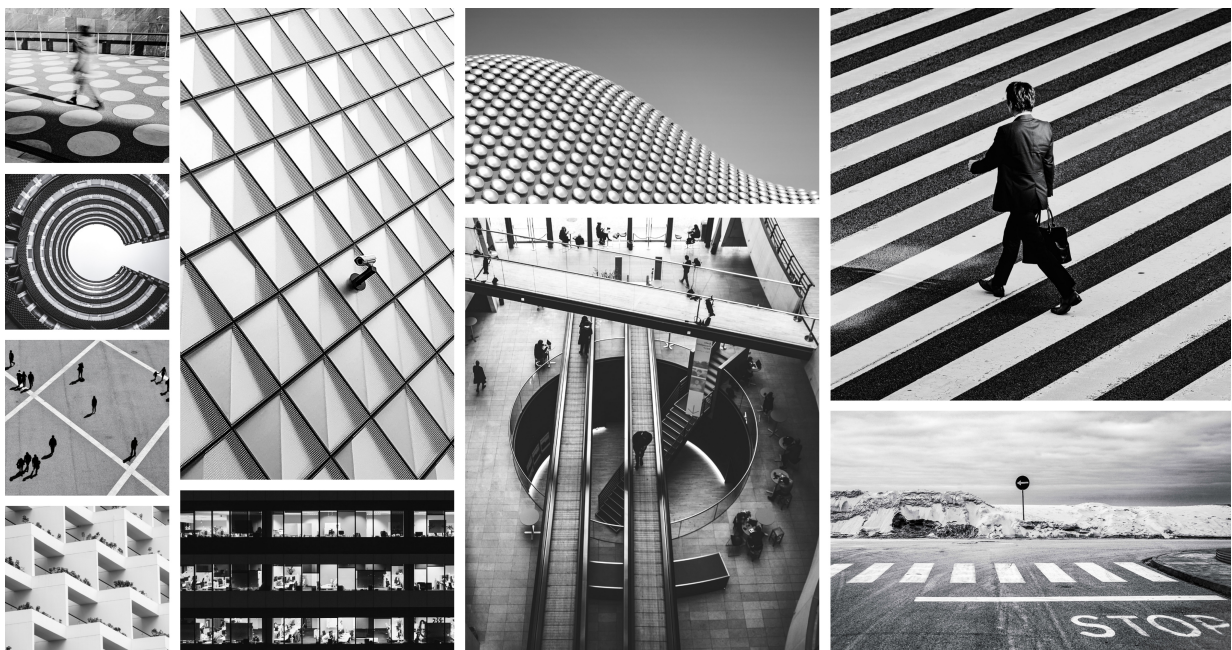




TECHNICAL
DOCUMENTATION

Illumio Core What's New and Release Notes for 23.5

Publication date Published: 2024



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

Table of Contents

What's New in 23.5	7
About This Release	7
Product Versions	7
General Advisories	7
Announcements	8
Welcome to the New Illumio Experience	9
Deprecation of the PCE Classic UI	9
What Are the Primary Benefits?	9
What is Changing?	10
Deprecated Features in the New UI	19
What's New and Changed in This Release	20
What's New and Changed in 23.5	20
Policy Templates	20
Ransomware Protection Dashboard Changes	21
Bulk Export/Import of Workload Labels	22
Enhancements in the Visualization Tools	22
Windows Outbound Process: A New Object Type	25
Limits on Flowlink Traffic Data	25
Splunk Integration Version Upgrade	26
Traffic from Unpaired VENs	26
Classic UI Removed	26
Illumio Core REST API in 23.5.0	26
What's New and Changed in Release 23.5.10	33
Rule Hit Count Report	34
CLAS Architecture in Illumio Core for Kubernetes and OpenShift	34
Illumio Core REST API in 23.5.10	35
Illumio Core REST API in 23.5.20	43
Illumio Core Release Notes 23.5	45
Welcome	45
Product Version	45
Resolved Issue in Release 23.5.31-PCE	45
Resolved Issues in Release 23.5.30-PCE	45
Known Issues in Release 23.5.30	47
Enterprise Server	47
Data Visualization	47
PCE Platform	48
VEN	48
Resolved Security Issues in Release 23.5.30-PCE	48
Resolved Security Issue in Release 23.5.22	49
Resolved Issues in Release 23.5.21+A4-PCE	49
Resolved Security Issue in Release 23.5.21+A4-PCE	49
Resolved Issue in Release 23.5.21+A3-PCE	50
Resolved Issue	50
Updates in Release 23.5.21+A2-PCE	50
Enhancement	50
Resolved Issue	50
Resolved Issues in Release 23.5.21+A1-PCE	50
Resolved Issues in Release 23.5.20	51
Enterprise Server	51
Containers	52
VEN	52
VEN Known Issue	53
Security Information	53

Resolved Issue in Release 23.5.21	53
Resolved Issues in Release 23.5.10	54
Enterprise Server	54
PCE Platform	55
UI Components	55
VEN	55
Resolved Issues in Release 23.5.1	56
Enterprise Server	56
Visualizations	58
UI Components	58
PCE Platform	58
What's New and Release Notes for LW-VEN 1.1	60
What's New in LW-VEN Release 1.1.0	60
Support for flow reporting for legacy Windows servers	60
Release Notes in LW-VEN 1.1	60
Resolved Issues in 1.1.10 LW-VEN	60
Resolved Issues in 1.1.0 LW-VEN	61
Illumio Core for Kubernetes Release Notes	62
Illumio Core for Kubernetes Release Notes 5.3	62
What's New in Illumio Core for Kubernetes 5.3.1	62
Resolved Issues in 5.3.1	64
Illumio Core for Kubernetes Release Notes 5.2	65
About Illumio Core for Kubernetes 5.2	65
Updates for Core for Kubernetes 5.2.3	65
Updates for Core for Kubernetes 5.2.2	65
What's New in Release 5.2.1	66
Updates for Core for Kubernetes 5.2.1	66
What's New in Release 5.2.0	67
Updates for Core for Kubernetes 5.2.0	71
Illumio Core for Kubernetes Release Notes 5.1	72
Core for Kubernetes 5.1.10	72
Limitations	73
Updates for Core for Kubernetes 5.1.10	73
Updates for Core for Kubernetes 5.1.7	74
Updates for Core for Kubernetes 5.1.3	74
Updates for Core for Kubernetes 5.1.2	75
Updates for Core for Kubernetes 5.1.0	75
Security Information for Core for Kubernetes 5.1	77
Illumio Core for Kubernetes Release Notes 5.0.0	77
About Illumio Core for Kubernetes 5.0	77
Product Version	78
What's New in C-VEN and Kubelink	78
NodePort Limitations	78
Updates for Core for Kubernetes 5.0.0-LA	79
Illumio Core for Kubernetes Release Notes 4.3.0	80
What's New in Kubernetes 4.3.0	80
Product Version	81
Updates for Core for Kubernetes 4.3.0	82
Illumio Flowlink Release Notes	83
Illumio Flowlink Release Notes for Release 1.4.0	83
Product Version	83
New Features in Illumio Flowlink 1.4.0	83
Resolved and Known Issues in FlowLink 1.4.0	83
Illumio Flowlink Release Notes 1.3.0	84
Product Version	84

New Feature in Flowlink 1.3.0	84
Resolved Issue in Flowlink 1.3.0	85
Illumio Flowlink Release Notes 1.2	85
Welcome	85
Product Version	85
What's New in FlowLink Release 1.2.3	86
What's New in FlowLink Release 1.2.2	86
What's New in FlowLink Release 1.2.1	86
What's New in FlowLink Release 1.2.0	87
Illumio Flowlink Release Notes 1.1.2	87
Welcome	87
Product Version	87
Resolved Issue in FlowLink 1.1.2+H2	88
Resolved Issues in FlowLink 1.1.2+H1	88
Enhancement in FlowLink 1.1.2	88
Resolved Issue in FlowLink 1.1.2	88
Resolved Issue in FlowLink 1.1.1+H2	89
Resolved Issues in FlowLink 1.1.1+H1	89
Resolved Issue in FlowLink 1.1.1	89
Resolved Issue in FlowLink 1.1.0+H1	89
Illumio NEN Release Notes	90
Illumio NEN Release Notes 2.6	90
Product Version	90
What's New in NEN 2.6.40	90
Resolved Issues in NEN 2.6.40	91
Known Issues in NEN 2.6.40	91
Resolved Issues in NEN 2.6.30	91
Known Issues in NEN 2.6.30	91
Resolved Issue in NEN 2.6.20	91
Known Issues in NEN 2.6.20	91
Resolved Issues in NEN 2.6.10	92
Known Issues in NEN 2.6.10	92
2.6.10 Security Information	92
Resolved Issues in NEN 2.6.1	92
Known Issues in NEN 2.6.1	93
Resolved Issues in NEN 2.6.0	93
Known Issues in NEN 2.6.0	93
Illumio NEN Release Notes 2.5	94
Product Version	94
Resolved Issue in NEN 2.5.2.A1	94
Known Issues in NEN 2.5.2.A1	94
Resolved Issues in NEN 2.5.2	94
Known Issues in NEN 2.5.2	95
Resolved Issue in NEN 2.5.1	95
Known Issues in NEN 2.5.1	95
Resolved Issues in NEN 2.5.0	95
Known Issues in NEN 2.5.0	96
Illumio NEN Release Notes 2.4	96
Product Version	96
Resolved Issue in NEN 2.4.10	97
Known Issues in NEN 2.4.10	97
Resolved Issues in NEN 2.4.0	97
Known Issues in NEN 2.4.0	98
Limitation in NEN 2.4.0	98
Illumio NEN Release Notes 2.3	98

Legal Notice	98
About This Document	99
Resolved Issues in NEN 2.3.10	99
Known Issues in NEN 2.3.10	100
Resolved Issues in NEN 2.3.0	100
Illumio Core PCE CLI Tool Guide	102
Illumio Core PCE CLI Tool Guide 1.4.3	102
What's New and Changed in Release 1.4.3	102
Support for Proxy	102
Security Advisories	105
September 2024 Security Advisories	105
Ruby SAML gem component authentication bypass vulnerability	105
Severity	105
Affected Products and Patch Information	105
Resolution	105
References	106
Skipped Critical Patch Updates	106
Discovered By	106
Frequently Asked Questions	106
Modification History	107
September 2023 Security Advisories	107
Authenticated RCE due to unsafe JSON deserialization	107
Severity	107
Affected Products and Patch Information	107
Resolution	108
References	108
Skipped Critical Patch Updates	108
Discovered By	108
Frequently Asked Questions	108
Legal Notice	110

What's New in 23.5

About This Release

This section describes the new features, enhancements, platform support, and new and modified REST APIs for the Illumio Core 23.5.x releases.



IMPORTANT

Illumio Core 23.5.1 is available for Illumio Core SaaS customers. Illumio Core 23.5.31 is available for Illumio Core On-Premises customers.

Product Versions

PCE Versions: 23.5.1 (SaaS) and 23.5.31 (On Premises)

VEN Versions: 18.2.3; 19.3.1 and above; 21.2 except for 21.1.0; 22.2.0 except for 22.2.40; 22.5.0 (Standard), 22.5.10, 22.5.12 (SaaS only)

NEN Versions: 2.5.2, 2.5.1, 2.5.0, 2.4.10, 2.4.0, 2.3.10

FlowLink Versions: 1.3, 1.2, 1.1

C-VEN Versions: 21.5.x, 21.2.x, 21.1.0, 19.3.6

General Advisories

The information in this section provides general advisories about important aspects of this release. To ensure proper operation of the system after upgrade, you might need to take account of these advisories.

Updated Minimum Browser Versions for the Core PCE UI

In Core 23.4.0, Illumio updated the minimum browser versions required to access the PCE UI.

Supported Operating Systems

The Illumio Core PCE is supported on operating systems detailed on the Illumio Support portal.

Open Source Package Updates

Illumio updated several open source packages for the PCE in 23.5.1.

The Upgrade to This Release

As part of the upgrade process, Illumio strongly encourages you to review the prior release notes from your previously installed version of Illumio Core to version 23.5.31.

You have the option to upgrade the VENs in your environment at any time. For information about the upgrade path and tools, go to the Illumio Support portal and review the [VEN Upgrade paths](#) (login required).

Announcements

This section contains End of Support Announcements, Deprecations, and Compatibility information.



IMPORTANT



IMPORTANT

Classic UI Removed

In Illumio Core 23.2.0, Illumio introduced a new PCE user interface (UI) designed to maximize user productivity and enable intuitive platform administration. Users had the option to toggle between the new UI and the earlier, classic UI.

In 23.5, the toggle option is removed. The classic UI is no longer available.

End of Support

Illumio REST API v1

The version 1 of Illumio REST APIs (API v1) is not supported effectively with the 21.1 and later releases. Illumio recommends that you upgrade to API v2.

Internet Explorer 11

Illumio Core 19.1 was the last release to support Internet Explorer 11. Internet Explorer 11 is no longer supported in Illumio Core 19.2 and later releases. Illumio recommends Chrome, Edge, or Firefox for use with the PCE web console.

Organization Events

Since the 19.1.0 release, the older form of events, known as “audit or organization events,” is no longer supported or available.

Any versions of the former SIEM Integration Guide that are earlier than version 18.2.1 are valid only for their corresponding versions, not version 18.2.1 or later releases.

Customers should upgrade to the latest version of Illumio Adaptive Security and take advantage of the newly designed auditable events.

Welcome to the New Illumio Experience

Illumio is excited to announce a new user interface for Illumio Core customers. Our New PCE user interface (UI) is designed to maximize user productivity and enable intuitive platform administration.

We think you'll love this cleaner, more flexible design – but while we always strive to keep Illumio Core easy-to-use, change is hard, so we've assembled this short guide to help you introduce you to this new Illumio Core experience.

We're sure this guide will help set you up for success!

Deprecation of the PCE Classic UI

All new customers and those existing customers who have upgraded to 23.3 or later see the New PCE UI when they log in. From onward, this is the only available UI.

In Core 23.4.0, Illumio deprecated the PCE classic UI.

Illumio introduced a new user experience for the PCE UI in Core 23.2.0. Since that release, customers have had the option to toggle between the classic PCE UI and the new UI. Illumio has kept the classic UI available for customers to use, giving you ample time to familiarize yourselves with the new user experience.

With Core 23.5.0, Illumio is removing the PCE classic UI, with some exceptions. It is time to use the new PCE UI exclusively to benefit from its extensive enhancements, such as the redesigned navigation, easy-to-use Quick Search, simplified naming, and updated look-and-feel.

The exceptions are Classic Illumination and Explorer. These UI elements are still accessible through a setting in the user's Profile page.

What Are the Primary Benefits?

We've designed these changes based on comprehensive analysis of how people are currently using Illumio functionality, and we've tested these changes thoroughly before releasing them to you.

Why is Illumio making these changes?

With the new Illumio experience, we are making it easy for you to access, find, and manage your servers and endpoints and their security policy so you can keep your work running smoothly.

Working with the New UI benefits you in the following ways:

- Easily work in the PCE with a simplified look-and-feel found in the UI headers, map, and selected pages.
- Achieve faster access to key features with updated navigation, including simplified terms.
- Learn key information about your environment by reviewing dashboards for Ransomware Protection and VEN statics, both with styling updates.
- Use Illumio maps more effectively due to significant usability enhancements.
- Start your work faster by using integrated quick search in the left navigation.

What is Changing?

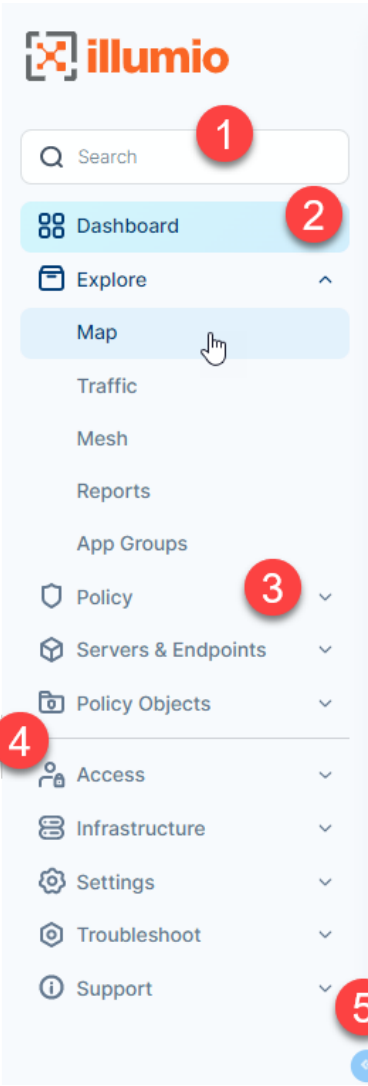
These changes include redesigned navigation, simplified naming, and an updated look-and-feel.

Redesigned Navigation

The redesigned left navigation menu in the PCE web console helps you navigate the tasks for each step in your workflow. It makes it easier for you to discover and get started with the features in the PCE web console. The menu offers clear entry points to key tasks. In the Classic UI, some of these functions were not placed in consistent locations or were hidden in sub-menus.

In the Classic UI, the navigation appeared as a hamburger menu, which you would click to display, and select fly-out sub-menus to locate features. In the New UI, the navigation is fixed and intuitively categorized, so that you can quickly select the feature you want to access.

In the following ways, the new navigation provides improved agility with a new, streamlined web-app experience:



The screenshot shows the Illumio navigation sidebar with the following items: Search, Dashboard, Explore, Map, Traffic, Mesh, Reports, App Groups, Policy, Servers & Endpoints, Policy Objects, Access, Infrastructure, Settings, Troubleshoot, and Support. A hand cursor is pointing at the 'Map' item. Red circles with numbers 1 through 5 highlight specific features: 1. Search bar, 2. Dashboard link, 3. Policy category, 4. Access category, and 5. Collapse button.

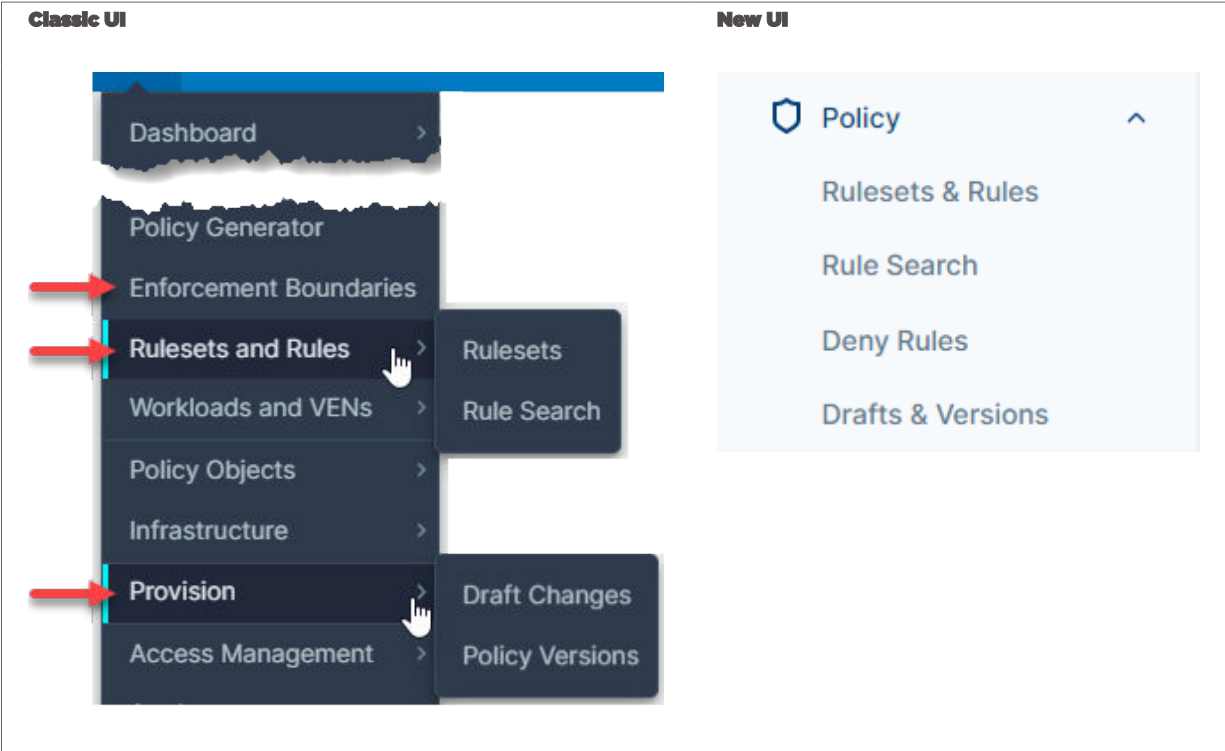
- (1)** The Quick Search feature has moved from the top-right toolbar to be integrated with navigation. The new placement highlights using Search as a quick alternative to clicking through the navigation to reach features.
- (2)** The fixed and always visible entry for the Dashboard makes it easy to return to your dashboard and view Ransomware and VEN statistics.
- (3)** New user-friendly category names that match industry-standard terms make it clear where to go to complete common tasks.
- (4)** New navigation icons visually reinforce context so that you always know your location in the UI. The icons consistently appear throughout the UI in breadcrumbs and page headings.
- (5)** Collapse the navigation to display only the icons. Navigation is always present but takes little room from displaying the feature page.

Navigation Changes at a Glance

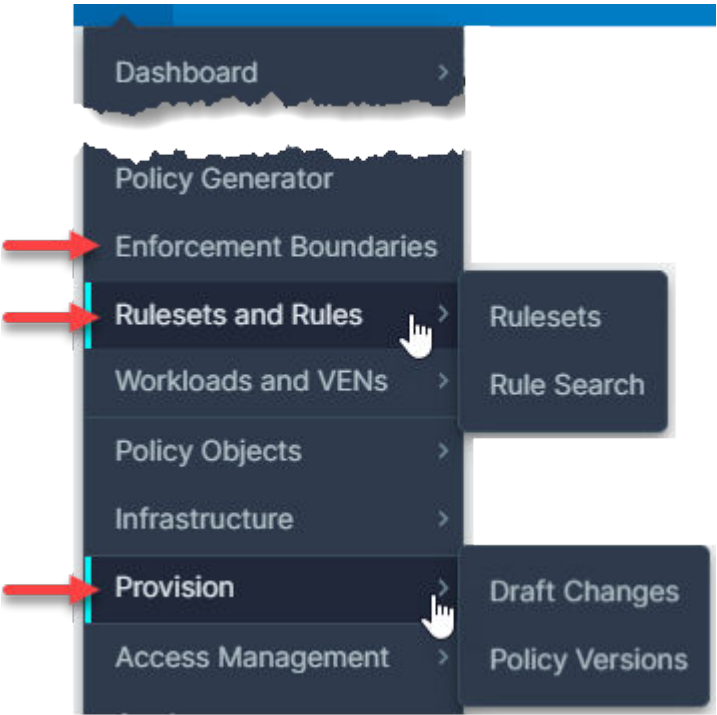
The PCE UI navigation redesign focused on surfacing common tasks and aiding discoverability. Consequently, key categories are renamed and reorganized in the New UI.

However, much of the navigation from the Classic UI carries forward into the New UI. Illumio Administrative categories that are clearly accessible in the Classic UI haven't changed, such as Infrastructure, Settings, Access Management, and Troubleshooting.

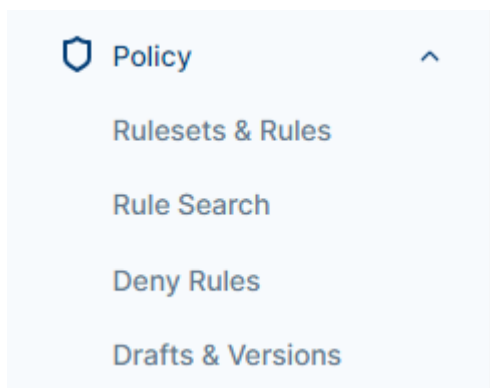
Categories used by Illumio users for creating policy, visualizing the managed environment, and working with devices (servers and endpoints) were the most impacted. The New UI now includes the Policy category, under which the essential tasks for creating and managing policy appear.



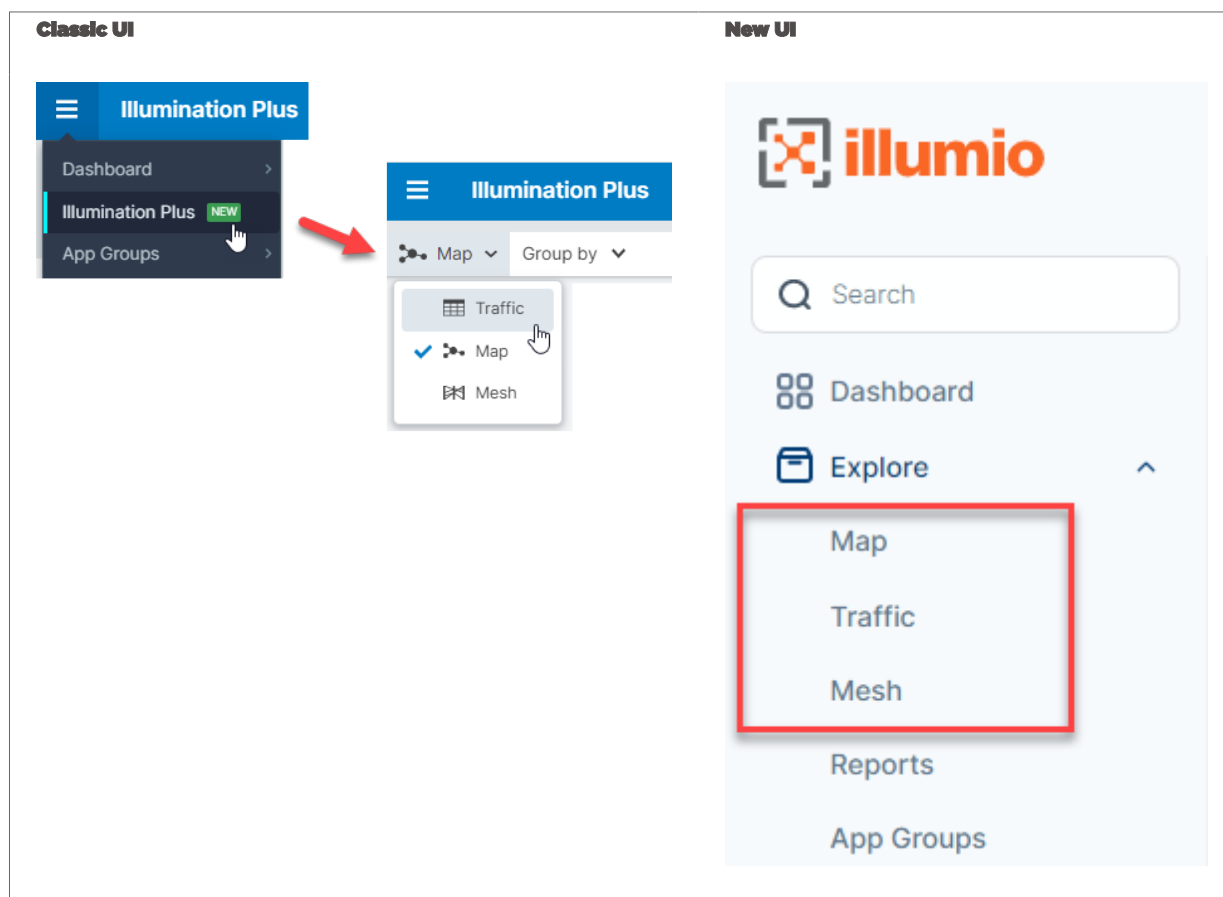
Classic UI



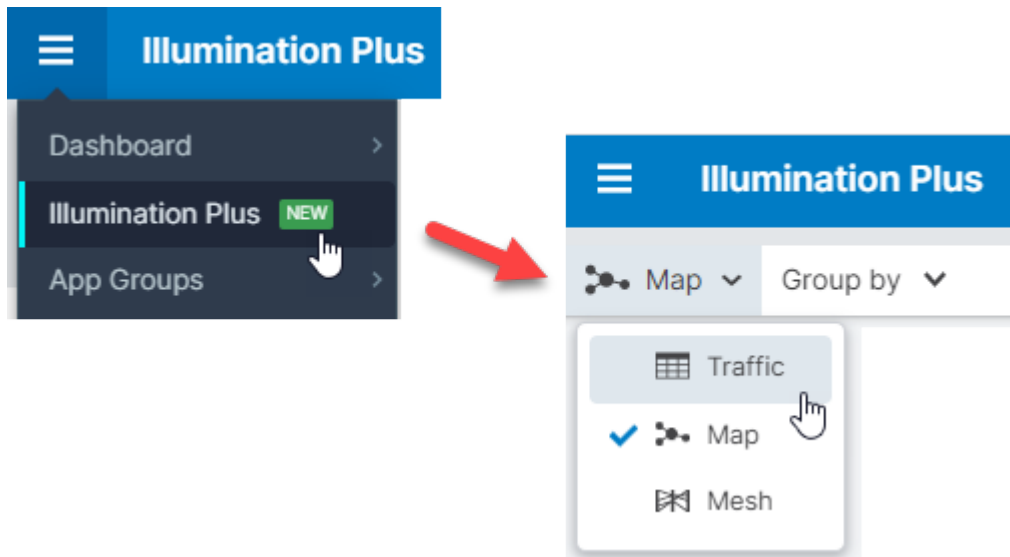
New UI



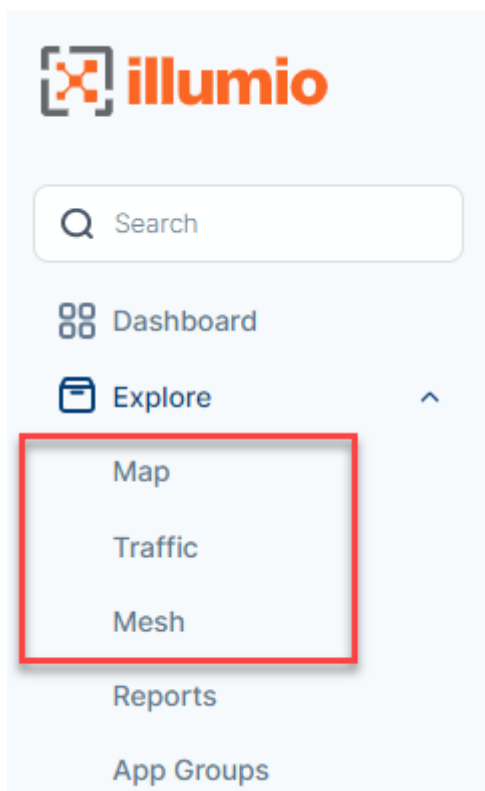
The New UI also centralizes all tasks related to visualization under the new Explore category. The Illumination Plus views (Map, Traffic, and Mesh) are easily accessible in the Explore category:



Classic UI

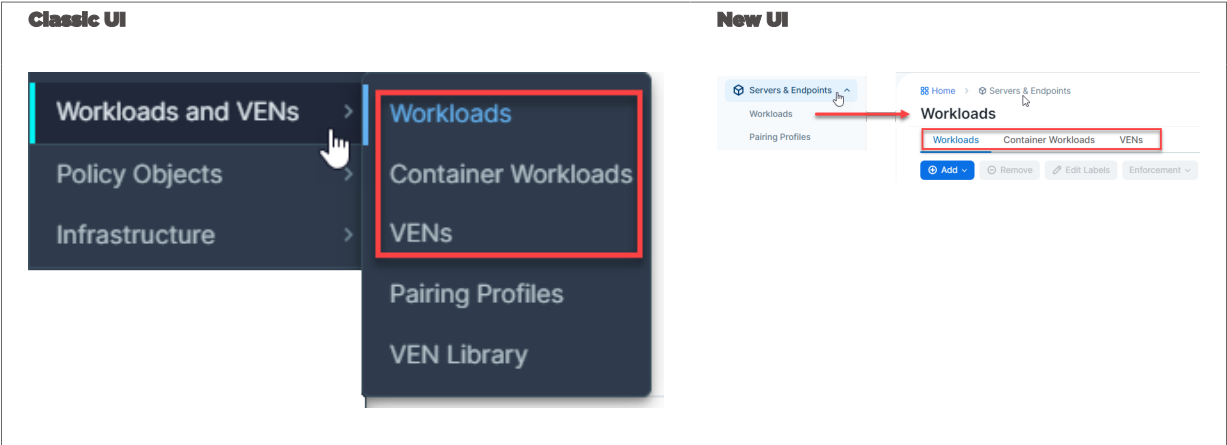


New UI

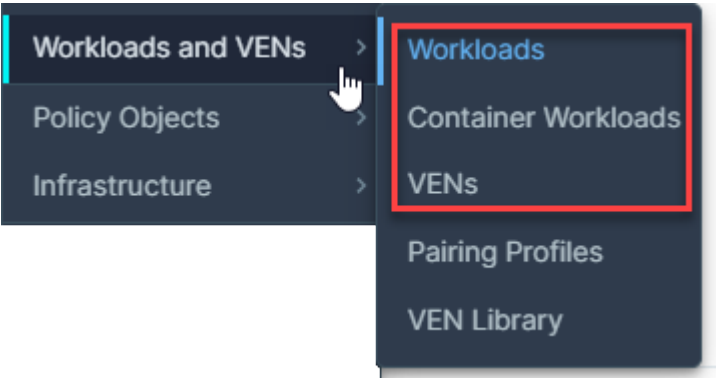


The **Workloads and VENS** category from the Classic UI is simplified and renamed in the New UI.

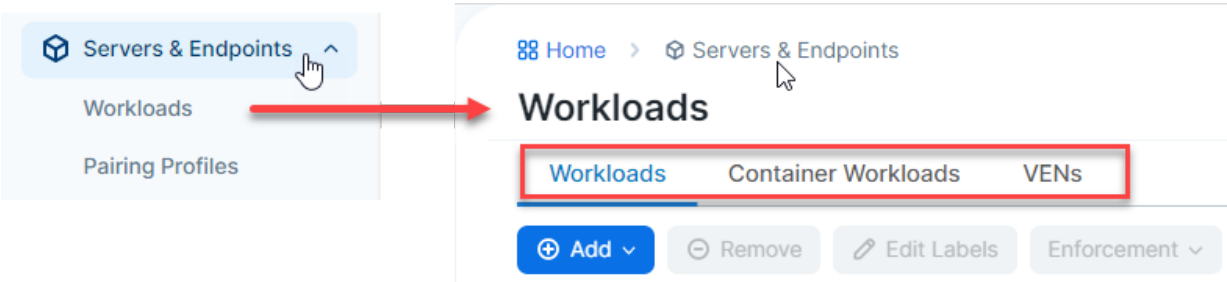
Historically, Illumio PCE UI has referred to server workloads as simply "workloads" and end-point workloads as simply "endpoints." The Classic UI navigation labeled this category using Illumio-specific terminology, namely "workload." The New UI clarifies this category by using terms customers are most familiar with.



Classic UI



New UI



Full Navigation Comparison between UIs

The following table compares the navigation between the two UIs.

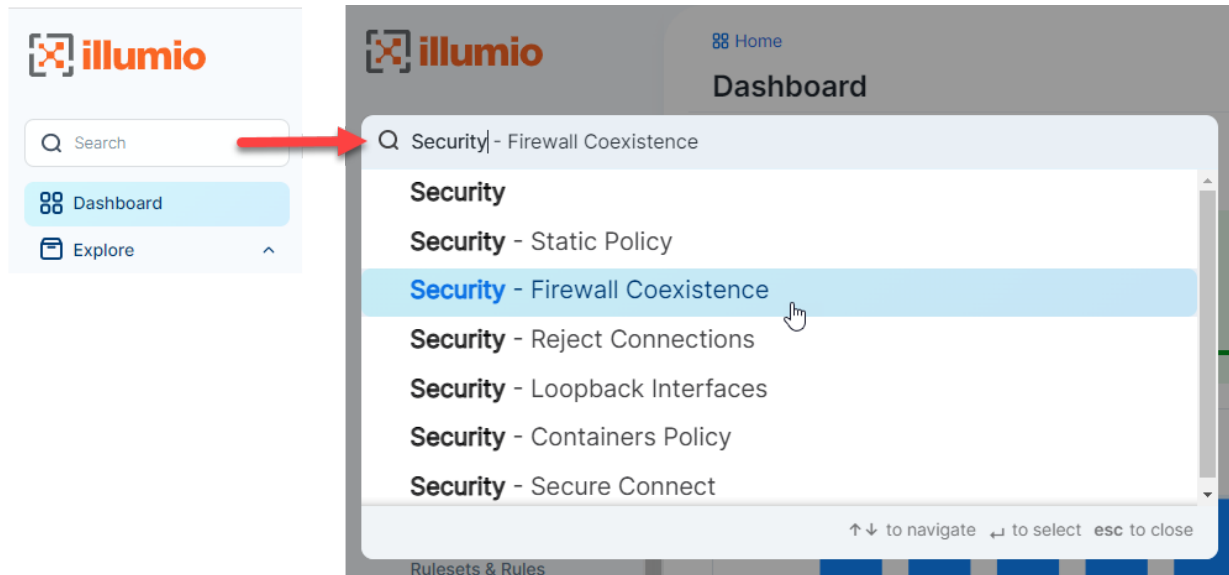
(Expand this section to see the full table)

Classic UI	New UI
Dashboard	Dashboard
VENs	Explore
Ransomware	Map
Illumination Plus	Traffic
Illumination Classic	Mesh
App Groups	Reports
App Group Map	App Groups
App Group List	Policy
Explorer	Rulesets & Rules
Reports	Rule Search
Policy Generator	Deny Rules
Enforcement Boundaries	Drafts & Versions
Rules and Rulesets	Servers & Endpoints
Rulesets	Workloads
Rule Search	Pairing Profiles
Workloads and VENs	Policy Objects
Workloads	Services
Container Workloads	IP Lists
VENs	Labels
Pairing Profiles	Label Groups
VEN Library	Virtual Services
Policy Objects	Virtual Servers
Services	Access
IP Lists	Global Roles
Labels	Scopes
Label Groups	External Groups
Virtual Services	External Users
Virtual Servers	Local Users
Segmentation Templates	Service Accounts
Infrastructure	User Activity
Core Services	Authentication
Load Balancers	Access Restrictions
Container Clusters	Infrastructure
SecureConnect Gateways	Core Services
Networks	Load Balancers
Cloud	

Provision	Container Clusters
Draft Changes	SecureConnect Gateways
Policy Versions	Networks
Access Management	Cloud
Global Roles	Settings
Scopes	Corporate Public IPs
External Groups	Event Settings
External Users	Flow Collection
Local Users	Label Settings
Service Accounts	Security
User Activity	Core Services
Authentication	Essential Service Rules
Access Restrictions	VEN Operations
Settings	Trusted Proxy IPs
Corporate Public IPs	Policy Settings
Event Settings	API Key Settings
Flow Collection	Offline Timers
Label Settings	Troubleshoot
Security	Blocked Traffic
Core Services	Events
Essential Service Rules	Exports
VEN Operations	VEN Support Bundles
Trusted Proxy IPs	PCE Support Bundles
Policy Settings	Policy Check
API Key Settings	Product Version
Offline Timers	Support
Troubleshooting	VEN Library
Blocked Traffic	Support Portal
Events	
Exports	
VEN Support Bundles	
PCE Support Bundles	
Policy Check	
Product Version	
Support	

Easy to Use Quick Search

At the top of the left navigation, you can use the Search feature to locate functionality within the PCE UI. This ability is especially useful for features that are integrated within the UI and not readily accessible from the left navigation because they require deeper navigation into the UI.



Additional Context through Breadcrumbs

The new UI also introduces helpful breadcrumbs, which update as you navigate through the PCE web console and provide context on where you are within the application.

Breadcrumbs are a secondary navigation aid that helps users easily understand the relation between their location on a page (like a page showing issues related to Policy) and higher-level pages (the dashboard, for instance).

Available for every page – allows you to easily navigate back to previous locations.



Simplified Naming

The big change you'll notice is that we've simplified our naming. The new simplified naming is most obvious in the new navigation.

The left navigation categorizes tasks that we have within our UI into terms that users are familiar with when they use the PCE UI for the first time. For example, they want to explore policy or find their servers and endpoints.

The navigation groups the terms and lays them out so that they act almost like a wizard. Customers can discover and learn about protection by using the UI.

Table 1. Full List of Changed Terms

22.5.x	Classic UI	New UI
Illumination Plus	Illumination Plus	Explore
Illumination Plus Table view	Illumination Plus Table view	Explore > Traffic
Enforcement Boundaries	Enforcement Boundaries	Deny Rules
Label-Set Connections	Label-Set Connections	Connections with common labels
Connections	Traffic	Traffic
Consumer and Provider	Consumer and Provider	Source and Destination

Updated Look-and-Feel

The new look-and-feel delivers a streamlined, modern approach that puts key information at your fingertips. We've updated the look-and-feel of the entire platform with an updated color palette, a new font, icons, and styles. In addition to being attractive, the updated look is designed to make it easier and more efficient to navigate the Illumio solution.

The headers of each section are easier to read, new fonts draw the eye to the data that matters most, and new button styles and colors intuitively highlight the next step a user should take to advance their workflow. The colors, icons, and lines between nodes in the map are fine-tuned to make the map easier to read and work with.

Deprecated Features in the New UI

The New UI deprecates the following features:

- Illumination Classic
- Explorer
- Policy Generator
- Segmentation Templates



NOTE

Illumination Classic and Explorer are still available in the Classic UI. You can toggle the UI at any time to use them.

Illumination Classic

The Illumio visualization features in the PCE are customer favorites. Illumio recognizes their customer appeal and continually works to expand their value.

In Illumio Core 22.5, Illumio introduced Illumination Plus. Illumination Plus includes many new features, better integration of visibility information, and support for flexible labeling.

While we always strive to keep Illumio Core easy to use, we recognize that change is hard, so we kept the familiar version of Illumination (referred to as Illumination Classic) available in the UI so that customers could adopt the new visualization features at their pace.

The availability of Illumination Classic remains, and can be selected through a setting in the user's Profile page. We strongly encourage customers to experience all the new visualization functionality in Illumination Plus and in the Explore category of the new UI.

Original Explorer

Illumio Core introduced the Explorer feature as a preview in Illumio Core 17.2.0. In Illumio Core 18.1.0, this feature became generally available. In Illumio Core 22.5, Illumio integrated the Explorer feature with Illumination Plus. The functionality for the Explorer feature was available in the Table view and Mesh view in Illumination Plus in the Classic UI.

However, original Explorer feature does not support the flexible label types feature introduced in Illumio Core 22.5, which allows you to create custom labels. The original Explorer feature only supports the standard Core RAEL labels. To use this functionality with the new flexible label types, you must use the Traffic and Mesh pages under Explore in the New UI.

The availability of Explorer remains in the Classic UI, when enabled through a setting in the user's Profile page. However, we strongly encourage customers to experience all the new visualization functionality in the Explore category of the New UI.

What's New and Changed in This Release

Before upgrading to Illumio Core 23.2, familiarize yourself with the following new and modified features in this release.

The information in this section describes the new and modified features to the PCE, REST API, and PCE web console.

What's New and Changed in 23.5

The following new features were added in Illumio Core 23.5.

Policy Templates

Policy templates provide out-of-the-box, pre-filled policy definitions for some of the most popular security practices. Templates are provided to control inbound internet access, ransomware, inbound and outbound administrator access, Active Directory, and ICMP.

Ransomware Protection Dashboard Changes

[Home](#) > [Ransomware Protection](#)

Ransomware Protection for Servers

[114B](#) [?](#) [M](#) [v](#)

[Refresh](#)



New Widgets

In Release 23.5, three new widgets have been added on the bottom of the Ransomware Protection Dashboard.

Workloads Exposure (Daily, Weekly, Monthly, Quarterly)

Workload Exposure widget shows, in percentages, how many of the existing workloads are protected from the ransomware vs. how many are still exposed. The unprotected workloads are further grouped in their exposure categories as Critical, High, Medium, and Low.

The exposure can be followed in time intervals: Daily, Weekly, Monthly, and Quarterly.

Protection Coverage Score (Daily, Weekly, Monthly, Quarterly)

The Protection Coverage Score is a metric used to measure the effectiveness of security policies in protecting workloads. It indicates the percentage of the entire possible attack surfaces that are actively protected by security policies. For example, a policy that allows all workloads as source will have a lower coverage score compared to a policy that only allows a small number of source workloads.

Protection coverage score takes all the protection-ready workloads into consideration across the organization.

The color of the widget changes from red to yellow and then to green as the protection coverage score increases.

Risky Ports by Type

This widget shows the percentage of risky ports by type: administrative vs. legacy ports. Each port type is presented with a bar that depicts the percentage of protected (green) and unprotected (orange) ports.

To help visualize the protection coverage by port type, five percentage data points are used: 20%, 40%, 60%, 80%, and 100%.

Existing Widgets

In Release 23.5, some changes have been introduced for the existing Dashboard widgets:

Protected Workloads

For the widget Protected Workloads, a list of services that are at risk of ransomware penetration and lateral movement is provided to help customers assess ransomware exposure on their Enterprise Service.

Protection Coverage Score

For this widget, guidelines and an example are provided to help calculate exact protection coverage score for selective vs. full enforcement.

Bulk Export/Import of Workload Labels

The export/import feature on the Workloads page allows you to create, assign, change, and unassign workload labels in bulk. With the Export feature, the PCE creates and downloads a file for you. Alternatively, you can skip the Export step and prepare your own CSV file and then import your file to the PCE. Use the import feature to specify updates in a CSV file and then import those updates to the PCE.

The image shows two side-by-side modal windows from the Illumio interface.

Export Workloads: This modal has a title bar with a close button. Below the title is a blue informational box stating: "You can export workload data for use in external applications." The main content area has three sections:

- Export:** A dropdown menu currently showing "All Workloads".
- Columns:** Two radio button options: "All Columns" (with subtext "Export all table columns (including hidden columns).") and "Labeling Columns" (which is selected, with subtext "Export columns required for workload labelling. Put each label type in a separate column.").
- File Format:** A dropdown menu showing "CSV" with a sub-menu open displaying "CSV" (checked) and "JSON".

Import a CSV to edit workload labels: This modal also has a title bar with a close button. It features a blue informational box: "You can update workload labels by importing a CSV file containing label information. The first two column headers must be 'href' and 'hostname'. The remaining column headers must match the keys assigned to each label type in the Label Settings page. E.g. 'role', 'app', 'env', and 'loc'." Below this is a section for the CSV file:

- CSV File:** A "Choose File" button followed by the text "No file chosen".
- Two checkboxes: "Create labels if they don't already exist" and "Remove existing label if imported label matches the string entered below:".

 At the bottom right are "Cancel" and "Preview Changes" buttons.

Enhancements in the Visualization Tools

Vulnerability Data Option

If you're in Vulnerability Data mode on the Map, a Vulnerabilities Tab is available on the right panel that opens when you click on a group in the Map. The tab appears only if the group you're evaluating contains vulnerabilities.

The image shows a portion of the Illumio visualization interface. At the top, there are three tabs: "Vulnerability Data" (highlighted with a red box and a dropdown arrow), "Circular Layout" (with a dropdown arrow), and "Reported View" (with a dropdown arrow). Below the tabs is a panel titled "Policy Data" with the subtitle "Show traffic based on Rules". Inside this panel, there are two options:

- Policy Data:** "Show traffic based on Rules".
- Vulnerability Data:** This option is selected, indicated by a checkmark and highlighted with a red box. Its description is: "Show severity and exposure of workload vulnerabilities and when traffic is inbound to a vulnerable port."

Summary	Traffic	Workloads	Vulnerabilities				
Customize columns ▾ 50 per page ▾ 1 – 42 of 42 Total ▾ < >							
V-E Score	Vulnerability Score	E/W Exposure	Northern Exposure	Workloads	Port/Protocol	CVE-IDs	Name
3.2	6.9	1		2	22 TCP	CVE-2013-2566 CVE-2015-2808	Name Does Not Match Server FQDN SSL/TLS use of weak RC4 cipher
3.2	6.9	1		2	22 TCP	CVE-2016-2183	Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)
3.2	6.9	1					
3.2	6.9	1		2	22 TCP		SSL/TLS Server supports TLSv1.0
3.2	6.9	1		2	22 TCP		SSL Certificate -

Legend for the New Vulnerability Data Option

The new Vulnerability Data option in the Map features a legend.

- The relative size of each node indicates the number of workloads in the node.
- The outer ring may be continuous or comprised of segments. The color of the segments shows the vulnerability level of workloads; segment sizes show the proportion of workloads assessed to be at the indicated vulnerability level.
- The color of each Traffic Link indicates the link's level of vulnerability.

Vulnerability Data ▾
Circular Layout ▾
Reported View ▾
Filter ▾
Legend ▾

HOW TO READ

NUMBER OF WORKLOADS

NODE TYPES

- Workload
- Virtual Server
- Virtual Service
- Container Workload
- Unmanaged
- Idle

VULNERABILITY

TRAFFIC LINKS

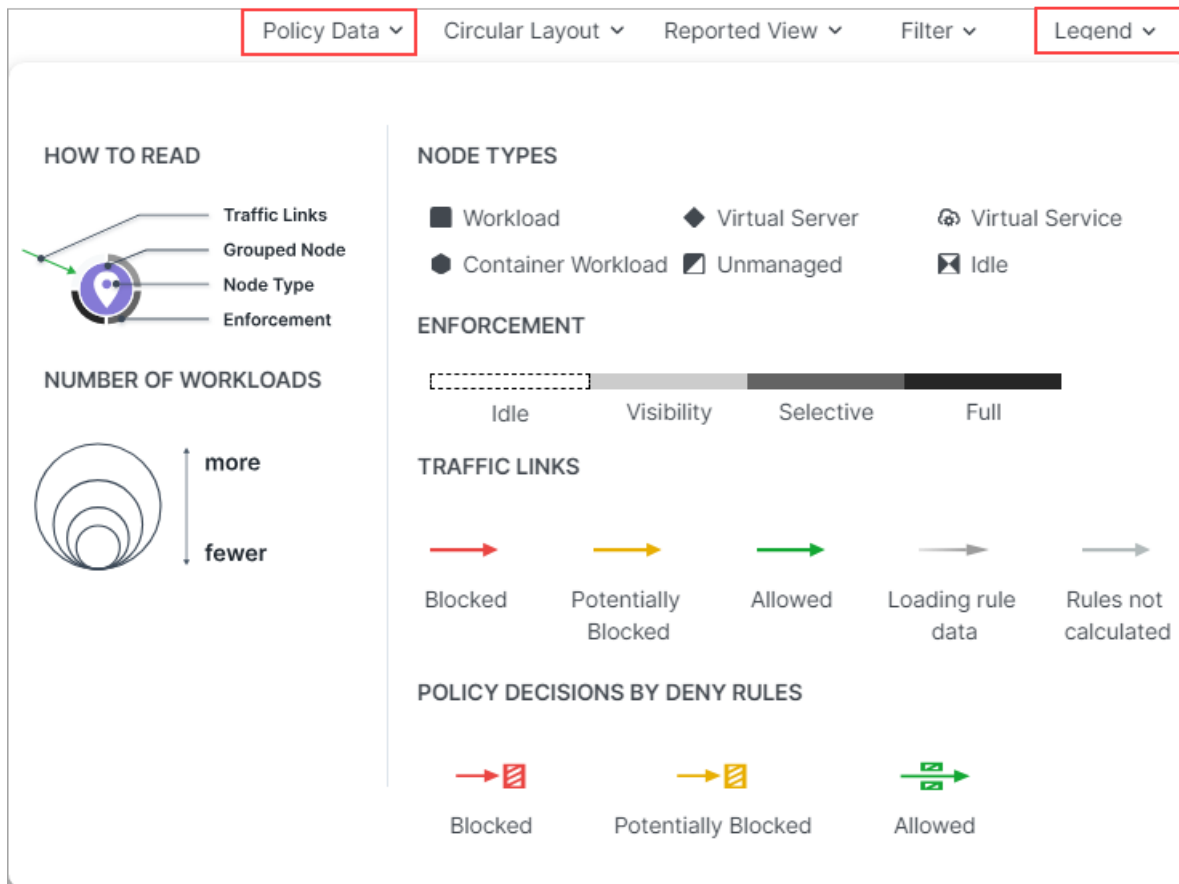
- Vulnerable (orange arrow)
- Potentially Blocked Vulnerable (yellow arrow)
- Not Vulnerable (grey arrow)

Updated Legend for the Policy Data option

The Policy Data option in the Illumination Map features an updated legend.

- The relative size of each node indicates the number of workloads in the node.

- The outer ring may be continuous or comprised of segments. The shade of the segments shows the enforcement level of workloads; segment sizes show the proportion of workloads under the indicated enforcement level.

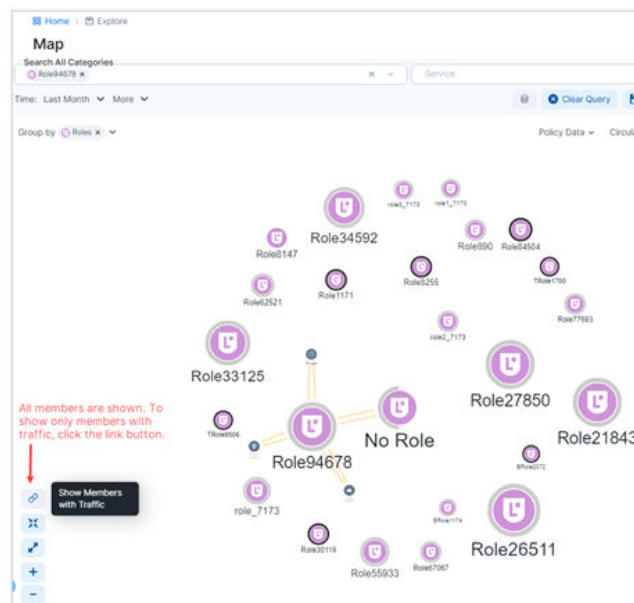


Show Members with No Traffic

Previously, running a query in the Map revealed only endpoints with traffic flows. A new feature redraws the map to reveal all endpoints, including those with no traffic.



Only workloads with traffic are shown (default)



All workloads are shown

New Group Member Tabs

To help you evaluate and secure your traffic, three new tabs detailing additional group members are now available in the right panel that opens when you click on a group in the Map. The tabs appear only if the group you're evaluating contains the corresponding group members.

- Container Workloads
- Virtual Services
- Virtual Servers

Summary	Traffic	Workloads	Container Workloads	Virtual Services	Virtual Servers
Container Workloads with Traffic ▾					
Customize columns ▾ 50 per page ▾ 1 – 9 of 9 Matched ▾ < >					
Policy Sync	Namespace/Project	Enforcement	Labels		
	↕ Name	Visibility			
	Last Applied Policy				

Windows Outbound Process: A New Object Type

In rulesets, you can now define and use a new type of object, a Windows outbound process. This provides visibility and policy enforcement at the source process level for granular control over the source traffic.

Limits on Flowlink Traffic Data

The PCE removes traffic flow data summaries (used by the Explore features in the PCE web console) when these conditions occur:

- The disk size of the traffic flow summaries exceeds the disk space allocated for the data.
- The traffic data database has been inactive for 90 days.

When Flowlink is used, the following limits apply on traffic data:

- The default storage limit on traffic data from all of an organization's Flowlink servers is 500 MB.
- The default storage size limit is based on the number of server VENs, endpoints, and container VENs. Kubelink flows (from container VENs) are grouped with server and endpoint flows.

When the storage limit or the 90-day limit is reached, traffic flow data is pruned. The order of pruning is first data from endpoints, then Kubelink, and lastly Server VENs.

Splunk Integration Version Upgrade

Splunk TA and app version 4.0.0 is now supported, including support for MT4L, multiple PCEs, multiple organizations, and faster search. Security operations personnel (SOC) can further enrich investigations and audits with Illumio data.

Traffic from Unpaired VENs

Traffic data for unpaired VENs can be seen by filtering on IP address. Get better visibility on unpaired VEN traffic for history and analysis.

Classic UI Removed

In Illumio Core 23.2.0, Illumio introduced a new PCE user interface (UI) designed to maximize user productivity and enable intuitive platform administration. Users had the option to toggle between the new UI and the earlier, classic UI. In 23.5.0, the toggle option is removed. The classic UI is no longer available.

There are two parts of the classic UI that are exceptions to this removal. The Explorer and Illumination Plus can be enabled with a setting in the user's Profile page.

Illumio Core REST API in 23.5.0

The Illumio Core REST API v2 has changed in 23.5 in the following ways.

New APIs

There are two new APIs in this release:

reports_risk_summary_ransomware_timeseries_statistics_post

This new Public Experimental API is used to show the new time series data:

- Number of managed workloads

- Percent of the ransomware protection coverage
- Number of workloads by exposure

Data is presented with the granularity of `day`, `week`, `month`, and `quarter`, where the default is `day`.

workloads/bulk_import

This new API is used to update workloads using a CSV file, and the only allowed input type is `'text/csv'`.

We recommend users to export a CSV file from the workloads page before they use this import function, so that they can just modify the CSV file they exported with the labels they would like to assign to the workloads.

- `PUT /api/v2/orgs/:xorg_id/workloads/bulk_import?delete_token`
If the value in the CSVfile for the `label_dimension` is the same as the delete token passed in the request, the label in that label dimension will be deleted for the workload. When users use CSV to update workload labels, they can pass in the delete token in the request to specify the labels to be deleted.
- `PUT /api/v2/orgs/:xorg_id/workloads/bulk_import?create_labels=true/false` (default is false)
Provides an option in the CSV labels update to create new labels if they don't exist. If the option is `false`, rows with non-existent labels will be skipped entirely.
- `PUT /api/v2/orgs/:xorg_id/workloads/bulk_import?dry_run=true/false` (default is false)
If users set this parameter to be `true`, the API will only return the potential changes and error tokens without making actual changes to the workloads.

common kubernetes_workloads_metadata

The new common schema `kubernetes_workloads_metadata` is referenced from `kubernetes_workload_get`.

It provides Kubernetes properties such as labels, annotations, and external service's UID.

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "description": "k8s object metadata",
  "additionalProperties": false,
  "type": "object",
  "properties": {
    "labels": {
      "description": "k8s key/value pairs attached to object that specify identifying attributes",
      "type": "object"
    },
    "annotations": {
      "description": "k8s key/value pairs representing arbitrary non-identifying metadata of object",
      "type": "object"
    },
    "external_service_uid": {
      "description": "k8s object uid of external traffic service"
    }
  }
}
```

```
        (NodePort or LoadBalancer)",
        "type": "string"
    }
}
```

Exposure and Authorization Changes

Network Enforcement Nodes Changes

Some existing Experimental APIs have been changed to facilitate creation of fully scripted integrations of endpoint management systems with the PCE using the Network Enforcement Nodes (NEN) Switch integration capabilities.

The default authorization for all Network Devices and Network Enforcement Nodes is "Global Administrator" and "Global Organization Owner".

In this release, additional authorizations have been extended as listed below:

API	Exposure Change	New Authorization Change
network_device_config	YES	NO
network_device_get	YES	NO
network_device_network_endpoint_get	YES	NO
network_devices_enforcement_instructions_applied_post	YES	"Global Policy Object Provisioner" and "Ruleset Provisioner"
network_devices_enforcement_instructions_request_post	YES	"Global Policy Object Provisioner" and "Ruleset Provisioner"
network_devices_get	YES	"Global Policy Object Provisioner", "Global Read Only", "Limited Ruleset Manager", "Ruleset Provisioner", "Ruleset Viewer", "Workload Manager"
network_devices_multi_enforcement_instructions_applied_post	YES	"Global Policy Object Provisioner" and "Ruleset Provisioner"
network_devices_multi_enforcement_instructions_request_post	YES	"Global Policy Object Provisioner" and "Ruleset Provisioner"
network_devices_network_endpoints_get	YES	NO
network_devices_network_endpoints_post	YES	"Workload Manager"
network_devices_network_endpoints_put	YES	"Workload Manager"
network_devices_put	YES	"Workload Manager"
network_endpoint_config	YES	NO
network_enforcement_node_get	YES	NO
network_enforcement_nodes_get	YES	"Full Ruleset Manager", "Global Policy Object Provisioner", "Global Read Only", "Limited Ruleset Manager", "Ruleset Provisioner", "Ruleset Viewer", "Workload Manager"
network_enforcement_nodes_network_devices_post	YES	"Workload Manager"
network_enforcement_nodes_put	YES	NO

Other Exposure Changes

supported_devices

API being made available to integrators.

Changed APIs

Ransomware Dashboard API Changes

In this release, these ransomware-connected APIs have been changed:

reports_risk_summary_get

This API was changed so that the property `risky_ports_by_category` was added to support the widget "Risky ports by type" in the UI.

```
"risky_ports_by_category": {
  "description": "Risky ports by Port type",
  "type": "object",
  "properties": {
    "admin": {
      "$ref": "num_protected_unprotected_ports.schema.json"
    },
    "legacy": {
      "$ref": "num_protected_unprotected_ports.schema.json"
    }
  }
}
```

reports_time_series_statistics_post

This API was changed so that besides the number of Managed Workloads, the following two other properties were added:

- `ransomware_protection_coverage_percent`: Percent of the ransomware protection coverage
- `num_workloads_by_exposure`: Number of workloads by exposure

Data is presented with the granularity of `day`, `week`, `month`, and `quarter`, where the default is `day`.

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "array",
  "items": {
    "type": "object",
    "required": [
      "property"
    ],
    "properties": {
      "property": {
        "description": "The property for which time series data is requested.",
        "type": "string",
        "enum": [
          "num_managed_workloads",
          "ransomware_protection_coverage_percent",
          "num_workloads_by_exposure"
        ]
      }
    }
  },
}
```

reports_time_series_statistics_post_response

Previously, the schema contained the integer count on the end date of the counted period. This item was removed:

```
"count": {
  "description": "The integer count on the end
```

```

        date of this period.",
        "type": "integer"
    },
    "unit": {
        "description": "The unit of the value returned.",
        "type": "string"
    },

```

This API now gives the percentage of the end date of the counted period.

This API is now referencing the schema `num_workloads_by_exposure_time_series`.

```

"data": {
  "oneOf": [
    {
      "$ref": "../../agent/schema/v2/num_workloads_by_
        exposure_time_series.schema.json"
    },
    {
      "count": {
        "description": "The integer count on the
          end date of this period.",
        "type": "integer"
      }
    },
    {
      "percentage": {
        "description": "The percentage on the end
          date of this period.",
        "type": "number",
        "minimum": 0,
        "maximum": 100
      }
    }
  ]
}

```

workload_ransomware_services

This schema is referenced from `workloads_risk_details_get` to supply the required service data:

- Service location and name
- Service Port and Protocol
- Severity and Protection state of this service
- Status of the port on the workload
- Active and Draft policy that allies to the Port

In release 23.5, additional information about the operating systems has been added for the ransomware service: Windows and Linux.

```

{
  "properties": {
    "os_platforms": {
      "description": "Operating system for this ransomware service",

```

```

    "type": "array",
    "minItems": 1,
    "items": {
      "type": "string",
      "enum": [
        "windows",
        "linux"
      ]
    }
  }
}

```

Other API Changes

sec_policy_rule_coverage_post_response

In this API, a new array `rule_edges` was added, which provides a list with a placeholder for each requested source and destination pair.

The previous object `rules` is replaced with a reference to `"$ref": "#/definitions/rule_href_mapping"`, and the previous array `edges` is replaced with a reference to `"$ref": "#/definitions/rule_edges"`.

```

"rule_edges": {
  "type": "array",
  "description": "A list with a placeholder for each requested
    source and destination pair",
  "items": {
    "type": "array",
    "description": "A list with with a placeholder for
      each requested service
        (per source and destination pair)",
    "items": {
      "type": "array",
      "description": "A list of indexes of matching rules
        (for each service per source and
          destination pair)",
      "items": {
        "type": "string",
        "pattern": "^[0-9]+$"
      }
    }
  }
}

```

optional_features_put

In 23.5, This API was changed so that an optional feature flag for Windows outbound process was added: `windows_outbound_process_enforcement`.

```

"properties": {
  "name": {
    "description": "Name of the feature",
    "type": "string",
    "enum": [

```



```

    "ip_forwarding_firewall_setting",
    "ui_analytics",
    "illumination_classic",
    "ransomware_readiness_dashboard",
    "per_rule_flow_log_setting",
    "lightning_default",
    "collector_scanner_filters",
    "corporate_ips_groups",
    "labels_editing_warning_for_enforcement_mode",
    "label_based_network_detection",
    "cloudsecure_enabled",
    "windows_outbound_process_enforcement"
  ],
},

```

This feature flag can be enabled or disabled using the following CURL command:

```

curl -u ${your_api_key}: ${your_api_secret} -H
"Content-Type: application/json" -X PUT -d
' [{"name": "windows_outbound_process_enforcement", "enabled": true}] ' https://$
{your_pce_server}:8443/api/v2/orgs/${your_ord_id}/optional_features

```

where you can define the part of the command: "enabled":true or "enabled":false.

kubernetes_workloads_get

For this API, these changes have been made:

- two arrays have been removed, k8s_labels and sk8s_annotation, and replaced with the property metadata

```

"metadata": {
  "$ref": "
    ../common/kubernetes_workloads_
      metadata.schema.json"

```

- HREF description has been changed from URI of the container workload, to URI of the kubernetes workload.

What's New and Changed in Release 23.5.10

The following new feature was added in Illumio Core 23.5.10.

Rule Hit Count Report



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

Requirements

- PCE Version:
 - SaaS: 24.2.0 or later
 - On-prem 23.5.10 or later
- VEN Version: 23.2.30 or later

Benefits

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.

CLAS Architecture in Illumio Core for Kubernetes and OpenShift

Illumio Core for Kubernetes 5.1.0 adds support for a new Cluster Local Actor Store (CLAS) mode, in which Kubelink becomes a full intermediary between PCE and C-VEs. With the CLAS architecture, Kubelink provides greater scalability, faster responsiveness, and streamlined policy convergence with several advantages:

- Reclassifies a container workload to more closely align to the Kubernetes concept of a workload (now called in PCE a *Kubernetes Workload*, to distinguish from a non-CLAS legacy Container Workload)
- Improved visibility to all containers/Kubernetes objects and changes
- Enforces traffic to/from containers, and responds dynamically to changes
- Improved performance as PCE does not have to keep track of every C-VEN change, which is now handled by CLAS
- Traffic flow data is now retained even after deleting the corresponding pods

Illumio Core REST API in 23.5.10

The Illumio Core REST API v2 has changed in 23.5.10 in the following ways.

The most important API changes for release 23.5.10 are connected to the following:

- [Rule Hit Count \[35\]](#)
- [Generating Rule Hit Count Reports \[37\]](#)
- [Organization Access \[42\]](#)
- [Cluster Mode for Container Cluster \[43\]](#)

Rule Hit Count

The Rule Hit Count feature is configured so that only certain VENs can compute the rule hit counts and send the rule ID info over to the PCE.

This feature is disabled by default on all the VENs and on the PCE.

Enabling Rule Hit Count

To use the Rule Hit Count feature, you first need to enable it on the PCE and the relevant VENs.

Enable Rule Hit Count on a VEN

Use the following API to enable the feature on a VEN on all scopes:

PUT api/v2/orgs/:xorg_id/sec_policy/draft/firewall_settings

The existing schema was changed so that the property `rule_hit_count_enabled_scopes` was added.

```
{
  "properties": {
    "rule_hit_count_enabled_scopes": {
      "description": "Workloads that match the scope will have rule hit \
count enabled",
      "$ref": "../common/rule_set_scopes_put.schema.json"
    }
  }
}
```

This is a sample API that can be used to enable the feature on specific scopes. In this example, it enables the features on all VENs with labels 7 and 12.

```
{
  "rule_hit_count_enabled_scopes": [
    [
      {
        "label": {
          "href": "/orgs/1/labels/7"
        }
      },
      {
        "label": {
          "href": "/orgs/1/labels/12"
        }
      }
    ]
  ]
}
```

Commit or provision these DRAFT changes.

POST /api/v2/orgs/:xorg_id/sec_policy

```
{
  "update_description": "Enable rule hit count",
  "change_subset": {
    "firewall_settings": [
      {
        "href": "/orgs/1/sec_policy/draft/firewall_settings"
      }
    ]
  }
}
```

Disable the feature Rule Hit Count on all VENs:

PUT api/v2/orgs/:xorg_id/sec_policy/draft/firewall_settings

The property rule_hit_count_enabled_scopes was added to this API:

```
{
  "properties": {
    "rule_hit_count_enabled_scopes": {
      "description": "Workloads that match the scope will have \
        rule hit count enabled",
      "$ref": "../common/rule_set_scopes_put.schema.json"
    }
  }
}
```

Enable Rule Hit Count on a PCE

Use the following API to enable the feature on a PCE:

PUT /api/v2/orgs/:xorg_id/report_templates/rule_hit_count_report

```
{
  "enabled": true
}
```

Generating Rule Hit Count Reports

A Rule Hit Count report can be either a scheduled report generated on a recurrent basis or an ad-hoc report.

To generate the Rule Hit Count report, two new schemas have been introduced: `rule_hit_count_report_params` and `rule_set_lists`:

rule_hit_count_report_params

The new schema returns the rule hit count statistics for all the rules in a ruleset during the specified time-range.

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "description": "Returns the rule hit count stats for all the rules in a
\
    ruleset during the specified time-range",
  "type": "object",
  "additionalProperties": false,
  "required": [
    "report_time_range",
    "rule_sets"
  ],
  "properties": {
    "report_time_range": {
      "description": "Time range the report is built across",
      "type": "object",
      "oneOf": [
        {
          "$ref": "report_time_range_definitions.schema.json#/
definitions/\
custom_date_range"
        },
        {
          "$ref": "report_time_range_definitions.schema.json#/
definitions/\
last_num_days"
        }
      ],
    },
    "rule_sets": {
      "$ref": "rule_set_lists.schema.json"
    },
    "max_results": {
      "description": "maximum number of rules to return in the
specified \
time-range in descending order of rule creation time",
      "minimum": 0,
      "maximum": 200000,
    }
  }
}
```

```

        "type": "integer"
    }
}

```

rule_set_lists

This schema returns the rule hit count statistics for all the rules in a ruleset during the specified time-range.

```

{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "description": "Returns the rule hit count stats for all the rules in a
ruleset
                        during the specified time-range",
  "type": "array",
  "items": {
    "type": "object",
    "additionalProperties": false,
    "required": [
      "href"
    ],
    "properties": {
      "href": {
        "description": "HREF of the ruleset",
        "type": "string"
      }
    }
  }
}

```

Generate an Ad-hoc Report

The following API can be used to create a report for the last x number of days. In the example, It generates a rule hit count report for the last 30 days for all rule sets.

POST /api/v2/orgs/:xorg_id/reports

```

{
  "report_template": {
    "href": "/orgs/1/report_templates/rule_hit_count_report"
  },
  "description": "My first rule hit count report",
  "report_parameters": {
    "report_time_range": {
      "last_num_days": 30
    },
    "rule_sets": []
  },
  "send_by_email": true
}

```

The example response is such as the following:

```

{
  "href": "/orgs/1/reports/d1b80240-ffa5-4e99-b2a0-c3d4946efe03",

```

```

"report_template": {
  "href": "/orgs/1/report_templates/rule_hit_count_report",
  "name": "Rule Hit Count Report"
},
"description": "My first rule hit count report",
"created_at": "2023-11-03T07:52:04.018Z",
"updated_at": "2023-11-03T07:52:04.018Z",
"progress_percentage": 0,
"generated_at": null,
"status": "pending",
"report_parameters": {
  "report_time_range": {
    "last_num_days": 30
  },
  "rule_sets": []
},
"send_by_email": true,
"created_by": {
  "href": "/users/1"
},
"updated_by": {
  "href": "/users/1"
}
}

```

To create a report for a custom date range, use the following API:

```

{
  "report_template": {
    "href": "/orgs/1/report_templates/rule_hit_count_report"
  },
  "description": "My first rule hit count report",
  "report_parameters": {
    "report_time_range": {
      "start_date": "2023-10-03T00:00:00Z",
      "end_date": "2023-11-03T23:59:59Z"
    },
    "rule_sets": []
  },
  "send_by_email": true
}

```

Check the Status of the Report

Use a GET API and the HREF from the POST response to check the status of the report:

GET /api/v2/orgs/:xorg_id/reports/:report_uuid

```

{
  "href": "/orgs/1/reports/d1b80240-ffa5-4e99-b2a0-c3d4946efe03",
  "report_template": {
    "href": "/orgs/1/report_templates/rule_hit_count_report",
    "name": "Rule Hit Count Report"
  },
  "description": "My first rule hit count report",
  "created_at": "2023-11-03T07:52:04.018Z",

```

```

    "updated_at": "2023-11-03T07:52:05.233Z",
    "progress_percentage": 100,
    "generated_at": "2023-11-03T07:52:05.233Z",
    "status": "done",
    "report_parameters": {
      "rule_sets": [],
      "report_time_range": {
        "last_num_days": 30
      }
    },
    "send_by_email": true,
    "created_by": {
      "href": "/users/1"
    },
    "updated_by": {
      "href": "/users/1"
    }
  }
}

```

Download the Report

When the status of the report is completed, it is emailed to the user who created the report if the option `send_by_email` is set.

Once the status of the report is set to "done", the report can be downloaded using the download API as follows.

GET /api/v2/orgs/:xorg_id/reports/:report_uuid/download

Here's a sample response that can be saved as CSV:

```

Rule HREF,Rule Name,Rule Set HREF,Rule Set Name,Rule Hit Count,Days Since
Last Hit,\
Last Updated Timestamp,Last Updated By,Start Date,End Date
/orgs/1/sec_policy/active/rule_sets/1/sec_rules/23,"",/orgs/1/sec_policy/
active/\
rule_sets/1,Default,0,-1,2023-08-07T22:55:37-07:00,
/users/1,2023-10-04T00:00:00Z,2023-11-02T23:59:00Z
/orgs/1/sec_policy/active/rule_sets/1/sec_rules/21,"",/orgs/1/sec_policy/
active/\
rule_sets/1,Default,0,-1,2023-07-25T04:48:09-07:00,
/users/1,2023-10-04T00:00:00Z,2023-11-02T23:59:00Z
/orgs/1/sec_policy/active/rule_sets/1/sec_rules/19,"",/orgs/1/sec_policy/
active/\
rule_sets/1,Default,0,1,2023-07-25T04:35:31-07:00,
/users/1,2023-10-04T00:00:00Z,2023-11-02T23:59:00Z
/orgs/1/sec_policy/active/rule_sets/1/sec_rules/8,"",/orgs/1/sec_policy/
active/\
rule_sets/1,Default,0,-1,2023-07-21T16:34:08-07:00,
/users/1,2023-10-04T00:00:00Z,2023-11-02T23:59:00Z
/orgs/1/sec_policy/active/rule_sets/1/sec_rules/3,"",/orgs/1/sec_policy/
active/\
rule_sets/1,Default,0,1,2023-07-20T04:22:23-07:00,
/users/1,2023-10-04T00:00:00Z,2023-11-02T23:59:00Z
/orgs/1/sec_policy/active/rule_sets/1/sec_rules/1,Allow outbound
connections,\

```



```

orgs/1/sec_policy/active/rule_sets/1,Default,0,1,2023-07-25T04:52:39-07:00,
    /users/1,2023-10-04T00:00:00Z,2023-11-02T23:59:00Z
/orgs/1/sec_policy/active/enforcement_boundaries/5,my test deny rule
with iplist, "", \
"",0,-1,2023-07-20T03:00:05-07:00,
    /users/1,2023-10-04T00:00:00Z,2023-11-02T23:59:00Z
/orgs/1/sec_policy/active/enforcement_boundaries/
3,ransomware_deny_rule2,"","",0,1,\
2023-06-30T17:16:38-07:00,
    /users/1,2023-10-04T00:00:00Z,2023-11-02T23:59:00Z
/orgs/1/sec_policy/active/enforcement_boundaries/1,ransomware deny
rule,"","",0,-1,\
2023-06-07T23:32:07-07:00,
    /users/1,2023-10-04T00:00:00Z,2023-11-02T23:59:00Z

```

Schedule a Recurrent Report

To create a recurring report, you need to create a report schedule. In this example, the report named "Monthly Rule Hit Count Report" is generated for the last 30 days, and will be sent via email to the person who requested the report.

Create a Report Schedule

```

{
  "report_template": {
    "href": "/orgs/1/report_templates/rule_hit_count_report"
  },
  "report_parameters": {
    "report_time_range": {
      "last_num_days": 30
    },
    "rule_sets": []
  },
  "send_by_email": true,
  "report_generation_frequency": "monthly",
  "name": "Monthly Rule Hit Count Report",
}

```

Other API Changes to Support the Rule Hit Count Feature

sec_policy_label_groups_get

The property rule_hit_count_enabled_scopes was added.

```

"properties": {
  "rule_hit_count_enabled_scopes": {
    "description": "Label Group is referenced by Rule Hit Count Enabled
Scopes",
    "type": "boolean"
  }
}

```

sec_policy_firewall_settings_get

The property rule_hit_count_enabled_scopes was added.

```

{
  "properties": {

```

```

        "rule_hit_count_enabled_scopes": {
            "description": "Workloads that match the scope will have rule
hit count \
enabled",
            "$ref": "../common/rule_set_scopes_get.schema.json"
        }
    }
}

```

report_schedules_get
report_schedules_put
report_schedules_post
reports_post
report_templates_get

```

{
    "$ref": "rule_hit_count_report_params.schema.json"
}

```

In all these listed APIs, a reference to the schema `rule_hit_count_report_params` was added:

Organization Access

Changes to the organization access introduced a new common schema:

common ipv4_ipv6_subnet

```

{
    "$schema": "http://json-schema.org/draft-04/schema#",
    "type": "string",
    "oneOf": [
        { "format": "ipv4" },
        { "format": "ipv6" }
    ]
}

```

This common schema is replacing the one that is now deleted: `common ipv4_subnet`

```

{
    "$schema": "http://json-schema.org/draft-04/schema#",
    "type": "string",
    "pattern": "^(25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)(\\.|\\s){3}(25[0-5]|2[0-4][0-9]|
[01]?[0-9][0-9]?)(\\s|/|(3[0-2]|[0-2]?[0-9]))?.$"
}

```

Three organization access APIs have been changed to substitute `common/ipv4_subnet.schema` with `common/ipv4_ipv6_subnet.schema`:

orgs_access_restrictions_post
orgs_access_restrictions_put

```

{
    "properties": {

```

```

    "ips": {
      "items": {
        "$ref": {
          "__old": "../common/ipv4_subnet.schema.json",
          "__new": "../common/ipv4_ipv6_subnet.schema.json"
        }
      }
    }
  }
}

```

settings_trusted_proxy_ips_put

```

{
  "properties": {
    "trusted_proxy_ips": {
      "items": {
        "properties": {
          "ip": {
            "$ref": {
              "__old": "../common/ipv4_subnet.schema.json",
              "__new": "../common/ipv4_ipv6_subnet.schema.json"
            }
          }
        }
      }
    }
  }
}

```

Cluster Mode for Container Cluster

The new property `cluster_mode` was added to describe the cluster mode for container cluster:

container_clusters_get

```

{
  "properties": {
    "cluster_mode__added": {
      "description": "Cluster mode of Container Cluster",
      "type": "string",
      "default": "legacy"
    }
  }
}

```

Illumio Core REST API in 23.5.20

The Illumio Core REST API v2 has changed in 23.5.10 in the following ways:

Changed APIs

Two APIs,

sec_policy_firewall_settings_put

and

sec_policy_firewall_settings_get

have the added property `ip_forwarding_enabled_scopes`:

```
"ip_forwarding_enabled_scopes": {  
  "description": "Host Workloads that match the scope will have IP  
forwarding \\  
enabled",  
  "$ref": "../common/rule_set_scopes_put.schema.json"
```

The property was added both to the Public Experimental and Public Stable schema in this release.

Public Stable exposure was requested by the customers who intend to programmatically configure which workloads can have `ip-forwarding` enabled. This assures that the API will not change or be removed.

Illumio Core Release Notes 23.5

Welcome

These release notes describe the resolved issues and known issues for Illumio Core 23.5.x releases:

- Illumio Core 23.5.31-PCE is available for Illumio Core On-Premises customers
- Illumio Core 23.5.21+A4-PCE is a Limited Availability release for select Illumio Core On-Premises customers
- Illumio Core 23.5.30-PCE is available for Illumio Core On-Premises customers.
- Illumio Core 23.5.21+A3-PCE is a Limited Availability release for select Illumio Core On-Premises customers
- Illumio Core 23.5.21 is available for Illumio Core On-Premises customers
- Illumio Core 23.5.20 is available for Illumio Core On-Premises customers.
- Illumio Core 23.5.10 is available for Illumio Core On-Premises customers.
- Illumio Core 23.5.1 is available for Illumio Core Cloud (SaaS) customers.

Document Last Revised: November 2024

Document ID: 14000-100-23.5.31-PCE

Product Version

PCE Version: 23.5.31-PCE (on-premises LTS release)

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 Release 23.5.31-PCE

- **Supercluster replication issues after upgrade to 23.5.x PCE** (E-120467)
In rare cases where VENs were previously moved among PCEs in a Supercluster, replication would fail after upgrading the PCE to 23.5.x.

Resolved Issues in Release 23.5.30-PCE

- **PCE setup does not work on RHEL 9.x in FIPS mode** (E-119668)
This release resolves an incompatibility with the PCE and RHEL 9.x in FIPS mode which caused the PCE to not start properly.
- **Errors in Flow Analytics** (E-118558)

Flows in Illumination or the traffic database summary were not appearing, and the traffic database size summary was being shown as zero on some PCE clusters.

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

PCE was sending partial IPP instructions to Kubelink, which resulted in incorrect policy in the destination cluster.

- **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".

- **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.

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

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

- **HTTP 500 error from Kubernetes Workloads filter** (E-115416)

After navigating to **Workloads > Kubernetes Workloads**, then setting the Filter to Category NO LABEL, Type == NO APPLICATION LABELS, after pressing Enter, the action fails with a **Navigation has been cancelled due to an error** message appears.

- **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.

- **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.

- **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 VENs tab and querying traffic.

Known Issues in Release 23.5.30

Enterprise Server

- **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.

- **Virtual services with over 50 IPs are not editable in the UI** (E-109431)

When editing a provisioned virtual service with over 50 IPs, ones over 50 are set to "dele-tion pending". Workaround: None.

- **UI gets stuck after deleting 500 workloads** (E-108849)

Workaround: None.

- **On some pages, label order is not controlled by Label Settings** (E-107605)

Workaround: None.

- **PCE application log files are not rotated** (E-105659)

Some PCE application log files (agent, collector, haproxy) are not rotated, while others are rotated correctly.

Workaround: None.

- **The contextual menu is not completely visible** (E-105143)

In the Traffic tab, when opening the contextual menu for a Service in the first row of the table, the menu is partially hidden and not completely visible.

- **The Save button is disabled while creating unmanaged workloads from the FQDN pan-
el** (E-105006)

The Save button is disabled while adding an unmanaged workload when creating it from the FQDN panel in the App Group Map view. The Save button is not enabled even after the mandatory fields are filled out.

Workaround: You can save the Unmanaged workload by entering a description, after which the Save button is enabled.

- **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.

Data Visualization

- **Updating max results in Illumination Plus (10K) updates the Explorer max re-
sults** (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 10,000 results.

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

Workaround: Save the query filter if needed.

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

The Explorer results are not filtered based on the custom labels.

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.

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

Workaround: None

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

The flow timestamp that is shown in visualizations is not reliable for ingress-only or egress-only reported flows.

Workaround: Use Explorer to see the correct timestamp.

PCE Platform

- **In a Supercluster, a syslog server cannot be configured for member PCEs** (E-106345)

The setup of a syslog server can be performed only from the leader PCE.

VEN

- **SecureConnect only logs the "E" on the provider** (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 the workload/VEN page** (E-100844)

Workaround: Verify the Windows release by using the workload operating system.

Resolved Security Issues in Release 23.5.30-PCE

This section provides important security information for this release.

- See [2023 Security Advisories](#) for more information.
- See [2024 Security Advisories](#) for more information.
- **redis** was upgraded to 6.2.16 to address CVE-2024-31449.
- **webrick** was upgraded to 1.8.2 to address CVE-2024-47220
- **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.
- **cgi-0.3.2.gem upgraded to v0.3.6 to address CVE-2021-33621**: This CVE did not impact Illumio PCE.
- **globalid upgraded to v1.0.1**: globalid upgraded to v1.0.1 to address CVE-2023-22799.
- **google-protobuf upgraded to v3.22.5**: google-protobuf upgraded to v3.22.5 to address CVE-2022-3171 and CVE-2021-22569.

- **rack upgraded to v2.2.7:** rack upgraded to v2.2.7 address CVE-2022-44572, CVE-2022-44571, CVE-2023-27530, CVE-2023-27539, and CVE-2022-44570.
- **rails, actionpack, activerecord, activesupport and related gems upgraded to v6.1.7.4:** rails, actionpack, activerecord, activesupport and related gems upgraded to v6.1.7.4 to address multiple CVEs including CVE-2023-28120, CVE-2023-23913, CVE-2023-28362, CVE-2023-22792, CVE-2023-22795, CVE-2022-3704, CVE-2023-22794, CVE-2022-44566, and CVE-2023-22796.

Resolved Security Issue in Release 23.5.22

In this release, the following security issue was resolved:

- 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 23.5.21+A4-PCE



NOTE

Illumio Core 23.5.21+A4-PCE is a Limited Availability (LA) release for selected on-premises customers only.

- **Container cluster service provisioning failures** (E-120243)
This release addresses transient container cluster service provisioning issues when the PCE is under high load.
- **High memory usage on PCE Core nodes** (E-119364)
This release optimizes memory usage on Core nodes in environments with a large number of Virtual Servers and policies targeting Virtual Servers.

Resolved Security Issue in Release 23.5.21+A4-PCE

In this release, the following security issue was resolved:

- 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 Issue in Release 23.5.21+A3-PCE



IMPORTANT

This release is a Limited Availability (LA) release

Resolved Issue

- **Virtual services provisioning failure** (E-114692)

In non-CLAS deployments, policy provisioning of Virtual Services reported by Kubelink sometimes failed. This was caused by concurrent reporting of containers by C-VEs. This has been fixed.

Updates in Release 23.5.21+A2-PCE



IMPORTANT

This release is a Limited Availability (LA) release.

Enhancement

- **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.

Resolved Issue

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

PCE was sending partial IPP instructions to Kubelink, which resulted in incorrect policy in the destination cluster.

Resolved Issues in Release 23.5.21+A1-PCE



IMPORTANT

This release is a Limited Availability (LA) release.

- **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 relabeled correctly to their assigned annotation values.

- **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.

Resolved Issues in Release 23.5.20

Enterprise Server

- **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.

- **Rule writing issue using Illumination Plus** (E-115225)

Users could not write rules based on a port number using the automatic rule creation tool in Illumination Plus. This issue is fixed.

- **Save and Provision for a rule failed** (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 net-ssh-6.1.0.gem to 9.5.0.0 or higher to address CVE-2023-48795** (E-114139)

Upgrade is performed.

- **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.

- **Sudo access for ilo-pce** (E-113745)

This issue is fixed, and the command `ilo-pce` does not require `sudo` access.

- **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.

- **The Policy check did not show disabled Pending Rules** (E-112974)

This issue is fixed.

- **Explore Traffic showing traffic for labels that do not match the query** (E-112968)

When running an Explore traffic query for a particular label combination, the results show traffic from a different query. This issue is resolved, and the results match the labels specified in the filters.

- **Changes to system_health events after upgrade to 23.2.20** (E-112922)

After upgrading to PCE 23.2.20, system health events included "illumio_pce/cli" rather than "illumio_pce/system_health". This issue is resolved.

- **Expose ip_forwarding_enabled as a public stable API** (E-112464)
GET/PUT firewall_settings API is exposed as public stable for the ip_forwarding_enabled field only.
- **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.
- **Replication/PCE Monitoring** (E-110216)
Replication Monitoring (Health and CLI) and PCE Monitoring tasks have been closed.
- **Explorer page bug** (E-108585)
When the policy was changed, the traffic view grid pagination in the draft view did not reset to page 1. This issue has been resolved.

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-paired/paired) while there were Kubernetes Workloads already present.

VEN



NOTE

These notes apply to version 23.2.23

- **Combination of factors caused policy sync failure on RHEL 9.X OS VENs** (E-115693)
Policy sync failed and an error was thrown when the PCE applied custom iptable rules to VENs installed on RHEL 9.X OS (or later) workloads with iptables-nft-1.8.10 package. The issue stemmed in part from invalid syntax introduced by iptables-nft-1.8.10. This issue is resolved on 22.2.45-9201 VENs and later.
- **Potential for FQDN-based rules to fail** (E-114964)
In an environment implementing an IPv6 nameserver, FQDN-based rules may not have been enforced as expected. This issue is fixed.
- **VEN installation failed on Amazon Linux 2023** (E-113934)
This issue was caused by a change Amazon made to the format of the release name in the system release file. This issue is fixed.
- **ICMP code misinterpretation caused a 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.
- **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.

VEN Known Issue



NOTE

This note applies to version 23.2.23.

- **False positive firewall tampering error** (E-113892)

If the PCE pushes a policy that is identical to the existing policy already on the VEN, the more recent policy is not applied, and the existing policy remains in the current directory. This results in the current directory and the runtime firewall having different policy IDs. Because the VEN interprets this difference as firewall tampering, it generates a tampering error. This is expected behavior. Workaround: restart or suspend/unsuspend the VEN manually or through the PCE Web Console. The VEN flushes the existing rules and then applies the rules in the current directory.

Security Information

This section provides important security information for this release. 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.

- **json-jwt-1.13.0.gem upgraded to json-jwt1.16.6** (E-114939)

json-jwt-1.13.0.gem upgraded to json-jwt1.16.6 to address CVE-2023-51774. This CVE did not impact Illumio PCE.

Resolved Issue in Release 23.5.21

- **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.

Resolved Issues in Release 23.5.10



IMPORTANT

Illumio Core 23.5.10 is available for Illumio On-Premises customers only.

Enterprise Server

- **Traffic query was returning unexpected results** (E-112418)
This issue is fixed, and the generated SQL queries for all scenarios look as expected.
- **The service background_worker crashed on large async API responses** (E-112383)
This issue was observed for async APIs on large workload collections. This issue is resolved.
- **An error was thrown during the bulk Import of Workload labels when the labels contained double-byte characters** (E-112278)
This issue is fixed, and users can import double-byte characters.
- **The Ransomware Dashboard was displaying the same port/process multiple times** (E-112055)
This issue is fixed.
- **ERROR: cannot DROP TABLE "event_bus_changes" was triggered with pending trigger events** (E-111745)
This regression was caused by an optimization introduced to drop a temp table to avoid vacuum buildup. This issue is resolved.
- **Upgrade PostgreSQL to address CVE-2023-5869 and CVE-2023-5868** (E-111556)
PostgreSQL was upgraded to mitigate exposure to two CVEs: CVE-2023-5868 and CVE-2023-5869. As the PCE uses PostgreSQL internally and does not offer external user access the likelihood of this exploit is low without additional access privileges. PostgreSQL was upgraded as a cautionary measure to address two CVEs.
- **Added unmanaged workloads from Explorer no longer use hostnames** (E-111363)
When unmanaged workloads were created from Illumination Plus (Explorer), the priority for the workload name was the hostname followed by the IP Address. IP Address will be considered when the hostname for a workload doesn't exist.
- **Vulnerability data was showing on the map only upon interaction** (E-111087)
Vulnerability data was shown on the Vulnerability Map only when users interacted with it. This issue is resolved.
- **The reported view was not showing if a flow was blocked** (E-111058)
The reported view did not show if a flow was blocked by a source or destination in Illumination Plus. This issue is resolved and works as expected.
- **The Traffic query against Windows outbound service objects was not working** (E-111046)
This issue is resolved and works as expected.
- **Traffic query was not showing blocked DHCPDISCOVERING flows** (E-110940)
Traffic query did not show blocked DHCPDISCOVERING flows with FlowCollection set to aggregate broadcast traffic. This is resolved and works as expected.
- **The source port/process was not showing for the selected flow** (E-110514)
This issue is resolved and works as expected.
- **Saving filter with duplicate name did not give an error** (E-110132)
No error was triggered when a filter containing a duplicate name was saved. This issue is resolved, and saving a duplicate name for a filter gives an error: "A filter with that name already exists. This will overwrite the existing filter".

- **The PCE was proposing to delete a valid rule when another rule was provisioned** (E-109240)

The resolution is to default to not consolidating the rules already existing in the ruleset.

- **IP list traffic did not appear in searches** (E-108490)

The IP list traffic was not appearing in searches due to including a list containing an FQDN in query parameters. This leads to the inclusion of region_id in the sql query that is executed in each region. However, the region_id being passed is the leader's region id. The issue happens only on a supercluster.

- **Creating a traffic report for the Default Graph resulted in an endless loop** (E-108203)

This issue is resolved and works as expected.

- **The Illumination Plus query involving a Process and a Port without traffic yielded no results** (E-108060)

However, removing the Port produced results. The services include filter should function as an OR, as the tooltip indicates, instead of an AND when specifying processes with ports.

- **Blank space in the IP address caused a query to fail** (E-106290)

When filtering by IP address in Explorer > Traffic, the query failed if a blank space appeared after an IP address in the filter criteria. This issue is resolved.

- **Mesh was re-rendering repeatedly and interactions did not work** (E-105167)

Hover and brush interactions on Mesh have not been working properly and images re-render repeatedly. This issue is resolved.

- **Proposed Rules - Status information was hidden** (E-105098)

The Proposed Rules status information was hidden by the Ruleset Summary page. This issue is resolved.

- **Selecting a saved filter did not return any results** (E-102257)

When loading a saved filter in Illumination Plus, the PCE did not return any results for the query. This situation occurred when users selected the Reported Policy Decision option in Illumination Plus. This issue is resolved.

PCE Platform

- **The PCE failed to initialize in FIPS mode on RHEL 8.3 or higher with Ruby 3.1.2** (E-111825)

When operating in FIPS mode on EL 8.3 or higher, the PCE could not start on an initial install. A change in the runtime environment introduced this issue, which has now been fixed.

UI Components

- **The Merge option for Proposed rules was merging Existing rules** (E-111593)

This issue is fixed, and the UI works as expected.

VEN

- **VEN asked for a maintenance token on unsupported OSes for tampering protection** (E-101470)

When VEN tampering protection was enabled, Solaris and macOS workloads (where VEN tampering protection is not yet supported) also requested a maintenance token for CLI commands. CLI commands other than suspend would succeed if a valid maintenance token was provided, while suspend did not work even when a valid token was provided. This issue is resolved.

Resolved Issues in Release 23.5.1



IMPORTANT

Illumio Core 23.5.1 is available for Illumio Cloud customers only.

Enterprise Server

- **Performance issue in new PCE UI** (E-110920)
Performance issues led to a slow and unresponsive UI experience when using the New PCE UI experience in Chrome and Edge browsers on the Windows operating system. This issue is resolved.
- **Reports not being generated to the selected filter** (E-110556)
When running a report for a filter with an IP list as a provider, the export CSV file ignored the filter and sent only all traffic. This issue is resolved.
- **Policy decision reported as potentially blocked for deleted workloads but not calculated in UI rules** (E-110145)
The draft policy decision returned from the backend was incorrect. It should have been labeled as 'unknown' for flows with deleted workloads. This issue is resolved.
- **Could not delete or edit the "Default" traffic filter** (E-110059)
The default filter was created randomly, without asking users and without giving them an option to change or edit the filter. This issue is resolved. A default query notification was added, which allows the user to remove the default query. The landing page text was also updated to be more descriptive.
- **UI Policy Rulesets diff page displayed the wrong user** (E-110022)
The Policy Version diff page was showing "updated by" and "updated at" values, but the column was incorrectly labeled as "provisioned by". This issue is resolved. The columns are now labeled correctly.
- **VENs failed to communicate after VEN upgrade in some cases** (E-109762)
When a VEN paired to a 23.2.10 or 23.2.11 PCE was upgraded to VEN version 23.2.0, 22.5.0 through 22.5.20, or earlier, the VEN lost connectivity with the PCE. This issue is resolved. For additional important details, log in to Illumio Support and see the Knowledge Base article "Upgraded VENs fail to communicate with the PCE due to an API version mismatch issue".
- **The flow_monitor service restarted due to an unhandled distribution transaction deadlock** (E-109758)
This issue is resolved.
- **UI was not consistently displaying service names in Traffic Query search results** (E-109701)
The Traffic Query UI failed to display labels correctly for ports with assigned service objects. This issue is resolved.
- **Unable to create FQDN IP Lists** (E-109576)
An 'Invalid IPv4' error occurred when validating Fully Qualified Domain Names (FQDN) during the creation or modification of IP Lists. This issue is resolved.
- **Ransomware dashboard showed only "No data to display"** (E-109441)
After enabling the Ransomware Protection Dashboard, it showed the message "No data to display". This issue is resolved. Now the UI shows "No services tagged with ransomware metadata" when a ransomware-risky service is available.

- **Occasional async API failures** (E-109356)
The PCE could enter a state where async API calls failed until a PCE restart is performed. This issue is resolved.
- **PCE performance could degrade** (E-109311)
Large amounts of FQDN traffic or large numbers of managed endpoints in the PCE could result in degraded PCE performance. In this situation, the PCE database could experience reference table deadlock. This issue is resolved. Transaction processing has been optimized for this type of traffic.
- **Could not rename same policy object by changing letter case** (E-109292)
Names could not be changed from capital to lowercase for the same policy object, creating an issue when the same label names with different capitalizations were used. This issue is resolved.
- **Source and destination labels were missing in visualizations** (E-109189)
Visualizations in the Explore UI could fail to display labels for source and destination policy objects. There was a non-deterministic issue. This issue is resolved.
- **The Reports tab was missing in the UI** (E-109126)
Access Wizard incorrectly indicated that users with Admin roles could access the Reporting page. This issue is resolved.
- **Locked out of Workload details** (E-109125)
You navigate to the workload Detail page by clicking on a managed workload on the List page. If you then navigate back and click on another managed workload, the page should successfully navigate to the Detail page of the second workload. However, navigating back and clicking on the previous workload was not successful. The navigation flow Workload A > List page > Workload B > List page > Workload A did not display the detail page of workload A. This issue is fixed.
- **Workload name and labels were updated when VEN modes changed** (E-109097)
Workload updates in the UI were sometimes producing the wrong data. This issue is resolved. To make sure that no stale data is picked from the UI cache, the UI now makes a fresh API call for data each time the page is edited.
- **The traffic panel in the map showed incomplete results** (E-109090)
The map's visualization traffic panel showed only a subset of the outbound process. This issue is resolved.
- **Version picker options were out of order on the VEN list page** (E-108953)
Version picker options in the VEN list were not sorted. This issue is resolved.
- **Report generation failed for Japanese characters** (E-108799)
Report generation was failing when Japanese characters were entered. This issue is resolved.
- **Service Group did not display more than 50 entries** (E-108500)
Service Group was not displaying more than 50 entries. This issue is resolved. Services are now displayed properly.
- **Traffic from unpaired VENs missing or not available** (E-108243)
The VEN traffic was not available to investigate an issue after a VEN was unpaired. This issue is resolved.
- **SAML ACS URL UI Naming** (E-107290)
The 'Assertion Consumer Service URL' terminology on the IDP configuration page was incorrect. This issue is resolved.
- **Ransomware Dashboard always showed a high Protection coverage score** (E-106996)
The protection coverage score shown in the dashboard and workload summary pages was 100%, even in an environment with no flow data for some time. This issue is resolved.
- **Global Admin unauthorized to update Ransomware "Workloads Requiring Protection"** (E-105756)
When Global Admins attempt to update the "Workloads Requiring Protection" in Ransomware, their action fails. Global Admins are currently not allowed to update this value.

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

When using an empty Label Group as a filter in Explorer or Illumination, the same results were returned as if the filter criteria was "Any Workloads." This issue is now resolved.

- **Mesh re-rendered repeatedly. Interactions were not working** (E-105167)

Hover and brush interactions on Mesh did not work properly, and images were re-rendered repeatedly. This issue is resolved.

- **Proposed Rules - Status information was hidden** (E-105098)

The Proposed Rules status information was hidden by the Ruleset Summary page. This issue is resolved.

- **App Group not showing for Workload Manager** (E-105068)

The workload manager could not see the App Group menu. This issue is resolved.

- **Standalone PCE was not starting up after service_discovery_encryption_key changed** (E-104880)

This issue is resolved. The explanation was added to the PCE Supercluster Deployment Guide in the "Deploy New Supercluster" topic under the section "Verify Supercluster Readiness".

- **UI displayed PCE support bundles by mistake** (E-104708)

UI mistakenly displayed the PCE support bundles as an option under the Troubleshooting menu for the SaaS cluster. This issue is resolved.

Visualizations

- **Visualizations and reports pages were blank when users created a custom time-saved filter in different time zone formats** (E-102528)

This issue is resolved.

- **Reports page displayed with a blank page when upgrading from v22.4.x to v22.5.0** (E-99327)

When users who had two-label app group filters upgraded from 22.4.x to 22.5.0, a JavaScript error caused reports to display as blank pages. This issue is resolved.

UI Components

- **UI Provisioned Policy Versions diff page not displaying full results** (E-110021)

The Policy Versions diff table did not allow users, such as auditors and administrators, to view the full changes that were provisioned for the provisioning event. This issue is resolved.

PCE Platform

- **metrics_database_service not starting** (E-105498)

The service metrics_database_service was not starting. This issue is resolved.

- **Visualization failed with 403 in Microsoft Edge** (E-102491)

When using visualizations, pages would sometimes fail to load with the Microsoft Edge browser. The same pages load only after subsequent attempts. This issue is resolved. The pages now load properly using the Microsoft Edge browser.

- **Occasional async API failures** (E-95932)

The PCE could enter a state where async API calls fail until a PCE restart is performed. This issue is resolved.

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

What's New in LW-VEN Release 1.1.0

The following new feature is added in this release:

Support for flow reporting for legacy Windows servers

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

Release Notes in LW-VEN 1.1

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

Resolved Issues in 1.1.10 LW-VEN

Issue	Description	Status
E-120840	ICMP rule generation created empty command 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	Excessive time needed for Windows firewall to apply Illumio rules 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	Policy conflict lead to policy sync failure and LW-VEN crash 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>LW-VEN activation failed on non-UTF-8 legacy Windows workloads</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>Activate option appeared during "non-fresh" LW-VEN installation</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>Users weren't prompted during LW-VEN activation if activation command was run without options</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>LW-VEN 1.0.1 failed to apply 2008 firewall policy that contained very large port range</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

Illumio Core for Kubernetes Release Notes 5.3

These release notes describe the new features, enhancements, resolved issues, and known issues for the 5.3.x releases of Illumio Core for Kubernetes,

What's New in Illumio Core for Kubernetes 5.3.1

These release notes describe 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.

Product Version

Compatible PCE Versions: 23.5.31 and later

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

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

Release Types and Numbering

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

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

What's New in Release 5.3.1

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

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

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

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

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

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

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

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

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

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

You can now map labels on Kubernetes Workloads to corresponding Illumio labels by using a `workloadLabelMap` section in a label mapping Custom Resource Definition (CRD) within a YAML, in a `kind: LabelMap` declaration. This Kubernetes Workload label mapping is otherwise defined like the existing feature for mapping Kubernetes node (or host workloads) labels to Illumio labels. See [Map Kubernetes Node or Workload Labels to Illumio Labels](#).



CAUTION

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

- **Added Support for hostPort**

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



CAUTION

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

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

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

- **Kubernetes Workloads Show Label Source**

A new `com.ilo.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.

Resolved Issues in 5.3.1

This section provides a list of resolved issues.

Resolved Issues

Issue	Description
E-123084	<p>Kubelink: wrong LabelMap feature flag for older 24.x PCE versions</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>Kubelink: labels defined by Container Workload Profile are ignored when Kubelink restarts</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>Kubelink: skip of ACK of unknown workload causes repeated policy calculations and sets ACK</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>C-VEN 23.4.x fw_tampering_revert_failure after upgrade</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>C-VEN activation failing</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>Kubelink: One service appears multiple times in service update</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>C-VEN: False positive vulnerability detection on Quay</p> <p>The Quay vulnerability scanner falsely detected C-VEN as having high severity vulnerabilities.</p>
E-120773	<p>Increasing memory use and "out of memory errors" occur on 22.5.14 C-VEN nodes</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-VE 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-VE version was reported with a "-dev" string appended (for example, "23.4.0-8-dev") in the PCE UI (at the VE details page) and other locations like in `/etc/agent_version`, but the image specified in the C-VE daemonset resource did not.
- **C-VE: unable to send flows if there is a lot of data** (E-119110)
When C-VE 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-VE 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-VE that disables NodePort forwarding on host workloads. After setting `enforceNodePortTraffic: never` in the Helm values file, C-VE 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-VE

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-VE.
- **Move C-VE base image to a smaller image** (E-118492)
C-VE 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 \[70\]](#).

- **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: (Note that the backslash (\) character is included to indicate the continuation of a long command line that will be truncated by the right margin of this document in PDF form.)

```
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 \[68\]](#)" 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	
Resources		C-VEN	Kubelink	Storage
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	
Resources		C-VEN	Kubelink	Storage
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 \[71\]](#) 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 \[79\]](#)
- [Kubelink \[79\]](#)
- [Security Information for Core for Kubernetes 5.0.0-LA \[80\]](#)

C-VEN

Resolved Issues

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

Known Issues

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

Kubelink

Resolved Issues

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

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

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

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

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

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

Known Issues

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

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

There is no workaround available.

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

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

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

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

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

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

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

No workaround is available.

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

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

There is no workaround available.

Security Information for Core for Kubernetes 5.0.0-LA

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

Illumio Core for Kubernetes Release Notes 4.3.0

What's New in Kubernetes 4.3.0

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

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

Here are the new and changed items in this release:

- **New Kubelink 3.3.1**

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

- **New C-VEN 22.5.14**

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



NOTE

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

Security Information

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

Base Image Upgraded

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

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

Product Version

Compatible PCE Versions: 22.5.0 and later releases

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

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

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

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

Updates for Core for Kubernetes 4.3.0

C-VEN

Resolved Issues

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

Known Issue

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

Kubelink

Resolved Issue

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

Known Issue

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

Illumio Flowlink Release Notes

Illumio Flowlink Release Notes for Release 1.4.0

December 2024

Product Version

Flowlink Version: 1.4.0

Compatible PCE Version: PCE 19.3.0 and later releases

Standard versus LTS Releases

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

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

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

New Features in Illumio Flowlink 1.4.0

The following new features were added in Illumio Flowlink 1.4.0.

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

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

- **Increased buffer size**

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

- **Support for ingesting multiple flow types**

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

Resolved and Known Issues in FlowLink 1.4.0

Resolved Issue

Flowlink became non-responsive (E-114431)

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

Known Issue

No Automatic Restart Following Reboot (E-15146)

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

Illumio Flowlink Release Notes 1.3.0

Product Version

Flowlink Version: 1.3.0

Compatible PCE Version: PCE 19.3.0 and later releases

Standard versus LTS Releases

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

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

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

New Feature in Flowlink 1.3.0

Support for HTTP/HTTPS Proxy

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

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

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

See the following example of Flowlink YAML configuration file:

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

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

Resolved Issue in Flowlink 1.3.0

The following security issue was resolved in this release:

go-lang upgraded to 1.19.11 (E-107998)

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

Illumio Flowlink Release Notes 1.2

Welcome

These release notes describe the enhancements, resolved, and known issues for Illumio FlowLink 1.2.x releases.

Document Last Revised: August 2023

Document ID: 28000-100-1.2.3

Product Version

FlowLink Version: 1.2.3

Compatible PCE Version: 23.3.0 (Standard) and earlier.

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”

What's New in FlowLink Release 1.2.3

This release provides no new features. Illumio made some changes for security purposes (see Security Information below).

Security Information

go-lang upgraded to 1.19.11 (E-107998)

The go-lang package was upgraded to 1.19.11 to address:

- CVE-2023-29406

What's New in FlowLink Release 1.2.2

This release provides no new features. Illumio made some changes for security purposes (see Security Information below).

Security Information

go-lang upgraded to 1.19.0 (E-106453)

The go-lang package was upgraded to 1.19.10 to address:

- CVE-2023-29405
- CVE-2023-29404
- CVE-2023-29403
- CVE-2023-29402
- CVE-2023-29400
- CVE-2023-24540
- CVE-2023-24539

What's New in FlowLink Release 1.2.1

This release provides no new features. Illumio made some changes for security purposes (see Security Information below).

Security Information

go-lang upgraded to 1.19.8 (E-104330)

go-lang has been upgraded to 1.19.8 to address:

- CVE-2022-41725
- CVE-2022-41724
- CVE-2022-41723
- CVE-2022-41717
- CVE-2023-24538

- CVE-2023-24537
- CVE-2023-24536
- CVE-2023-24534
- CVE-2023-24532

What's New in FlowLink Release 1.2.0

FIPS Compliance

Support for Federal Information Processing Standard Publication (FIPS). FIPS (FIPS PUB) 140-2 is a U.S. government computer security standard used to approve cryptographic modules.

Resolved Issue in FlowLink 1.2.0

FlowLink crashed when pushing NetFlow v9-formatted traffic flow data from Fortinet devices (E-95072)

When attempting to push NetFlow v9-formatted traffic flow data from Fortinet devices, FlowLink stopped processing data and the error message "unexpected EOF" appeared. The issue was caused by incorrect handling of padding bytes in the NetFlow v9 template record. This issue is resolved.

Illumio Flowlink Release Notes 1.1.2

Welcome

These release notes describe the enhancements, resolved, and known issues for the Illumio FlowLink 1.1.x release.

Document Last Revised: April 2021

Document ID: 28000-100-1.1.2

Product Version

FlowLink Version: 1.1.2+H2

Compatible PCE Version: 21.1.0 (Standard), 20.2.0 (Standard), 20.1.0 (Standard), 19.3.x (LTS)

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 FlowLink 1.1.2+H2

- **FlowLink encountered a fatal error** (E-77177)

Further investigation of this issue uncovered that FlowLink could still encounter the fatal error. While processing reported IPs in sFlow data, FlowLink could experience a race condition due to simultaneous update and read operations of the `reportedIps` table. This issue is resolved. The race condition no longer occurs which caused FlowLink to stop responding and close.

Resolved Issues in FlowLink 1.1.2+H1

- **FlowLink printed error messages when parsing sFlow data** (E-77019)

When parsing sFlow data, FlowLink continuously wrote the following errors to the `flow-link.log`, causing the log to fill:

```
2021-03-16T22:21:10.038051-07:00 Error: unexpected EOF
```

```
2021-03-16T22:21:10.038120-07:00 Line: /usr/local/bin/flowlink/sflow_collector.go:742
```

```
2021-03-16T22:21:10.052053-07:00 Error: unexpected EOF
```

```
2021-03-16T22:21:10.052102-07:00 Line: /usr/local/bin/flowlink/sflow_collector.go:750
```

```
2021-03-16T22:21:10.052053-07:00 Error: unexpected EOF
```

```
2021-03-16T22:21:10.052102-07:00 Line: /usr/local/bin/illumio/flowlink/sflow_collector.go:758
```

This issue is resolved. FlowLink no longer continuously writes these errors to the `flow-link.log`.

- **FlowLink encountered a fatal error** (E-77177)

While processing reported IPs in sFlow data, FlowLink encountered the following fatal error:

```
fatal error: concurrent map read and map write
```

The fatal error caused FlowLink to stop responding and close. This issue is resolved. FlowLink is no longer affected by this fatal error, which caused it to stop responding and close.

Enhancement in FlowLink 1.1.2

Newly Discovered IP Addresses Displayed

Previously, you did not know which unmanaged workloads you may need to create because you did not know which IP addresses FlowLink was reporting to the PCE. From the FlowLink 1.1.2 release onwards, every time FlowLink sends flow data to the PCE, it reports the newly discovered IP addresses in its log.

Resolved Issue in FlowLink 1.1.2

- **FlowLink was storing zero byte data file and not sending the data** (E-70217)

FlowLink was storing a zero byte data file. It was not sending the data with a response code 403 from the PCE. This issue is resolved and a zero length traffic flow file is not created in the data directory.

Resolved Issue in FlowLink 1.1.1+H2

- **FlowLink time format incompatibility with IPFix on NetScaler** (E-70139)

FlowLink was incompatible with the time format used by IPFix on NetScaler, which led to traffic processing errors on the PCE. This issue is resolved.

Resolved Issues in FlowLink 1.1.1+H1

- **Compatibility issues with NetFlow V9 and V10/IPFix formats** (E-69173)

NetFlow V9 and V10/IPFix formats failed to handle timestamps information in the 150-156 fields types correctly and that caused FlowLink to crash . This issue is resolved.

- **FlowLink data not displayed in Explorer** (E-69016)

Due to incorrect (future) timestamps being assigned, data flows were not being displayed in Explorer. This issue only affected flows generated by NetFlow V5 and V7 and is resolved.

Resolved Issue in FlowLink 1.1.1

- **Unable to install FlowLink on RHEL 6.10** (E-68015)

Installing the FlowLink RPM on RHEL 6.10 would fail and display an error. This issue is resolved and FlowLink can be successfully installed.

Resolved Issue in FlowLink 1.1.0+H1

- **sFlow traffic not displayed in Illumination** (E-65899)

The FlowLink application relies on sFlow to provide network traffic flow data for Illumination. FlowLink received sFlow events that it did not handle correctly and caused the traffic handler to crash. This issue is resolved and sFlow traffic is now visible in Illumination.

Illumio NEN Release Notes

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 2.6.40

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.

Resolved Issues in NEN 2.6.40

Issue	Description
E-119690	<p>NEN setup command failed and 'unknown property' error thrown</p> <p>After the user configured the <code>proxy_config</code> entry in the <code>runtime_env</code>, the <code>illumio-nen-env set-up</code> command failed with an 'unknown property' error.</p>
E-119644	<p>NEN activation failed and SSL error thrown</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>Not all Virtual IPs appeared on the PCE</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 time-outs.

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 NEN Release Notes 2.3

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](#)

About This Document

These release notes describe the resolved and known issues for the Network Enforcement Node (NEN) 2.3.x releases.

The NEN is the Illumio Core switch and Server Load Balancer (SLB) interface that provides visibility and enforcement on switches and SLBs.

See the NEN Installation and Usage Guide for information.

Product Version

NEN Version: 2.3.10

Compatible PCE Versions: 21.5.10 (LTS Candidate), 21.5.2 (Standard), 21.5.1 (Standard), 21.4.1 (Standard)

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).

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”
- “+e”: Hot Fix release descriptor, for example “+H1”, “+H2”, “+H3”.

What's New In This Release

To learn what's new and changed in this and earlier NEN releases, see *What's New in The Releases* in the latest NEN Installation and Usage Guide.

Resolved Issues in NEN 2.3.10

- **Network enforcement log showed exception when switching from node 2 to the primary node** (E-85609)
On the NEN server, in the network_enforcement.log, an error was shown with an exception message when switching from Node 2 to the primary node. This issue is resolved.
- **Deleting VS policy from the F5 might leave AS3 declare in an unstable state** (E-85489)
When deleting a VS policy from the F5, the code ignored the response from the AS3 PATCH command and deleted the policy. However, if the AS3 declare PATCH failed, this left the system in a state where subsequent AS3 PATCH commands failed due to an inconsistency with the AS3 declare and the state of the F5. This caused the policy to not be applied. This issue is resolved.
- **Failed to apply policy to a virtual server after NEN upgrade** (E-85412)
A policy change could generate a 409 error. Policy for the virtual server would then fail to update. This happened because during policy changes, the PCE failed to detect and

correct of out-of-sync F5 AS3 declarations and virtual server configuration. The NEN would therefore try to create a policy that already existed. This issue is resolved. A subsequent tamper check fixes the policy for the virtual server.

- **NEN logs DEBUG info in prod level** (E-85363)

The NEN was not setting the default log level for the production environment correctly, causing DEBUG information to be logged into the `network_enforcement` log.

This issue is resolved and the NEN now works as expected.

- **Some NEN logs should be at debug level** (E-85341)

Some logs were growing very large (over 5GB) in a very short time because policy information was mistakenly added to the logs.

This issue is resolved so that some parts of that information are added at DEBUG log level instead of INFO log level, while some parts (such as PNports info) are not added to the log.

- **Discovery loop not working on NEN 2.2.0 in production environment** (E-85307)

The discovery job was sometimes not working properly. It did discovery, but for only one SLB. The symptom was increased Ruby gems errors in logs. The issue was caused by an insufficient number of database connections in the pool. The issue is resolved. The default number of connections in the database pool is increased from 4 to 50.

- **NEN health status could display incorrect cluster status** (E-85301)

Running the `illumio-nen-ctl health` command could provide incorrect information for the NEN HA cluster in the Cluster Mode field. For example, the command output could incorrectly display "Standalone (split brain)" when the NEN service on one of the nodes was stopped. The field should have displayed "Standalone (failover)." This issue is resolved and the Cluster Mode field now displays the correct information.

- **NEN - Failover not working if NEN primary freezes** (E-85256)

The NEN primary node could stop logging unexpectedly because of an unforeseen event such as a full disk. The lack of logs made the node appear frozen, but the NEN was still running, so the NEN secondary node did not take over. However, if the disk on the primary node got full and caused the database and node to fail, the primary node would fail, and then failover to the secondary node would occur. This issue is resolved. To address the disk full issue and the lack of logging, if a disk gets 95% or more full, the node will now be stopped, and the NEN fails over to the other node.

- **NEN didn't delete empty iRule and create a new non-empty rule** (E-85211, E-84872)

iRules are a feature within the F5 BIG-IP local traffic management (LTM) system. An iRule can become empty due to tampering. If the NEN detects that an iRule is empty, it's supposed to delete it and then create a new non-empty rule. In this case, the NEN failed to delete the empty iRule and create a new non-empty rule. This issue is resolved.

- **Policy updates and tampering check weren't working** (E-85197)

When the NEN service on the primary node of a NEN HA cluster was stopped, the secondary NEN node did not apply policy updates that the primary node was processing when the primary node failed. This issue is resolved. The secondary NEN node now correctly applies the policy updates from the primary node when it failed over.

Known Issues in NEN 2.3.10

There are no known issues in this release.

Resolved Issues in NEN 2.3.0

NEN 2.3.0 was a Limited Availability (LA) release. However, these issues are also resolved in NEN 2.3.10.

- **PCE and NEN became stuck in a provisioning loop** (E-84712)

Implementing an actor-only policy change caused a provisioning loop in which the PCE continually sent the same policy to the NEN which in turn applied it continually to the F5 SLB. The loop was reported in the `network_enforcement` log and F5 logs. This problem occurred because actor-only policy changes lack a rule version and NENs don't store or acknowledge policy changes that lack a rule version. This issue is fixed. Now, NENs that receive actor-only policy changes use the last-stored rule version from their database, allowing these NENs to acknowledge such policy changes to the PCE.

- **Full policy update not performed on tampered DVSs** (E-84614)

When a NEN was triggered to perform a tampering check on Discovered Virtual Servers (DVS), a full policy update didn't occur and only the address list was updated. This issue is fixed: tampered DVSs now receive a full policy update.

- **Maximum number of auth tokens exceeded** (E-84573) The error *maximum active login tokens* occurred when too many F5 authentication tokens were generated in a 20 minute period. Prior to this fix, a new F5 authentication token was generated whenever a Discovered Virtual Server (DVS) was unprogrammed (for example, when its status changed to unmanaged) or was reprogrammed (for example, when it was identified as tampered). This issue is fixed. NENs now use a single token for these actions.

- **Primary NEN node would hang in some cases** (E-84111)

A logging problem that occurred in the `network_enforcement` service caused the primary NEN node in an HA cluster to hang, which was subsequently not recognized by the secondary NEN node. This issue is fixed. The primary NEN node can now tolerate logging issues that occur during the `network_enforcement` service and the Secondary NEN node now recognizes when the Primary node hasn't sent its status to the PCE for 3 minutes.

Illumio Core PCE CLI Tool Guide

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.

Security Advisories

This category includes announcements of security fixes and updates made in critical patch update advisories, security alerts and bulletins.

September 2024 Security Advisories

Here's a list of the security advisories for 2024.

Ruby SAML gem component authentication bypass vulnerability

The Ruby SAML gem is affected by an authentication bypass vulnerability, which impacts the Illumio PCE in both SaaS and on-premises deployments. An authenticated attacker could potentially leverage this vulnerability to authenticate as another SAML user. For SaaS customers, the target user can be in a different org and on a different cluster.

Severity

Critical: CVSS score is 9.9

CVSS: AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Affected Products and Patch Information

Security vulnerabilities addressed by this Security Alert affect the products listed below.

Table 4. Products Affected by the Security Vulnerability

Affected Products	Affected Versions	Fixed Version
Illumio Core PCE	<= 21.5.36	>= 21.5.37
	<= 22.2.42	>= 22.2.43
	<= 22.5.32	>= 22.5.34
	<= 23.2.30	>= 23.2.31
	<= 23.5.21	>= 23.5.22
	<= 24.2.0	>= 24.2.10

Resolution

Upgrade to the latest release for a given major version.

References

- <https://nvd.nist.gov/vuln/detail/CVE-2024-45409>
- <https://github.com/advisories/GHSA-jw9c-mfg7-9rx2>

Skipped Critical Patch Updates

Illumio strongly recommends that customers apply security patches as soon as possible. For customers that have skipped one or more Critical Patch Updates and are concerned about products that do not have security patches announced in this Critical Patch Update, please review previous Critical Patch Update advisories to determine appropriate actions.

Discovered By

External Security Firm

Frequently Asked Questions

- What software components are affected?
Only the Illumio PCE is impacted by this vulnerability.
- What products did this affect?
This vulnerability impacts the PCE, including Core on-premises deployments, Core SaaS, Endpoint, MSP, and Edge.
- Is Core SaaS affected?
SaaS PCE clusters were impacted. Those environments have been patched.
- I'm using Cloud. Am I impacted?
The Cloud platform is not affected.
- Will the patch affect performance?
The update is not expected to affect performance.
- How can I tell if this vulnerability was used against my on-premises PCE?
Illumio is creating queries that can be used by customers to detect known vectors for exploitation of this vulnerability. Please contact Illumio Support or your account team for assistance. If you suspect this vulnerability was used within your environment, please reach out to Illumio Support.
- Has Illumio investigated if this vulnerability was used on any SaaS PCEs?
Illumio is currently investigating all available data from the production SaaS environment and has so far found no indications that the issue has been exploited.
- I can't apply the patch immediately. How can I mitigate the issue in the meantime?
This vulnerability requires SAML to be enabled on the customer's PCE in order to be exploited. Customers who cannot patch their PCEs immediately, and who wish to mitigate this issue, can choose to disable SAML authentication on the PCE. For details, see the "Authentication" topic in the PCE Administration Guide. Additionally, customers can enable IP restrictions to limit access to only trusted source IPs (for example, for privileged accounts). For details, see the "Configure Access Restrictions and Trusted Proxy IPs" topic in the PCE Administration Guide.
- How long will the upgrade take?
The fix will be provided in a normal code release so this will take the same amount of time as any PCE upgrade.
- Were any Illumio customers impacted by this vulnerability?

Illumio is not aware of any exploitation of this vulnerability within any customer environments.

Modification History

- September, 2024: Initial Publication of CVE

September 2023 Security Advisories

Here's a list of the security advisories for 2023.

Authenticated RCE due to unsafe JSON deserialization

Unsafe deserialization of untrusted JSON allows execution of arbitrary code on affected releases of the Illumio PCE. Authentication to the API is required to exploit this vulnerability. The flaw exists within the network_traffic API endpoint. An attacker can leverage this vulnerability to execute code in the context of the PCE's operating system user.

Severity

Critical: CVSS score is 9.9

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Affected Products and Patch Information

Security vulnerabilities addressed by this Security Alert affect the products listed below.

Table 5. Products Affected by the Security Vulnerability

Affected Products	Affected Versions	Fixed Version
Illumio Core PCE	<= 19.3.6	>= 19.3.7
	<= 21.2.7	>= 21.2.8
	<= 21.5.35	>= 21.5.36
	<= 22.2.41	>= 22.2.42
	<= 22.5.30	>= 22.5.31
	<= 23.2.10	>= 23.2.11

Resolution

Upgrade to the latest release for a given major version.

References

<https://www.cve.org/CVERecord?id=CVE-2023-5183>

Skipped Critical Patch Updates

Illumio strongly recommends that customers apply security patches as soon as possible. For customers that have skipped one or more Critical Patch Updates and are concerned about products that do not have security patches announced in this Critical Patch Update, please review previous Critical Patch Update advisories to determine appropriate actions.

Discovered By

External Security Firm

Frequently Asked Questions

- What software components are affected?
Only the Illumio PCE is impacted by this vulnerability.
- What products did this affect?
This vulnerability impacts the PCE, including Core on-premises deployments, Core SaaS, Endpoint, MSP, and Edge.
- Is Core SaaS affected?
SaaS PCE clusters were impacted. Those environments have been patched.
- I'm using Cloud. Am I impacted?
The Cloud platform is not affected.
- How can I tell if this vulnerability was used against my on-premises PCE?
Illumio is creating queries that can be used by customers to detect known vectors for exploitation of this vulnerability. Please contact Illumio Support or your account team for assistance. If you suspect this vulnerability was used within your environment, please reach out to Illumio Support.
- Has Illumio investigated if this vulnerability was used on any SaaS PCEs?
Illumio is currently investigating all available data from the production SaaS environment and has so far found no indications that the issue has been exploited.
- I can't apply the patch immediately. How can I mitigate the issue in the meantime?
This vulnerability requires SAML to be enabled on the customer's PCE in order to be exploited. Customers who cannot patch their PCEs immediately, and who wish to mitigate this issue, can choose to disable SAML authentication on the PCE.
- Reference
For details, see the topic Authentication in the PCE Administration Guide.
Additionally, customers can: Enable IP restrictions to limit access to only trusted source IPs (for example, for privileged accounts). For details, see the topic Configure Access Restrictions and Trusted Proxy IPs in the PCE Administration Guide.

- How long will the upgrade take?
The fix will be provided in a normal code release so this will take the same amount of time as any PCE upgrade.
- Were any Illumio customers impacted by this vulnerability?
Illumio is not aware of any exploitation of this vulnerability on any customer environments.

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](#)