....	41
Illumination Plus .....	42
PCE Platform .....	42
Data Platform .....	42
PCE Web Console UI .....	43
Security Information .....	43
Illumio LW-VEN Release 1.1 .....	44
What's New in LW-VEN Release 1.1.0 .....	44
Support for flow reporting for legacy Windows servers .....	44
Resolved Issues in 1.1.10 LW-VEN .....	44
Resolved Issues in 1.1.0 LW-VEN .....	45
Illumio Core for Kubernetes Release Notes .....	46
Illumio Core for Kubernetes What's New and Release Notes for 5.3 .....	46
What's New in Illumio Core for Kubernetes 5.3.2 .....	46
What's New in Illumio Core for Kubernetes 5.3.1 .....	46
Release Notes for 5.3.2 .....	48
Resolved Issues in 5.3.1 .....	49
Illumio Core for Kubernetes Release Notes 5.2 .....	50
About Illumio Core for Kubernetes 5.2 .....	50
Updates for Core for Kubernetes 5.2.3 .....	51
Updates for Core for Kubernetes 5.2.2 .....	51
What's New in Release 5.2.1 .....	52
Updates for Core for Kubernetes 5.2.1 .....	52
What's New in Release 5.2.0 .....	52
Updates for Core for Kubernetes 5.2.0 .....	57
Illumio Core for Kubernetes Release Notes 5.1 .....	58
Core for Kubernetes 5.1.10 .....	58
Limitations .....	59
Updates for Core for Kubernetes 5.1.10 .....	59
Updates for Core for Kubernetes 5.1.7 .....	60
Updates for Core for Kubernetes 5.1.3 .....	60
Updates for Core for Kubernetes 5.1.2 .....	61
Updates for Core for Kubernetes 5.1.0 .....	61

Security Information for Core for Kubernetes 5.1 .....	63
Illumio Core for Kubernetes Release Notes 5.0.0 .....	63
About Illumio Core for Kubernetes 5.0 .....	63
Product Version .....	64
What's New in C-VEN and Kubelink .....	64
NodePort Limitations .....	64
Updates for Core for Kubernetes 5.0.0-LA .....	65
Illumio Core for Kubernetes Release Notes 4.3.0 .....	66
What's New in Kubernetes 4.3.0 .....	66
Product Version .....	67
Updates for Core for Kubernetes 4.3.0 .....	68
Illumio NEN Release Notes 2.6 .....	69
Product Version .....	69
Release Types and Numbering .....	69
What's New in NEN 2.6.x Releases .....	69
NEN 2.6.40 New Feature .....	69
NEN 2.6.30 New Features .....	71
NEN 2.6.20 New Features .....	71
NEN 2.6.10 New Features .....	72
NEN 2.6.1 New Features .....	72
NEN 2.6.0 New Features .....	72
Resolved Issues in NEN 2.6.40 .....	73
Known Issues in NEN 2.6.40 .....	74
Resolved Issues in NEN 2.6.30 .....	74
Known Issues in NEN 2.6.30 .....	74
Resolved Issue in NEN 2.6.20 .....	74
Known Issues in NEN 2.6.20 .....	74
Resolved Issues in NEN 2.6.10 .....	74
Known Issues in NEN 2.6.10 .....	75
2.6.10 Security Information .....	75
Resolved Issues in NEN 2.6.1 .....	75
Known Issues in NEN 2.6.1 .....	75
Resolved Issues in NEN 2.6.0 .....	75
Known Issues in NEN 2.6.0 .....	76
Illumio NEN Release Notes 2.5 .....	77
Product Version .....	77
Resolved Issue in NEN 2.5.2.A1 .....	77
Known Issues in NEN 2.5.2.A1 .....	77
Resolved Issues in NEN 2.5.2 .....	78
Known Issues in NEN 2.5.2 .....	78
Resolved Issue in NEN 2.5.1 .....	78
Known Issues in NEN 2.5.1 .....	78
Resolved Issues in NEN 2.5.0 .....	78
Known Issues in NEN 2.5.0 .....	79
Illumio NEN Release Notes 2.4 .....	80
Product Version .....	80
Resolved Issue in NEN 2.4.10 .....	80
Known Issues in NEN 2.4.10 .....	80
Resolved Issues in NEN 2.4.0 .....	80
Known Issues in NEN 2.4.0 .....	81
Limitation in NEN 2.4.0 .....	81
Illumio CLI Release Notes 1.4.4 .....	82
What's New in CLI Tool 1.4.4 .....	82
Support for Proxy Communication .....	82
Illumio Core PCE CLI Tool Guide 1.4.3 .....	83

What's New and Changed in Release 1.4.3 .....	83
Illumio CLI Tool 1.4.3 .....	83
Support for Proxy .....	83
Connecting via a Proxy .....	84
Using API Keys and Secrets with a Proxy Server .....	85
Legal Notice .....	86

## Licenses for PCE UI Visualization Components

A license used by PCE UI components expires on May 30, 2025. This impacts all on-premise PCE versions from 22.5 and later.

### License Expired Watermark Message

Beginning May 31, 2025, you may see a "License Expired" watermark message for any on-premises PCE version from 22.5 and later in these PCE UI visualization components:

- Explore > Map
- App Groups > App Group Name > Map
- Workloads > Blocked Traffic
- Deny Rules > Blocked Connections

### Download and Apply the Patch

You must download and apply the patch available on the [Support Portal](#) **before May 31st, 2025** to make sure that you have uninterrupted access to PCE UI visualization components and functionality.



#### NOTE

If you don't apply the patch by May 31st, 2025, you will see a "License Expired" watermark message on the affected UI pages. However, the maps will continue to work.



#### IMPORTANT

If you don't apply the patch by July 11th, 2025, the affected PCE UI visualization components will no longer display content and your pages will be blank.

Review the [Knowledge Base article](#) or contact [Illumio Support](#) if you need help.

## What's New in 24.2

### What's New and Changed in Release 24.2.30-PCE

#### 24.2.30-PCE Maintenance Release

Illumio Core 24.2.30-PCE includes an updated version of the PCE software.

Illumio provides regular maintenance updates for reported bugs and security issues, and to add support for new operating system versions. As a maintenance release, Illumio Core 24.2.30-PCE solved software and security issues for the PCE to improve its reliability and performance. For the complete list of 24.2.30-PCE resolved issues, see [Resolved Issues in Release 24.2.30-PCE \[27\]](#).

### What's New and Changed in Release 24.2.30-VEN

This release provides support for the following:

#### Enhanced VEN resiliency

As part of Illumio's ongoing efforts to improve the operational resiliency of the VEN, beginning with this release VENs now roll back to the previous known-good policy if a policy update prevents VEN-to-PCE connectivity.

#### Drop pre-existing open connections not covered by Illumio policy



#### **WARNING**

Installing VEN release 24.2.30 or later on AIX workloads can result in blocking traffic in your environment that you currently allow. Please read carefully.

Beginning with VEN release 24.2.30, AIX VENs are now at parity with Windows and Linux VENs with regard to how they handle pre-existing open connections not covered by Illumio policy. Consider the following example use case:

1. An application in your tenant holds open a pre-existing connection to a database server (for example) and the connection is not covered by an Allow rule in your Illumio policy.
2. You transition the VEN to Full Enforcement (a strict Allow-list mode).
3. Analysis:



- Windows and Linux VENs have always dropped such pre-existing connections when transitioned to Full Enforcement because there is no Allow rule allowing them in this scenario.
- Prior to VEN release 24.2.30, AIX VENs left such pre-existing connections open in this scenario (despite no rule allowing it) until the application closed the connection and later tried to make a new connection. At that point, the VEN blocked the connection (because there is no rule allowing it).
- **Result:** Now, with VEN release 24.2.30 and later, AIX VENs, in parity with Windows and Linux VENs, drop the existing connection if IP Filter 5.3.0.5004 or later is installed on the workload.

## **Illumio IPFilter Update**

The release of IPFilter version 5.3.0.5004 removes a mutex present in 5.3.0.5003 that caused the CPU to become a bottleneck for IPFiltering, as many CPU cores tried to access the counter variables concurrently. In IPFilter version 5.3.0.5004, counter variables are incremented / decremented using atomic operations, such as `fetch_and_add`.

## **What's New and Changed in Release 24.2.21-PCE**

### **Illumio Core 24.2.21-PCE LTS Maintenance Release**

Illumio Core 24.2.21-PCE includes an updated version of the PCE. Illumio provides regular maintenance updates for reported bugs and security issues, and to add support for new operating system versions. As a maintenance release, Illumio Core 24.2.21-PCE solved a security issue for the PCE to refine the software and improve its reliability and performance.

For the complete list of improvements and enhancements to the PCE in Illumio Core 24.2.21, see [Security Information for 24.2.x \[43\]](#).

## **What's New and Changed in Release 24.2.21-VEN**

### **Illumio Core 24.2.21-VEN Maintenance Release**

Illumio Core 24.2.21 includes an updated version of the VEN software.

Illumio provides regular maintenance updates for reported bugs and security issues and to add support for new operating system versions. As a maintenance release, Illumio Core 24.2.21 solved a software issue for the VEN to improve its reliability and performance.

## **What's New and Changed in Release 24.2.20-PCE**

## **Illumio Core 24.2.20-PCE Maintenance Release**

Illumio Core 24.2.20-PCE includes an updated version of the PCE. Illumio provides regular maintenance updates for reported bugs and security issues, and to add support for new operating system versions. As a maintenance release, Illumio Core 24.2.20-PCE solved software and security issues for the PCE to refine the software and improve its reliability and performance.

For the complete list of improvements and enhancements to the PCE, see [Resolved Issues in Release 24.2.20-PCE \[31\]](#).

## **Whats New and Changed in Release 24.2.20-VEN**

This release provides support for the following:

### **Support for Windows Server 2025**

With this release, Server VENs now support the Windows Server 2025 operating system.

### **Support for Endpoint VENs on macOS Sequoia 15 and 15.1**

With this release, Endpoint VENs now support macOS Sequoia 15 and 15.1. For information about the Endpoint for macOS, see the [Endpoint Concepts Guide](#) and the [Endpoint User Guide](#).

### **Support for Endpoint VENs in Microsoft Global Secure Access environments**

Beginning with this release, Endpoint VENs support environments that implement Microsoft Global Secure Access (GSA). GSA is the unifying term used for both Microsoft Entra Internet Access and Microsoft Entra Private Access, which together comprise Microsoft's Security Service Edge (SSE) solution. For more information about GSA, see the Microsoft document [What is Global Secure Access?](#)

## **What's New and Changed in Release 24.2.11**

### **Illumio Core 24.2.11-VEN Maintenance Release**

Illumio Core 24.2.11-VEN includes an updated version of the VEN software.

Illumio provides regular maintenance updates for reported bugs and security issues, and to add support for new operating system versions. As a maintenance release, Illumio Core 24.2.11 solved software and security issues for the VEN to improve its reliability and performance. For the complete list of improvements and enhancements to the PCE, see [Resolved Issues in Release 24.2.11-VEN \[33\]](#).

## What's New and Changed in Release 24.2.10

The following new features were added in Illumio Core 24.2.10.

### Compare V-E scores by Enforcement Type

The Show Vulnerability Exposure (V-E) Score tool makes it easy to see how the security of your workloads and app groups would change if you were to change their current enforcement mode. New columns in the Workload and App Group list and details pages provide a side-by-side comparison of the effect different enforcement modes would have on Vulnerability Exposure (V-E) scores. A toggle allows you to simulate the switch between Full Enforcement and Visibility Only enforcement modes.



#### NOTE

This option allows you to simulate the switch between Full Enforcement and Visibility Only modes. It doesn't change the actual enforcement mode of your workloads or app groups.

For more information, see:

- [Compare Workload V-E Scores by Enforcement Type](#)
- [Compare App Group V-E Scores by Enforcement Type](#)

Home > Servers & Endpoints

### Workloads

Workloads Container Workloads VENs

+ Add - Remove Edit Labels Enforcement Visibility

Select properties to filter view


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

	Connectivity	Full Enforcement V-E Score	Current V-E Score	Enforcement	Visibility	Policy Sync	Ransomware Exposure	Protection Coverage Score	Name
<input type="checkbox"/>	Online	0	3.1	Visibility Only	Blocked + Allowed	Active	Critical	0%	409_vm4.local
<input type="checkbox"/>	Online	0	3	Selective	Blocked + Allowed	Active	Critical	0%	409_vm1.local
<input type="checkbox"/>	Online	0	0	Full	Blocked + Allowed	Active	Protected	82%	409_vm2.local
<input type="checkbox"/>	Online			Full	Blocked + Allowed	Active	Protected	82%	409_vm3.local



### New icon indicates vulnerability severity level


This release introduces a familiar gradient icon to indicate the vulnerability severity level of workloads and app groups. The new icon improves UI accessibility by conveying a range of severity without relying on a color scheme.

Previous	New Icon
<div>V-E Score</div> <div>356</div>	<div>Current V-E Score</div> <div>6.1 </div>

### Support for Endpoint VENs on macOS Sonoma 14.4

With this release, Endpoint VENs now support macOS Sonoma 14.4. For information about the Endpoint for macOS, see the Endpoint Installation and Usage Guide.

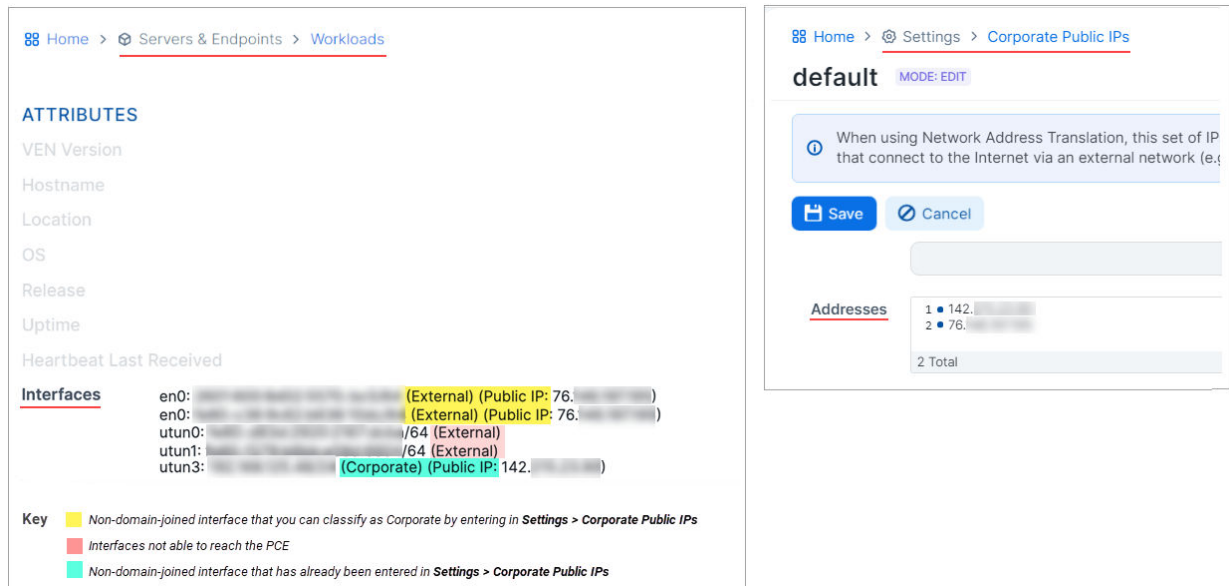
### Easier Identification of Public IP Addresses for Endpoint VENs

**NOTE**

This is an enhancement to the network profile detection feature. Network profile detection allows the PCE to determine whether a workload interface is connected to your Corporate network or to an external network (for example, a cafe or airport Wifi). The PCE uses this information to program network-specific rules on each of the endpoint's interfaces. For more information about Illumio's NLA implementation, see NLA Support for Endpoints.

Beginning with this release, in the workload details pages in the PCE, the word Public is now prepended to the IP address (as seen by the PCE) of non-domain-joined Windows

workloads and macOS endpoint interfaces reachable by the PCE. When you enter these Public IP addresses in the PCE (**Settings > Corporate Public IP**), the PCE classifies them as Corporate and programs their corresponding endpoint interfaces with the appropriate Illumio security policies. See [Add Public IP addresses to the Corporate Public IPs list](#).



## Keep in mind:

- As non-domain joined Windows endpoints or macOS endpoint VENs make network location detection calls to the PCE from each workload interface, the public IP address they report is the source of the IP address as seen by the PCE.
- In SaaS, the IP is also an organization's public egress IP to the Internet.
- If a given interface is not reachable by the PCE, its IP address is classified as "External" on the workload's details page and "Public" does not appear.
- If you enter the IP address of a non-domain-joined Windows workload or macOS endpoint in **Settings > Corporate Public IPs**, the PCE classifies its associated interface as "Corporate." Otherwise, the PCE classifies the interface as "External."

## Enhanced VEN Platform Resiliency

To mitigate the effects of data loss and file corruption that can result from a sudden loss of power or the host crashing, VEN release 24.2.10 provides enhanced resiliency as follows:

- When VEN data is written to volatile memory, it's now simultaneously written to disc, ensuring a higher likelihood of successful recovery.
- In the event of file corruption, certain VEN configuration files are now backed up and then restored automatically.

## Discontinued Dependency on PowerShell

Starting with VEN release 24.2.10, customers can perform VEN tasks in any Windows Command Line shell capable of executing \*.exe commands. This includes Command Prompt (cmd.exe) and PowerShell, among others. As all modern Windows machines include Com-

mand Prompt by default, all PowerShell commands in Illumio VEN documentation have been changed to equivalent \*.exe commands.

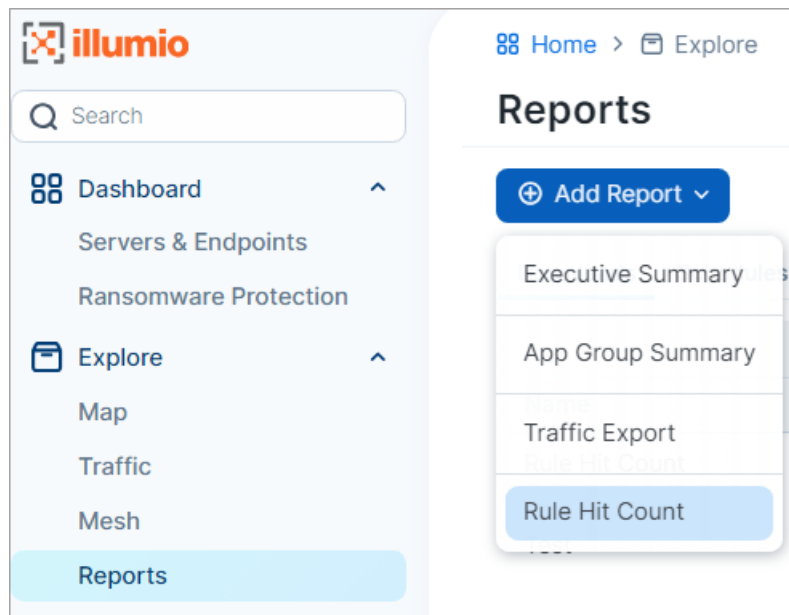
## Illumio IPFilter Update

The release of IPFilter 5.3.0.5003 provides increased throughput over the loopback interface when the VEN is in Visibility, Selective Enforcement, or Full Enforcement mode. This improves performance for some applications and tools that are sensitive to latency of the loopback interface.

## What's New and Changed in Release 24.2

The following new features were added in Illumio Core 24.2.

### Rule Hit Count for Illumio Core SaaS



Beginning with this release, the Rule Hit Count feature is now available for Illumio Core SaaS customers. (Requires VEN 23.2.30 or later).

You can add a Rule Hit Count Report through the PCE UI or the Illumio REST API.

The Rule Hit Count Report provides the following:

- Policy Compliance: Generate a Rule Hit Count Report to provide evidence that security controls are in place and working effectively, demonstrating compliance to auditors.
- Redundancy Removal: Identify unused or less-used rules so you can remove or modify them to reduce redundancy and clutter in your implementation.
- Troubleshooting: When network issues arise, identify the rules that were in effect during the relevant traffic flow, allowing you to resolve problems faster and more efficiently.

The PCE and VENs require enablement through the Illumio REST API.

## Policy is a new section in the left navigation

The Policy section replaces Rules & Rulesets in the left navigation.



### NOTE

For now, the stand-alone Deny Rules page still appears in the left navigation, but it's slated to be deprecated for future releases. If your Core instance was upgraded to release 24.2.x, Illumio recommends that you migrate your Deny rules from the Deny Rules page to the Policies page and add Deny Rules from the Policies page from now on.

**Home > Policy > Policies**

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

Database Add Scope

Add Rule Remove Disable

Select properties to filter view

Override Deny Rules 1		
Provision Status	No.	Status
Pending	1	Enabled

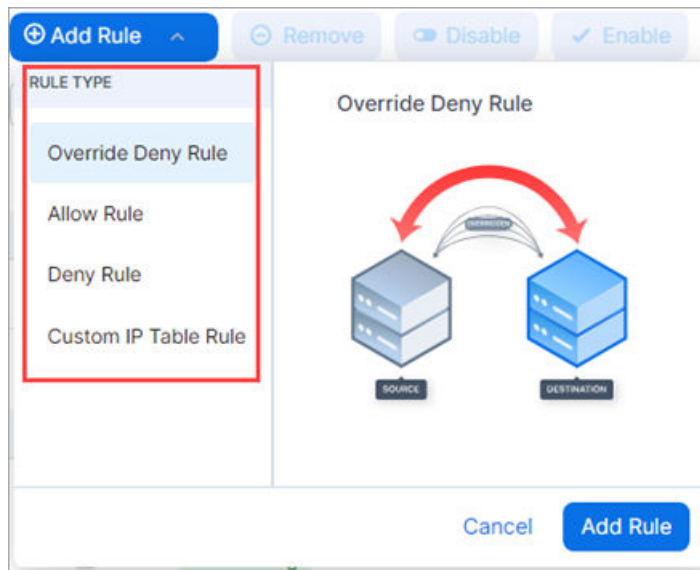
Allow Rules 2		
Provision Status	No.	Status
Pending	1	Enabled
Pending	2	Enabled

Deny Rules 1		
Provision Status	No.	Status
Pending	1	Enabled

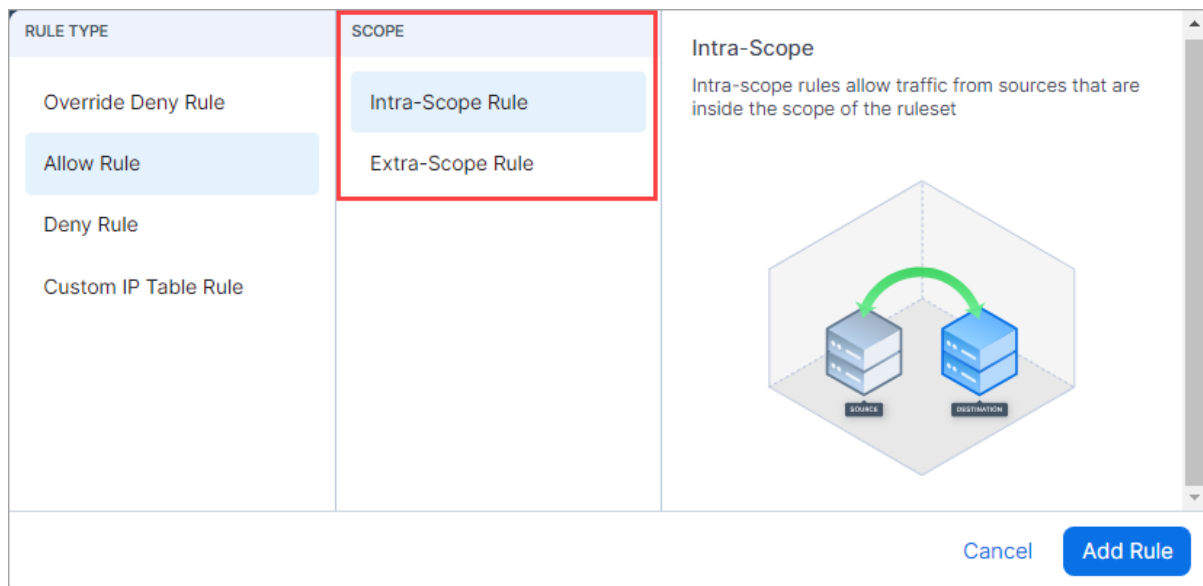
The Policies page differs from Rulesets & Rules in the following ways:

- Rule types appear in a list when you click **Add Rule**.

- All rule types can now be added from a single page.
- You can add and view Override Deny rules
- Rule types are listed in the order of their precedence.



- Scope types are listed in a Scope category when you choose Allow Rule.



## Override Deny Rules



### NOTE

- Override Deny rules require VEN release 22.3.0 or later.
- Deny and Override Deny rules are implicitly Intra-Scope rules. Extra-Scope deny rules are not supported currently.

This release introduces Override Deny rules. These are "without exception" deny rules that have precedence over all other types of rules and can't be overridden. Use Override Deny



rules to block communication that should always be blocked. For example, if an administrator in your organization creates an Allow rule that would permit communication that should always be denied, having an Override Deny rule in place denying that communication serves as a safeguard. Override Deny rules:

- Provide an additional type of granular control for blocking network traffic, helping to ensure that only explicitly authorized communications are permitted.
- Block traffic with a type of Deny rule that can't be overridden.
- Can be used in scoped and un-scoped rulesets.
- Impact the calculation of ransomware protection coverage and V-E scores.
- Support the Rule Hit Count feature.
- Support compliance with stringent regulatory requirements by enforcing the principle of least privileged access.

### Example

- Suppose you want to block all traffic between your Production and Development environments except over `splunk-data` (9997 TCP) (existing capability).
- Additionally, you want to block all traffic between all workloads over SSH with no exceptions possible (highest precedence; new capability with this release).

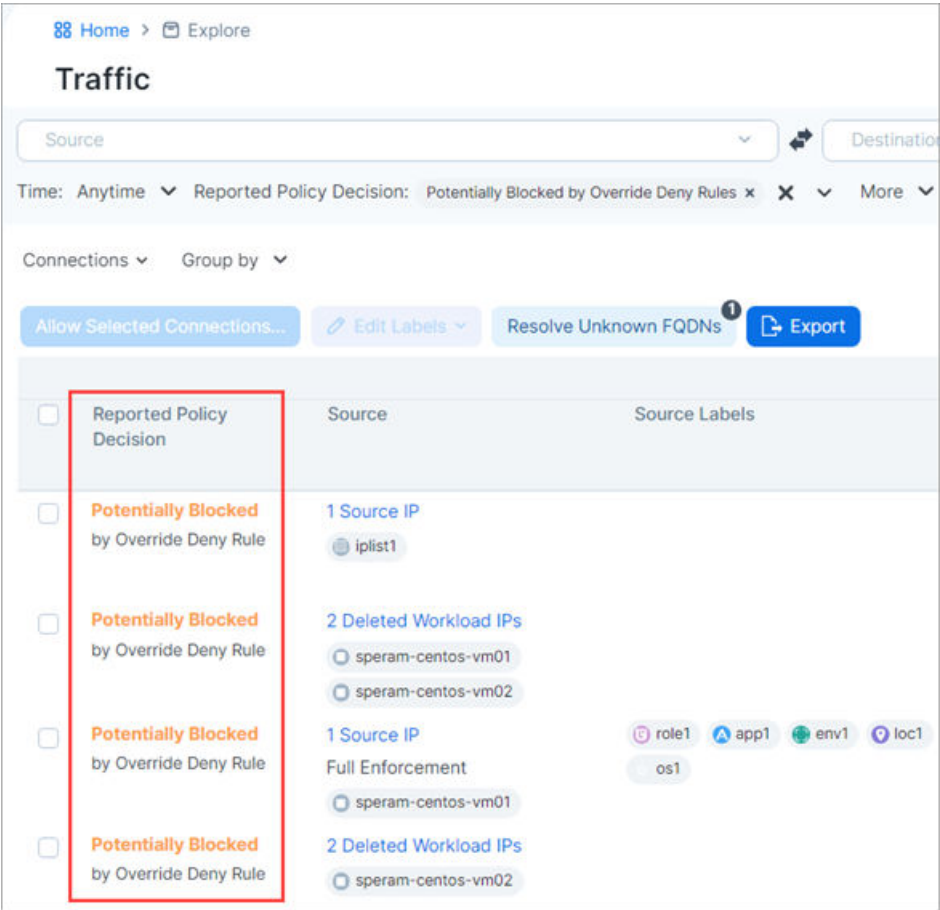
1. Add a **Deny rule** specifying Production as the source and Development as the destination, blocking all services.
2. Add an **Allow rule** specifying the same source and destination, permitting traffic over `splunk-data` (9997 TCP).
3. Add an **Override Deny** rule blocking all traffic between all workloads over SSH. Because this rule has the highest precedence, it can't be overridden by an Allow rule.

Override Deny Rules									
<input type="checkbox"/>	Provision Status	No.	Status	Sources	→	Destinations	Destination Services	Rule Options	
<input type="checkbox"/>	Pending	1	Enabled	All Workloads	→	All Workloads	ssh	Deny	
Allow Rules									
<input type="checkbox"/>	Provision Status	No.	Status	Sources	Source Process / Service	→	Destinations	Destination Services	Rule Options
<input type="checkbox"/>	Pending	1	Enabled	E-Dev		→	E-PROD	splunk-data	Allow
Deny Rules									
<input type="checkbox"/>	Provision Status	No.	Status	Sources	→	Destinations	Destination Services	Rule Options	
<input type="checkbox"/>	Pending	1	Enabled	E-Dev	→	E-PROD	All Services	Deny	

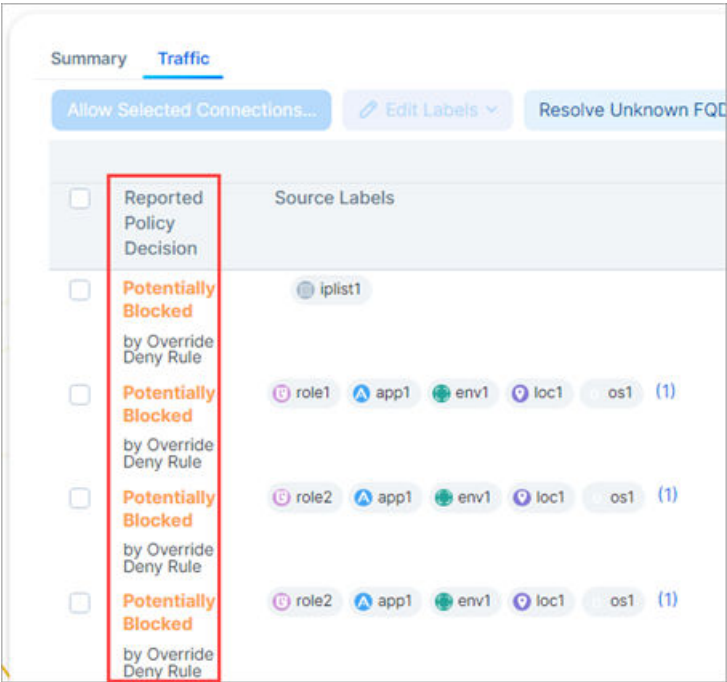
### Appearance in Visualization tools

When Override Deny rules block or potentially block traffic in your environment, the policy decision is indicated in the Map and Traffic views in the PCE UI.

### As seen in Traffic view



As seen in the details panel in Map view



Impact on key security measurements

Adding Override Deny rules to your security policy affects the calculation of the following security measurements:

- Ransomware protection coverage
- V-E score

## UI Updates for Extra-Scope and Intra-Scope rules

- The separate tabs that contained Intra-Scope and Extra-Scope options in previous releases are removed and a new column called Scope Type appears in the Allow rules section of the Policies page.
- Extra-Scope and Intra-Scope rules occupy different sections within Allow Rules, separated by a gray line.
- You can move rules up or down but only within their respective section.
- Extra-Scope rules are now distinguished by an icon.

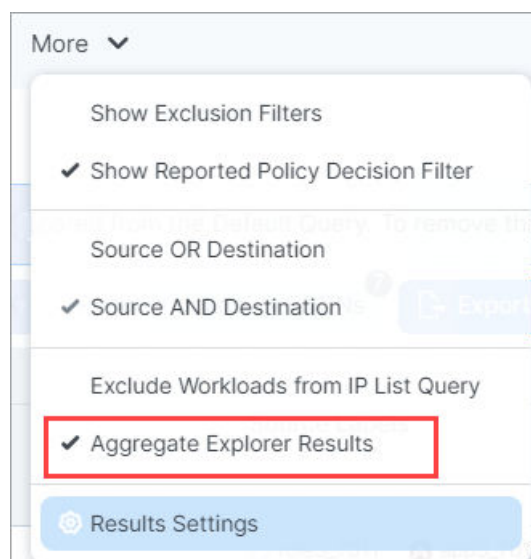
Provision Status	No.	Status	Scope Type	Sources	Source Process / Service	Destinations	Destination Services	Rule Options
Pending	1	Enabled	Intra-Scope	Any (0.0.0.0/0 and ::0)		All Workloads	srvName2_2995	Allow
Pending	2	Enabled	Intra-Scope	All Workloads		All Workloads	All Services	Allow
Pending	3	Enabled	Extra-Scope	Any (0.0.0.0/0 and ::0)		All Workloads	srvName2_2995	Allow
Pending	4	Enabled	Extra-Scope	All Workloads		All Workloads	All Services	Allow

## Only Allow Rules are listed on some pages

The badge **ALLOW RULES ONLY** appears in the following areas of the PCE UI where only Allow Rules are listed. Illumio plans to list other rule types in those pages in a future release.

- Troubleshoot > Policy Check
- App Groups details page > Rules tab
- Policy > Policies > Rule Search tab

## Get faster query results by turning off Aggregate Explorer Results



If it's taking too long for query results to appear in the Map or the Traffic table, you can now try to speed things up by turning off Aggregate Explorer Results (on by default) through the More menu. Be aware that turning off aggregation means you may see more duplicate flows, which can result in a slight loss of fidelity in data reporting.

1. Click **More**.
2. Click **Aggregate Explorer** Results on the menu to turn it off/on.
3. Click **Run**.

## Illumio Core REST API in 24.2

The Illumio Core REST API v2 has changed in 24.2 in the following ways.

See the REST API Developer Guide for more information.

## Rule-based Label Mapping



### NOTE

APIs for Rule-based Label Mapping have been released in 24.1.1.

The new and changed APIs in release 24.1.1 support the following product features:

In version 24.1.1, several APIs are added to support rule-based label mapping.

Illumio administrators can use rule-based label mapping to assign relevant labels to workloads through various methods, such as:

- Labels are automatically applied to workloads based on the subnets in which they reside.
- Labels are assigned according to the operating system platform of the workloads.
- New applications can be bootstrapped with appropriate labels using a one-time action.

This approach allows administrators to transform workload attributes (like subnet, OS platform) into standardized (R, A, E, L) or custom labels, ensuring consistent and accurate labeling across the PCE environment.

### Key Features of Rule-based Label Mapping

Rules are evaluated in a predetermined order. Once a label is assigned for a specific label type, further processing for that type stops, while evaluation continues for other label types.

- Labels are appended only to empty label types associated with the workload. Pre-existing labels remain unaffected.
- Label mapping rules are triggered manually on an ad-hoc basis.
- All label mapping rules are executed collectively, precluding individual rule activation.

- Rule evaluation is restricted to workload attributes accessible to the PCE within its internal database. External data sources (for example, VMware and AD) are not supported.
- The one-click labeling process incorporates a review step, allowing users to examine the impact of applied labels on workloads through a downloadable CSV file. Confirmation is required to finalize the labeling process.
- The label assignment is permanent and cannot be undone.
- The rule execution process does not facilitate the creation of new label types; it operates exclusively on pre-defined label types.
- Rule-based label mapping is supported for both on-premise and SaaS PCE deployments.

This functionality provides administrators granular control over workload labeling, streamlining categorization, and management within the PCE ecosystem.

## New APIs for Rule-based Label Mapping

New APIs for managing the new feature Rule-based label mapping are the following:

### GET /api/v2/orgs/:xorg\_id/label\_mapping\_rules

Returns the collection of label mapping rules

Example response:

```
[
  {
    "href": "/orgs/1/label_mapping_rules/
48ed8903-878e-4010-859a-63d19be797c3",
    "enabled": true,
    "position": 40,
    "created_at": "2024-04-24T06:54:00.530Z",
    "updated_at": "2024-04-24T06:54:00.535Z",
    "expression": {
      "property": "hostname",
      "values": [
        "this"
      ],
      "operator": "starts_with"
    },
    "created_by": {
      "href": "/users/2"
    },
    "updated_by": {
      "href": "/users/2"
    },
    "label_assignments": [
      {
        "label": {
          "href": "/orgs/1/labels/24"
        }
      },
      {
        "label": {
          "href": "/orgs/1/labels/11"
        }
      }
    ]
  }
]
```

```

        {
          "label": {
            "href": "/orgs/1/labels/20"
          }
        }
      ],
      {
        "href": "/orgs/1/label_mapping_rules/d1479032-f7cb-479f-87bd-1bc7bd816a74",
        "enabled": true,
        "position": 41,
        "created_at": "2024-04-26T18:18:10.238Z",
        "updated_at": "2024-04-26T18:18:10.256Z",
        "expression": {
          "property": "hostname",
          "values": [
            "perf-workload-1"
          ],
          "operator": "equals"
        },
        "created_by": {
          "href": "/users/1"
        },
        "updated_by": {
          "href": "/users/1"
        },
        "label_assignments": [
          {
            "label": {
              "href": "/orgs/1/labels/9"
            }
          }
        ]
      },
      {
        "href": "/orgs/1/label_mapping_rules/d4ddb653-56e9-4150-a93e-8a734c510c03",
        "enabled": true,
        "position": 43,
        "created_at": "2024-04-28T00:05:38.146Z",
        "updated_at": "2024-04-28T00:05:38.150Z",
        "expression": {
          "property": "hostname",
          "values": [
            "perf-workload-2"
          ],
          "operator": "equals"
        },
        "created_by": {
          "href": "/users/2"
        },
        "updated_by": {
          "href": "/users/2"
        },
      }
    ]
  }
}

```

```

    "label_assignments": [
      {
        "label": {
          "href": "/orgs/1/labels/7"
        }
      }
    ]
  }
]

```

### POST /api/v2/orgs/:xorg\_id/label\_mapping\_rules

Creates a new label-mapping rule.

Example Request:

```

{
  "expression": {
    "logical_operator": "and",
    "child_expressions": [
      {
        "property": "os",
        "operator": "equals",
        "values": ["linux"]
      },
      {
        "property": "process",
        "operator": "contains",
        "values": ["mysql"]
      }
    ]
  },
  "label_assignments": [
    {
      "label": {
        "key": 'os',
        "value": 'Linux'
      }
    },
    {
      "label": {
        "key": 'role',
        "value": 'Database'
      }
    }
  ]
}

```

Example Response:

```

{
  "href": "/orgs/1/label_mapping_rules/4512e359-bda3-49d1-8f9e-b9a03357e4ee",
  "enabled": true,
}

```

```

    "position": 2,
    "created_at": "2024-04-18T23:45:49.237Z",
    "updated_at": "2024-04-18T23:45:49.290Z",
    "expression": {
      "property": "os",
      "operator": "contains",
      "values": [
        "windows"
      ]
    },
    "created_by": {
      "href": "/users/1"
    },
    "updated_by": {
      "href": "/users/1"
    },
    "label_assignments": [
      {
        "label": {
          "key": "os",
          "value": "Windows"
        }
      }
    ]
  }
}

```

#### **PUT /api/v2/orgs/{org\_id}/label\_mapping\_rules/delete**

Deletes multiple label mapping rules

#### **GET /api/v2/orgs/:xorg\_id/label\_mapping\_rules/:label\_mapping\_rule\_id**

Gets the instance of a single label-mapping rule.

#### **PUT /api/v2/orgs/:xorg\_id/label\_mapping\_rules/:label\_mapping\_rule\_id**

Updates the instance of a single rule

#### **DELETE /api/v2/orgs/:xorg\_id/label\_mapping\_rules/:label\_mapping\_rule\_id**

Deletes the specified label-mapping rule.

#### **PUT /api/v2/orgs/{org\_id}/label\_mapping\_rules/{label\_mapping\_rule\_id}/re-order**

Reorder label-mapping rules

#### **POST /api/v2/orgs/:xorg\_id/label\_mapping\_rules/run**

This asynchronous API runs a set of label-mapping rules on a set of workloads.

#### **GET /api/v2/orgs/:xorg\_id/label\_mapping\_rules/run/:job\_uuid**

Gets the status of the async job to run the rules

#### **GET /api/v2/orgs/:xorg\_id/label\_mapping\_rules/run/:job\_uuid/download**

Downloads the results of the run rules job.



### **PUT /api/v2/orgs/:xorg\_id/label\_mapping\_rules/run/:job\_uuid/assign\_labels**

Assigns labels from the results of the label-mapping rules run job.

### **Changed APIs**

#### **optional\_features\_put**

This API has one new property:

```
[  
  "rule_based_label_mapping"  
]
```

It was added to include the new feature for rule-based label mapping in release 24.1.1

## Illumio Core Release Notes for 24.2

### Product Versions 24.2.x

#### 24.2.30-PCE

- **PCE Version:** 24.2.30 (Illumio On-Premises customers only)

#### 24.2.30-VEN

- **PCE Version:** 24.2.30

#### 24.2.21-VEN

- **PCE Version:** 24.2.21 (Illumio On-Premises customers only)

#### 24.2.21+A1-PCE

- **PCE Version:** 24.2.21+A1-PCE (Limited Availability release for select Illumio On-Premises customers only)

#### 24.2.21-PCE

- **PCE Version:** 24.2.21 (Illumio On-Premises customers only)

#### 24.2.20-PCE

- **PCE Version:** 24.2.20 (Illumio On-Premises customers only)

#### 24.2.20-VEN

- **PCE Version:** 24.2.20

#### 24.2.11-VEN

- **PCE Version:** 24.2.10

### 24.2.10-PCE and VEN

- **PCE Version:** 24.2.10 (Illumio On-Premises customers only)
- **VEN Version:** 24.2.10
- **LW-VEN Version:** 1.1.0

### 24.2.0+UI2-PCE

- **PCE Version:** 24.2.0+UI2 (Illumio Cloud and Illumio On-Premises customers)
- **VEN Version:** 23.2.30
- **LW-VEN Version:** 1.0.10

### 24.2.0-PCE

- **PCE Version:** 24.2.0 (Illumio Cloud customers)
- **VEN Version:** 23.2.30
- **LW-VEN Version:** 1.0.10

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 Issues in Release 24.2.30-PCE

These release notes describe the resolved and known issues for this release.

## Resolved Issues

Issue	Fix Description
E-127745	<p><b>Editing the scope now possible when adding a policy</b></p> <p>Users were unable to edit the scope when adding a policy from the "Inbound Admin Access" template. This occurred when the PCE didn't have the necessary scope labels. Normally, these labels and other dependencies are auto-generated when the template is created and saved.</p> <p>The issue is resolved. Users can now successfully access, edit, and save the scope as expected when applying the template.</p>
E-127078	<p><b>Override Deny and Deny rules now counted toward the rule object limit</b></p> <p>Before this issue was fixed, the deny and override deny rules weren't added to rules counts, and thus, rule limits didn't apply to them. After the fix, deny and override deny rules are counted together with allow rules.</p>
E-126022	<p><b>Count of VS IDs in the source_rule_ids is now correct</b></p> <p>When multiple virtual services (VS) were assigned to a single workload, part of the policies had only one VS ID in the <b>source_rule_ids</b> instead of all of them. This resulted in some VS rules not having any hits at all. This is now fixed.</p>
E-124261	<p><b>CVEN Convergence Issue</b></p> <p>These two problems have been resolved:</p> <ul style="list-style-type: none"> <li>• <b>Out-of-sync problem:</b> The customer fixed the problem with the Load Balancer.</li> <li>• <b>Higher CPU utilization</b> <ul style="list-style-type: none"> <li>• Part of the policy Kubelink receives from the PCE for disconnected C-VEs was not acknowledged by the PCE, causing unnecessary policy calculations and a high PCE load. This issue is addressed in EYE-122830, Kubelink: Skipping the ACK of an unknown workload causes repeated policy calculations and sets ACKs. This issue is covered in the release notes for containers.</li> <li>• Kubelink was unable to process the PCE policy due to the incorrect format of the policy used for the selected agents. This issue is covered in EYE-117311, Unpair existing CVEN if a new one calls 'activate' with the same <b>machine_id</b>. This issue was not added to the release notes.</li> </ul> </li> </ul>
E-123013	<p><b>Services on the standby cluster following the upgrade</b></p> <p>Redis job services on the standby PCE didn't stay in the running state.</p>
E-121874	<p><b>Core services data creation</b></p> <p>The Core Services page incorrectly displayed no data. This issue is resolved.</p>
E-120467	<p><b>Supercluster replication after upgrade to 23.5.x PCE</b></p> <p>In rare cases where VEs were previously moved among PCEs in a Supercluster, replication failed after upgrading the PCE to 23.5. x. This issue is resolved.</p>
E-108511	<p><b>PCE "Upgrading" Status now Cleared</b></p> <p>The PCE "Upgrading" Status was not cleared when the VE was upgraded. This issue is resolved.</p>

## Resolved Issues in Release 24.2.30-VE

These release notes describe the resolved issues for this release.

## Resolved Issues

Issue	Fix Description
E-127950	<p><b>Traffic flowing on ignored interfaces is now ignored as expected</b></p> <p>On Windows workloads, ICMP error packets traversing ignored network interfaces were not ignored as expected and were then blocked. This issue is resolved.</p>
E-126071	<p><b>Linux and AIX VEN activation issue is now fixed in SOCKS Proxy environment</b></p> <p>Where a web proxy server was configured for a VEN, activation could fail on Linux and AIX workloads if the web proxy server also supported the SOCKS Proxy protocol.</p>
E-125712	<p><b>Excessive SID logging is fixed</b></p> <p>This release fixes an issue that caused excessive logging of SIDs in <code>agentmgr.log</code> on Windows Domain Controllers.</p>
E-125300	<p><b>Traffic directionality and source/destination representation is fixed</b></p> <p>When the Container Inherits Host Policy (CIHP) feature is enabled on a workload hosting a container, the VEN reports traffic flowing into the workload (that is, traffic flowing both to the host and to the hosted container(s)). The VEN collects and reports all traffic flows in the host network namespace. In some cases, the host and the PCE interpreted the directionality of the traffic differently. For example, the host interpreted traffic flowing inbound to the container as outbound traffic because it flowed out from the host. Conversely, the PCE interpreted the same traffic as flowing inbound to the container. Prior to VEN release 24.2.30, such traffic was depicted in the Traffic page as outbound traffic (consistent with the host's interpretation), which caused confusion. Beginning with VEN release 24.2.30, traffic in this case is now shown as inbound traffic (consistent with the customer and the PCE's interpretation).</p>
E-123210	<p><b>Policy no longer fails when Machine Auth and Rule Hit Count are both enabled on Windows</b></p> <p>On Windows workloads, VENs failed to generate policy if Machine Authentication (AdminConnect) and Rule Hit Count were both enabled. This issue is resolved.</p>
E-123154	<p><b>FQDN rules now function properly</b></p> <p>FQDN rules did not function properly on systems using IPv6 DNS servers and nftables firewall. This issue is resolved.</p>
E-122188	<p><b>Policy sync error no longer occurs when a VEN operates in a web proxy environment</b></p> <p>In environments where a web proxy was configured to direct the VEN to use the proxy to communicate with the PCE and the VEN was switched to Selective mode, new policy may not have been accepted even if there was no Deny rule blocking communication to the proxy. This issue is resolved.</p>

## Resolved Issue in Release 24.2.21-VEN

This release note describes a resolved issue in this release.

Issue	Fix Description
E-127137	<p><b>VEN Platform Handler is now responsive on systems with Name Resolution Policy enabled</b></p> <p>The VEN Platform Handler became non-responsive on systems with Name Resolution Policy enabled. In this case, the issue prevented the user from uninstalling the VEN but it could have appeared in other situations. This issue is resolved.</p>

## Resolved Issues in Release 24.2.21+A1-PCE



### NOTE

Illumio Core 24.2.21+A1-PCE is a Limited Availability release for select Illumio on-premise customers only.

- **Upgrades from 22.5.32 now succeed without ruby core dumps** (E-124881)

Ruby 3.1 used by the PCE starting in 23.2.20 introduced a memory compaction feature that can cause crashes or core dumps when processing a large number of workloads. To address this we have patched Ruby to avoid this functionality in 24.2.21+A1. Notably, the Ruby maintainers themselves have done this in Ruby 3.2. This is therefore a temporary requirement until the customer migrates to 25.x which uses a later version of Ruby that should not have this issue.

## Resolved Issues in Release 24.2.20-PCE

Issue	Description
E-1218 46	<p><b>Blank screen appeared when attempting to edit a NEN-managed switch through the PCE</b></p> <p>In an environment with NENs managing switch traffic, clicking <b>Edit</b> in the PCE UI to edit a switch or add an interface to an already-managed switch resulted in a blank screen.</p>
E-1215 67	<p><b>Traffic results blank when using a large IP list as an exclusion filter</b></p> <p>When on a supercluster leader, running a traffic query that uses a large IP list as a filter failed to produce any search results, and generated an "Incomplete Results" error message from several PCE members.</p>
E-1205 37	<p><b>Traffic filter option slowed traffic queries</b></p> <p>The option to <code>aggregate_flows_across_days</code> is set to <b>true</b> by default. The capability that allowed users to change it to <b>false</b> through the UI has been removed because that setting caused traffic queries to take too long to complete.</p>
E-1202 43	<p><b>Container cluster service provisioning failures</b></p> <p>This release addresses transient container cluster service provisioning issues when the PCE is under high load.</p>
E-1196 68	<p><b>PCE setup does not work on RHEL 9.x in FIPS mode</b></p> <p>This release resolves an incompatibility with the PCE and RHEL 9.x in FIPS mode which caused the PCE to not start properly.</p>
E-1193 21	<p><b>Rule-Based Label scheduler causes a JavaScript error</b></p> <p>The scheduler for Rule-based Labeling was causing a JavaScript error that was breaking the page.</p>
E-1185 58	<p><b>Flows in Illumination or traffic database summary not visible</b></p> <p>In Flow Analytics an error occurred, and users could not see flows in Illumination or the traffic database summary.</p>
E-1166 48	<p><b>UI fields fail to occasionally load under Rulesets and Rules</b></p> <p>Sometimes when writing a rule in 24.1.3-PCE, the <b>Sources</b> or <b>Destination</b> fields never properly loaded or were not populated with labels that were chosen. This could occur when viewing a grid layout in smaller screen sizes, which reduced the source/destination selector dropdown height and caused options to be improperly displayed or hidden completely with a scroll.</p>

## Resolved Issues in Release 24.2.20-VEN

Issue	Description
E-1224 52	<p><b>macOS VEN authentication failed sporadically</b></p> <p>Under certain race conditions, macOS VENs failed to authenticate with the Network Location Detection PCE API and incorrectly marked corporate interfaces as external interfaces, leading to corporate network traffic being dropped sporadically.</p>
E-1224 17	<p><b>Policy failed to load on some OEL 5.11 UEK workloads with 24.2.10 VENs</b></p> <p>Policy failed to load on workloads running Oracle Enterprise Linux 5.11 Unbreakable Enterprise Kernel (UEK) and with 24.2.10 VENs installed.</p>
E-1215 79	<p><b>Policy application failure</b></p> <p>In some cases, policy application failed in orgs with Rule Hit Count enabled.</p>
E-1213 42	<p><b>VEN unable to create a support report</b></p> <p>VENs installed on workloads configured with the Windows Server Core option failed to create a support report.</p>
E-1212 87	<p><b>Customer's pre-existing iptables rules were 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. The issue was caused by the use of a dash instead of an underscore between "non" and "primary" in the coexistence mode setting.</p>
E-1212 51	<p><b>Connectivity lost following VEN upgrade</b></p> <p>On Solaris v11.4 workloads, immediately after upgrading a VEN to version 24.2.11, in some cases the VEN lost connectivity with the PCE. The issue stemmed from a change in the accepted <code>/etc/firewall/pf.conf</code> syntax.</p>
E-1212 20	<p><b>Policy sync error thrown following Solaris VEN update</b></p> <p>A policy sync error was thrown after updating a VEN on a Solaris workload from VEN release 21.5 to release 23.2. The error appeared after switching the VEN out of Idle mode.</p>
E-12115 7	<p><b>Programming error when proxy communication was allowed in some cases</b></p> <p>For a VEN behind a web proxy, a policy programming error occurred if communication with the proxy was allowed by an FQDN in an IPList.</p>
E-1209 83	<p><b>False-positive firewall tamper alerts appeared after upgrading Linux VEN to 24.2.10</b></p> <p>After updating VENs on Linux workloads to VEN release 24.2.10, false-positive firewall tampering alerts appeared on the PCE every ten minutes. The issue stemmed from the presence of a deprecated conntrack chain in the firewall.</p>
E-1202 02	<p><b>From the PCE, unable to upgrade or uninstall VENs installed on certain Windows workloads</b></p> <p>An issue in Illumio Core Release 24.2.10-VEN prevented upgrading or unpairing VENs installed on Windows 7 and Windows Server 2008R2 workloads through the PCE web console. The ability to manually upgrade and uninstall VENs was unaffected.</p>



Issue	Description
E-1196 24	<p><b>Excessive number of API requests impacted performance</b></p> <p>In some circumstances, performance was impacted when the PCE tried to fulfill a higher-than-normal number of API requests from VENs.</p>
E-1194 47	<p><b>VEN-PCE Communication Failed in a Proxy Environment</b></p> <p>After upgrading a VEN in an environment where workloads are behind a proxy server and unable to resolve the PCE's FQDN, the VEN's communication with the PCE failed. The problem stemmed from an API version mismatch.</p>
E-1194 46	<p><b>Re-activating a deactivated VEN fails on AIX workloads</b></p> <p>If you deactivate a VEN installed on an AIX workload and later re-activate it, activation fails and a 401 error is thrown. This is a known issue. Workaround: After you deactivate the VEN, remove the backup folder under the VEN's data directory. With the backup folder removed, re-activation succeeds.</p>
E-1155 00	<p><b>VEN failed to apply policy in certain circumstances</b></p> <p>When operating in a proxy environment, VENs failed to apply the proxy bypass list, resulting in a failure to apply Illumio firewall policy.</p>
E-1077 78	<p><b>VEN in degraded mode reports illumio-ven-ctl status is healthy</b></p> <p>The output of the VEN status command <code>illumio-ven-ctl status</code> indicated a healthy VEN-PCE connection even though the VEN was in a degraded state throwing errors and blocking flows in response to API requests.</p>

## Resolved Issues in Release 24.2.11-VEN

- **Connectivity loss following VEN upgrade** (E-121251)

On Solaris v11.4 workloads, after upgrading a VEN to version 24.2.11, the VEN may lose connectivity with the PCE. The issue stems from a change in the accepted `/etc/firewall/pf.conf` syntax. Workaround: The issue does not occur if the VEN is first upgraded to version 23.2.x. Illumio plans to fix this issue in a future release. Until then, do the following if you experience this issue: After successfully upgrading the VEN, reset the host firewall by issuing the following command from the workload CLI: `sudo pfctl -F`

- **VEN unpairing command options failed to return the firewall to the expected state** (E-121066)

In VEN release 24.2.10, when unpairing a VEN from a command line and specifying either the "recommended" or "open" post-deactivation option, the firewall wasn't restored to the expected state. Instead, those options restored the firewall rules and configuration to the state it was in before the VEN was installed. This issue only affected unpairing from the command line. Unpairing through the PCE Web Console was unaffected. This issue is resolved.

- **Possible VEN policy generation failure for some custom iptables rules** (E-120387)

On Linux RHEL workloads, VENs were susceptible to generating syntactically incorrect firewall rules for nftables if certain types of custom iptables rules (for example, NAT rules) were included in the Illumio security policy, resulting in nftables failing to load the generated policy. This issue is fixed.

- **From the PCE, unable to upgrade or uninstall VENs installed on certain Windows workloads** (E-120202)

An issue in Illumio Core Release 24.2.10-VEN prevented upgrading or unpairing VENs installed on Windows 7 and Windows Server 2008R2 workloads through the PCE web console. The ability to manually upgrade and uninstall VENs was unaffected. This issue is resolved.

## Resolved Issues in Release 24.2.10

### Resolved Security Issue in Release 24.2.10-PCE

- **ruby-saml**

ruby-saml, a third-party component in the PCE, was impacted by CVE-2024-45409. It is now fixed, as the impacted component was upgraded.

### Resolved Issues in Release 24.2.10-PCE

- **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.

- **Navigation error while navigating to Authentication Settings > SAML: Not Found** (E-118183)

In PCEs running 22.5.32, sometimes going to Authentication Settings > SAML resulted in the attempted navigation being cancelled, and a "Navigation error details" popup appearing.

- **PCE sending partial IPP instructions** (E-117863)

PCE was sending partial IPP instructions, which was causing instruction replacement due to the current Kubelink's inability to receive partial instructions. This issue is resolved.

- **Erroneous Ransomware Exposure status for AIX and Solaris workloads** (E-117858)

Solaris and AIX workloads always showed their Ransomware Exposure status as Protected. This issue is resolved.

- **Unmanaged workloads created incorrectly** (E-117637)

Unmanaged workloads created via the Deny Rules menu were incorrectly created with the previous creation's Name and hostname. This issue is fixed.

- **Policy generator throwing an error when saving rules** (E-117499)

When users tried to save the rule with custom iptables rules, the Policy generator was throwing an "Unexpected input validation error". This issue is resolved.

- **"Duplicate key value" error occurs during database migration phase of PCE upgrade** (E-117235)

When upgrading the PCE from 22.5.32 to 23.2.21, during database migration the following error occurred: `ERROR: duplicate key value violates unique constraint "flow_process_references_7_org_id_region_id_value_idx"`.

- **Missing app-tiers label on pod using annotation** (E-117004)

In non-CLAS (legacy) container clusters, when applying Illumio labels through Kubernetes annotations, a label key containing a dash is not properly assigned to Container Workloads. For example, a pod annotation of `annotation.com.illumio.app-tiers` with a label value of `AT_A` is not created with label type `App-Tiers` nor the label `AT_A`. This issue is now resolved for new Container Workloads created on this release. However, upgrading the PCE to this release does not fix existing Container Workloads that have labels containing a

dash character. To fix such existing Container Workloads, you can edit the Container Workload Profile to add another possible value for the dash-containing label. After saving this edit, existing Container Workloads get re-labelled correctly to their assigned annotation values.

- **NEN 2.6.20 is stuck in "ACL generation pending"** (E-116805)

In a configuration with a 2.6.20 NEN paired with a supercluster member on PCE Version 22.5.32-12, running "Generate ACLs" never completed, and only showed the "ACL Generation Pending" message without ever producing an ACL.

- **CLAS - Rules are not created for Kubernetes Workloads and VIPs** (E-116721)

In CLAS-enabled deployments, rules created between a Kubernetes Workload and a VIP (from a virtual server, for example a F5 Virtual Server) are not created even after provisioning. These rules fail to appear in the PCE Web Console. This issue is resolved. The new runtime environment variable `clas_workloads_ipset_only_changes_enabled` must be set to `false` in the PCE `runtime_env.yml` file (under `agent_service`;) for the PCE to correctly send Virtual Server instructions to Kubernetes Workloads.

- **UI fields fail to occasionally load under Rulesets and Rules** (E-116648)

Sometimes when writing a rule in 24.1.3-PCE, the Sources or Destination fields never properly loaded or were populated with labels that were chosen. This could occur when viewing a grid layout in smaller screen sizes, which reduced the source/destination selector drop-down height and caused options to be improperly displayed or hidden completely with a scroll.

- **Last updated policy timestamp for C-VEs reflects Kubernetes Workload policy changes** (E-116258)

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

- **Header manipulation issue fixed** (E-116114)

Appropriate validation for host header was added to avoid any host header manipulation.

- **curl upgraded to v8.8.0** (E-115842)

curl was upgraded to v8.8.0 to address CVE-2024-7264, CVE-2024-6197, CVE-2024-2466, CVE-2024-2398, CVE-2024-2379, and CVE-2024-2004.

- **External users with multiple scopes reporting PCE slowness** (E-109314)

External users with many scopes in their RBAC permission have been reporting PCE UI slowness, especially when browsing the VEs tab and querying traffic. This issue is resolved.

## Resolved Issues in Release 24.2.10-VE



### CAUTION

#### Maintain VE Operating System Support

Compatibility and performance issues can occur if the operating system version running on your workloads and endpoints is upgraded to a version that is not supported by the VEs on those machines. Before upgrading the operating system on workloads and endpoints, first make sure that the VEs installed on these machines support the new OS version. For workload VEs, see [VE OS Support Package Dependencies](#). For Endpoint VEs, see [Endpoint VE OS Support Package Dependencies](#).

- **False positive IPsec tampering error in platform.log** (E-118562)  
After disabling rules with SecureConnect options, the error IPsec policy tampered nonetheless appeared in the platform.log every 10 minutes. This issue is resolved. The error no longer appears in this circumstance.
- **VEN misinterpreted flow direction** (E-118007)  
Linux VENs could fail to determine the flow direction correctly in some circumstances, (for example, for UDP packets sent to a broadcast IP address), resulting in the VEN reporting an inbound flow as an outbound flow. This issue is fixed.
- **Transient environmental variable could prevent applying policy** (E-117699)  
While upgrading any VEN version on Solaris workloads, it was possible for VEN processes to inherit transient environment variables from the OS pkgadd command (for example, \$TMPDIR). This issue could've prevented the VEN from applying policy until the VEN was manually restarted. This issue is resolved.
- **Policy application failed in some circumstances** (E-117246)  
Some earlier VEN versions failed to apply policy if the workload on which it was installed had multiple valid IPv6 DNS addresses. This issue is fixed.
- **Bug in nftables versions pre-0.9.2 prevented policy application** (E-116635)  
Policy failed to load on VENs installed on RHEL Linux 8/9 workloads with a version of nftables earlier than 0.9.2. This issue is resolved.
- **Issue affecting the persistent connection between PCE and VEN** (E-116177)  
A regression was introduced into 22.5.33 and 23.2.23 Windows VEN, which could cause the Event Channel between VEN and PCE to stop functioning, resulting in a policy convergence delay. This issue is resolved.
- **PCE didn't recognize external IP address of external Azure VM** (E-115935)  
Unix VENs failure to correctly detect Azure environment prevented the PCE from recognizing the external IP addresses of the workloads. This issue is resolved. VENs now correctly detect when they're operating in an Azure environment.
- **ICMP code misinterpretation caused false positive tampering error** (E-113439)  
After misinterpreting a rule specifying the ICMP protocol, the VEN generated a false positive tampering error. This issue was resolved by updating the VEN to normalize ICMP code.
- **Improper VM shutdowns caused VEN data file corruption** (E-113231, E-109231)  
If a workload was shut down improperly, such as by a sudden loss of power, and the kernel crashed, some critical VEN data files could've gotten corrupted, preventing the VEN from loading policy. This issue is resolved. Critical VEN data files are now more resilient if the workload is shut down improperly.
- **Support for pairing VENs on AWS Workloads with IMDS v2** (E-109528)  
This VEN release provides support for pairing VENs on AWS workloads with Instance Metadata Service Version 2 (IMDS v2). This update was necessary to support IMDS v2 session-oriented authentication.
- **Improper VM shutdowns caused VEN data file corruption** (E-109231)  
If a workload was shut down improperly, such as by a sudden loss of power, and the kernel crashed, some critical VEN data files could've gotten corrupted, causing the VEN to lose connectivity with the PCE. This issue is resolved. Critical VEN data files are now more resilient if the workload is shut down improperly.

## Known Issues in Release 24.2.30

These release notes describe the new features, enhancements, resolved issues, and known issues for this release.

## Known Issues

Issue	Description	Status
E-127170	<b>Additional scripts required to enable maintenance tokens</b>  Enabling maintenance tokens for VEN tampering protection in a Supercluster deployment requires additional scripts.	Reach out to your Illumio account team for assistance.

## Known Issue in Release 24.2.20-PCE

Issue	Description	Status
E-121874	<b>Core Services Data Creation Issue</b>  The Core Services page incorrectly displays no data. The page displays the following messages: "Core service detection algorithm has not run yet. Scanner detection algorithm has not run yet."	Unresolved

## Known Issues in Release 24.2.20-VEN

Issue	Description	Status
E-123299	<p><b>CLI required to upgrade certain Amazon Linux VENs</b></p> <p>You must use a command line to upgrade certain VEN versions installed on Amazon Linux workloads.</p> <p>There are two ways to upgrade a VEN:</p> <ul style="list-style-type: none"> <li>Through the PCE User Interface (UI). See <a href="#">VEN Upgrade Using VEN Library in PCE</a>.</li> <li>Using a command line interface (CLI). See <a href="#">VEN Installation &amp; Upgrade with VEN CTL</a>.</li> </ul> <p><b>When to use which method?</b></p> <p>Use the <b>CLI</b> upgrade method when upgrading <b>pre-22.5.30</b> VENs to release <b>22.5.30 or later</b> on Amazon Linux workloads. The upgrade fails if you try to use the PCE UI upgrade method in this scenario.</p> <p>Use <b>either</b> method for these upgrade scenarios on Amazon Linux workloads:</p> <ul style="list-style-type: none"> <li><b>Pre-22.5.30</b> VENs to another <b>pre-22.5.30</b> VEN version.</li> <li><b>22.5.30 or later</b> VENs to another <b>22.5.30 or later</b> VEN version.</li> </ul>	Works as designed
E-122188	<p><b>In some cases, policy sync error occurs when a VEN operates in a web proxy environment</b></p> <p>Given an environment where a web proxy is configured to direct the VEN to use the proxy to communicate with the PCE and the VEN is switched to Selective mode, new policy may not be accepted even if there is no Deny rule blocking communication to the proxy. Workaround: add an Allow rule allowing communication to the proxy.</p>	Unresolved

## Known Issue in Release 24.2.10-VEN

- **AIX / Solaris 10 policy update fails in some circumstances** (E-118539)  
Updating policy on AIX and Solaris 10 workloads fails if the workloads are in Full Enforcement mode and flow visibility is turned off. This issue is caused by some incorrectly generated syntax. This is a known issue. Workaround: Go to **Servers & Endpoints > Workloads**, select AIX/Solaris 10 workloads that are in Full Enforcement mode, and then in the Visibility drop-down menu enable flow visibility by making sure the setting isn't **Off**.

## UI improvements in Release 24.2.0+UI2

This release provides user interface updates for Extra-Scope and Intra-Scope rules.

- The separate tabs that contained Intra-Scope and Extra-Scope options in previous releases are removed and a new column called **Scope Type** appears in the Allow rules section of the Policies page.
- Extra-Scope and Intra-Scope rules occupy different sections within Allow Rules, separated by a grey line.
- You can move rules up or down but only within their respective section.
- Extra-Scope rules are now distinguished by an icon.

Allow Rules <span></span>									
	Provision Status	No.	Status	Scope Type	Sources	Source Process / Service	→	Destinations	Destination Services
<input type="checkbox"/>	Pending	1	Enabled	Intra-Scope	Any (0.0.0.0/0 and ::0)		→	All Workloads	srvName2_2995
<input type="checkbox"/>	Pending	2	Enabled	Intra-Scope	All Workloads		→	All Workloads	All Services
<input type="checkbox"/>	Pending	3	Enabled	Extra-Scope	Any (0.0.0.0/0 and ::0)		→	All Workloads	srvName2_2995
<input type="checkbox"/>	Pending	4	Enabled	Extra-Scope	All Workloads		→	All Workloads	All Services

## Resolved Issues in Release 24.2.0

### Enterprise Server

- Bug in nftables versions pre-0.9.2 preventing policy application** (E-116635)  
 The policy would fail to load on VENs installed on RHEL Linux 8/9 workloads with a version of nftables earlier than 0.9.2. This issue is fixed.
- On occasion, ransomware dashboard widgets were not updating or populating** ( E-116603)  
 The issue was resolved by updating the dashboard widgets.
- App Group's enforcement state shows as "Mixed" by mistake** (E-116536)  
 The enforcement state of the App Group incorrectly displays 'Mixed' when a workload has 'Selective' enforcement along with unmanaged workloads. To accurately define the enforcement state as 'Mixed' for an app group, the issue was resolved by excluding the state of unmanaged workloads.
- High latency was observed when loading an app group list page** (E-116521)  
 This issue is fixed.
- Traffic queries would fail when the "Source OR Destination" field had an APP label** ( E-116365)  
 Traffic searches failed when the search type was set to "Source OR Destination" and when an APP label was used.  
 This issue is fixed.
- Issue affecting the persistent connection between PCE and VEN** (E-116177)  
 A regression was introduced into 22.5.33 and 23.2.23 Windows VEN, which could cause the Event Channel between VEN and PCE to stop functioning, resulting in a policy convergence delay.  
 This issue is fixed.
- FQDN missing from the "Connections with unknown IP" view** ( E-116077)  
 This issue is fixed.
- Different behavior of filters was observed in the map versus traffic views** ( E-115933)  
 Works as designed.
- AND operator showing between labels of the same type** (E-115653)  
 The AND operator was showing between labels of the same type in Traffic query fields (UI display only).  
 This issue is fixed.
- In Illumination Plus, users were unable to write rules based on port numbers** (E-115225)  
 This issue is fixed.
- Unable to create new service from within rules ad ruleset page** (E-115210)  
 Users experienced slow performance, resulting in a long time to create a new service from the rules and rulesets page.  
 This issue is resolved.
- Saving filters in Illumination Plus** (E-115189)  
 Since the SCP2 upgrade, a customer was unable to save filters in Illumination Plus. This issue is fixed.

- **Save and Provision for a rule fails** (E-115047)  
After performing Save and Provision for the rule, the Comment field did not show up and the rule was not provisioned.  
This issue was fixed.
- **Upgrade json-jwt-1.13.0.gem to N/A or higher to address CVE-2024-51774** (E-114939)  
The json-jwt (aka JSON::JWT) gem version 1.16.3 for Ruby sometimes allows bypass of identity checks via a sign/encryption confusion attack.  
This issue is resolved after upgrading json-jwt to version 1.16.6.
- **Script needed for default profile recreation and sync migration** ( E-113855)  
A script was needed for default profile recreation and sync migration with release 23.2 and later.  
This issue is fixed.
- **Upgrade rails-6.1.7.4.gem to 6.1.7.7, 7.0.8.1, or higher to address CVE-2024-26144** ( E-114138)  
Starting with Rails version 5.2.0, there was a possible sensitive session information leak in Active Storage. This vulnerability was fixed in Rails releases 7.0.8.1 and 6.1.7.7 and this issue will not be addressed.
- **The ilo-pce command should not require sudo access** (E-113745)  
Remove 'sudo' in `services/cron_perfmon/bin/avn_perfmon.sh` and then test. It is not critical to know the program name of processes users don't own.
- **Script needed for default profile recreation and sync migration** (E-113855)  
A script was needed for default profile recreation and sync migration with release 23.2 and later.  
This issue is fixed.
- **App Group Rule Listing is missing Rulesets** (E-113259)  
Intra-scope rules were not showing up in the App Group rules menu. This issue is fixed.
- **report\_monitor and traffic\_query services flapping on coordinator replica node after OS upgrade** (E-113024)  
On DX configurations, adding a new CC (Citrus Coordinator) node or a new CW (Citrus Worker) node to the cluster sometimes caused flapping of some services, such as `report_monitor` or `traffic_query`. This flapping occurred because IP restrictions on some current nodes of the cluster did not account for the new node IP addresses.
- **Policy check not properly showing Rules Pending status** (E-112974)  
The Policy check did not show that Rules Pending was disabled. This issue is fixed.
- **Lookup by external\_data\_reference not working** (E-111950)  
When a label was created using the API and later edited in the UI, the lookup by `external_data_reference` did not work. This issue is fixed.
- **Unresponsive web page when writing rules** (E-110946)  
When users were writing a rule in the PCE, the webpage became unresponsive. This issue is fixed.

## Containers

- **Kubernetes Workload service network interfaces are unnecessarily updated upon every Node update** (E-114962)  
On every network interface update of a cluster node, the network interfaces of every Kubernetes Workload of type Service were getting updated. This caused a large amount of ``workload_ip_address_change`` event creations when used with thousands of services. This behavior worsened when many nodes were re-deployed at the same time (un-pair/pair) while there were Kubernetes Workloads already present.



- **Container cluster reporting "Virtual service is still active on a workload" after upgrading to "clusterMode: migrateLegacyToClas"** (E-114727)

After a non-CLAS (legacy) deployment was upgraded to CLAS mode, existing container clusters running multiple ClusterIP virtual services each went into an Error Status, with each cluster detail page also displaying a "Virtual service is still active on a workload" message.

## Known Issues in Release 24.2.0

### Enterprise Server

- **Creating same name workloads from the ip address contextual menu** (E-116711)  
On the main workloads component (WorkloadEdit) users are able to create workloads with the same name.  
Workaround: none
- **Refused connection to the Support portal with Segmentation Templates > sign in** (E-113084)  
Clicking on **segmentation templates > sign in** in the support portal returns an error.  
Workaround: none.
- **Unable to select a workload inside an open combo node** (E-112344)  
Clicking on a workload inside a combo node does not select a workload and the traffic links connected to it are not showing.  
Workaround: none
- **The Explorer page is not loading and redirects to the Traffic page** (E-111574)  
Workaround: The Explorer page loads if users enable both Explorer and Classic Illumina-tion.
- **Deleted Workload traffic link shows a policy decision** (E-110143)  
A deleted workload traffic link shows a policy decision by mistake.  
Workaround: None
- **Ransomware Dashboard always shows high Protection coverage score** (E-106996)
- **Global admin prompted to update Ransomware "Workloads Requiring Protection" but not authorized to do so** (E-105756)
- **PCE application log files are not rotated** (E-105659)  
Some PCE application log files (agent, collector, haproxy) are not rotated, while the other files are rotated correctly.  
Workaround: none.
- **Standalone PCE not starting up after service\_discovery\_encryption\_key change** (E-104880)  
Workaround: none
- **Removal of inactive accounts ignores API use** (E-103316)  
In PCE release 22.4.1+A3, user accounts that have been inactive for more than 90 days are removed automatically. However, the active status is determined based only on whether the account has logged in to the web console UI. If the account is used only to issue API requests, it is counted as inactive and removed after 90 days.
- **Updating max results in Illumination Plus (10K) updates the Explorer max results** (E-102742)  
The maximum connection number in Explorer gets updated to the same maximum number as the update in Illumination Plus. However, the maximum number in Illumination Plus is 10,000, while in Explorer, it is 100,000.

Workaround: Update the max results setting in Explorer to get more than 10K results.

- **Recent filters become empty when users run a query from Explorer** (E-102525)

Workaround: None

- **When users load saved filters in Explorer, more than four labels are showing up** (E-102438)

Workaround: None

- **After creating a new organization, users are unable to load saved filters** (E-102268)

Workaround: Create the save filter once you issue a new query from Explorer or Illumination Plus.

- **Enforcement boundaries filters are still showing after enforcement boundaries are deleted** (E-102251)

Workaround: None

- **SecureConnect only logs the "E" on the source** (E-101229)

Works as designed. There is no way to tell whether SecureConnect is in the egress path.

- **Windows 11 shows as Windows 10 on workload/VEN page** (E-100844)

Workaround: none.

- **Flow timestamp incorrect in Illumination for inbound-only or outbound-only reported flows** (E-96595)

The flow timestamp shown in Illumination is unreliable for ingress- or egress-only reported flows.

Workaround: Use Explorer to see the correct timestamp.

## Illumination Plus

- **Explorer/Illumination Plus filter was incorrectly interpreting flows with an empty label group** (E-105503)

When using an empty Label Group as a filter in Explorer or Illumination, the same result was returned as expected if the filter criteria were "Any Workloads."

This issue is resolved and works as designed.

- **Saved filter for Explore and Loading showing empty data by default** (E-102257)

The created Saved filter for Explore and Loading is showing reported policy decisions with empty data by default.

Workaround: None

## PCE Platform

- **chronyd usage failure** (E-111664)

- 'illumio-pce-env check' cmd relies on 'chronyc' for checking the clock drift.
- There is a STIG (Security Technical Implementation Guide) security advisory which recommends users disable access to chronyd.
- As of today, on implementing the STIG directive, 'illumio-pce-env check' results in a warning message: '506 Cannot talk to daemon error'.
- Federal customers/government agencies are more likely to follow the STIG advisories.

## Data Platform

- **Missing vulnerability data in the Workloads Export** (E-114354)

The Workload export feature does not include vulnerability data.

Workaround: none.

## PCE Web Console UI

- **Proposed Rules - Status information is being hidden** (E-105098)

The Proposed Rules status information is hidden by the "Add to Ruleset" page.

Workaround: The information is shown on the Ruleset Summary page.

## Security Information

This section provides important security information. For additional information about security issues, security advisories, and other security guidance pertaining to this release, see Illumio's Knowledge Base in Illumio's Support portal (log in required).

- **Resolved Security Issue in Release 24.2.30-PCE**

- Upgraded Postgres to address CVE-2024-10979, CVE-2025-1094, CVE-2024-10977, CVE-2024-10976, and CVE-2024-10978.

- **Resolved Security Issue in Release 24.2.21**

- **ruby-saml**

ruby-saml, a third-party component in the PCE, was impacted by CVE-2025-25291, CVE-2025-25292, and CVE-2025-25293. It is now fixed, as the impacted component was upgraded.

- **Resolved Security Issue in Release 24.2.10**

- **ruby-saml**

ruby-saml, a third-party component in the PCE, was impacted by CVE-2024-45409. It is now fixed, as the impacted component was upgraded.

- **Resolved Security Issue in Release 24.2.0**

- **postgreSQL**

postgreSQL was upgraded to v15.7.

## Illumio LW-VEN Release 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](#).

### Resolved Issues in 1.1.10 LW-VEN

Issue	Description	Status
E-120840	<b>ICMP rule generation created empty command</b>  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>  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>  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 Release Notes

This section provides release notes for the following versions of Kubernetes:

- 5.2.x
- 5.1.x
- 5.0.x
- 4.3.x

### 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 \[48\]](#).

#### 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 source. 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 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, E-125362	<b>C-VEN - Improve performance by adjusting retry handling</b>  Retry logic has been adjusted to reduce latency times, and improve performance.
E-125661	<b>Kubelink: Improved PCE load handling</b>  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 \[56\]](#).

- **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 \[54\]](#) 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 \[57\]](#) 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 `kubectx1 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 \[65\]](#)
- [Kubelink \[65\]](#)
- [Security Information for Core for Kubernetes 5.0.0-LA \[66\]](#)

## 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 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**s 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 NEN Release Notes 2.4

### Product Version

**NEN Version:** 2.4.10

**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 2.4.10

#### **F5 AFM 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 already, 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 a deleted VS.

### Known Issues in NEN 2.4.10

There are no known issues in this release.

### Resolved Issues in NEN 2.4.0

#### • **VS filtering failed to work correctly on secondary NEN nodes** (E-90850)

The secondary NEN node didn't perform Virtual Server (VS) filtering even though VS filtering was enabled on the NEN. This meant that VS filtering occurred only on the primary NEN node, which sometimes caused the VS to appear and disappear in the PCE Web Console.

#### • **For an AVI SLB, NENs reported tenant names incorrectly in the non-admin tenant space** (E-90758)

When discovering non-admin tenant Virtual Servers on an AVI multi-tenant Server Load Balancer (SLB), the NEN reported Virtual Server names according to their tenant **UUID**



instead of their tenant **name** (**Infrastructure > Load Balancers > AVI SLB > Virtual Servers** tab). The NEN also used the tenant UUID in the API header it sent to the AVI SLB when it tried to program the Virtual Server. This prevented policy from being programmed on those Virtual Servers. This issue is resolved; NENs now correctly use the tenant name of discovered Virtual Servers.

- **When adding a switch, the list of supported switches was incomplete for the attached NENs** (E-85844)

Given two active NENs attached to a PCE, each a different version supporting different switches:

When adding a new switch through the PCE Web Console, the **Manufacturer** drop down list showed only switches that are supported by the first NEN in the **NEN host name** drop down list. This occurred regardless of which NEN host the user selected. The incomplete list of switches could've prevented users from selecting the precise switch type they were trying to integrate or might have lead them to select a switch type that's not supported by the selected NEN host. This issue is resolved. The **Manufacturer** list now shows the switch(es) supported by whichever host is selected in the **NEN host name** drop down list.

- **Memory leak in NEN process** (E-85114)

When programming a large number of virtual servers, excessive memory consumption in the `network_enforcement_ndconfig` process could've resulted in an out-of-memory exception in rare circumstances. This issue is resolved.

## Known Issues in NEN 2.4.0

There are no known issues in this release.

## Limitation in NEN 2.4.0

### Enforcement Boundaries not supported for NENs

The PCE doesn't support Enforcement Boundary policies for devices attached to the NEN.

Enforcement Boundaries are a security policy model available in the Core PCE for broadly managing communication across a set of workloads, ports, and/or IP addresses. They allow you to define the end state and then the PCE implements an Enforcement Boundary to create the appropriate native firewall rules. For more, see [Enforcement Boundaries](#).

## 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](#)