



# Illumio<sup>®</sup> Core

Version 23.5.21

## Release Notes

06/07/2024

14000-100-23.5.21

# Contents

- Welcome..... 3**
  - What's New in This Release.....3
- Product Version ..... 3**
- Resolved Issue in Release 23.5.21..... 3**
- Resolved Issues in Release 23.5.20..... 4**
  - Enterprise Server ..... 4
  - Containers.....5
  - VEN .....5
  - VEN Known Issue..... 6
  - Security Information..... 6
- Resolved Issues in Release 23.5.10..... 6**
  - Enterprise Server ..... 6
  - PCE Platform ..... 8
  - UI Components..... 8
  - VEN ..... 9
- Resolved Issues in Release 23.5.1 ..... 9**
  - Enterprise Server ..... 9
  - Visualizations.....12
  - UI Components.....12
  - PCE Platform .....12
- Known Issues in Release 23.5.20 ..... 13**
  - Enterprise Server .....13
  - Data Visualization.....13
  - PCE Platform .....14
  - VEN .....14
  - Security Information.....14
  - Legal Notices.....15

## Welcome

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

- 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 customers.

**Document Last Revised:** June 2024

**Document ID:**14000-100-23.5.21

## What's New in This Release

To learn what's new and changed in 23.5.x, see the [What's New in This Release](#) guide.

## Product Version

**PCE Version:** 23.5.21 (on-premises)

### 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, "23.5"
- ".c": Maintenance release number, for example, ".10"
- "-d": Optional descriptor for pre-release versions, for example, "preview2"

## 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 23.5.20

### 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 release 7.0.8.1 and 6.1.7.7. and this issue will not be addressed.
- **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_fowarding_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 (unpaired/paired) while there were Kubernetes Workloads already present.

## VEN



These notes apply to VEN 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 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

 This note applies to VEN 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 NA (E-144939)**  
json-jwt-1.13.0.gem upgraded to NA to address CVE-2023-51774. This CVE did not impact Illumio PCE.

## Resolved Issues in Release 23.5.10

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

## Enterprise Server

- **Sudo access for ilo-pce (E-113745)**  
This issue is fixed, and the command ilo-pce does not require `sudo` access.
- **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/processes 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** (EYE-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 a 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 (EYE-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

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 distributed 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"** (EYE-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 appgroup 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** (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.

## Known Issues in Release 23.5.20

### 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 Illumination.
- **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 "deletion 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 workload from the FQDN panel** (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.  
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 results** (E-102742)  
The maximum connection number in Explorer gets updated to the same maximum number as

the update in Illumination Plus. However, the maximum number in Illumination Plus is 10,000, while in Explorer, it is 100,000.

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

- **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.

## 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.

## 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.

- **cgi-0.3.2.gem upgraded to v0.3.6**  
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.

## Legal Notices

Copyright © 2024 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.