TECHNICAL
DOCUMENTATION

Illumio Core What's New and Release Notes 23.2

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

Table of Contents

Whats New

Welcome to the New Illumio Experience

Illumio is excited to announce a new user interface for Illumio Core Cloud 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

In Core 23.2.20, Illumio is deprecating 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 23.2.20, Illumio is strongly encouraging customers 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. At a release in the near future, Illumio will remove the classic PCE UI from the Core product. Illumio will provide notice before the end-of-life of the classic UI.

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.
- Adopt the new Illumio experience at your own pace because the PCE UI supports quickly switching between the New and Classic PCE UI.

Enabling the New Experience

Illumio values the customer experience; therefore, it's extremely important to us that current customers can continue to work with a user experience they are familiar and comfortable with.

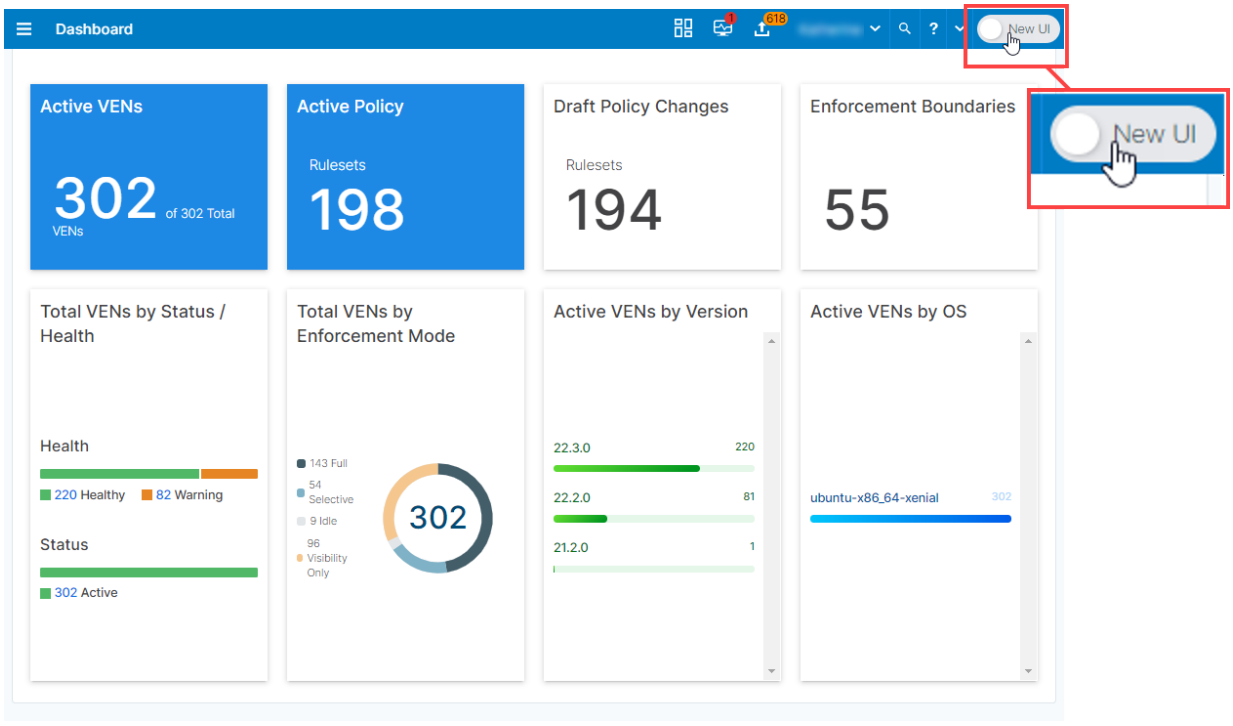
Current Illumio Core Cloud customers control the pace at which they adopt the New PCE UI. By default, current customers see the Classic PCE UI when they log in.

NOTE

If you are a new Illumio Core Cloud customer, the PCE displays the New UI experience by default. You still have the option to explore the Classic UI by using the UI toggle.

The PCE Dashboard appears and includes a prominent switch to open the New PCE UI. Customers can enable the New UI from any page within the PCE UI.

To enable, flip the New UI toggle in the top right corner of the UI:



Because the toggle is available from any page within the PCE UI, customers can switch back to the Classic UI at any point in their workflow to return to a familiar user experience. When toggling between UIs, the PCE remembers your location in the UI and opens the corresponding page in the other UI.

For example, you are in the New UI creating a ruleset. You've just saved the rule but want to return to the Classic UI to review the new rule using the UI you are comfortable with. Toggle the New UI switch off and the PCE UI refreshes, still displaying the Ruleset page in the Classic UI with the same information as the New UI. It even includes the banner informing you that you are viewing draft policy and prompts you to provision the addition.

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 appears as a hamburger menu, which you click to display, and select fly-out sub-menus to locate the features you need. 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:

(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.

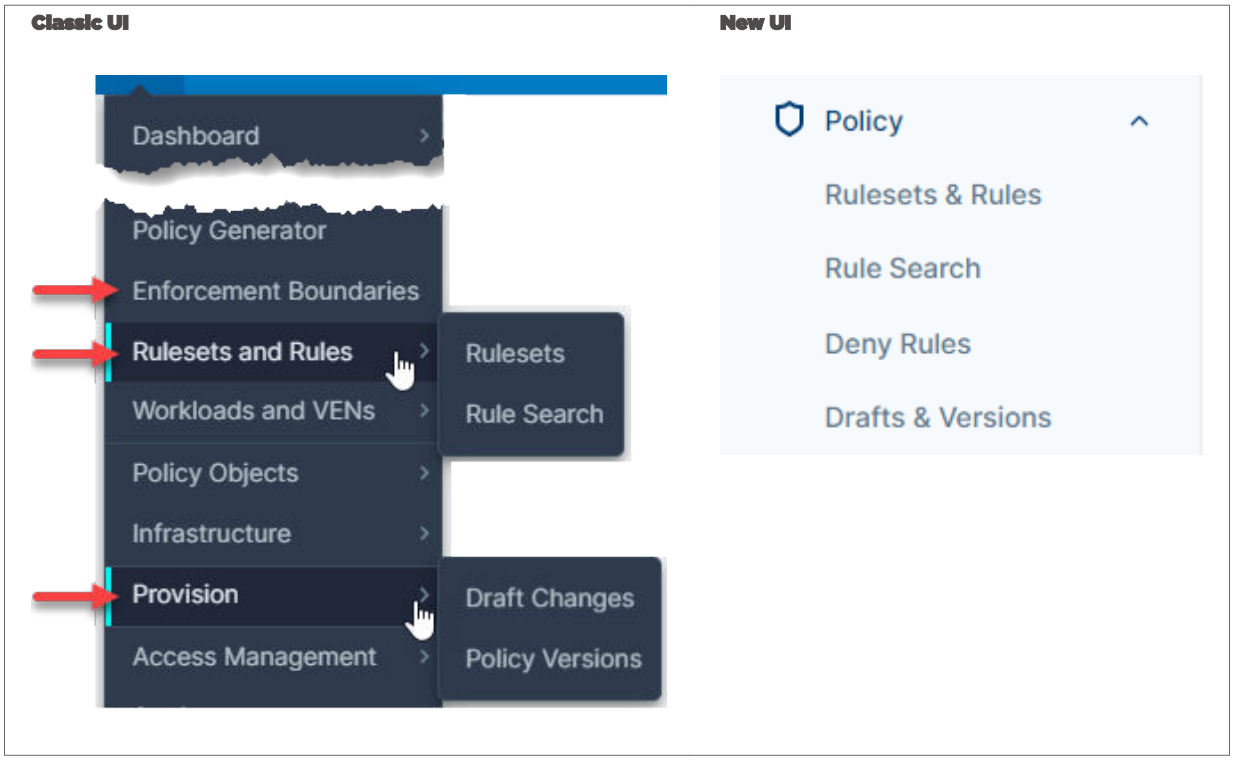
(5) Collapse the navigation to display only the icons. Navigation is always present but takes little room from displaying the feature page.

Navigation Changes at a Glance

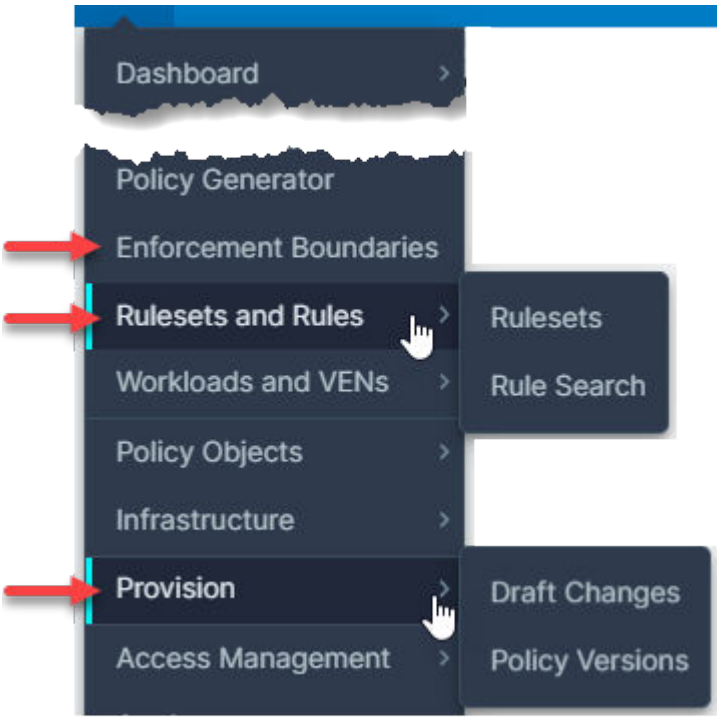
The PCE UI navigation redesign focused on surfacing common tasks and aiding discoverability. Consequently, key categories are renamed and reorganized in the New UI.

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.

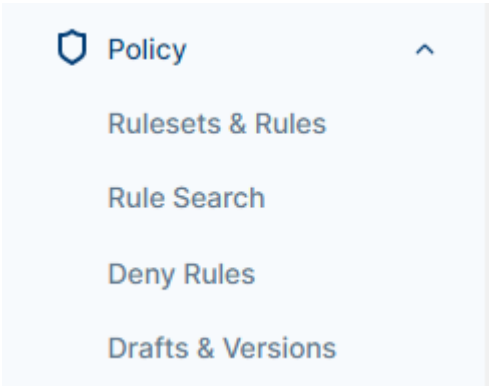
Categories used by Illumio users for creating policy, visualizing the managed environment, and working with devices (servers and endpoints) were the most impacted. The New UI now includes the Policy category, under which the essential tasks for creating and managing policy appear.



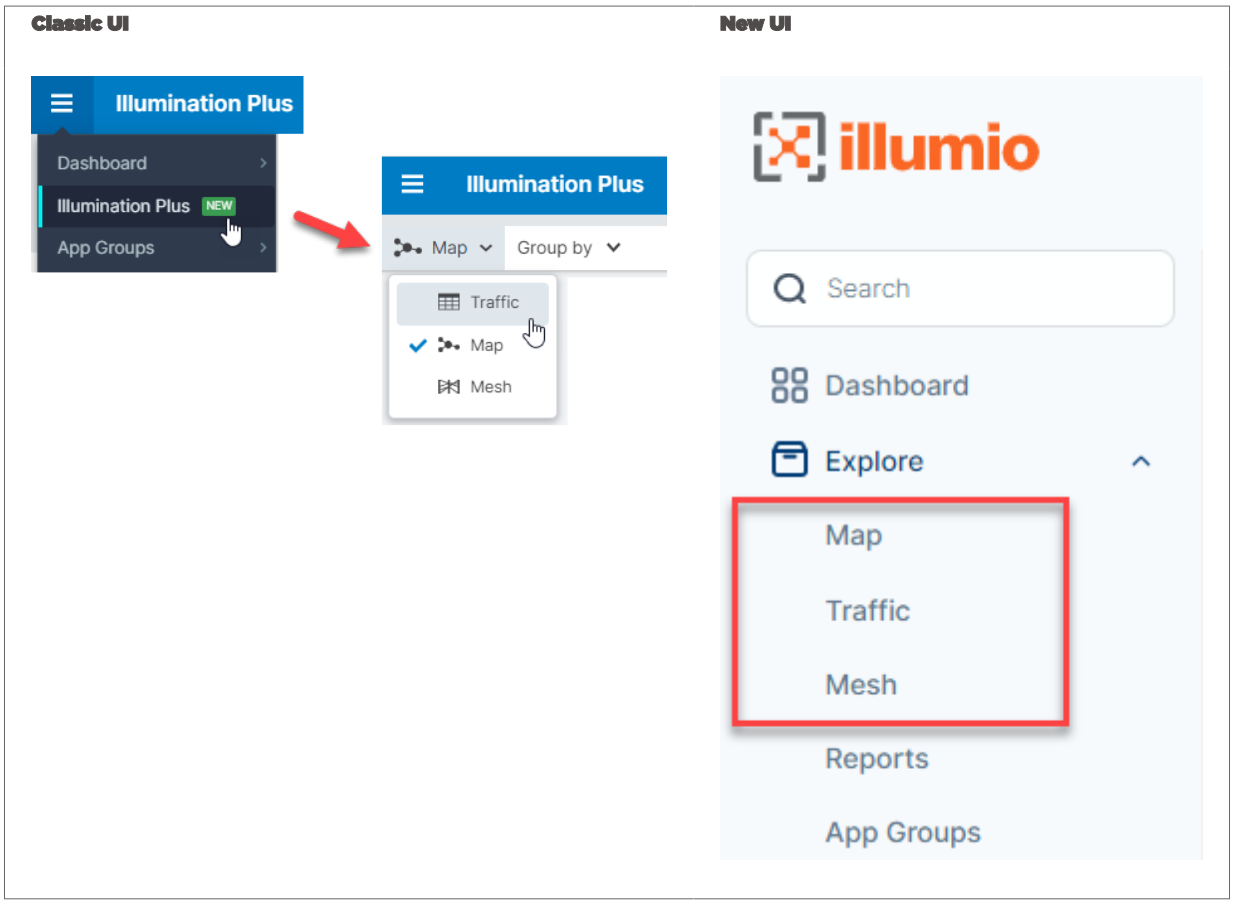
Classic UI



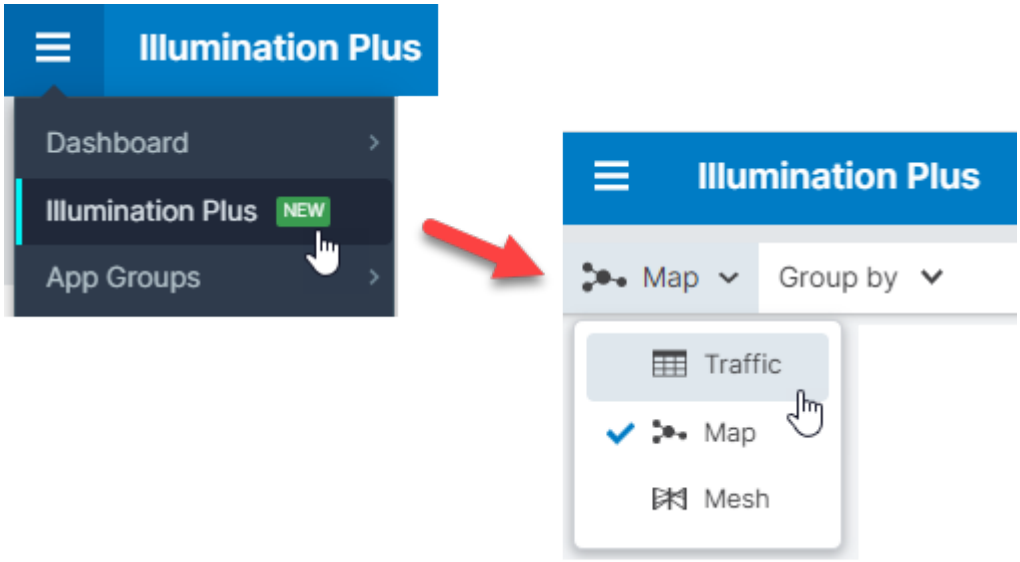
New UI



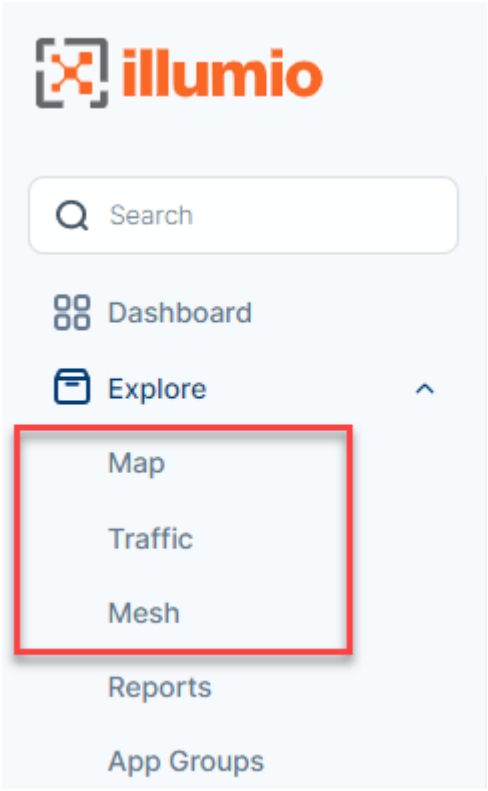
The New UI also centralizes all tasks related to visualization under the new Explore category. The Illumination Plus views (Map, Traffic, and Mesh) are easily accessible in the Explore category:



Classic UI

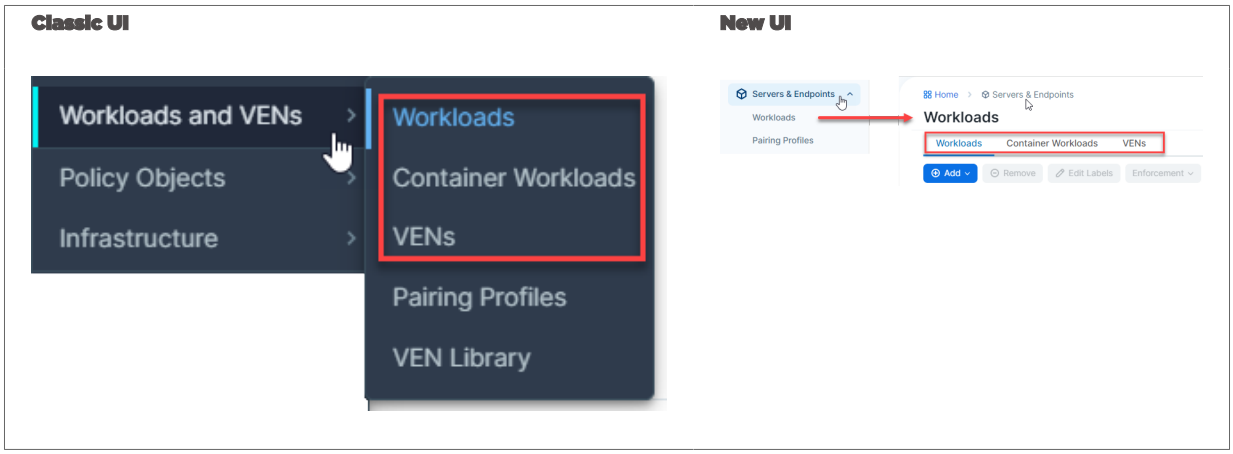


New UI

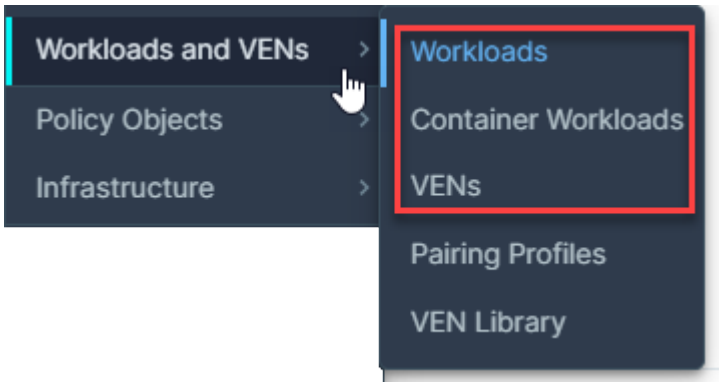


The **Workloads and VENs** category from the Classic UI is simplified and renamed in the New UI.

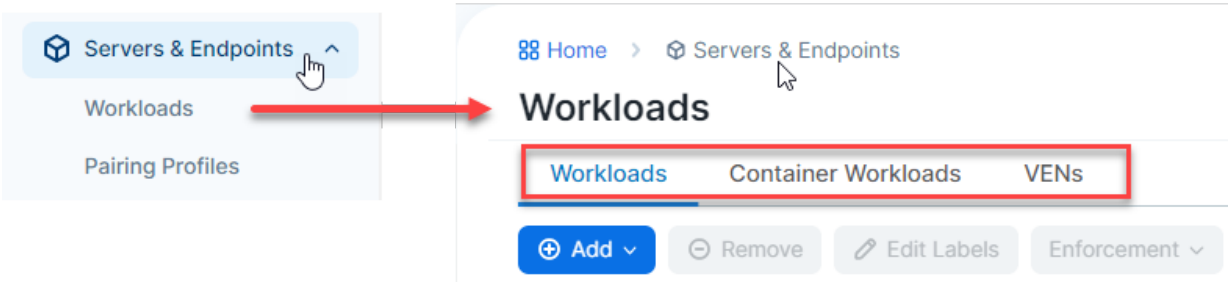
Historically, Illumio PCE UI has referred to server workloads as simply "workloads" and endpoint workloads as simply "endpoints." The Classic UI navigation labeled this category using Illumio-specific terminology, namely "workload." The New UI clarifies this category by using terms customers are most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



Classic UI



New UI



Full Navigation Comparison between UIs

The following table compares the navigation between the two UIs in Core 23.2.0.

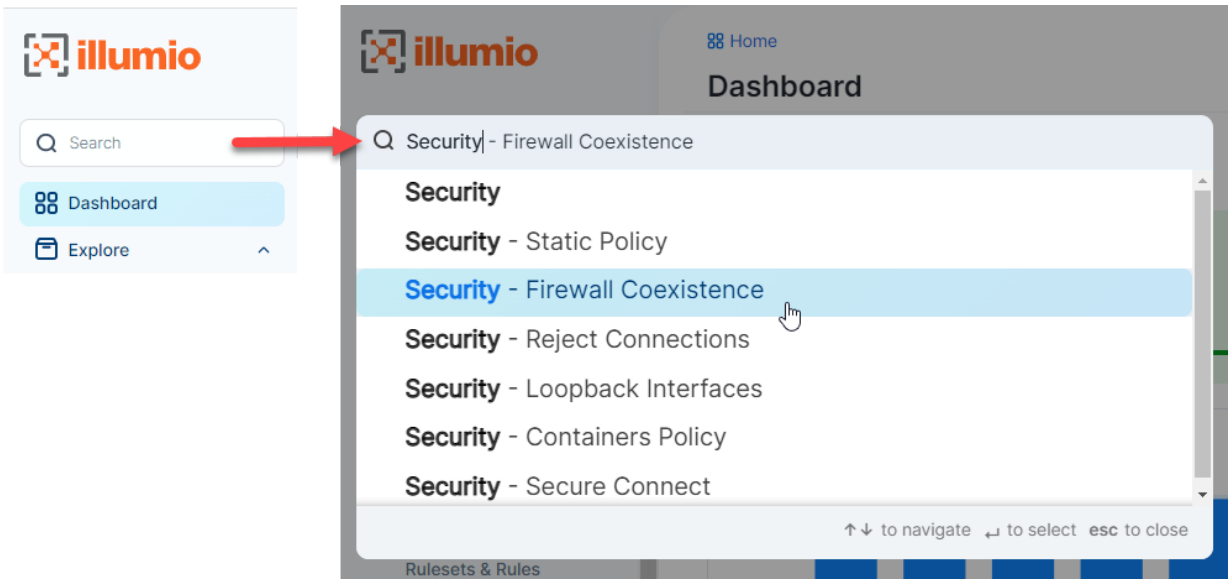
(Expand this section to see the full table)

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

We're also introducing 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.

Full List of Changed Terms

22.5.x	23.2.0 Classic UI	23.2.0 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

In Core 23.2.0, the New UI deprecates the following features:

- Illumination Classic
- Explorer
- Policy Generator
- Segmentation Templates

NOTE

These features 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 included 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.

In Core 23.2.0, the availability of Illumination Classic remains in the Classic UI. We strongly encourage customers to experience all the new visualization functionality in Illumination Plus (Classic UI) and in the Explore category (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 is available in the Table view and Mesh view in Illumination Plus.

However, the original Explorer feature does not support the new Illumio Core 22.5 flexible label types feature, 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 Table view and Mesh view in Illumination Plus (Classic UI) or the Traffic and Mesh pages under Explore (New UI).

In Core 23.2.0, the availability of Explorer remains in the Classic UI. We strongly encourage customers to experience all the new visualization functionality in Illumination Plus (Classic UI) and in the Explore category (New UI).

Policy Generator

In Core 23.2.0, the availability of Policy Generator remains in the Classic UI.

Segmentation Template

In Core 23.2.0, the availability of the Segmentation Template remains in the Classic UI.

What's New and Changed in This Release

Before upgrading to Illumio Core 22.5, 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 Release 23.2.32

Illumio Core 23.2.32-PCE LTS Maintenance Release

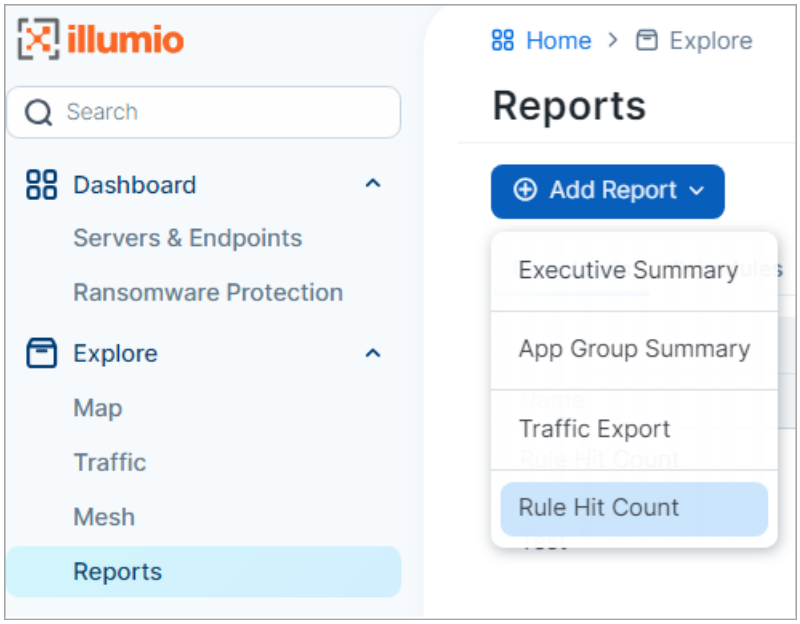
Illumio Core 23.2.32 includes an updated version of the PCE software. Illumio provides regular maintenance updates for reported bugs and security issues, and to add support for new operating system versions. As a maintenance release, Illumio Core 23.2.32 solved software and security issues for the VEN to refine the software and improve its reliability and performance. For details see Resolved Security Issue in 23.2.32-PCE [61].

What's New and Changed in Release 23.2.30

The following new features were added in Illumio Core 23.2.30.

Changes in Release 23.2.30-VEN

Support for Rule Hit Count Report



When paired with the SaaS and On-prem PCEs listed below, VEN-23.2.30 supports creating a Rule Hit Count Report through the PCE UI or through the Illumio REST API.

PCE Version:

- **SaaS:** Core 24.2.0 or later
- **On-prem:** Core 23.5.10 or later

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

Support for Endpoint VENs on macOS Sonoma 14.5

With this release, Endpoint VENs now support macOS Sonoma 14.5. This adds to Endpoint VEN's existing support for all earlier versions of macOS Sonoma.

VEN Support Bundle Improvement

To aid troubleshooting, the VEN Support Bundle now includes the `show-proxy` command to check if a proxy is configured and collect proxy settings. To execute, issue:

```
ven-ctl show-proxy
```

Expanded VEN Support for Interface Types

This release addresses an issue where the VEN may not have reported interfaces to the PCE interfaces if their *Media Type* was `NdisMediumIP` and their *Interface Type* was anything other than `IF_TYPE_TUNNEL`. Now the VEN reports all `NdisMediumIP` interfaces regardless their interface type.

What's New and Changed in Release 23.2.22

The following new features were added in Illumio Core 23.2.22.

Illumio Core 23.2.22-VEN Maintenance Release

Illumio Core 23.2.22 includes an updated version of the VEN software.

Illumio provides regular maintenance updates for reported bugs and security issues, and to add support for new operating system versions. As a maintenance release, Illumio Core 23.2.22 solved software and security issues for the VEN to refine the software and improve its reliability and performance.

Changes in the Release 23.2.22

Support for Endpoint VENs on macOS Sonoma, 14.0, 14.1, and 14.2

Beginning with VEN release 23.2.22, Endpoint VENs are now supported for use on macOS Sonoma, versions 14.0, 14.1, and 14.2.

Support for CRI-O API on C-VENs

In addition to existing support for v1alpha2, C-VENs now support CRI-O API version v1.

AIX VEN Installation with Pairing Script

When installing a new AIX VEN, you can now use a pairing script and the VEN Library in the PCE. Previously, AIX VENs could be installed only from the command line using the CLI.

Because the `curl` utility is not available by default on AIX platforms, you must first install `curl` from the AIX Toolbox for Open Source Software in order to use this feature. Download the AIX Toolbox at https://www.ibm.com/support/pages/node/883796. It may be necessary to set the environment variable `CURL_CA_BUNDLE=/var/ssl/certs/ca-bundle.crt`.

AIX VEN Upgrade from PCE

When upgrading AIX VENs, you can now upgrade one or more VENs by using the PCE web console and the VEN library.

VEN Tampering Protection Support Extended to macOS Endpoints

The VEN tampering production feature has been extended in this release to include protection for macOS endpoints.

VEN Proxy Support Extended to macOS Endpoints

In this release, VEN proxy support is extended to macOS Endpoints.

VEN Support for Red Hat 5

In Core 23.2, Illumio provides support to run the VEN on the Red Hat 5 OS. This support is only for VENs at release 23.2 or later.

Enhancements for VEN Type During Activation

In this release, Illumio has enhanced the VEN so that the VEN displays activation failure reasons in VEN CLI.

In previous releases, the VEN CLI did not display errors in the following situations:

- When you specified the Endpoint mode via the `--endpoint true` option to pair a VEN while using a pairing profile for a server
- When you used a server pairing profile to install the VEN on a macOS endpoint
- When you used an endpoint pairing profile to install the VEN on a Linux server

What's New and Changed in Release 23.2.20

The following new features were added in Illumio Core 23.2.20.

PCE distribution filename changed

For those performing an on-premises installation of Illumio Core, you will notice a new naming convention for the distributed PCE software file that you download from Illumio Support at the start of the installation procedure. The RPM file for the PCE now uses the “el” suffix in the filename instead of the "c" suffix so the files are consistent for RHEL 7, 8, and 9. For example, illumio-pce-23.2.20-161.c8.x86_64.rpm is now distributed as illumio-pce-23.2.20-161.el8.x86_64.rpm.

RHEL 9 Support for PCE

The PCE can now be installed on the RHEL 9 operating system.

Some considerations and recommended steps should be followed when upgrading from an earlier RHEL version and earlier PCE version.

Illumio Core REST API in 23.2.20

The Illumio Core REST API v2 has changed in 23.2.20 in the following ways:

Changed APIs in this Release

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.

Changes involve the following:

- Exposure changes from Public Experimental to Public Stable. With the exposure changes, the affected APIs are being made available to integrators.
- Authorization changes to limit the type of user that can add, update, or delete network devices and network endpoints
- Authorization changes to limit the type of user that can generate and acknowledge policy for network device(s)

Changes in release 23.2.20 include:

- `GET /api/v2/orgs/:xorg_id/network_enforcement_nodes`: Exposure change
- `GET /PUT /api/v2/orgs/:xorg_id/network_enforcement_nodes/:uuid`: Exposure change
- `POST /api/v2/orgs/:xorg_id/network_enforcement_nodes/:uuid`: Exposure & Authorization change (Allow workload admins to add network device to Network Enforcement node)
- `GET /api/v2/orgs/:xorg_id/network_devices`: Exposure change
- `GET /api/v2/orgs/:xorg_id/network_devices/:uuid`: Exposure change
- `PUT/POST/DELETE /api/v2/orgs/:xorg_id/network_devices/:uuid`: Exposure & Authorization change (Allow workload admins to update/delete network devices and add network endpoints to a network device)
- `POST /api/v2/orgs/:xorg_id/network_devices/:uuid/enforcement_instructions_request`: Exposure & Authorization change (Allow provisioning admins to request policy generation for multiple network devices)
- `POST /api/v2/orgs/:xorg_id/network_devices/:uuid/enforcement_instructions_applied`: Exposure & Authorization change (Allow provisioning admins to acknowledge policy applied to multiple network devices)
- `GET /api/v2/orgs/:xorg_id/network_devices/:uuid/network_endpoints`: Exposure change
- `GET /api/v2/orgs/:xorg_id/network_devices/:uuid/network_endpoints/:ep_uuid`: Exposure change
- `PUT/POST/DELETE /api/v2/orgs/:xorg_id/network_devices/:uuid/network_endpoints/:ep_uuid`: Exposure & Authorization change (Allow workload admins to update/delete network endpoints and assign workloads to a network endpoint)

These changes are all captured in the file illumio.api.json, where you can see the following changes:

- for `network_endponts`: change from `end_user_experimental` to `end_user_public`; authorization extended to **workload manager**

- for `network_endpoint`: change from `end_user_experimental` to `end_user_public`; authorization extended to **workload manager**
- for `network_devices`: change from `end_user_experimental` to `end_user_public`
  - for `multi_enforcement_instructions_request`: authorizatiin expanded to **Global Policy Object Provisioner** and **Ruleset Provisioner**
  - for `multi_enforcement_instructions_applied`: authorizatiin expanded to **Global Policy Object Provisioner** and **Ruleset Provisioner**
- for `network_enforcement_nodes`: change from `end_user_experimental` to `end_user_public`
- for `network_enforcement_node`: change from `end_user_experimental` to `end_user_public`

What's New and Changed in Release 23.2.2

Illumio Core 23.2.2-PCE Maintenance Release

Illumio Core 23.2.2 includes an updated version of the PCE and VEN software.

IMPORTANT

Illumio Core22.5.12-PCE and 22.5.12-VEN are available for Illumio Core Cloud customers only depending on the version of the Illumio Core PCE running in your Cloud environment. For information about which version of the PCE you are running, check the PCE version in your PCE web console.

Illumio provides regular maintenance updates for reported bugs and security issues, and to add support for new operating system versions. As a maintenance release, Illumio Core 23.2.2 solved software and security issues for the PCE to refine the software and improve its reliability and performance.

What's New and Changed in Release 23.2.10

The following new features were added in Illumio Core 23.2.10.

Ransomware Protection Dashboard

In this release, access to the Ransomware Protection Dashboard was extended to Supercluster users in the following way:

- The Supercluster Leader is able to see the Ransomware Dashboard icon in the side menu and to visit dashboard page after clicking on it.

- Supercluster members are **not** able to see the Ransomware Dashboard icon in the side menu and have no access to the dashboard page.

- Both the Supercluster Leader and members can view the workload information in the workload page and the service page.

Policy Check is Aware of Network Type

Rules for outbound traffic can now check the network profile to be sure allowed traffic is not blocked.

This feature was originally made available to Illumio Core Cloud customers in the Core 23.3.0. This feature is now available to Illumio Core On-Premises customers in this Core 23.2.10 release. Additionally, this feature provides support Endpoint VENs running on the macOS platform.

Illumio Core REST API in 23.2.10

The Illumio Core REST API v2 has changed in 23.2.10 in the following ways:

Changed APIs in this Release

In release 23.2.10, there are two minor changes to the existing REST APIs.

`traffic_flows_async_queries_download_get`

In this API, the optional property `draft_policy_decision` was added, which describes the draft policy decision of the flow. The value assigned to this property is expected to be a string.

```
{
    "items": {
        "properties": {
            "draft_policy_decision": {
            "description": "draft policy decision of the flow",
            "type": "string"
        }
    }
}
```

`optional_features_put`

In this API, for the required property `name` an additional predefined value (enum) was added: `labels_editing_warning_for_enforcement_mode`. This value was added to the existing list:

- `ip_forwarding_firewall_setting`
- `ui_analytics`
- `illumination_classic`
- `ransomware_readiness_dashboard`
- `per_rule_flow_log_setting`
- `lightning_default`
- labels_editing_warning_for_enforcement_mode

```
],
```

```
    "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",
               "labels_editing_warning_for_enforcement_mode"
            ]
```

What's New and Changed in Release 23.2.0

The following new features were added in Illumio Core 23.2.0

New UI

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

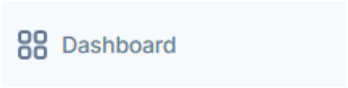
We think you'll love this cleaner, more flexible design – but while we always strive to keep Illumio core easy-to-use, change is hard, so we've assembled this short guide to help you introduce you to this new Illumio Core experience.

Ransomware Protection Dashboard

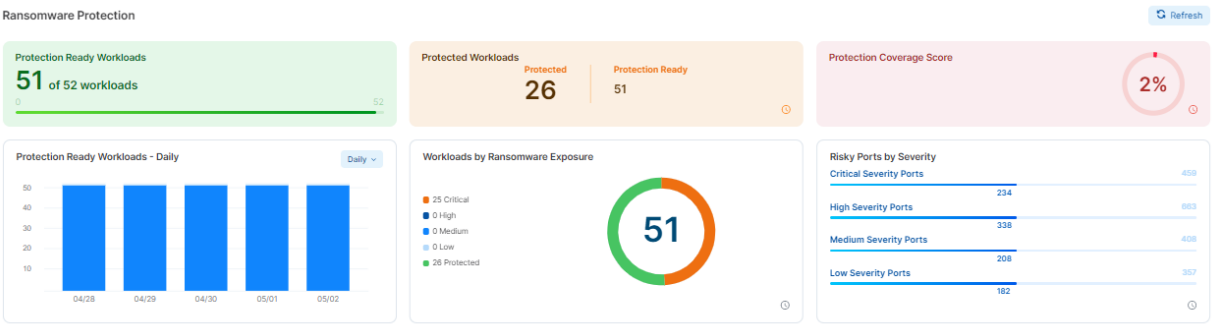
The Ransomware Protection tab provides detailed protection information for the workloads regarding each of the ransomware-risky services.

Information about the ransomware risk is then aggregated into the Ransomware Protection Dashboard for the system-side ransomware risk analysis.

You can access the Dashboard by clicking on the Dashboard button in the left menu.



The new Ransomware Protection Dashboard is located above the VEN Dashboard in a single screen. To see the VEN Dashboard, scroll down until the heading VEN Statistics appears.



In this release, only the following global user roles are allowed to use the Ransomware Protection Dashboard:

- Global Org Owner
- Global Administrator
- Global Viewer

Only managed server workloads are included in the Dashboard statistics. Endpoints and container workloads are not included.

Write a Ringfencing Rule

Using the Illumination Plus Map view (in the Classic UI) or the Explore > Map (in the New UI), you can quickly create a ringfencing rule by adding that rule to a new ruleset within the scope of the selected group.

Ringfencing shrinks the security perimeter from a subnet or VLAN to a single application. It provides the largest impact with the least amount of work, requiring only one line of security policy per application to close off 90 percent of the potential attack surface for east-west traffic movement.

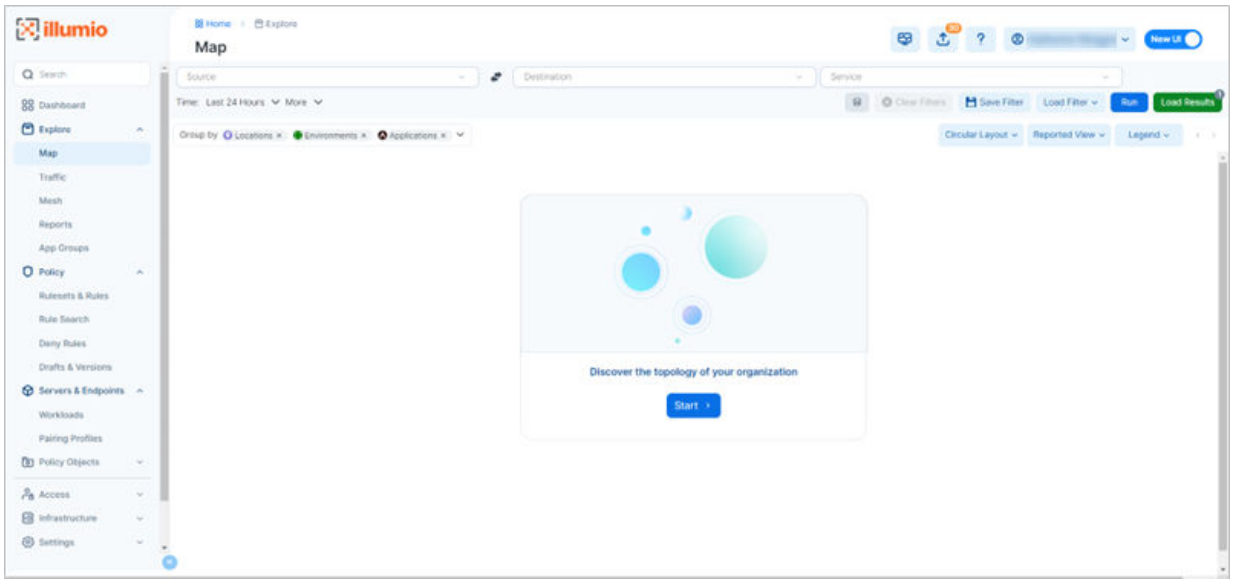
Enhancements to the Explore Features

In Illumio Core 23.2.0, Illumio has enhanced the Explore features in the following ways.

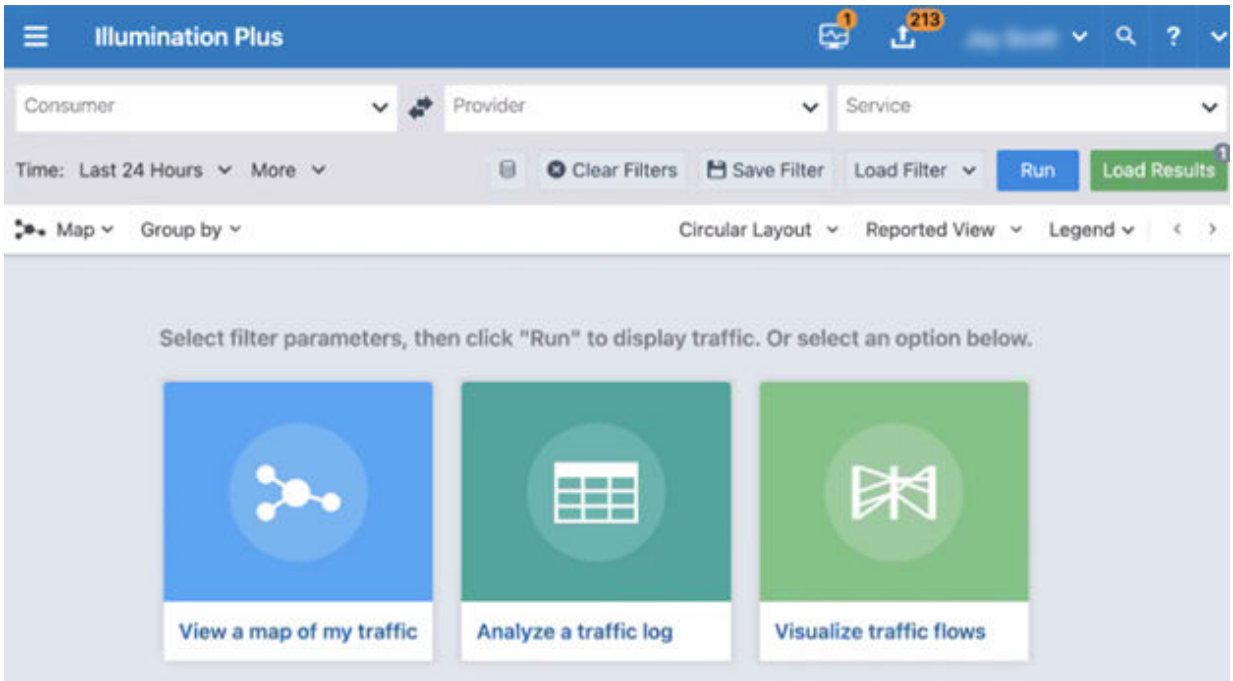
Default Graph

In Core 22.5.x, the PCE cached the Illumination Plus queries (for the Map and Table views) that you ran and were saved for a 24-hour period. Caching your query results allowed the PCE to display Illumination Plus pages quickly. To view and access your cached queries, you clicked **Load Results** at the top-right corner of the Map page. The Results page appeared.

In 23.2.0, if you don't have a default graph in the PCE, the page below is your start page for the Map and Traffic pages.



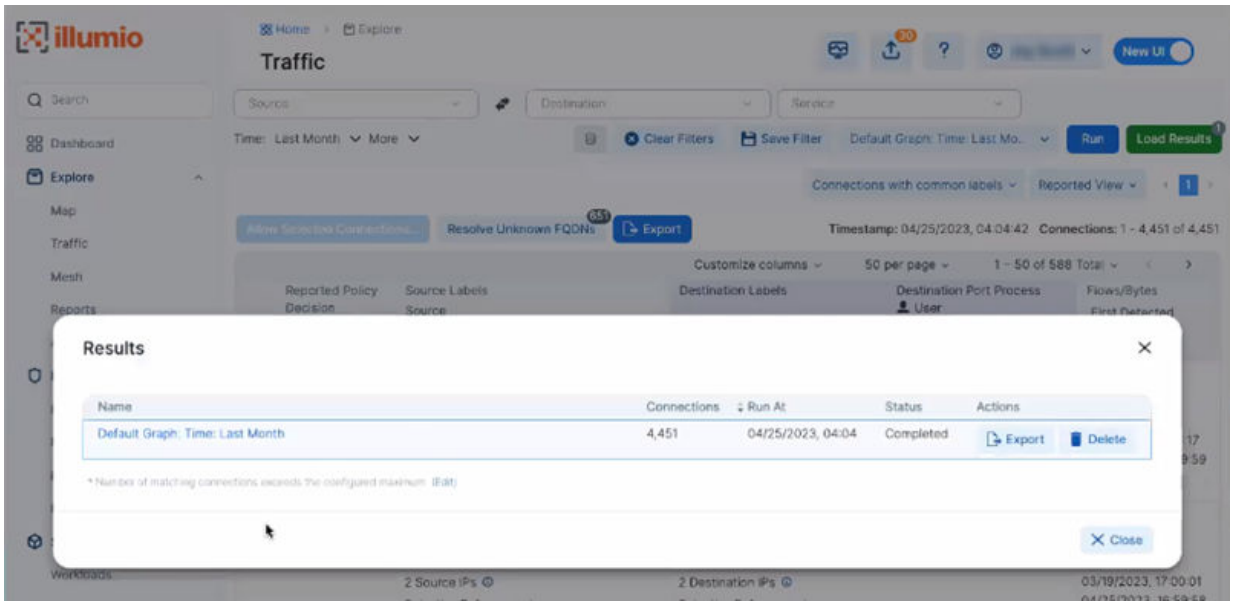
The new page above has replaced this Start page that you saw in Core 22.5.x:



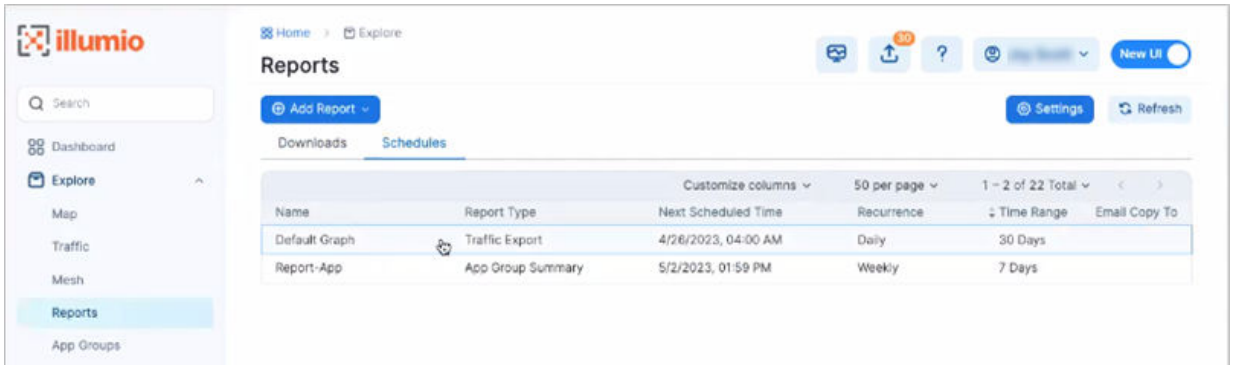
When you click **Start**, the PCE creates a map or traffic table based on the values you have in the filters at the top of the page. The PCE saves this query with those filters as the default graph The graph expires in 24 hours; however, the PCE saves the default graph as a scheduled report that runs every 24 hours (between 12:00 midnight and 8:00 AM).

Then, when you return to the Map or Traffic page, the PCE loads that saved default graph, unless you already have another graph (different filters) displayed. You won't see this Start page again, unless you delete the default graph.

This page now appears when you click **Load Results** in the Map page to display the entry for the Default Graph:



When you open the **Reports** feature from the left navigation and select the **Schedules** tab, you see the scheduled report for the Default Graph.



IMPORTANT

Not all Illumio users can access the Default Graph scheduled report. You must have the correct Access permissions.

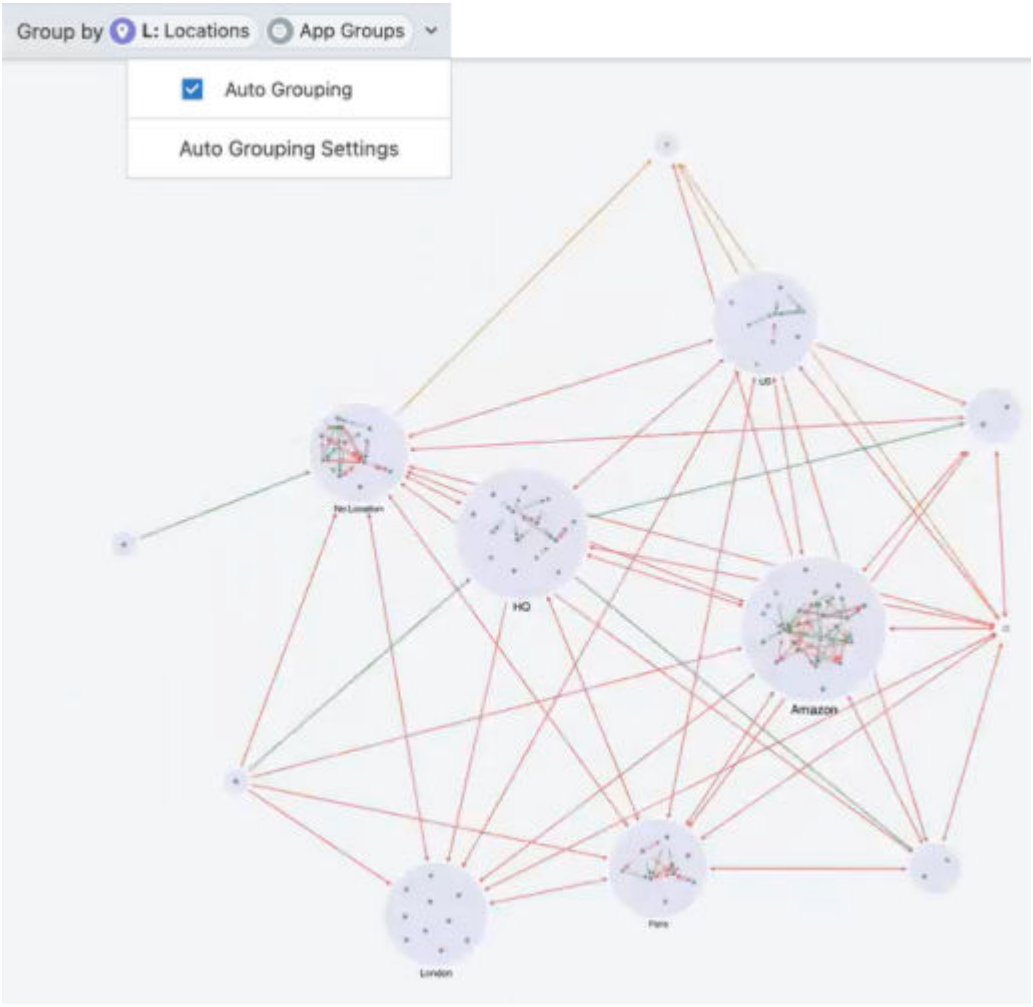
Tips for Using the Default Graph

To change the query that the PCE runs for the Map and Traffic page:

- Go to the Reports page and select a different saved query.
- Delete the default graph by clicking Load Results in the Map or Traffic page and clicking Delete in the Load Results dialog box. Then, navigate to the Map or Traffic page so that the Start page appears. Click Start to create a default graph.
- Click the Schedule Time field and select a new time to change when the default graph report runs each 24 hours. However, you must have the correct permission to edit the Default Graph (RBAC roles and permissions).

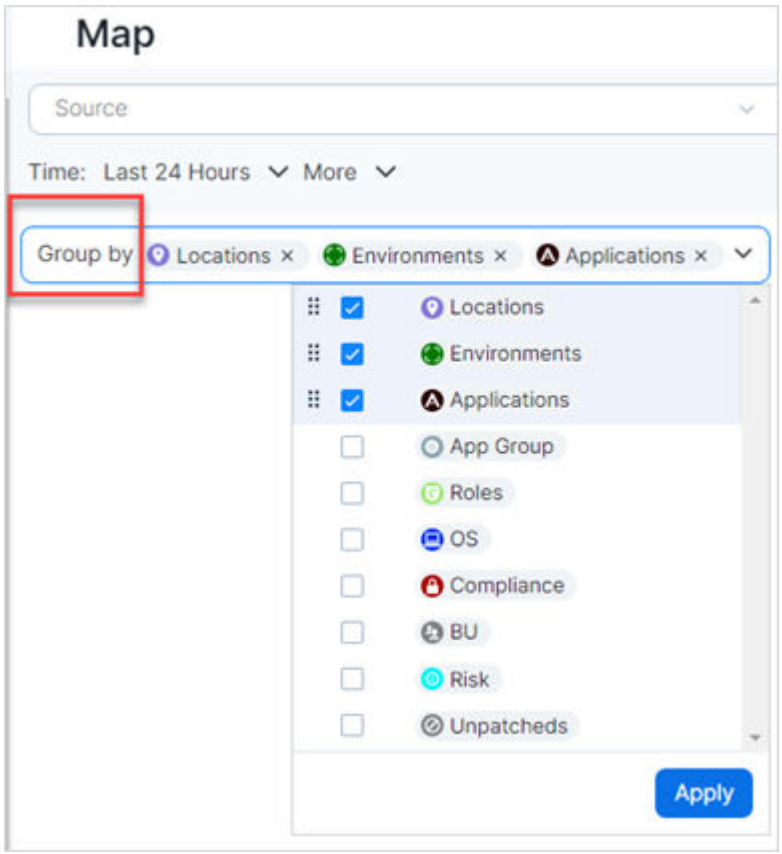
Auto Grouping Feature Removed

In Illumio Core 22.5.x, you could select the Auto Grouping option to have the PCE calculate the best grouping for your managed environment.



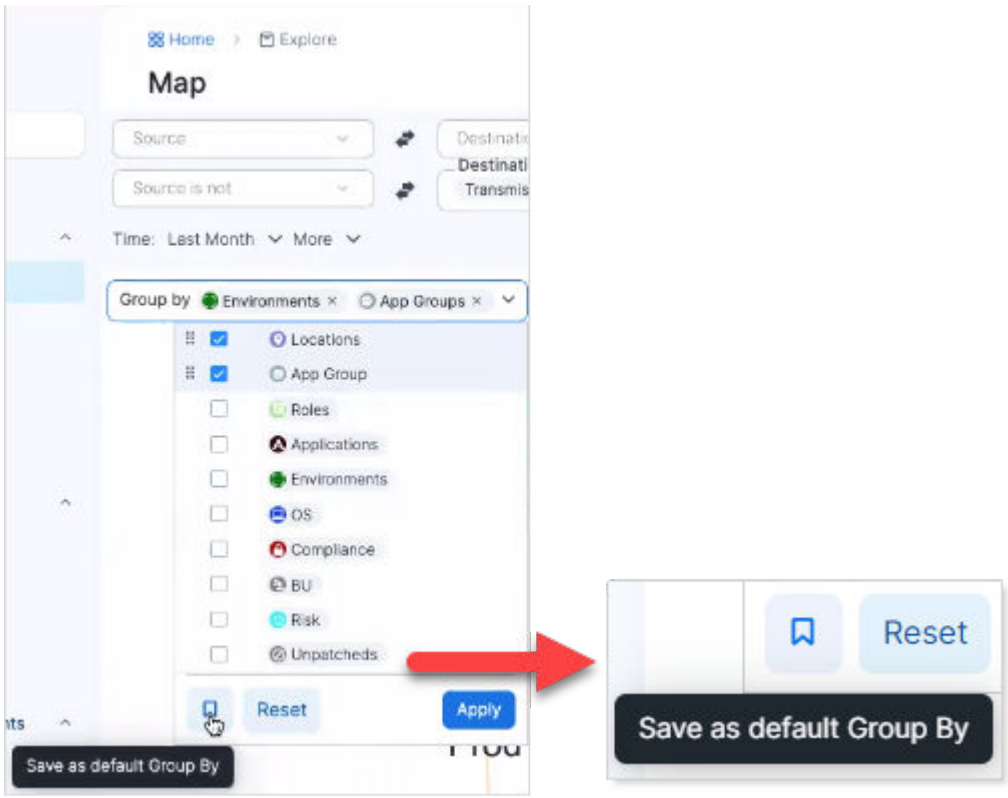
In Illumio Core 23.2.0, this feature is removed, and the map grouping was simplified.

In this release, you now specifically choose which labels that you want to group your map by:



In 23.2.0, whatever labels you select from the Group by drop-down list, is the grouping that your Map uses. By default, the Map uses the labels Locations, Environments, and Applications. However, you can change the grouping to whatever labels you want.

To save your grouping selections, select the bookmark icon. When bookmarked, the grouping becomes your default setting. If you change the grouping for a specific view of your data, click Reset to go back to your default grouping.

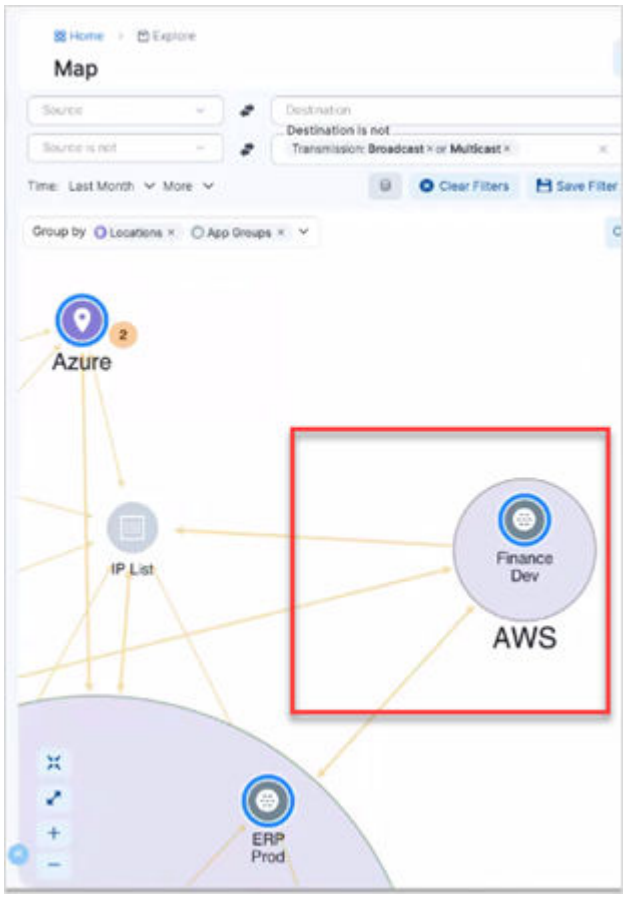


Opening Right Panel

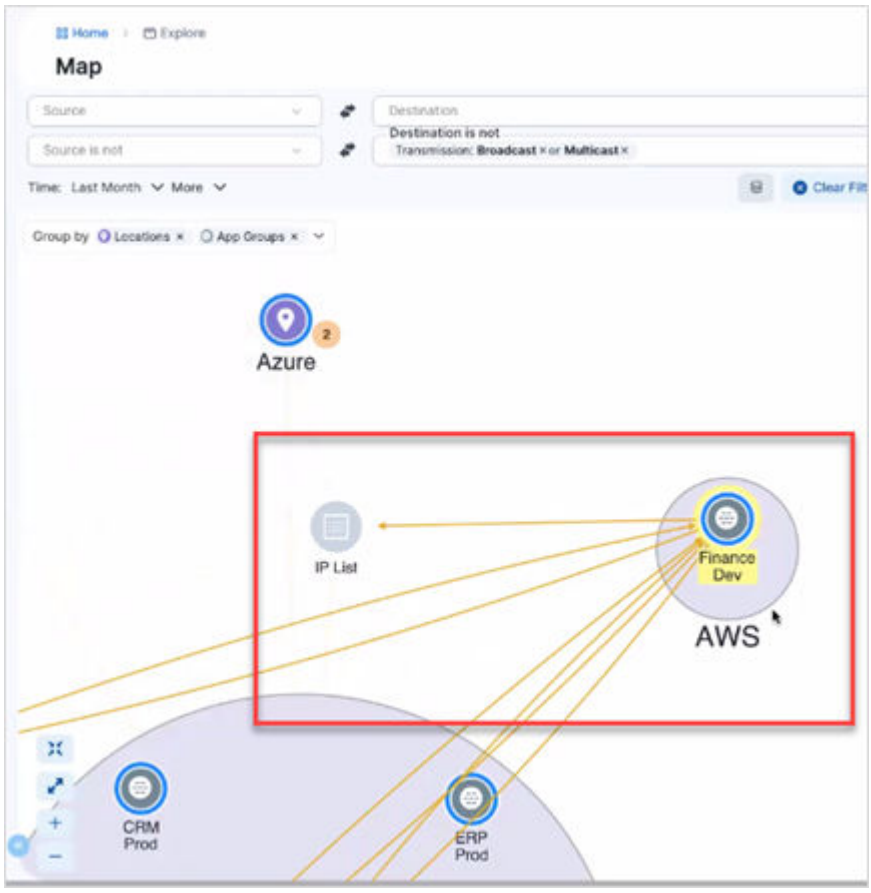
In Core 22.5.x, clicking a group in the map opened the right panel with the details about the group.

In core 23.2.0, you must click two times to open the right panel with group details.

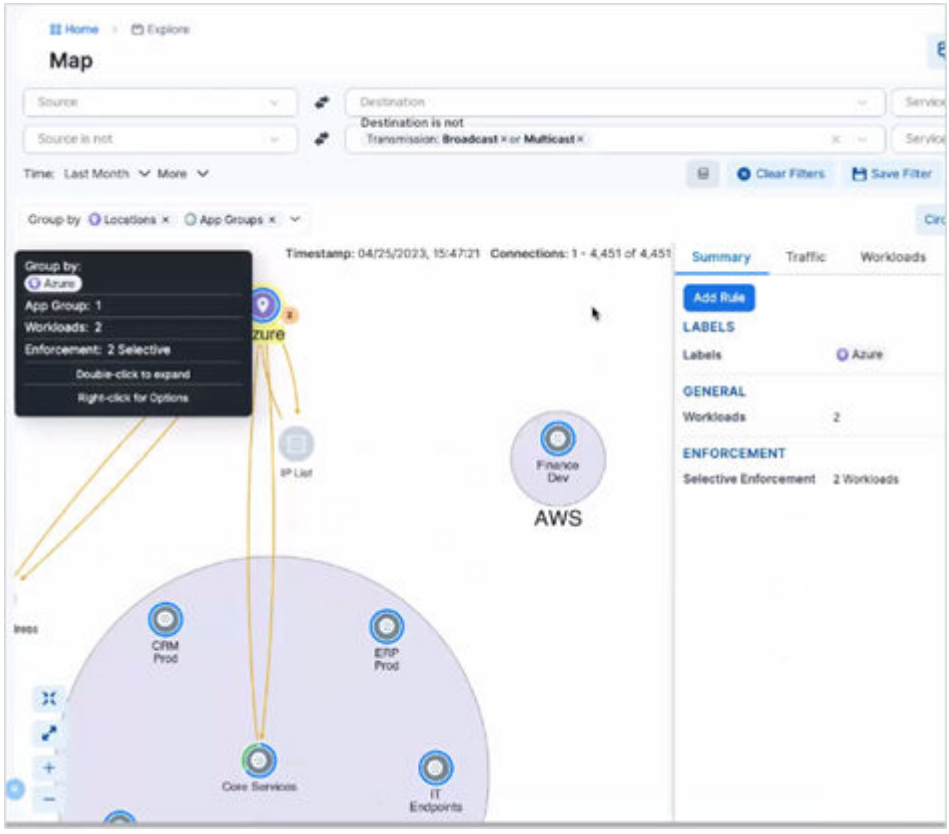
Prior to clicking:



The first click selects and highlights the group and all connections associated with the group.



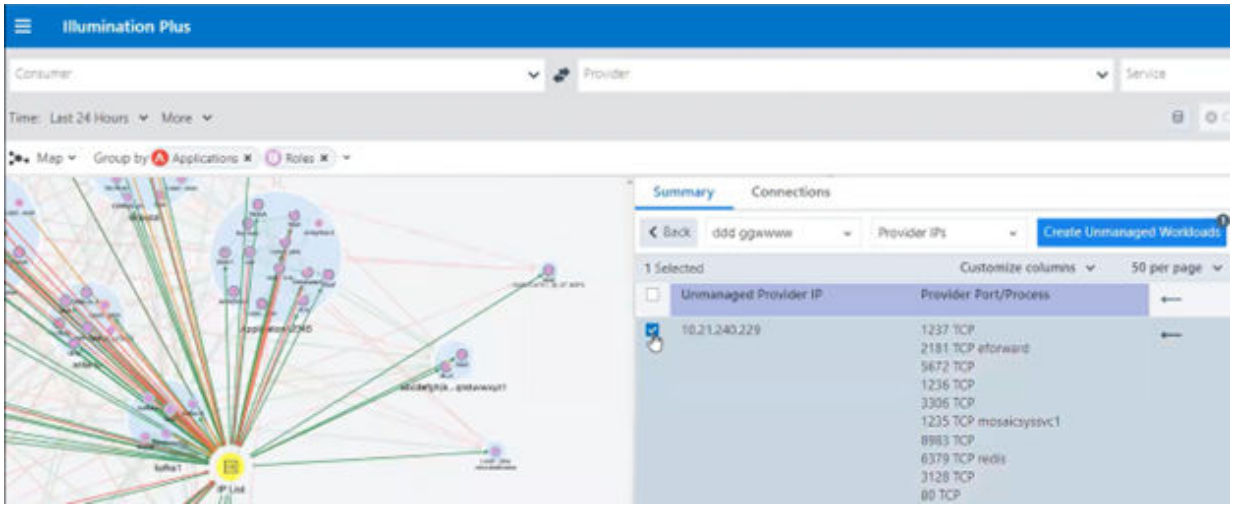
The second click opens the right panel:



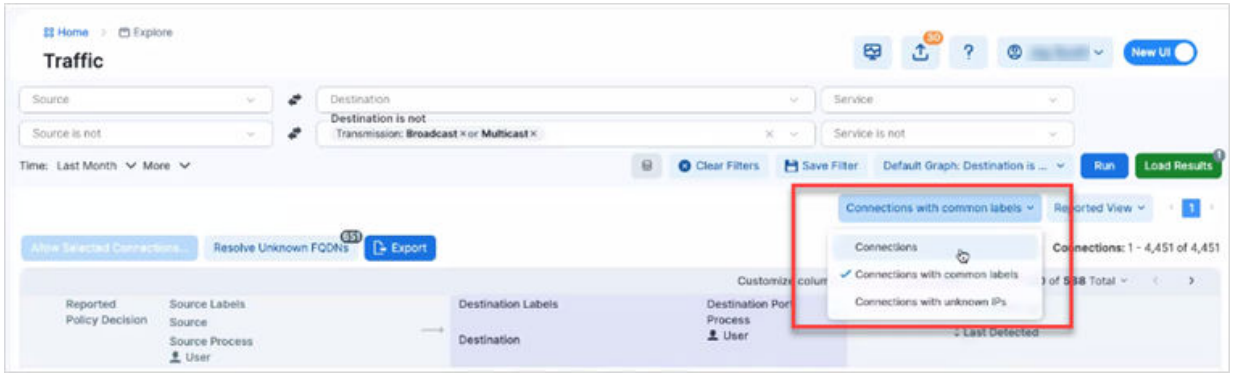
Clicking a link opens the right panel immediately; or, if the panel is open, clicking a group once refreshes the details in the panel with the new group.

Unmanaged IP Addresses

In Illumio Core 22.5.x, unmanaged IP addresses were accessible as a node in the Illumination Plus map.

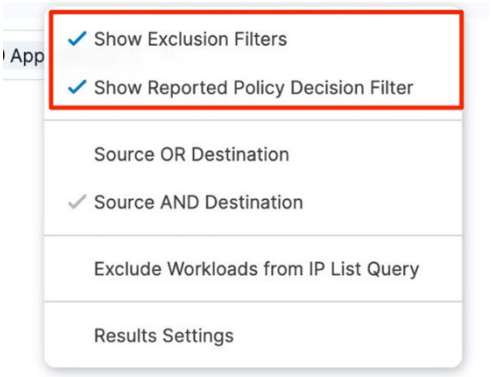


In Illumio Core 23.2.0, unmanaged IP addresses are accessible from the following map drop-down list:



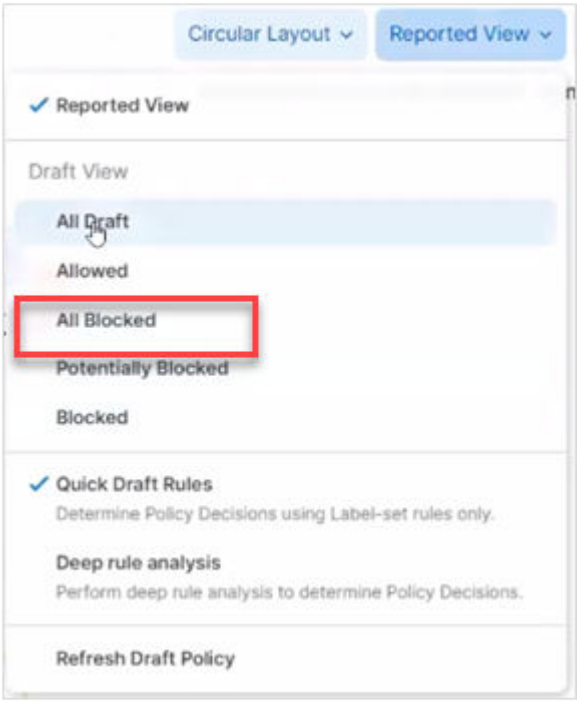
Enhancement in Map Filter

The Exclusions filter and Reported Policy Decision filters enabled by default:



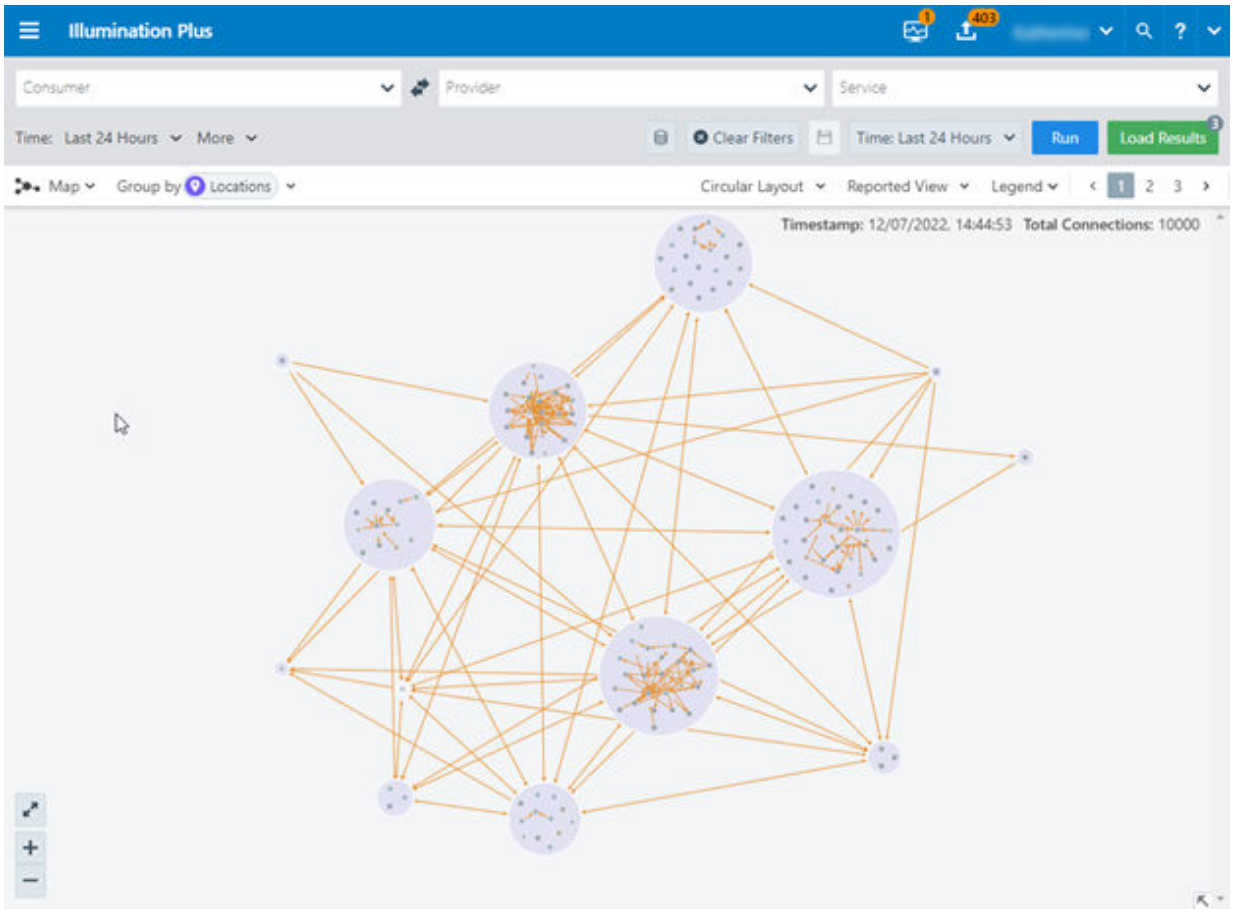
View Drop-Down Menu

The View drop-down list includes a new option to show all blocked traffic.

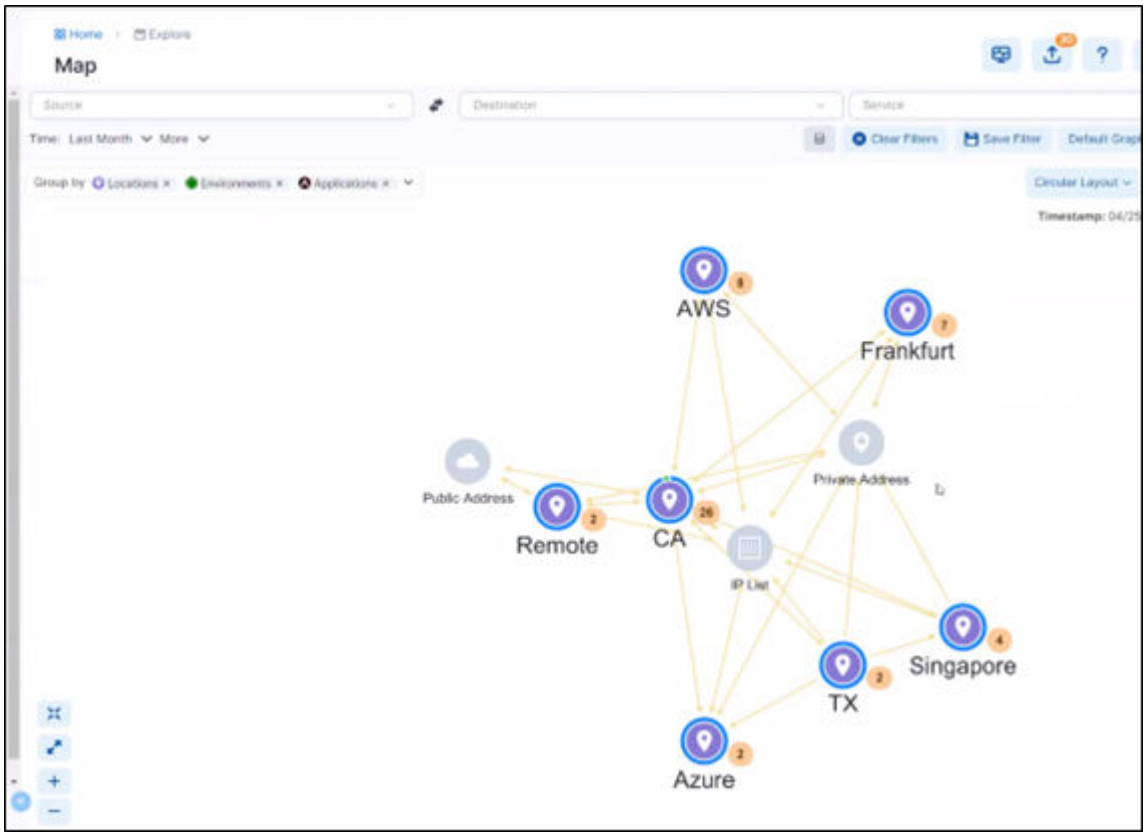


Grouping in the Map Collapsed

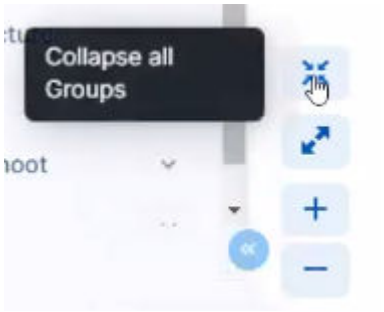
In Core 22.5.x, all the top groups in the Map were expanded so that you could see their contents:



In Core 23.2.0, these top groups are collapsed by default



In addition, you have a new control to collapse all expanded groups:



Set VEN Type in the Pairing Profile

In Illumio Core 23.2.0, each Pairing Profile now includes information about Enforcement Node. This column lets you know the type of device you can run the pairing script on, namely servers versus endpoints.

Or, you can choose not to set the type in the Pairing Profile and let the PCE determine the correct type when the VEN activates with the PCE.

Enforcement Node Type column and values

Set VEN Upgrade Expiration Time

When upgrading VENs, you can specify how much time the VENs have to successfully upgrade by entering a value and units of time in the new **VEN Upgrade Expiration** field of the VEN Upgrade dialog. The VEN upgrade timeout value can be specified in minutes, hours, or days. The timeout must be between 15 minutes and 180 days. For server VENs, the recommended upgrade timeout is 1 day. For endpoint VENs, the recommended timeout is 7 days. After the expiration time passes, the PCE will no longer instruct the VEN to upgrade, and the VEN will be in a warning state.

Configure Second FQDN for Southbound Traffic

You can specify a second fully-qualified domain name (FQDN) for VENs to use to send communications to the PCE with the new optional Public Experimental runtime parameter `agent_pce_fqdn`.This is in addition to the existing required parameter `pce_fqdn`.

RHEL 5 Support

Red Hat Enterprise Linux (RHEL) 5 is supported for VENs, with some limitations.

The following are not supported:

- FQDN-based rules
- Machine authentication
- IPv6
- Byte counting

When a curl command is used to run the VEN pairing script, additional configuration steps are required:

- Downgrade the minimum TLS version. Set `min_tls_version` to `tls1_0`.
- Update the CA certificate file on the RHEL 5 machine. Download the latest `cacert.pem` and append it to the `ca-bundle.crt` file.

RHEL 9 Support

Red Hat Enterprise Linux (RHEL) 9 is supported for VENs.

Illumio Core REST API in 23.2.0

The Illumio Core REST API v2 has changed in 23.2 in the following ways.

In release 23.2 0, most of the new APIs are introduced to power the Ransomware Dashboard. These new ransomware APIs together with some changed APIs are collected under the heading APIs for Ransomware.

NOTE

This document combines API changes for releases 23.2.0 and 23.1.0, which was not provided for customers.

APIs for Ransomware Protection

Ransomware Protection Dashboard

New APIs introduced to power the Ransomware Protection Dashboard are:

- reports/risk_summary_get [40]
- num_protected_unprotected_ports [40]
- reports_time_series_statistics_post [40]
- reports_time_series_statistics_post_response [42]

APIs in this release that have been changed to work with the Ransomware Protection Dashboard:

- workloads_get [43]
- workloads_risk_details_get [44]
- workload_ransomware_services [46]
- settings_get [48]
- settings_put [48]
- sec_policy_services_post [49]
- sec_policy_services_put [49]
- sec_policy_services_get [49]

The Ransomware Dashboard image and quick description are available in Ransomware Dashboard. [25]

For more detailed description see the Visualization Guide, Ransomware Dashboard and the API Guide, Ransomware APIs.

reports/risk_summary_get

Security administrators use this API to view how many workloads are ransomware protection ready and then assess the degree of protection in their whole system. This schema supplies the required information to run the Ransomware Dashboard:

- Number of total workloads
- Number of protected workloads
- Number of risky ports by the severity of their risk exposure (low, medium, high, and critical)
- Workload protection by the port type (admin and legacy)
- Ransomware protection coverage percent
- Date when the status was last updated

Sample Response for reports/risk_summary_get

```
{
   "ransomware":{
    "num_total_workloads":98,
    "num_protected_workloads":22,
    "workload_protection_by_severity":{
      "low":{
        "protected_workload_count":2,
        "unprotected_workload_count":8
       },
       "medium":{
        "protected_workload_count":3,
        "unprotected_workload_count":6
       },
      "high":{
        "protected_workload_count":2,
        "unprotected_workload_count":8
       },
       "critical":{
        "protected_workload_count":3,
        "unprotected_workload_count":6
       }
            },
   "workload_protection_by_port_type":{
    "admin":{
       "protected_workload_count":2,
       "unprotected_workload_count":8
    },
    "legacy":{
       "protected_workload_count":3,
       "unprotected_workload_count":6
    }
   },
   "ransomware_protection_coverage_percent":56,
   "last_updated_at":"2023-01-21 23:32:42.679673"
   }
}
```

num_protected_unprotected_ports

This schema is referenced from `reports_risk_summary_get.schema.json` to supply the number of protected and unprotected ports for a specified risk level:

```
{
   "$schema": "http://json-schema.org/draft-04/schema#",
   "type": "object",
   "required": [
    "num_protected_ports",
    "num_unprotected_ports"
  ],
   "properties": {
    "num_protected_ports": {
       "description": "Number of protected ports for this risk
            level, across all protection ready workloads",
       "type": "integer"
       },
    "num_unprotected_ports": {
       "description": "Number of unprotected ports for this risk
                level, across all protection ready workloads",
       "type": "integer"
    }
   }
}
```

reports_time_series_statistics_post

This schema supplies the granularity of the time series data.

The API `reports_time_series_statistics_post` includes the property `num_managed_workloads`, which is requested by the payload. The resolution might be `day`, `week`, `month`, and `quarter`, which defines what the UI will show.

The default value 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"
        ]
    },
    "resolution": {
        "type": "string",
        "description": "The granularity for the time series data.
                  E.g. day, week, month, quarter",
        "enum": [
           "day",
           "week",
```

```
            "month",
            "quarter"
         ],
        "default": "day"
    },
    "max_results": {
        "type": "integer",
        "default": 5
    }
    }
  }
}
```

reports_time_series_statistics_post_response

This API specifies the time series data about the protected workloads, such as the start and end date of the protection period.

```
{
   "$schema": "http://json-schema.org/draft-04/schema#",
   "type": "array",
   "items": {
    "type": "object",
    "required": [
       "property",
       "time_series"
    ],
    "properties": {
       "property": {
        "description": "The property for which data has been
                  requested.",
          "type": "string"
        },
       "time_series": {
        "type": "array",
        "items": {
        "type": "object",
        "required": [
           "start_date",
           "end_date"
       ],
        "properties": {
           "start_date": {
              "description": "The start date of the time period.",
            "type": "string",
            "format": "date-time"
           },
          "end_date": {
              "description": "The end date of the time period.",
              "type": "string",
              "format": "date-time"
          },
          "count": {
              "description": "The integer count on the end date
                       of this period.",
              "type": "integer"
```

```
          },
          "unit": {
              "description": "The unit of the value returned.",
              "type": "string"
        }
       }
      }
}
```

Sample Requst Body for `reports_time_series_statistics_post_response`

```
[
    {
    "property": "num_managed_workloads",
    "resolution": "week",
    "max_results": 4
    }
]
```

Response for `reports_time_series_statistics_post_response`

A week starts Monday and ends Sunday and the VEN count is from Sunday of that week. The last week could be a partial week hence the count will be of the last day.

The last month could be a partial month, and hence the count will be from the last day.

Workloads APIs Changed for Ransomware

workloads_get

This Public Stable API was changed to support the Ransomware Dashboard in the following way:

- One new object was added: `risk_summary`, which explains the risk summary for the workload. This object includes a required object `ransomware`, which supplies these properties:
  - `workload_exposure_severity`
  - `ransomware_protection_percent`
  - `last_updated_at`

```
{
 "properties": {
   "risk_summary": {
    "description": "Risk Summary for this workload",
    "type": "object",
    "required": [
       "ransomware"
    ],
    "properties": {
       "ransomware": {
        "type": [
           "object",
           "null"
        ],
        "required": [
```

```
            "workload_exposure_severity",
            "ransomware_protection_percent",
            "last_updated_at"
         ],
         "properties": {
            "workload_exposure_severity": {
             "description": "Exposure severity of the workload",
             "type": "string"
             },
            "ransomware_protection_percent": {
             "description": "Ransomware protection percentage
                            for this workload",
             "type": "number"
             },
            "last_updated_at": {
             "description": "The time at which the ransomware
                             stats are last computed at",
             "type": "string",
             "format": "date-time"
             }
         }
    }
}
```

workloads_risk_details_get

This API, which supplies the risk details, you can see in action on the Workloads page, tab Ransomware Protection.

In addition to the organization admin, the users who have access to the workload can view the ransomware protection details for that workload, or how many risky ports are protected and how many risky ports are not protected.

```
{
   "$schema": "http://json-schema.org/draft-04/schema#",
   "type": "object",
   "properties": {
    "risk_details": {
    "type": "object",
    "required": [
       "ransomware"
    ],
    "ransomware": {
       "type": [
        "object",
        "null"
       ],
       "properties": {
          "details": {
        "type": "array",
        "items": {
           "$ref": "workload_ransomware_services.schema.json"
        }
       },
       "last_updated_at": {
        "description": "The time at which the protection stats
```

```
                    were last computed at",
        "type": "string",
        "format": "date-time"
       }
      }
}
```

Sample Response for `workloads_risk_details_get`

```
{
   "risk_details":{
    "ransomware":{
       "services":[
          {
        "href":"/api/v2/orgs/8/workloads/
23131cf5-1d70-42de-9242-39055338d0ef",
        "name":"SSH",
        "port":22,
        "protocol":17,
        "severity":"low",
        "port_status":"listening",
        "protection_state":"unprotected",
        "active_policy":"allowed",
        "draft_policy":"blocked",
        "recommendation":"add_boundary"
       },
       {
        "href":"/api/v2/orgs/8/workloads/
23131cf5-1d70-42de-9242-39055338d0ef",
        "name":"SSH",
        "port":22,
        "protocol":6,
        "severity":"high",
        "port_status":"listening",
        "protection_state":"protected",
        "active_policy":"allowed",
        "draft_policy":"blocked",
        "recommendation":"has_draft_policy_needs_provisioning"
       }
    ],
    "last_updated_at":"2023-01-21 23:32:42.679673"
    }
   }
}
```

The full response looks as follows:

```
[
   {
    "property":"num_managed_workloads",
    "time_series":[
       {
        "start_date":"2022-10-31",
        "end_date":"2022-11-2",
        "count":120
```

```
        },
        {
         "start_date":"2022-10-24",
         "end_date":"2022-10-30",
         "count":115
        },
        {
         "start_date":"2022-10-17",
         "end_date":"2022-10-23",
         "count":110
        },
        {
         "start_date":"2022-10-10",
         "end_date":"2022-10-16",
         "count":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

```
{
   "$schema": "http://json-schema.org/draft-04/schema#",
   "type": "object",
   "required": [
     "href",
      "port",
      "protocol",
      "severity",
      "port_status",
      "protection_state",
      "active_policy",
      "draft_policy"
    ],
   "properties": {
      "href": {
       "description": "Reference of the service",
       "type": "string"
    },
      "name": {
       "description": "Name of the service",
       "type": "string"
    },
    "port": {
       "description": "Port Number",
       "type": "integer",
```

```
      "minimum": 0,
      "maximum": 65535
   },
   "proto": {
      "description": "Protocol Number",
      "type": "integer"
   },
   "severity": {
      "description": "Severity of this service",
      "type": "string",
      "enum": [
         "low",
         "medium",
         "high",
         "critical"
      ]
   },
      "category": {
      "description": "Category of this service",
      "type": "string",
      "enum": [
         "admin",
         "legacy"
      ]
     },
   "port_status": {
      "description": "Status of the port on the workload",
      "type": "string",
      "enum":
            "listening",
         "inactive"
         ]
      },
   "protection_state": {
      "description": "Protection state of this service",
      "type": "string",
      "enum": [
          "unprotected",
          "protected_open",
          "protected_closed"
         ]
   },
   "active_policy": {
         "description": "Active Policy that applies to this port",
         "type": "string",
         "enum": [
         "allowed",
         "allowed_across_boundary",
         "blocked_by_boundary",
        "blocked_no_rule"
         ]
      },
     "draft_policy": {
         "description": "Draft Policy that applies to this port",
         "type": "string",
```

```
            "enum": [
           "allowed",
           "allowed_across_boundary",
           "blocked_by_boundary",
           "blocked_no_rule"
         ]
        },
        "recommendation": {
         "description": "Recommendation for this port based on enforcement
                        state, allow and deny rules and active/draft rule",
         "type": "string",
         "enum": [
           "add_boundary",
           "has_draft_policy_needs_provisioning"
         ]
         }
       }
}
```

Settings APIs Changed for Ransomware

settings_get

This Public Stable API was changed to include a new property `num_assets_requiring_ransomware_protection`.

```
{
   "$schema": "http://json-schema.org/draft-04/schema#",
   "type": "object",
   "properties": {
    "href": {
       "description": "Org Setting URI",
       "type": "string",
       "format": "uri"
    },
    "num_assets_requiring_ransomware_protection": {
       "description": "number of assets that need ransomware
                 protection for this org",
       "type": [
         "integer",
          "null"
       ]
    },
        ====================================
```

settings_put

This Public Stable API was changed to include a new property `num_assets_requiring_ransomware_protection`, which provides a number of assets that need ransomware protection in a specific organization. Number of assets is between one and 9999999 .

```
{
   "$schema": "http://json-schema.org/draft-04/schema#",
   "type": "object",
   "additionalProperties": false,
   "properties": {
```

```
      "num_assets_requiring_ransomware_protection": {
        "description": "number of assets that need
                    ransomware protection for this org",
        "type": "integer",
        "minimum": 1,
        "maximum": 9999999
        ==================================
```

Security Policy Changed for Ransomware

sec_policy_services_post

sec_policy_services_put

sec_policy_services_get

These APIs have been changed as follows:

The new object `risk_details` was added and supplies the same data as the previously deleted three properties: `ransomware_category`, `ransomware_severity`, and `ransomware_os_platforms`.

```
{
    "$schema": "http://json-schema.org/draft-04/schema#",
    "type": "object",
    "additionalProperties": false,
    "required": [
       "name"
       ],
    "properties": {
       "name": {
        "description": "Name (does not need to be unique)",
        "type": "string"
        },
       "description": {
        "description": "Description",
        "type": "string"
        },
       "risk_details": {
        "type": "object",
        "properties": {
           "ransomware": {
            "type": "object",
            "properties": {
               "category": {
                "description": "Categorization based on Admin
                                    or Legacy port used in the service",
                "type": "string",
                "enum": [
                   "admin",
                   "legacy"
                  ]
            },
            "severity": {
                "description": "Severity of this service",
                "type": "string",
```

```
                "enum": [
                   "low",
                   "medium",
                   "high",
                   "critical"
                   ]
                },
            "os_platforms": {
                "description": "Operating system for this
                                    ransomware service",
                "type": "array",
                "minItems": 1,
                "items": {
                   "type": "string",
                   "enum": [
                    "windows",
                    "linux"
                      ]
                  }
                 }
            }
        }
    }
},
        ============================================
```

These Security Policy APIs are explained in the topic Services

VEN APIs

New VEN APIs

The new common schema `release_ven_types` is introduced to show `ven_types` for each release and to filter releases by `ven_type`.

Previously, the `ven_type` was not stored for the release, and database records looked as follows:

- Release 22.5 : Distribution CentOS
- Release 22.5.1: Distribution MacOS
- Release 22.5.1: Distribution Windows

With the property `ven_type` added, the database records are expanded with an additional `ven_types` column:

- Release 22.5; Distribution CentOS; `ven_types`: `server + endpoint`
- Release 22.5; Distribution MacOS; `ven_types`: `server + endpoint`
- Release 22.5.1; Distribution Windows; `ven_types`: `server + endpoint`

Note that in release 22.5.1 the code supports the type `server+endpont`. However, Centos (Linux) supports a server-only VEN image, MasOS supports endpoint-only image, and Windows supports both server and endpoint.Gne actiual dictribution looks as follows:

- Release 22.5; Distribution CentOS; `ven_types`: `server + endpoint`
- Release 22.5; Distribution MacOS; `ven_types`: `endpoint`
- Release 22.5.1; Distribution Windows; `ven_types`: `server + endpoint`

When a user opens the list of release images via the UI and looks for the type `server + endpoint`, only the Windows image will show up as the complete match.

To fix this issue, the `ven_type` is now based on release and distribution:

- All releases before 21.2.2 were just `server` (there was no endpoint)
- Any release with 22.3.x was `endpoint` (there was no server)
- Any other releases were `server + endpoint` , but instead of setting `server + endpoint` to all the images (database records), the `ven_types` are set in a way that is specific for the Os.

common release_ven_types

```
{
    "$schema": "http://json-schema.org/draft-04/schema#",
    "description": "Supported ven types in this release",
        "type": "array",
        "items": {
        "type": "string",
        "enum": ["server", "endpoint"]
    }
}
```

The schema `release_ven_types` is referenced from the APIs `software_ven_releases_get` and `software_ven_releases_images_get`, which have been updated and changed for this release:

software_ven_releases_get

```
{
    "properties": {
    "ven_types": {
        "$ref": "../common/release_ven_types.schema.json"
        }
    }
}
```

The API `software_ven_releases_get` shows the VEN releases available to the org, one per VEN version, along with some metadata such as whether it is the default version, whether that release supports servers and/or endpoints, and so on. The list of images is longer than the list of releases, and multiple images belong to the same release version.

One new property was added:

- `default_release_ven_types`: The type of the release marked as default

```
{
   "properties": {
    "default_release_ven_types": {
```

```
       "type": "array",
       "items": {
        "type": "string",
        "description": "The type of the release marked as default"
       }
    }
   }
}
```

software_ven_releases_images_get

```
{
    "items": {
    "properties": {
    "ven_types": {
        "$ref": "../common/release_ven_types.schema.json"
        }
    }
    }
}
```

The API `software_ven_releases_images_get` shows the full list of VEN images. There is one image for each supported Linux distribution (such as RHEL, Ubuntu), plus images for Windows and macOS.

VEN API Changes

vens_get

This API has several changes:

These two new properties were added:

- `upgrade_expires_at`: Time (rfc3339 timestamp) at which the PCE stops attempting VEN upgrade
- `upgrade_target_version`: Software release to which to upgrade

```
{
   "properties": {
    "upgrade_expires_at": {
       "description": "The time (rfc3339 timestamp) at which the
                PCE stops attempting VEN upgrade",
       "type": [
        "string",
        "null"
       ],
       "format": "date-time"
       },
    "upgrade_target_version": {
       "description": "The software release to upgrade to.",
       "type": [
        "string",
        "null"
       ]
     }
```

```
    }
}
```

- `hostname` is now required
- Type `null` was added to string/object for the following properties: `name`, `description`, `hostname`, `uid`, `os_id`, `os_detail`, `os_platform`, `active_pce_fqdn`, `target_pce_fqdn`, `public_ip`, `security_policy_applied_at`, `container_cluster`, `secure_connect`, `security_policy_received_at`, `last_goodbye_at`, and `container_cluster`
- These properties have been added: `instance_id`, `data_center`, `data_center_zone`, `service_principal_name`, `security_policy_sync_state`
- The property `minItems` was removed

vens_upgrade_put

One new property was added:

- `upgrade_timeout_seconds`: Number of seconds during which the PCE tries to trigger the agent upgrade

```
{
    "properties": {
    "upgrade_timeout_seconds": {
       "description": "Number of seconds during which the PCE
                   tries to trigger the agent upgrade.",
       "type": "integer",
       "minimum": 900,
       "maximum": 15552000
    }
   }
}
```

common software_ven_default_release

This is a new API that supplies the VEN bundle release, including the VEN UTI associated with the release and the VEN type property (type of the release marked as default).

```
{
   "$schema": "http://json-schema.org/draft-04/schema#",
   "type": "object",
   "required": [
      "href",
     "ven_type" ],
   "description": "The ven bundle release with the ven type property",
   "additionalProperties": false,
   "properties": {
    "href": {
        "description": "URI associated to this release",
        "type": "string"
    },
    "ven_type": {
       "type": "string",
       "description": "The type of the release marked as default",
       "enum": [
              "server",
              "endpoint"
       ]
```

```
      }
   }
}
```

Endpoint Offline Timer

The Endpoint Offline Timer was introduced to overcome the 24-hour limitation that was hard-coded for endpoints heart beating.

If the endpoints did not heartbeat for 24 hours, they were marked as being offline and the endpoint timer was hard coded to 24 hours. However, the 24-hour limit was found to be limiting and was now adjusted to allow for endpoint mobility and usability.

The following APIs have been changed:

- `GET /api/v2/orgs/:xorg_id/settings/workloads`: Added properties to reflect the endpoint timeout values: disconnect,
- `PUT /api/v2/orgs/:xorg_id/settings/workloads`: Updated the endpoint offline, heartbeat, and disconnect and quarantine warning timeout values

The three workload timeout setting fields have been updated:

- `workload_disconnected_timeout_seconds`: Timer setting triggered if the server or endpoint has not heart beaten to the PCE.
- `workload_goodbye_timeout_seconds`: Timer setting triggered if the server or endpoint operation is performed (stop, disable, ...)
- `workload_disconnected_notification_seconds`: Time period to wait with no heartbeat before a warning is emitted.

The fourth field use for timeout settings is named `ven_uninstall_timeout_hours` and was available before. It defines the period (in hours) to wait before uninstalling a VEN.

The updated workload settings fields reference the following schemas:

- `workload_disconnected_timeout_seconds` : is referencing `settings_workload_detailed.schema.json`
- `workload_goodbye_timeout_seconds`: is referencing `settings_workload_detailed.schema.json`
- `workload_disconnected_notification_seconds`: is referencing `settings_workload_notifications.schema.json`
- `ven_uninstall_timeout_hours`: is referencing the old common schema `settings_workload.schema.json`

More about the updated schemas:

settings_workload_notifications

This schema file now has an additional property `ven_type` to support the ven type by the referenced timeout fields.

```
{
    "$schema": "http://json-schema.org/draft-04/schema#",
```

```
    "type": "array",
    "items": {
        "type": "object",
        "additionalPropertes": false,
        "required": [
            "scope",
            "warning"
        ],
        "properties": {
            "scope": {
            "$ref": "labels.schema.json"
        },
        "warning": {
        "description": "Workload disconnect warning timeout",
            "type": "integer",
            "minimum": -1,
            "maximum": 2147483647
        },
        "ven_type": {
        "description": "The ven type that this property is applicable to",
            "type": [
            "string",
            "null"
        ],
            "enum": [
            "server",
            "endpoint"
        ]
    }
}
    },
    "uniqueitems": true
}
```

settings_workload_detailed

The new schema `settings_workload_detailed` is expanded from the previous schema `settings_workload` so that additional information about the `ven_type` was added.

```
{
    "$schema": "http://json-schema.org/draft-04/schema#",
    "type": "array",
    "items": {
        "type": "object",
        "additionalProperties": false,
        "required": [
            "scope",
            "value"
        ],
        "properties": {
            "scope": {
            "$ref": "labels.schema.json"
            },
        "value": {
        "description": "Property value associated with the scope",
            "type": "integer",
```

```
            "minimum": -1,
            "maximum": 2147483647
            },
        "ven_type": {
        "description": "The ven type that this property is applicable to",
            "type": [
            "string",
            "null"
            ],"enum": [
            "server",
            "endpoint",
            null
            ]
        }
    }
},
    "uniqueItems": true
}
```

To ensure backend compatibility, the new field `ven_type` is specified as optional. If it is missing in the request, the parameter is considered as being of a server type.

Examples

The example below represents the complete JSON string returned by the GET `/api/v2/orgs/:xorg_id/settings/workloads` request:

```
{
    "href": "/orgs/1/settings/workloads",
    "workload_disconnected_timeout_seconds": [
        {
        "scope": [],
        "value": 10800,
        "ven_type": "server"
    },
    {
        "scope": [],
        "value": 3600,
        "ven_type": "endpoint"
    },
    ],
    "workload_goodbye_timeout_seconds": [
        {
        "scope": [],
        "value": 12000,
        "ven_type": "server"
    },
    {
        "scope": [],
        "value": 7200,
        "ven_type": "endpoint"
        }
    ],
    "workload_disconnected_notification_seconds": [
```

```
        {
        {
        "scope": [],
        "info": 1800,
        "warning": 3600,
        "error": 5400,
        "ven_type": "server
        },
        {
        "scope": [],
        "info": 1801,
        "warning": 3602,
        "error": 5403,
        "ven_type": "server
        }
    }
    ],
    "ven_uninstall_timeout_hours": [
        {
        "scope": [],
        "value"=>300
    }
    ]
}
```

In the following example, all four workload timeout setting properties are set via the PUT `/api/v2/orgs/:xorg_id/settings/workloads` request:

```
{
    "workload_disconnected_timeout_seconds": [
        {
        "scope": [],
        "value": 10800,
        "ven_type": "server"
    },
    {
        "scope": [],
        "value": 3600,
        "ven_type": "endpoint"
    },
    ],
    "workload_goodbye_timeout_seconds": [
        {
        "scope": [],
        "value": 12000,
        "ven_type": "server"
    },
    {
        "scope": [],
        "value": 7200,
        "ven_type": "endpoint"
    }
    ],
    "workload_disconnected_notification_seconds": [
    {
```

```
        {
        "scope": [],
        "info": 1800,
        "warning": 3600,
        "error": 5400,
        "ven_type": "server"
    },
    {
        "scope": [],
        "info": 1801,
        "warning": 3602,
        "error": 5403,
        "ven_type": "endpoint"
        }
    }
    ],
    "ven_uninstall_timeout_hours": [
    {
        "scope": [],
        "value"=>300
        }
    ]
}
```

Other Changed APIs

common label_mappings

Kubelink reports all label mappings to the PCE through the endpoint.

`PUT /api/v1/:org_id/:container_cluster_uuid/label_mappings`

When there is more than one LabelMap defined in the cluster, Kubelink will combine all labelMaps together.

When Kubelink detects duplicate entries or other validation errors, it will put the offending CRD into an error state. In reality, we will recommend that customers always create only one labelMap per cluster.

Container Workload Profiles

`container_clusters_container_workload_profiles_update_put`

This API is different from `container_clusters_container_workload_profiles_put` in the following way:

- the deprecated property `assign_labels` is removed
- the new property `container_workload_profiles` is added and gives a list of container workload profiles HREFs and Container Workload Profile URIs.
- The property `name` was removed was removed

common resource_condition

In this common schema, the name of the property `error` was changed into `err`.

Settings Traffic collector

The Settings Traffic Collector APIs have been changed to support more granular filters, for endpoints in particular.

There are three updated APIs in this group:

settings_traffic_collector_get

settings_traffic_collector_put

settings_traffic_collector_post

Two new properties have been added to all of them:

- `data_source`: Flow summary data source
- `network`: Flow summary network

For `settings_traffic_collector_put` and `settings_traffic_collector_post`, these properties contain additional definitions for their type.

Pairing Profiles

pairing_profiles_get

pairing_profiles_post

Fot these API, a new property can be listed or created: `ven_type`.

Workloads Interfaces

workloads_interfaces_get

For this API, the following changes have been made:

- Two required properties were removed: `ip_version` and `network_id`
- One required property was added: `network`
  - For this property, type `null` was added for `network_detection_mode` and `friendly_name`
- Other property changes:
  - Property `href` was added
  - Type `null` was added for `link_state`, `cidr_block`, and `default_gateway_address`

workloads_interfaces_network

For this API, a new property `name` was added to describe the name of the network.

workloads_with_ven_put

For this API, the property type `null` was added.

Deprecated APIs

common pairing_profile_ven_type

Deprecation announcement for the option `specified_during_activation`.

```
{
    "$schema": "http://json-schema.org/draft-04/schema#",
    "type": "string",
    "description": "Type of VEN that this pairing profile will enforce.
            specified_during_activation option is deprecated and will be
removed
        in the next API version.",
    "enum": ["specified_during_activation", "server", "endpoint"]
}
```

Illumio Core Release Notes 23.2

Welcome

These release notes describe the resolved issues and known issues for Illumio Core 23.2.*x* releases

Document Last Revised: March 2025

Document ID:14000-100- 23.2.32-PCE

Product Version

PCE Version: 23.2.32 (LTS Release)

VEN Version: 23.2.31 (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 Security Issue in 23.2.32-PCE

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

Resolved Security Issue in 23.2.31-PCE

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

Resolved Security Issue in 23.2.31-VEN

Upgraded cURL to v8.9.1 to address multiple CVEs.

Resolved Issues in 23.2.31 VEN

- **Harmless errors logged to OS syslog when nf_conntrack kernel modules were missing** (E-118298)

  Prior to this release, VENs installed on Linux workloads attempted to load current and deprecated `nf_conntrack` kernel modules. Because a subset of these modules were typically missing, potentially alarming but actually harmless errors were logged to the OS syslog. For example, `"modprobe: FATAL: Module nf_conntrack_ipv4 not found in directory."` This issue is resolved. In these circumstances, missing `nf-conntrack` modules no longer generate such errors.
- **VEN-PCE Communication Failed in a Proxy Environment** (E-110516)

  After upgrading a VEN in an environment where workloads are behind a proxy server and unable to resolve the PCE's FQDN, the VEN's communication with the PCE failed. This issue is fixed.

Known Issues in 23.2.31-VEN

- **Policy sync error thrown following Solaris VEN upgrade** (E-121220)

  A policy sync error was thrown after upgrading a VEN on a Solaris workload to release 23.2.31. The error appeared after switching the VEN from Idle to any other mode. Workaround: If you've encountered this issue, upgrade to VEN release 24.2.20 or later.
- **AIX / Solaris 10 policy update fails in some circumstances** (E-118539)

  Updating policy on AIX and Solaris 10 workloads fails if the workloads are in Full Enforcement mode and flow visibility is turned off. This issue is caused by incorrectly generated syntax. This is a known issue. Workaround: Go to **Servers & Endpoints > Workloads**, select AIX/Solaris 10 workloads that are in **Full Enforcement** mode, and then in the Visibility drop-down menu enable flow visibility by making sure the setting isn't **Off**.
- **Re-activating a deactivated VEN fails on AIX workloads** (E-118055)

  If you deactivate a VEN installed on an AIX workload and later re-activate it, activation fails and a 401 error is thrown. This is a known issue. Workaround: After you deactivate the VEN, remove the backup folder under the VEN's data directory. WIth the backup folder removed, re-activation succeeds.

Resolved Issues in 23.2.30-PCE

- **All Saved Filters Disappear after Running Topology Discovery** (E-116829)

  After running the Discover the Topology of your Organization option at the Traffic page, and the default graph was created, all previously saved filters would disappear.
- **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.
- **Header manipulation issue** (E-116114)

  Appropriate validation for host header was added to avoid any host header manipulation.
- **Script needed for default profile recreation and sync migration** (E-113855)

  A script was needed for default profile recreation and sync migration with release 23.2 and later.
- **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.
- **report_monitor and traffic_query services flapping on coordinator replica node after OS upgrade** (E-113024)

  On DX configurations, adding a new CC (Citus Coordinator) node or a new CW (Citus 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.
- **FQDN 'Provider is not' filter not working** (E-112068)

  When filtering using an FQDN, only one IP address was being filtered, and not the actual FQDN. Also, many remaining instances of the FQDN that were intended to be excluded from the search were instead being shown.
- **The Ransomware Dashboard was displaying the same port/process multiple times** (E-112055)

  This issue is fixed.
- **Received an empty response when navigating to the CWP (Container Workload Profile) page on the PCE UI** (E-111845)

  When the default container workload profile was deleted, a blank page was displayed when navigating to that container workload profile page.
- **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.
- **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.
- **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.
- **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.
- **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.
- **IP list traffic not appearing in searches** (E-108490)

  The IP list traffic was not appearing in searches due to the inclusion of an iplist containing an FQDN in query parameters. This led to the inclusion of region_id in the SQL query executed in each region. However, the region_id being passed is the leader's region ID. The issue happened only on a supercluster.

Resolved Issues in 23.2.30-VEN

IMPORTANT

Compatibility and performance issues can occur if the operating system version running on your workloads and endpoints is upgraded to a version that is not supported by the VENs on those machines. Before upgrading the operating system on workloads and endpoints, first make sure that the VENs installed on these machines support the new OS version. For workload VENs, see https://support.illumio.com/software/os-support-package-dependencies/ven.html . For Endpoint VENs, see https://support.illumio.com/software/os-support-package-dependencies/endpoint.html.

- **Policy application failed in some circumstances** (E-117246)

  Some earlier VEN versions failed to apply policy if the workload on which it was installed had multiple valid IPv6 DNS addresses. This issue is fixed.
- **Some endpoint VENs experienced high CPU usage and slow firewall programming** (E-116252)

  On Endpoint VEN's installed on MackBook macOS v14.x (Ventura), PlatformHandler exhibited high CPU usage and increasingly longer times to program firewall rules over time. The issue stemmed from an Apple bug that leaked `pfctl` anchors over time. The issue could be solved temporarily by rebooting the endpoint. Illumio resolved the issue by engineering a workaround.
- **Bug in nftables versions pre-0.9.2 prevented policy application** (E-116635)

  Policy failed to load on VENs installed on RHEL Linux 8/9 workloads with a version of nftables earlier than 0.9.2. This issue is resolved.
- **Issue affecting the persistent connection between PCE and VEN** (E-116177)

  A regression was introduced into 22.5.33 and 23.2.23 Windows VEN, which could cause the Event Channel between VEN and PCE to stop functioning, resulting in a policy convergence delay. This issue is resolved.
- **Some endpoint VENs experienced high CPU usage and slow firewall programming** (E-116006)

  On Endpoint VEN's installed on MackBook macOS v14.x (Ventura), PlatformHandler exhibited high CPU usage and increasingly longer times to program firewall rules. The issue stemmed from an Apple bug that leaked pfctl anchors over time. The issue could be solved temporarily by rebooting the endpoint. Illumio resolved the issue by engineering a workaround.
- **PCE didn't recognize external IP address of external Azure VM** (E-115935)

  Unix VENs failed to correctly detect Azure environment prevented the PCE from recognizing the external IP addresses of the workloads. This issue is resolved. VENs now correctly detect when they're operating in an Azure environment,
- **Failure to apply policy update caused by excessive pfctl table generation** (E-115342, E-113337)

  In some circumstances, Endpoint VENs failed to program firewall policy updates. The issue occured because the number of pfctl tables generated by customer rules exceeded the default limit, which has since been adjusted. This issue is resolved.
- **RHEL5 VEN didn't apply generated IPv6 rule** (E-113324)

  The RHEL5 VEN failed to ignore rules that reference IPv6 IPsets as designed, and as a result also failed to apply the generated IPv6 rules. This issue is resolved.

- **Windows VEN over-restricted cipher suites selection for Event Channel** (E-113245)
  When the PCE was set to disable weak ciphers, a service on the VEN restricted the selection of some TLS cipher suites on the Event Channel. This prevented the PCE from updating policy on Windows VENs using Lightning Bolts (event service), meaning policy could be updated only during scheduled heartbeats (5 minutes). This issue is resolved: Lightning Bolt communication now works as designed.
- **Improper VM shutdowns caused VEN data file corruption** (E-113231, E-109231)
  If a workload was shut down improperly, such as by a sudden loss of power, and the kernel crashed, some critical VEN data files could've gotten corrupted, preventing the VEN from loading policy. This issue is resolved. Critical VEN data files are now more resilient if the workload is shut down improperly.
- **Outbound source process rule failed with FQDN in the destination IP List** (E-112838)
  Rules that specified a Windows Outbound process or service failed to allow the configured connection(s) if the Destination IP List included an FQDN. This issue is resolved.
- **Generating an Individual Maintenance Token Failed** (E-111662)
  When the Agent Tampering Detection feature was enabled and a user generated a token for a specific VEN (as opposed to tokens for all VENs), in some cases it wasn't possible to perform a protected illunio-ven-ctl action such as stop. For example: P`S C:\Program Files> .\Illumio\illumio-ven-ctl.ps1 stop --maintenance-token <token for a specific VEN> Failed to verify maintenance token`.
- **Make policy fetch non-blocking** (E-104718, E-111622)
  This issue is resolved. Policy fetch requests now have a timeout of 15 minutes, which is longer than the standard VEN → PCE API timeout of 3 minutes. These requests also now send TCP keepalive probes to keep the connection active. Policy fetch requests are now performed on a separate thread, ensuring that the VEN can continue to operate and make other API calls without being blocked on policy fetch.
- **C-VENs failed to synchronize policy** (E-108536, E-111490)
  C-VENs running 21.5.33 showed "Error" for the Policy Sync state with the message "Failed to load policy line." Concurrent threads (`MsgHandler` and `downloadPolicyFromPCE`) caused a race condition because of shared variables. This issue is resolved.
- **VEN failed to process FQDN rules, caused blocked traffic** (E-111486, E-108639)
  After upgrading VENs from version 19.3.5 to version 22.5 and greater, some VENs failed to process FQDN rules, causing traffic to be blocked. Due to a transient error, the VEN may fail to detect the DNS server(s) on the workload and fail to program FQDN rules correctly. This issue is resolved. Now VENs will continue trying to detect a DNS server after the initial detection fails.
- **Policy sync error if no Allow rule for proxy server** (E-110516)
  If your environment included a proxy server and your Illumio policy didn't include a rule allowing the proxy's IP:port, the VEN reported a policy sync error and tried continually to sync policy. This issue is resolved.
- **PCE clone detection led to continual retry loop** (E-110732)
  After the PCE detected a cloned workload, multiple API failures occurred in **venAgentMgr** in a continual retry loop. This issue is fixed.
- **Message about stopping the venAgentMonitor appears in error** (E-110150) On macOS 14.3 Endpoints running VEN 23.2.22, you may see the following failure message if you issue `/opt/illumio_ven/illumio-ven-ctl restart` to restart the ven: `Stopping venAgent-Monitor: ...fail!` In this circumstance, this failure message appears in error and you can safely ignore it.
- **VEN IPSec policy tampering detection not supported with RHEL5** (E-110015)
  In Illumio Core 23.2.20-GA, VEN IPSec policy tampering detection and recovery doesn't work with VENs running on RHEL5 workloads. On all other supported Linux distributions, tampering detection works as designed.
- **Support for pairing VENs on AWS Workloads with IMDS v2** (E-109528)

This release provides support for pairing VENs on AWS workloads with Instance Metadata Service Version 2 (IMDS v2). This update was necessary to support IMDS v2 session-oriented authentication.

- **Improper VM shutdowns caused VEN data file corruption** (E-109231)
  If a workload was shut down improperly, such as by a sudden loss of power, and the kernel crashed, some critical VEN data files could've gotten corrupted, causing the VEN to lose connectivity with the PCE. This issue is resolved. Critical VEN data files are now more resilient if the workload is shut down improperly.

Resolved Security Issues in 23.2.30-VEN

- **curl was upgraded to v8.7.1** cURL is upgraded from 8.4.0 to 8.7.1 to address CVE-2023-38545 and CVE-2023-38546. The VEN is not impacted by these vulnerabilities.

Resolved Security Issues in 23.2.30-PCE

- **Upgraded cURL to v8.7.1 to address multiple CVEs**
- **json-jwt 1.13.0.gem upgraded to json-jwt-1.16.6** (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.
- **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.
- **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 acces, the likelihood of this exploit is low without additional access privileges.

Resolved Issue in 23.2.24-VEN

Issue	Fix Description
E-116177	**Issue affecting the persistent connection between PCE and VEN** Under certain cipher suite configurations, the persistent connection between the PCE and the VEN could not be established. This issue is fixed.

Resolved Issues in 23.2.23-VEN

- **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.

Known Issue in 23.2.23-VEN

- **False positive firewall tampering error** (EYE-113892)
  If the PCE pushes policy that is identical to 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 PCE Web Console. The VEN flushes the existing rules and then applies the rules in the current directory.

Resolved Issues in 23.2.22-VEN

Illumio 23.2.10 and 23.2.20 VEN releases were decommissioned for technical reasons. VENs from these releases are no longer available for installation. Features and bug fixes for these releases are available in Illumio 23.2.22-VEN.

- **VEN releases 23.2.21 and earlier crash on macOS 14.2 (Sonoma) machines** (E-111819) This issue is fixed in VEN release 23.2.22. If you're running 23.2.21 or earlier VENs and experience this issue, update your VENs to release 23.2.22 or later.
- **Connections dropped after upgrading older VENs to 23.2.10 or 23.2.20** (E-111663)
  After upgrading from VEN versions earlier than 23.2.10 to release 23.2.10 or 23.2.20, established connections could've been dropped whenever the VEN in full Enforcement mode received a policy update from the PCE. The issue occurred because VENs mistakenly removed conntrack entries even when there was a rule allowing such connections. The dropped connections were restored when the workload attempted to re-establish the dropped connection. This issue only affected Linux VENs using iptables. VENs for other operating systems and Linux VENs using nftables were not affected.
- **Generating an Individual Maintenance Token Failed** (E-111662) When the Agent Tampering Detection feature was enabled and a user-generated a token for a specific VEN (as opposed to tokens for all VENs), in some cases, it wasn't possible to perform a protected `illumio-ven-ctl` action such as stop. For example: `PS C:\Program Files> .\Illumio\illumio-ven-ctl.ps1 stop --maintenance-token <token for a specific VEN> Failed to verify maintenance token`
- **VEN failure to process FQDN rules caused blocked traffic** (E-111486)
  After upgrading VENs from version 19.3.5 to version 22.5 and greater, some VENs failed to process FQDN rules, causing traffic to be blocked. Due to a transient error, the VEN may

fail to detect the DNS server(s) on the workload and fail to program FQDN rules correctly. This issue is resolved. Now VENs will continue trying to detect a DNS server after the initial detection fails.

Resolved Issues in 23.2.21

- **Backport SC replication stats/improvement/monitoring changes to 23.2.21** (E-113021)
  After the fix, this issue is resolved as follows:
  Replication lag info now shows the actual pending replication count per region to confirm how many rows are pending replication from each region.
  It detects slon remote worker thread failures or deadlocks caused by replication and alerts the replication status to the PCE Health page.
- **Changes to system_health evnts 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.
- **PCE 22.5.32 not honoring disk usage** (E-112477)
  When traffic data weekly rollup and disk limit enforcement happen simultaneously, there's a potential race that could result in a crash of flow_analytics_monitor service, ultimately causing the traffic data disk limits not to be enforced properly.

Resolved Issue in Illumio Core 23.2.20+UI2

NOTE
This resolved issue applies to the PCE web UI for Illumio Core On-Premises customers only.

Performance issue in new PCE UI (E-111820, 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.

Resolved Issues in Core 23.2.20

Enterprise Server

- **Can't rename same policy object by changing letter case** (E-109292)
  Users were unable to change names from capital to lowercase for the same policy object. This is an issue when the same label names with different capitalization are used. The workaround is to change the existing name by adding or removing a letter, then saving, editing with the correct name, and saving again.

- **Linux pairing failing while pairing VMs** (E-109256)
  Linux paring was failing while pairing VM using the paring line. This issue is resolved.
- **The Reports tab missing in the UI** (E-109126)
  The issue where Access Wizard incorrectly indicated that users with Admin roles could access the Reporting page is resolved.
- **"Missing interface name" error reported after pasting IPs to an IPlist** (E-108877)
  PCE UI reported the error "Missing interface name" after pasting IPs to an IPlist. This issue is resolved.
- **Report generation fails for Japanese characters** (E-108799) Report generation was failing when Japanese characters were entered. This issue is resolved.
- **Workload Rules page could be slow to display** (E-108465)
  In the PCE UI, navigating to the **Rules** tab for a workload (choose **Workloads** from the menu > click a workload > click the **Rules** tab) could display the following warning and the page could fail to display information:
  "The next page seems to be taking longer than usual to load, continue waiting or press stop to cancel navigation"
  This issue was more likely to occur in customer environments that had thousands of IP addresses attached to each rule in the workload **Rules** tab. This issue is resolved. Illumio has simplified the processing to display the page as is without sorting the list of IP addresses.
- **PCE UI wasn't reflecting new rules in the Traffic table** (E-108313)
  When using the Traffic table to allow selected connections from potentially blocked traffic flows, the data in the table didn't update to reflect the new rules that allowed the connections. The rules were actually saved but the Traffic table data wasn't refreshed. You could work around the issue by switching your view between "Potentially Blocked" and "All Blocked" to force the table to refresh. In this release, creating rules to allow blocked connections update the Traffic table data to show the effect of the new rules.
- **UI not displaying services properly** (E-108057)
  Two issues have been discovered that hindered the proper display of services and are both resolved.
- **RHEL 5.x leaves symlinked files behind after unpairing the VEN** (E-108046)
  There was an issue affecting RHEL 5.x users, where symlinked files remained after unpairing the VEN. For a cleaner unpairing process, update to the latest release to apply this fix.
- **Issues with traffic analysis script** (E-107931)
  This script is mainly used by Support to help customers do traffic pattern analysis. For on-premises customers it requires access to PCE nodes; for Illumio Core Cloud customers, an Illumio operations ticket needs to be created. The details are described in this document: Traffic pattern analysis script.
- **Traffic not updated when switching from reported to draft view** (E-107766)
  Traffic was not updated when switching from 'reported view', 'draft view all blocked', and 'draft allowed'. This issue is resolved.
- **AIX VEN installs partway and never activates** (E-107369) In one case, the AIX workload system pidof binary had errors that blocked VEN installation and activation.
  This issue was resolved in 23.2.20. The incorrect pidof binary will only affect retrieving the correct PID of processes and will not block VEN installation and activation. When the pidof binary itself is resolved, VEN functions as expected.
- **New UI - Ruleset: The More and Edit icons were enabled for a deleted rule** (E-107147)
  This issue is resolved and icons appear as designed.
- **Allow time for ransomware exposure score to recalculate following PCE upgrade** (E-106619)
  Following an upgrade from a pre-23.3.0 Core release to Core 23.3.0, the value shown in the Protection Coverage Score on the Dashboard and the Ransomware Exposure column (Servers & Endpoints > Workloads) might be temporarily inaccurate while the PCE recalculates the value. Please allow a few hours for recalculation.

- **Query "Exclude Workloads from IP List" showing Workloads** (E-106292)
  When using the same IP list with "Consumer or Provider" and "Exclude Workloads from IP List Query", the results were unexpectedly returned for the workload. This issue is resolved.
- **Unable to add multiple IP ranges to a large IP list** (E-106025)
  Customers with large IP lists were unable to add multiple IP ranges. This issue is resolved.
- **Proposed Rules - Status information is being hidden** (E-105098)
  The Proposed Rules status information was hidden by the Ruleset Summary page. This issue is resolved.

Endpoint

- **macOS issue regarding proxy setup** (E-108402)
  In VEN 22.5.20, there was an issue with activation when Proxy was set up. This issue is resolved.
- **WinHttp and IE proxy info for Windows support report** (E-108387)
  There was a request to add WinHttp and IE proxy info for the Windows support report. This issue is resolved.
- **TCP with Broadcast/Multicase in the Flow Collection UI** (E-107013)
  The user should not be able to select TCP with broadcast or multicast. This issue is resolved.

PCE Platform

- **Backport to 23.2.20: Information Disclosure through Error Handling** (E-107463) When passing a specially crafted URL the PCE returns a verbose error stack trace.
- `metrics_database_service` **not starting** (105498)
  The service `metrics_database_service` was not starting. This issue is resolved.
- **Don't compute workloads affected by policy provision above a certain number of sets** (E-99868)
  Provisioning policy for organizations with a large number of workloads having too many updated rules often timed out because of the time-consuming algorithm resolving all the affected sets. Instead, all workloads are invalidated if the number of the affected sets is above the configurable threshold. This issue is resolved.
- **UI Policy Vacuum reports warning state when the backlog is 3.6%** (E-99322)
  The vacuum backlog health metrics can be in 'WARNING' status for two reasons: (1) The percentage of dead tuples reaches a certain threshold; (2) Some tables are considered at risk because they have not been auto-vacuumed for a while. In the latter case, the alert could appear even if the actual percentage of dead tuples is low. This might confuse the end user. This issue is resolved by adding an alert message if the alert is caused by some tables being at risk.
- **Keys were missing from agent_missed_heartbeats_check event detail page** (E-97912)
  When viewing a system_task.agent_missed_heartbeats_check event in the UI, the "resource changes" and "notifications" fields were missing from the UI. The data existed in the API JSON but these values didn't appear in the UI. This issue is resolved.

Data Experience

- **Existing policy with label group not displayed in the UI** (E-101505)

In Illumination Classic, when adding a new rule from the App Group Map view, label groups were not displayed in the auto-populate window. This issue is resolved and Illumio Core works as expected.

UI Components

- **Miscellaneous user interface issues** (E-105294)
  The following user interface issues are now resolved:
  - The **Reset** button was not enabled when selections in **Destinations|Sources|Destination Services** were modified. This prevented a user from resetting to previous values.
  - Dashboard and Cloud were not displayed in Instant Search options when trying to search these pages in Instant Search.
- **App Group is not showing for Workload Manager in the New UI** (E-105068)
  Workload manager couldn't see the **App Group** menu in the New UI. If users navigated from the Old UI to the App Group page, and then switched to the New UI, they could see the data for the App group, but still could not see an **App Group** option in the menu. This issue is resolved.
- **Usernames with non-English characters appear garbled** (E-104956)
  Characters under the consumer process column were showing garbled output when the username had non-English characters (such as Japanese). This issue is resolved.
- **Unable to add subnet mask CIDR to unmanaged workload interface** (E-104729)
  In certain conditions, a CIDR could not be applied to an unmanaged workload interface. Note that the CIDR is used for informational purposes only to encode information about a subnet mask, and does not add the entire IP range to the unmanaged workload. This issue is resolved.

UI Framework

- **Locked out of Workload details** (E-109125)
  Users navigate to the workload Detail page by clicking on a managed workload on the List page. If a user then navigates back and clicks 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 take users to the Detail page of Workload A. This issue is resolved.

Illumination Plus

- **Illumination Plus and reports pages displaying blank** (E-102528)
  Illumination Plus and reports pages were displaying blank when users created a custom time-saved filter in different time zone formats. This issue is resolved.

RBAC

- **RBAC permission leakage across async APIs** (E-109132)
  The scoped user was unable to download the correct information according to the granted access. Instead, the user was seeing the data not accessible to the scope he had been assigned. This issue is resolved.

- **RBAC permission leakage across async APIs** (E-109102)
  The scoped user was not able to download the correct information according to the granted access. Instead, the user was seeing the data not accessible to the scope he has ben assigned. This issue is resolved.

VEN

IMPORTANT

Illumio 23.2.10 and 23.2.20 VEN releases were decommissioned for technical reasons. VENs from these releases are no longer available for installation. Features and bug fixes for these releases are available in Illumio 23.2.22-VEN.

- **Activation Code Logged in Plaintext** (E-110125) 22.5.0 and later VENs expose the activation code in plaintext. The affected log file is accessible by the root/admin user only. This issue is resolved. The activation code is censored from the logging of the activation payload.
- **VENs fail to communicate after VEN upgrade in some cases** (E-109968, E-109762) When a VEN paired to a 23.2.10 or 23.2.11 PCE is upgraded to VEN version 23.2.0, 22.5.0 through 22.5.20, or earlier, the VEN loses connectivity with the PCE. This is resolved in this PCE version. 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 .
- **False nftables firewall tampering error** (E-109623)
  In some cases, on operating systems using nftables, a false positive firewall tampering error was reported on enforced workloads with FQDN rules. This issue is resolved.
- **Agent Manager process crash on VENs using Kerberos** (E-109606)
  When Kerberos was used for VEN-PCE authentication, a VEN process (Agent Manager) could crash after the VEN was upgraded from an older version, or after the VEN was restarted. The crash occurred due to a defect in the VEN code, due to which a NULL pointer was dereferenced. This issue is resolved in this release of the VEN.
- **Occasional async API failures** (E-109356)
  The PCE could enter a state where async API calls failed until a PCE restart was performed. This issue is resolved.
- **Resolved issues for AIX VENs:**
  - **Manual testing: AIX OS Pairing Script** (E-109328)
  - **UI automation to test the AIX VEN upgrade paths** (E-108631)
  - **Ultron Upgrade Test** (E-108630)
    AIX VENs can only be upgraded starting rom 23.2.0. If you try to upgrade from an earlier version, you will get an error message that you cannot upgrade for that AIX VEN. This is due to the addition of the AIX pairing script that was added in VEN SW 23.2.20.
- **Windows VENs went offline after upgrading from version 22.3.0-9540 to 23.2.0-129** (E-108661) On Windows, the VEN upgrade could fail if a VEN service was taking longer than 30 seconds to stop. The issue was resolved.
- **PCE AIX VEN upgrade from 22.5.30 to 23.2.10 and 23.2.21 fails** (E-108216)
  The PCE AIX VEN upgrade from 22.5.30 to 23.2.10 and 23.2.20 was failing. This issue is resolved.
- **REST calls to the PCE failed when `libcurl` was set globally** (E-108192)

Direct REST calls to the PCE failed when the `libcurl` environmental variable `https_proxy` was set globally. This issue is resolved.

- **VEN Upgrade - Pick the LTS or default System version** (E-107402)

  The default VEN version is now at the top, and then the most recent VEN version is first on the VEN library page and VEN upgrade modal.
- **Unexpected output in `/var/log/messages` after upgrade to VEN 22.5.20-9798** (E-106827)

  On RHEL8+ workloads, sometimes an error might be shown in `/var/log/messages:`

  ```
  venPlatformHandler [236775] : /dev/stdin:1:1-82: Error: Could not process rule: No such file or directory
  ```

  This error message is harmless. Starting with 23.2.20-VEN, this harmless error was removed from `/var/log/messages.`
- **SLES 15 SP4 VEN tampering** (E-106131) On SLES15 SP4, the `iptable_nat` module file has a different file extension, which results in false negative firewall tampering. From this release, 23.2.20 VEN can recognize these module files.
- **Disabled boundary rules causing potentially blocked by boundary flows in Explorer** (E-98104)

  Explorer was displaying traffic that is potentially blocked by a boundary even if there were no active boundary rules. This issue is resolved.
- **Activation scripts (sed) do not tolerate `https:// prefix in --management-server` argument** (E-89443)

  Activation scripts invoked by `illumio-ven-ctl` used to fail if given a prefix of `https://` . Instead, an argument with no protocol was preferred, such as : `example.com:8443` instead of `https://example.com:8443`. After this fix, either format is acceptable.

Containers

- **Deadlocks in Container Workload Purging** (E-106907)

  There is a background job in the PCE to remove decommissioned container workloads from the database. This background job could fail in highly dynamic container environments due to PostgreSQL deadlocks. This job is more resilient to this and other failures.

Documentation Updates for Illumio Core 23.2.20

PCE in Supercluster did not start when service discovery key changed (E-104880)

The following explanation has been added to the PCE Supercluster Deployment Guide, in the "Deploy New Supercluster" topic under the section "Verify Supercluster Readiness":

If the new PCE being added to the Supercluster has a different value for the parameter `service_discovery_encryption_key` defined in its `runtime_env.yml` file than the value specified in the `runtime_env.yml` files in all the other PCEs in the Supercluster, the new PCE will fail to join the Supercluster.

To remedy this possible problem when a new PCE does not join the Supercluster, follow these steps:

1. On the new PCE, edit its `runtime_env.yml` file so that its value for `service_discovery_encryption_key` is identical to the value set in the `runtime_env.yml` files of all other Supercluster nodes.
2. Reset all nodes:
   ```
   $ sudo -u ilo-pce illumio-pce-ctl reset
   ```
3. Start services at runlevel 1 on all nodes:
   ```
   $ sudo -u ilo-pce illumio-pce-ctl start --runlevel 1
   ```
   Note: If a node gets stuck in the PARTIAL state, reboot the node.
4. On any node, set up the database:
   ```
   $ sudo -u ilo-pce illumio-pce-db-management setup
   ```
5. On any node, set runlevel 5:
   ```
   $ sudo -u ilo-pce illumio-pce-ctl set-runlevel 5
   ```

Resolved Issues in Core 23.2.10

PCE Platform

- **Maximum user session limit was exceeded by impersonated sessions** (E-106017)
  Each PCE cluster has a maximum number of user sessions that can be logged in at the same time (configured in the object limit `total_active_sessions`). Impersonated sessions, such as scheduled jobs that were logging in to access PCE data, could cause the limit to be exceeded improperly. This issue is resolved. The total number of user sessions now includes only actual logged-in PCE users.
- **Incomplete static policy caused VENs to go offline** (E-105833)
  In some circumstances, VENs went offline after the PCE sent an incomplete static policy to VENs. This issue is resolved.
- **High memory consumption on Supercluster data nodes could occur** (E-105671, E-104608)
  Due to a memory leak in the database replication process, the memory consumption on data nodes of a Supercluster could gradually increase. This issue is resolved. In this release, a memory leak no longer causes memory consumption by the PCE to continuously increase.

Policy Platform

- **Workloads page did not update on external IP changes** (E-106847, E-106806)
  When VENs are deployed on VMs in certain well-known public clouds (such as AWS), the PCE attempts to detect the public NAT address (e.g. elastic IP) of those workloads and use them in policy. The logic that updates the NAT address upon a VEN heartbeat was not working properly. When the NAT address of a public cloud VM changed, the PCE did not program the new address in the policy unless there was an interface change on that VM. This issue is now resolved.
- **Supercluster PCE upgrade failure from PCE version 22.x with endpoint VENs** (E-106479)
  The supercluster PCE upgrade failed in the `illumio-pce-db-management migrate` step when upgrading from PCE version 22.2.x to 22.5.x when endpoint VENs were present before the PCE upgrade. This issues is resolved.
- **Keys were missing from agent_missed_heartbeats_check event detail page** (E-97912)
  When viewing a `system_task.agent_missed_heartbeats_check` event in the UI, the "resource changes" and "notifications" fields were missing from the UI. The data existed in the API JSON but these values didn't appear in the UI. This issue is resolved.

Data Experience

- **List of VENs on the Dashboard was incomplete** (E-105827)

  On the Illumio Dashboard, a UI problem allowed only a partial list of VENs to appear in the **Active VENs by Version** section. The issue occurred regardless of the zoom level of the browser. This issue is resolved.

UI Components

- **Miscellaneous user interface issues** (E-105294)

  The following user interface issues are now resolved:
  - The **Reset** button was not enabled when selections in **Destinations|Sources|Destination Services** were modified. This prevented a user from resetting to previous values.
  - Dashboard and Cloud were not displayed in Instant Search options when trying to search these pages in Instant Search.
- **Virtual server rules weren't displayed in the Rules tab** (E-103687)

  When viewing a virtual server page, the **Rules** tab could be empty. This issue occurred when you navigated to the **Rules** tab from the **Summary** tab using the following path: PCE web console main menu > **Policy Objects** > **Virtual Servers** > **Summary** tab > **Rules** tab.

  This issue is resolved. In this release, the virtual server rules appear in the **Rules** tab when navigating from the **Summary** tab.

Endpoint

- **VEN pairing fails with some macOS updates** (E-106229)

  A recent security update from Apple caused the macOS VEN pairing to fail. An error appeared, "Could not set environment: 150: Operation not permitted while System Integrity Protection is engaged." This issue is resolved.
- **VEN services started unnecessarily** (E-106136)

  On some Windows workloads, VEN services were restarted unnecessarily after waking up from sleep. This issue is resolved.
- **Double colons in FQDNs with quad A records caused policy sync error** (E-104996)

  A policy sync error affecting multiple VENs occurred in the following circumstances:

  1. The PCE policy includes rules specifying FQDNs, *and . . .*
  2. The customer environment has FQDNs that contain AAAA (IPv6) records ending in double colons (::). For example, 2603:1037:1:60::

     This issue is resolved. This error no longer occurs in these circumstances.

Illumination Plus

- **Illumination Plus and reports pages display blank when time-saved filters are created** (E-102528)

  Illumination Plus and reports pages were displaying blank when users created a custom time-saved filter in different time zone formats. This issue is resolved.

Enterprise Server

- **Draft Policy Decision shows empty** (E-107172)

  When running a draft query on a traffic table with cleared filters, users encountered an empty Draft Policy Decision column in the report. This issue is resolved.
- **Rule reordering not working for Intra-Scope rules if the ruleset includes an Extra-Scope rule** (E-107148)

  In the new user interface, users were unable to reorder Intra-Scope rules within rulesets also containing Extra-Scope rules, or the other way around. This issue is resolved.
- **Services Windows: Process/Service-Based: delete port/protocol functionality failing** (E-107099)

  When users added a single port and then added multiple items for Windows service-based processes, the process paths, and port names displayed incorrectly. When users then deleted a single port, data not marked for deletion were nonetheless deleted. These issues are resolved.
- **Some buttons in the Services UI were disabled** (E-107097)

  After opening the Edit mode for any service with Operating System attribute **All Operating Systems: Port-Based** and adding a new Service Destination, the **Add** and **Save** buttons on the page were disabled. This issue is resolved and those buttons are now enabled in this circumstance.
- **Ransomware Dashboard always shows a high Protection coverage score** (E-106996)

  In an environment with no flow data for two weeks, the protection coverage score shown in the dashboard and workload summary pages is 100%. This issue is resolved.
- **Default collector filters/aggregation incorrectly filters TCP Multicast/Broadcast** (E-106955)

  Multicast and Broadcast cannot be TCP, yet default filters for new organizations incorrectly included Multicast TCP and Broadcast TCP. The following filters have been removed from the default list:
  - Netbios 137: Action - Drop, Transmission - Broadcast, Protocol - TCP, Port - 137
  - WS Discovery 3702: Action - Drop, Transmission - Multicast, Protocol - TCP, Port - 3702
- **Workloads page not updating external IP changes** (E-106892)

  Workloads page was not updating external IP changes to release 22.5. and 23.2. This issue is resolved.
- **Illumination Plus Explorer saved traffic filters missing** (E-106770)

  In the new UI, the saved traffic filters were missing in Illumination Plus. This issue is resolved.
- **Events page showing repeated 'clone.detected' messages** (E-106579)

  After upgrading from release 21.5 to 22.5, the Events page was flooded with 'clone.detected' messages up to 5 times per second. This issue is resolved.
- **Global Viewer seeing "Add Rule" option in the UI Map** (E-106288)

  A user with the Global Viewer role was able to see the option "Add Rule" in the UI by mistake. This issue is resolved.
- **On-Prem 21.5.34 Workload Filter Inconsistency** (E-106223)

  Using multiple filters for the workload page that includes IP addresses might have produced an inaccurate result set. This issue is resolved.
- **Unable to edit Label in the Scope of a duplicated Ruleset** (E-106200)

  Users were unable to see the ENV label type until they remove the ENV labels from the Consumer in the Extra-scope rules contained in the Ruleset. This issue is resolved.
- **"All blocked" filter not showing flows blocked by deny rules** (E-106163, E-106140)

  When "All Blocked" filter was used, the flows blocked by the "deny" rules were not showing up. This issue is resolved.
- **UI does not allow copying of IPs from the traffic view** (E-106030)

In the new UI, users were unable to copy IPs from the Traffic view. This issue is resolved.

- **PCE upgrade failure from PCE version 22.2.x and earlier to 22.5.20 and later with endpoint VENs** (E-105999)

  The PCE upgrade failed in the `illumio-pce-db-management migrate` step when upgrading from PCE version 22.2.x and earlier to 22.5.20 and later when endpoint VENs were present before the PCE upgrade. This issue is resolved.
- **Workloads filter returned an incomplete list** (E-105920) Specifying a particular subnet when filtering for workloads returned an incomplete list if any of the workloads had more than one interface in that subnet. This issue is resolved.
- **Mesh: Re-renders repeatedly. Interactions are not working** (E-105167)

  Hover and brush interactions on Mesh have nit not been working properly and images re-render repeatedly. This issue is resolved.
- **Menu option "Core Services" appeared in error** (E-105141)

  In a cluster in which Core Services was not enabled, the **Infrastructure > Core Services** option appeared in the left pane. This issue is resolved. 'Core Services' no longer appears when it's not enabled in the cluster.
- **After upgrade, the VEN could lose connectivity to the PCE** (E-105022)

  After upgrading the VEN to 22.5.10, it could lose connectivity with the PCE. This issue only occurred with PCEs that were part of a Supercluster deployment. This issue is resolved. After upgrading the VEN to 22.5.22, the VEN can connect with PCEs in a Supercluster.
- **OS, Severity, and Port Type should be omitted in the service edit** (E-104301, E-106881)

  Ransomware attributes OS, Severity, and PortType were added to a non-ransomware port and protocol for a ransomware service.

  In the Service editing page, attributes specific to ransomware services are now placed in a clearly differentiated part of the page.

VEN

IMPORTANT

Illumio 23.2.10 and 23.2.20 VEN releases were decommissioned for technical reasons. VENs from these releases are no longer available for installation. Features and bug fixes for these releases are available in Illumio 23.2.22-VEN.

- **Improve CLI messages to help troubleshoot activation problems** (E-106492)

  The illumio-ven-ctl status command output now shows the Agent Type of the specified VEN (endpoint or server), which can be useful in troubleshooting activation failures caused by mismatched VEN types. The illumio-ven-ctl activate command provides an error reason and error message details for identifying agent type (ven_type) mismatches like this, and other similar potential reasons for activation failure.

Containers

- **Potential PCE performance impact in highly dynamic container environments** (E-106906)

  When C-VENs acknowledged to the PCE that policy had been applied, the PCE in turn updated all records associated with the C-VENs, including records for previously-deleted

container workloads still in the PCE database. While this caused no functional issues, it could possibly result in a large number of writes with the potential to degrade performance in highly dynamic container environments where containers were being created and deleted very quickly. This issue is resolved.

- **Kubelink could restart when container cluster services were deleted** (E-104786)

  Kubelink could restart due to an unexpected PCE error when reporting to the PCE that container cluster services were deleted. This issue occurred when PCE port separation was enabled. This issue is resolved.

New Feature in 23.2.22+A1-VEN

This VEN release supports the **Rule Hit Count Report** feature, available in Illumio Core release 23.5.10. For details, see What's New and Changed in Release 23.5.10.

Resolved Security Issue in 23.2.22-VEN

In this release, the version of cURL embedded in the VEN code is updated to **8.4.0**.

Resolved Issues in 23.2.0

Illumination Plus

- **Reported policy decision is incorrect when the flow is blocked by boundary** (E-102588)

  Draft policy decision now shows as 'By Boundary' if the traffic is 'blocked by a boundary'. This issue is resolved.
- **Filtered Objects lists are not displayed properly** (E-102466)

  When users add a filter after the PCE has generated two columns of objects, the first column (workloads) stays empty and the second one (container workloads) contains the filtered object. This issue is resolved.
- **Delete icon not visible when a filter has a long name** (E-102359)

  The Delete icon was not properly visible in Illumination Plus and Explorer if a filter with a lengthy name was saved. This issue is resolved.
- **Connections tab customized columns not sticky** (E-101574)

  In Illumination Plus Map split view, with Maps and Connections, when users choose to customize columns on the connections panel, the options revert back to none for each line clicked. This issue is resolved.
- **Provider/Consumer order mismatched between filters and column headers** (E-101156)

  Configuring the provider/consumer order in the Policy Settings did not control the filters and the column headers in the table view of Illumination Plus. Instead, the filters and column headers were displayed in the opposite order. This issue is resolved.
- **Illumination Plus - Reports page displaying with blank page when upgrading from v22.4.x to 22.5.0** (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.

Core Services

- **Traffic worker not coming up after stop/start** (E-104519)
  After operations involving changes in the runlevel and/or service restart, in rare circumstances, the app gateway service generated duplicate proxy ports. This resulted in the failure of services, such as traffic worker, to connect to Redis-related services, with a "wrong password" exception. This issue is resolved.
- **In Traffic Pattern Mode detection, clicking the button won't show traffic** (E-102906)
  There should be no information icon for detected Scanner Core service in Recommended and Accepted Grid. This issue is resolved.

PCE Platform

- **Memory Monitor Fails Intermittently** (E-103608)
  The PCE has a Ruby memory monitor that is supposed to prune processes that are consuming too much memory over time. Occasionally, this memory monitor would fail to prune processes, causing increased memory usage. This issue is resolved.
- **Potential PCE DOS caused by malicious IF-None-Match header** (E-102567)
  This issue is resolved.
- **Apply label mapping for nodes reported by Kubelink** (E-102074)
  The PCE is now able to handle Kubernetes node's labels and properly map them to Illumio labels. Note that it is possible to automatically override the values of the new Illumio node's labels in this process.
- **Verbose Error Generation within the PCE** (E-99880)
  When passing a specially crafted URL the PCE returns a verbose error stack trace. This issue is resolved.
- **Data node stuck in PARTIAL during regression test** (E-89797)
  This PCE Platform issue applies to Illumio Core On-Premises customers only. It does not apply to Illumio Core Cloud customers.
  In rare cases, if application metrics is enabled, the data node could be seen in PARTIAL state both from the illumio-pce-ctl cluster-status and illumio-pce-ctl status. In those cases, if metrics_database_service/influxdb is not running, move the influxdb bolt file located in PERSISTENT_DIR/influxdb/meta/influxd.bolt to any directory outside this InfluxDB directory. This issue is closed and does not require a fix.
- **Show last login dates for API Keys** (E-81919)
  The date and time of the last login that used the API api_keys_get is now properly described in the API documentation. Previously, this information was shown in the UI only.

Data Experience

- **Context menu moves out of view when close to Map edge** (E-101545) When right-clicking on a node that is near the edge of the screen in Map view, the context menu goes out of view.
- **Illumination Plus - Reports page displaying with a blank page when upgrading from v22.4.x to 22.5.0** (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.
- **Incorrect mapping to Container Network** (E-99193)
  In Illumination Plus and Explorer table, we used to display the network name in consumer and provider columns, which made users associate the network name to both the consum-

er and provider side. It is reasonable to put the network name in its own column. Therefore, in Illumination Plus we make another column "Network" and stack in the flows/bytes column; in Explorer, we add a separate "Network" column. This issue is resolved.

- **22.5.0 Illumination Plus search properties aren't persistent** (E-99125)

  If a user picked certain properties in the Explorer queries to be visible, and ran a query, it reverted back to a default view. This issue is resolved.
- **Illumination Plus - Add dragging icons for Mesh axis** (E-98339)

  The Mesh view in Illumination Plus did not have a selectable drag element on the vertical axis. It now does. This issue is resolved.

UI Components

- **Rules on the Virtual Servers section are not visible when directly navigated to from the Summary section** (E-103687)

  When the user browsed directly to the Rules tab from the Virtual Servers Summary section, no rules were displayed unless the user selected the Members section and then selected Rules again. This issue is resolved.
- **Unable to use 0.0.0.0/0 in iplist** (E-102198)

  When users entered 0.0.0.0/0 to create an iplist, the values were rejected. This issue is resolved.
- **'No X Label' filters are not working when selected from 'Search All Categories'** (E-102000)

  When users chose a filter like 'No Application' or 'No Location' on the Workloads and VENs page, the page did not refresh with the filtered results. This issue is resolved.

UI Platform

- **Filter for 'Setting' item not working** (E-104235, E-104236)

  When users viewed Draft Changes and filtered by setting, the results did not reflect the setting filter. This issue is resolved.
- **Unable to distinguish between unmanaged workload and managed in Illumination Plus** (E-101069)

  Illumination Plus icons for managed and unmanaged workloads were misleading. As a result, it was impossible to distinguish between the unmanaged "Router" and the managed "WIN10-225" workload. This issue is resolved.
- **Frequent nft table tampering warnings** (E-100010)

  On VENs using nftables 1.0.0 or later, tampering events occurred every 10 minutes, even though no actual tampering occurred. This was caused by a change in nftables 1.0.0. This issue is resolved. The VEN now responds correctly, no matter whether the nftables version is earlier or later than 1.0.0.
- **Autocomplete not filtering labels based on user scope** (E-98207)

  The VEN page displayed all labels instead of solely the ones applicable to scoped users. This issue is resolved.
- **Rule search: 'Extra-Scope Rules' option is missing in filter dropdown** (E-97637)

  When using the Rule Search page, the Extra-Scope Rules option was missing from the filter dropdown menu. This issue is resolved.
- **Browser unresponsive while editing a huge IP list** (E-96832)

  Browsers were unresponsive when users edited large IP lists for policy objects. IP list validation is now disabled above a certain threshold, mitigating the load on browsers. This issue is resolved.

- **Filtering by an invalid Protocol in the Services List page displays all services** (E-68251)

  If a user typed an invalid protocol and pressed **Enter**, the entered protocol appeared as a filter item, but the list page was not refreshed. The UI validated the entered protocol and refreshed ONLY if the protocol was valid. The UI made no API calls for an invalid protocol. This issue is resolved.
- **Filtering by the invalid port in the Services List page displays an error** (E-68249)

  If users filtered the service list using an invalid port, they received a 406 error: "Port value out of range". The port filter category is a free search, and the user input was passed to the API request without validation. An invalid entry resulted in an API error. This issue is resolved.

Policy Platform

- **Workload in Selective Enforcement is fully protected by protection coverage 0%** (E-103808)

  A user could choose Selective Enforcement, with ports fully protected (blocked by the boundary) for a workload, but the protection coverage score was 0%. This issue is resolved.
- **Constant policy churn due to "All Workloads" with "Use Workload Subnets"** (E-102250)

  When either the provider or consumer of a rule is set to "all workloads" and the "use workload subnets" option was enabled for that side of the rule, the PCE did get into a state where VENs are almost always in "Active (Syncing)". This issue is resolved.
- **IP address filter for IP Lists doesn't consider exclusions** (E-97009)

  Filtering did not work correctly for IP lists with exclusions. This issue is resolved.
- **Rule coverage for endpoints is timing dependent** (E-96488)

  Workload > workload rule coverage queries checked to verify that workloads were on the same network before returning any rules between them. This was very confusing with endpoints, because endpoint network membership changes frequently, which broke the explorer/illumination-driven policy-checking workflow. This issue is resolved.

Platform

- **Validation Error when changing IPv6 settings on SC PCE** (E-102469)

  When using a supercluster, 406 input_validation_errors occurred when changing IPv6 settings on the UI. This issue is resolved.
- **PCE should stop requesting client cert** (E-93147)

  The PCE tried to request a client certificate every time and allowed it even if the client did not send a certificate. It was an extra handshake that could have caused delays. This issue is resolved.

Data Platform

- **Deduping in the flow analytics daemon did not sum byte counts properly** (E-107303)

  This issue is resolved.
- **flow-dg ingestion service restarts when trying to process a deleted file** (E-104068)

  The relevant service ran into errors and got restarted because of pruned backlog files. This issue is resolved.

RBAC

- **Reports show in main menu for user with Global Administrator role** (E-102127)
  Global Administrator Role users were able to see a Reports option in the hamburger menu, causing an error when selected. This issue is resolved.

VEN

- **Unable to use Windows VEN set-proxy commands** (E-103704)
  The Windows VEN did not allow the use of the set-proxy command and instead returned an error. This issue is resolved.
- **VEN Dashboard 403 Error with Scoped User** (E-103570)
  Dashboard was not supported for scoped users. The `isUserWithReducedScope()` check for the Dashboard Icon in the Header Menu was not working. As a result, clicking on the Dashboard icon threw errors for scoped users. This issue is resolved.
- **Pairing Profile VEN version drop-down list is not in any discernable order** (E-102162)
  The version list did not display in a discernible order. The UI was corrected, and the version list was put in numerical order. This issue is resolved.
- **Support CloudLinux for VEN** (E-101473)
  This release of the VEN adds support for a new distribution of Linux. CloudLinux versions 6, 7, 8, and 9 are now supported.
- **VEN clone fails with "supported_ven_types outside of the schema" error** (E-100717)
  There was an issue introduced in 22.5.0 where a clone would no longer re-activate successfully, and users saw an error message in the PCE event log. This issue is resolved with 22.5.10 and subsequent releases.
- **Improper certificate validation on macOS VEN** (E-100532)
  Certificate validation was improperly performed on the macOS VEN, impacting traffic between the VEN and the PCE. This issue is resolved.
- **Frequent nftables tampering warnings** (E-100010)
  On VENs using nftables 1.0.0 or later, tampering events occurred every 10 minutes, even though no actual tampering occurred. This was caused by a change in nftables 1.0.0. This issue is resolved. The VEN now responds correctly, no matter whether the nftables version is earlier or later than 1.0.0.
- **False nftables firewall tampering error** (E-99516)
  In some cases, on operating systems using nftables, a false positive firewall tampering error is reported on enforced workloads with FQDN rules. This issue is resolved.
- **Unauthorized VENs are causing frequent events related to interface_statuses/update** (E-98612)
  When a VEN is unpaired from the PCE, it is possible for the VEN to not receive the unpair message. This can happen, for example, if the host is down for an extended time. When the host comes back up, VEN requests to the PCE is rejected, and the PCE emits `request.authentication_failed` events. This issue is resolved. The VEN no longer makes frequent requests to the PCE after receiving consistent authentication errors.
- **Solaris 11.4 VEN tampering events with ipf.rules.v6.normalized** (E-96378)
  When firewall tampering was detected, the following warnings were in `platform.log`.

```
WARNING:: normalize_rules: File /opt/illumio_ven_data/etc/firewall
/workload/XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX/current/ipf.rules.v6
does not exist Error 0.
log/platform.log-2022-09-15T10:15:02.806-05:00
WARNING:: normalize_firewall_state: Failed to persist normalized
```

```
firewall state to /opt/illumio_ven_data/etc/firewall/workload/
XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX/tampered/ipf.rules.v6.normalized.
```

This issue is resolved.

- **Solaris 11.4 Cannot Allocate Memory errors** (E-93290)

  The VEN failed to remove the old policy in some cases after applying a new policy. The accumulation of the old policy led to additional memory consumption in pf and eventually pf ran out of memory. The new version of the VEN corrects this issue by removing the old policy after applying a new policy.

PCE Web Console UI

- **An incorrect error is displayed when an invalid port is entered while creating a service** (E-68181)

  When creating or editing a Service, entering an invalid value (for example, 12334454) in the **Port and/or Protocol** field produced an incorrect and misleading error of "Port or Process is required." This issue is resolved. When a user does not enter a valid value, a dropdown menu shows a message of "0 matching results."

Known Issues

Enterprise Server

- **Unable to select workload inside an open combo node** (E-112344)

  Clicking on a workload inside a combo node does not select a workload and the traffic links connected to it are not showing.

  Workaround: none
- **The Explorer page is not loading and redirects to the Traffic page** (E-111574)

  Workaround: The Explorer page loads if users enable both Explorer and Classic Illumination.
- **Vulnerability data shows on the map only when interacted with** (E-111087)

  Vulnerability data shows on the Vulnerability Map only when interacted with. Workaround: none.
- **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 is incorrect, it should be 'unknown' for flows with deleted workloads.

  Workaround: none.
- **Deleted Workload traffic link shows a policy decision** (E-110143)

  A deleted workload traffic link shows a policy decision by mistake.

  Workaround: none.
- **Allow time for ransomware exposure score to recalculate following PCE upgrade** (E-106619)

  Following an upgrade from a pre-23.3.0 Core release to Core 23.3.0, the value shown in the Protection Coverage Score on the Dashboard and the Ransomware Exposure column (Servers & Endpoints > Workloads) might be temporarily inaccurate while the PCE recalculates the value. Please allow a few hours for recalculation.
- **Blank space in IP address causes a query to fail** (E-106290)

When filtering by IP address in **Explorer > Traffic**, if a blank space appears after an IP address in the filter criteria, the query fails. Explorer doesn't auto-correct blank spaces in this circumstance, which might be unexpected.

Workaround: If your query fails, examine the filter criteria and ensure that no blank spaces appear after IP addresses.

- **App Group is not showing for Workload Manager in New UI** (E-105068)

  Workload manager cannot see the **App Group** menu in the New UI. If you navigate from the Old UI to the App Group page, and then switch to the New UI, you can see the data for the App Group, but still cannot see an **App Group** option in the menu.
- **Standalone PCE not starting up after service_discovery_encryption_key change** (E-104880)

  Workaround: none
- **Incomplete data for Workloads by ransomware exposure/Ports by severity** (E-104745)

  Workloads by ransomware exposure and Ports by severity sometimes have incomplete data on scale setup.

  Workaround: None
- **Fedramp: 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.
- **When users load saved filters in Explorer, more than four labels are showing up** (E-102438)

  Workaround: None
- **Saved filter for Explore and Loading showing empty data by default** (E-102257)

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

  Workaround: None

Illumination Plus

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

  Using an empty Label Group as a filter in Explorer or Illumination returns the same results that would be expected if the filter criteria was "Any Workloads." This is incorrect. Filtering on an empty Label Group should return no results.

  Workaround: To avoid this issue, make sure that Label Groups contain at least one label.
- **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 max number in Illumination Plus is 10,000 while in Explorer it is 100,000.

  Workaround: Update the max results setting in Explorer to get more than 10K results.
- **After creating a new organization, users are unable to load saved filters** (E-102268)

  Workaround: Create the Save filter once you issue a new query from Explorer or Illumination Plus.
- **Recent filters became empty when users run a query from Explorer** (E-102525)

  Workaround: None.
- **Enforcement boundaries filters are still showing after enforcement boundaries are deleted** (E-102251)

  Workaround: None

- **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
- **User isn't automatically redirected to the Extra-Scope tab in some cases** (E-98507)

  In **Illumination Plus > Rulesets and Rules > Rulesets** >, if you are on the **Intra-Scope** tab and add a label to the scope of the ruleset (which will convert all Intra-Scope rules to Extra-Scope), you aren't automatically redirected to the **Extra-Scope** tab.

  Workaround: Click the **Extra-Scope** tab to go there manually.

Data Visualization

- **Special character in Label Type Key causes the app to crash when resized** (E-98984)

  When Illumination Plus is configured to display in **Mesh View**, resizing the page causes the app to crash. The problem is caused by the use of a special character in the user-defined **Label Type Key** (**Settings > Label Settings**). Currently, some special characters aren't supported for the key value.

  Workaround: Avoid using special characters when specifying the Label Type Key.
- **User column remains empty in Explorer by mistake** (E-89313)

  The user column remains empty in Explorer when selecting the Blocked by Boundary filter.

  Workaround: None
- **Problem when running multiple Explorer queries in separate tabs** (E-82385)

  If you have Illumio Explorer open in multiple browser tabs and set up separate queries to run in each tab, the query parameters you selected for one query could end up replacing the parameters you selected for the other query.

  Workaround: None
- **Time between two traffic flow events might be misreported** (E-79204)

  In Explorer, when viewing a traffic flow allowed by FQDN rules that was initially dropped and then allowed, the time between the "drop" and the "allow" events might be reported erroneously. The actual time between the two events could be only a matter of seconds (as expected), but the reported time could be more than one minute, which would be erroneous.

  Workaround: None
- **Total V-E (Vulnerability) score is slightly inaccurate** (E-75418, E-73277)

  The Total V-E score indicated on the upper right-hand corner of the **App Group > Vulnerabilities** tab is higher than the sum of the values in the V-E score column. For example, in one case the sum of the values in the V-E scores column was 69.8 but the Total V-E score was 71 instead of 70.

  Workaround: None
- **VES and E/W exposures wrong for the internet and other workloads** (E-73023)

  If a rule provides a service on a vulnerable port/protocol to the internet and to some set of workloads, the workloads in the port exposure are not counted. This leads to a VES of 0 instead of larger than 0. The exposure calculation is correct if the internet is not provided as a consumer.

  Workaround: None

Data Experience

- **Illumination Plus (App Group Map) - Tooltips not showing for connected app groups** (E-96033)

When users expand (right-click) a traffic link between connected app groups and then hover around any of the expanded links, the tooltip does not show up. Users can still click on the link and display the Summary and Connections panel with details.

Workaround: None

UI Components

- **Mesh: Re-renders repeatedly. Interactions are not working** (E-105167)

  Hover and brush interactions on Mesh are not working. Images re-render repeatedly.

  Workaround: None
- **Contextual menu is not completely visible** (E-105143)

  When at 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.

  Workaround: None
- **Proposed Rules - Status information is being hidden** (E-105098)

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

  Workaround: The information is shown on the Ruleset Summary page.
- **Save button is disabled while creating unmanaged workload from FQDN panel** (E-105006)

  The **Save** button is disabled while adding an unmanaged workload when trying to create it from the FQDN panel in the App Group Map view. The **Save** button is not enabled even after the mandatory fields are filled. This occurs in both Classic UI and New UI.

  Workaround: You can save the Unmanaged workload by entering a description, after which the **Save** button is enabled.
- **Add Report gives blank screen** (E-104949)

  After going to the **Explore > Reports** page, clicking on any option in the **Add Report** menu produces only a blank screen.

  Workaround: None
- **Scopes are not getting displayed on User Activity details and Local User details screen** (E-104175)

  In automated environments, labels can be created or can exist with invalid label types. In this case, scopes are not displayed on the User Activity or Local User details pages. But if you click **Edit**, scopes are displayed.

  Workaround: None

Data Platform

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

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

  Workaround: Use Explorer to see the correct timestamp.

PCE Web Console

- **Incorrect count in selector static categories** (E-68895)

  When a user enters a value in a selector in the PCE web console, the options matching the input are displayed along with the matched and total count. In the case of Static categories, the matched count is correct but the total count displayed is incorrect.

Workaround: While a workaround is not available, the issue occurs only when the user filters a static category. The matched count is correct but the total count is incorrect and will be resolved in a future release.

- **No error message is displayed after typing in an invalid port** (E-68255)

  When you enter an invalid port number while editing a service, the PCE still displays options to select from. When you move to another field without making a selection, the entered letters/digits are not cleared to reflect that the entered value was not selected. It can appear that the value you entered was accepted even though invalid.

  Workaround: Press ENTER after entering text. When the combination was valid, it will be selected. Otherwise, it will be cleared.

- **Wildcard in workloads filter not working** (E-65232)

  The PCE web console Workloads page supports filtering using special characters such as an asterisk (*). However, instead of displaying an error message when *only* special characters are used, the Workloads page neither filters the result nor gives an error message.

  Workaround: None

- **Filter doesn't handle the percentage symbol** (E-64904)

  When users select a filter option from the drop-down list, the selected value is added to the URL. If the selected value contains the percentage symbol (%), the UI throws an error, and a blank page shows up.

  There is no workaround, but this is a rare situation because the % symbol is not used often in values.

- **API call to switch multi_enforcement_instructions_request returns error** (E-59518)

  A REST API call to switch `multi_enforcement_instructions_request` returns an incorrectly handled error.

  This issue will be resolved in a future release.

- **Pressing Enter doesn't select the default option in the dialog box** (E-53831)

  When the PCE web console displays a dialog box, pressing **Enter** might select an action other than the default.

  Workaround: Use your mouse to click the required button in the dialog.

Policy and Workloads

- **VEN agent_master config is not upgrading after PCE starts using separate FQDN with dual certs** (E-104171)

  When two VENs that initially have the same FQDN are changed so one VEN uses a different FQDN, after the VENs and the PCE are restarted, the VEN's master config does not update, and FQDN stays the same. In addition, the PCE loses connection to the VEN, and the VENs are marked as offline in the PCE after the offline timer is reached. No workaround is available.

- **Container workload profile updates could generate a PCE error** (E-84624) Occasionally, updating the labels or enforcement mode of a container workload profile fails with a 500 Internal Server Error. This is caused by concurrent C-VEN and Kubelink background activity.

  Workaround: The update should succeed by retrying the PUT request.

- **Tunnel IP appears on VM's inbound port unnecessarily in Illumio policy** (E-84081)

  In a policy managing traffic between a Kubernetes pod (Consumer) and an external managed Virtual Machine (Provider), the managed VM has both the Host IP and the Tunnel IP on the inbound port. Illumio needs only the pod's Host IP on the external VM; the host's tunnel IP address is unnecessary.

  While this situation doesn't impact functionality, Illumio plans to correct this in a future release.

- **Enforcement Boundary filter returns Potentially Blocked flows mislabeled "no Rule"** (E-83415)

  Enforcement Boundaries filtered by IP Lists and displayed in the Draft View include Potentially Blocked flows that are labeled "no Rule" instead of "Blocked by Boundary." As it's not possible to enforce a boundary on flows with no rules, the "no Rule" status appears in error.

  Workaround: If you see the "no Rule" status in these circumstances, assume that the flows are "Blocked by Boundary."
- **Virtual Server Mode does not map directly to the management state in the Web Console** (E-78370)

  Any virtual server discovered on an SLB is considered to be in the “Managed” state when it has a corresponding entry in the virtual server list page. A managed virtual server could be either Not Enforced or Enforced. The `virtual_servers` object in the API returns a “Managed: Not Enforced” virtual server as “unmanaged.”

  Workaround: None
- **Incorrect error message displayed when ruleset renamed to a name that's in use** (E-74498)

  When creating and provisioning a rule set (for example, ruleset A, renaming it ruleset B, then creating ruleset A and reverting modifications to ruleset B), the UI displays an incorrect “500” error instead of an error message stating that the ruleset name is already in use.
- **Policy restore impacts the virtual services of a container cluster** (E-73979)

  The issues are as follows:
  - When policy is restored to a version before the creation of a container cluster’s virtual services, the container cluster’s virtual services are marked for deletion in the draft change.
  - When a container cluster is deleted, restoring its virtual services is possible through policy restore.

  Workaround: None
- **Inconsistencies in rule coverage for the Windows process-based rules** (E-71700)

  The draft view of Illumination and Explorer could show an incorrect draft policy decision for traffic covered by a rule using a service with a Windows process or service name. This generally happens when there is a port/protocol specified in the rule in addition to the process/service name, or when a non-TCP/UDP protocol is used in the rule. In these cases, the reported view provides the correct policy decision as reported by the VEN based on the active policy.

  Workaround: None
- **Rule search with virtual service and labels returns an incorrect rule** (E-65081)

  When a rule is written with a virtual service whose labels conflict with the ruleset scope, and a rule search is done for the virtual service, the rule search could return the rule even though the rule does not apply due to the scope conflict.

  Workaround: Use rule search to ensure that the rule applies to the virtual services and the scope labels separately.

Policy Platform

- **Incorrect behavior when an empty label group is used with a non-empty label group in a rule** (E-103556)

  When a user writes a rule with two label groups **of the same dimension** (for example, two app label groups), and one of the label groups is empty, that rule is not delivered to workloads whose labels fall within the nonempty label group.

  Workaround: Either remove the empty label group from the rule or add a label to it to make it nonempty.

PCE Platform

- **In a supercluster environment, member PCEs should be allowed to configure the local syslog server** (E-106345)

  In a Supercluster, 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 other files are rotated correctly.

  Workaround: None
- **A large app_stats log file (8GB and more) is continuing to grow** (E-95636)

  On some systems, logrotate for the internal log files is sometimes not successful, which causes these files to continue to grow in size.

  Workaround: None
- **XFF not working properly** (E-88891)

  The user activity page in the UI reports the LB SNAT IP address instead of the user's IP address from the XFF header even when SNAT IP is configured as a Trusted Proxy. In addition, accessing a non-existent API endpoint also logs the SNAT IP address in audit events instead of the client IP address from the XFF header.

  Workaround: None
- **The `agent.activate` events are not always classified correctly** (E-74682)

  Events generated when an agent is activated (`agent.activate` events) are categorized inconsistently. Success events are classified as auditable, and failure events are categorized as `system_events`.

  Workaround: None

VEN

Illumio 23.2.10 and 23.2.20 VEN releases were decommissioned for technical reasons. VENs from these releases are no longer available for installation. Features and bug fixes for these releases are available in Illumio 23.2.22-VEN.

- **RHEL5 and Solaris VENs fail to apply policy containing virtual services with FQDNs** (E-110016) This failure occurs if a RHEL5 or Solaris VEN is associated with a rule that allows communication to a virtual service with FQDNs defined or the virtual service's labels. Workaround: none currently.
- **VEN IPSec policy tampering detection not supported with RHEL5** (E-110015)

  In Illumio Core 23.2.20-GA, VEN IPSec policy tampering detection and recovery doesn't work with VENs running on RHEL5 workloads. On all other supported Linux distributions, tampering detection works as designed.
- **Upgrade for AIX 6.x and 7.x VEN triggered from PCE failed** (E-109282)

  VEN upgrade for AIX 6.x and 7.x failed when upgrading from the PCE.

  Workaround: None.
- **VEN should not ask for maintenance token on unsupported OSes for tampering protection** (E-101470)

  When VEN tampering protection is enabled, Solaris and macOS workloads (where VEN tampering protection is not yet supported) also ask for a maintenance token for CLI commands. CLI commands other than suspend will succeed if a valid maintenance token is provided. Suspend does not work even if a valid token is provided.

  There is no workaround. If you will enable the VEN tampering protection feature, do not upgrade Solaris or macOS workloads to 22.5.10.

- **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.
- **Workload keeps emitting agent.tamper error events after configured custom iptables rule** (E-101029)
  A firewall policy with a custom iptables rule might get vvin a different format than the one it was in when ingested. When using `-key value` arguments to iptables such as `--k2 v2 --k1 v1`, it does not matter which order you add them in for correctness in the system. However, if the Linux kernel dumps the arguments back to the VEN in a different order, the VEN falsely considers it a tamper. For example, if the kernel always dumps "`-k1 v1 --k2 v2`" even if you give "`-k2 v2 --k1 v1`", then the VEN will think somebody has changed the firewall.
  Workaround: Order the custom iptables rules the same way that the Linux kernel dumps them in.
- **Windows 11 shows as Windows 10 on the workload/VEN page** (E-100844)
  Workaround: None
- **Process-based rule not showing properly in Explorer** (E-89749)
  A process-based rule was defined but was shown as "no rule" in Explorer.
  Workaround: Do not specify the service name in the process-based rules.
- **On CentOS 8, VEN can't load the FTP or TFTP modules** (E-85127)
  On CentOS 8, the VEN can't load the `nf_conntrack_ftp` and `nf_conntrack_tftp` modules, which blocked the workload from uploading and managing files. Due to this issue, customers can't upgrade the VEN on CentOS 8 workloads.
  Workaround: None
- **[CentOS 8] Custom IPtables rule does not work with -j REDIRECT** (E-80818)
  After creating a custom rule on the PCE with -j REDIRECT in the nat table, the CentOS 8 VEN enters an error state because the VEN could not correctly handle the -j REDIRECT part of the rule. The custom rule performs a NAT operation that requires a different chain type therefore, nftables does not allow the VEN to perform the redirect in our chains.
  Workaround: Remove the custom Iptables rule and restart the VEN. This brings the VEN back to a healthy state.
- **Established connections are not removed when the VEN is restarted** (E-63072)
  After the VEN is paired and restarts using the `Illumio-ven-ctl` options, it dumps suspicious log entries into vtap.log twice per minute. The log type is INFO and they appear to be caused by an error related to the restart of the VEN. This issue is observed in the global zone and the exclusive IP zone.
  Workaround: Not available; however, this issue has no major impact except for vtap.log receiving these log entries.

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.

23.2.21 Security Information

- **Security fix applied for a Deserialization of Untrusted Data Vulnerability in 23.2.20**
  CVE-2023-5183: An unsafe deserialization in the Illumio PCE API can lead to remote code execution. This issue is resolved. The public advisory can be found at https://docs.illumio.com/Guides/security-advisories/september-2023/cve-2023-5183.htm.

- **Security fix applied for Information Disclosure through Error Handling**
  When passing a specially crafted URL, the PCE returned a verbose error stack trace. This is resolved.
- **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 v3.21.7**
  google-protobuf upgraded to v3.21.7 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.
- **ruby upgraded to v3.1.4**
  ruby was upgraded to v3.1.4.

23.2.20 Security Information

- **Security fix applied for a Deserialization of Untrusted Data Vulnerability in 23.2.20**
  CVE-2023-5183: An unsafe deserialization in the Illumio PCE API can lead to remote code execution. This issue is resolved. The public advisory can be found at https://docs.illumio.com/Guides/security-advisories/september-2023/cve-2023-5183.htm.
- **Security fix applied for Information Disclosure through Error Handling**
  When passing a specially crafted URL, the PCE returned a verbose error stack trace. This is resolved.
- **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 v3.21.7**
  google-protobuf upgraded to v3.21.7 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.
- **ruby upgraded to v3.1.2**
  ruby was upgraded to v3.1.2.

23.2.11-PCE Security Information

IMPORTANT
This release is for Illumio Core On-Premises customers only.

In this release, Illumio applied a security fix to the PCE for deserialization of an untrusted data vulnerability. An unsafe deserialization in the Illumio PCE REST API could lead to remote code execution. This issue is resolved.

For more information, see the Illumio public advisory: CVE-2023-5183

23.2.10 Security Information

- **OpenSSL was upgraded to v3.0.8**
  OpenSSL was upgraded to v3.0.8 on the Illumio VEN to address CVE-2022-3996, CVE-2022-4203, CVE-2022-4304, CVE-2022-4450, CVE-2023-0215, CVE-2023-0216, CVE-2023-0217, CVE-2023-0286, and CVE-2023-0401. Illumio VENs were not impacted by these CVEs.
- **curl was upgraded to v7.88.1**
  curl was upgraded to v7.88.1 on the Illumio VEN to address CVE-2022-22576, CVE-2022-27774, CVE-2022-27775, CVE-2022-27776, CVE-2022-27779, CVE-2022-27780, CVE-2022-27781, CVE-2022-27782, CVE-2022-30115, CVE-2022-32205, CVE-2022-32206, CVE-2022-32207, CVE-2022-32208, CVE-2022-35252, CVE-2022-32221, CVE-2022-42915, CVE-2022-43551, CVE-2022-43552, CVE-2022-42916, CVE-2023-23914, CVE-2023-23915, and CVE-2023-23916. Illumio VENs were not impacted by these CVEs.
- **sqlite was upgraded to v3.41.0**
  sqlite was upgraded to v3.41.0 to address CVE-2022-46908. Illumio products were not impacted by this CVE.

23.2.0 Security Information

- **Rails upgraded to address CVE-2023-22795**
  The rails package was upgraded to 6.1.7.2 to address CVE-2023-22795. The PCE is not impacted by this vulnerability.

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-VENs to PCE, and policies from PCE to C-VENs. 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

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 Work-

loads. 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-VENs 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-VENs not automatically cleaned up after AKS upgrade** (E-103895)
  After upgrading an AKS cluster, sometimes a few duplicate C-VENs 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-VENs 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.

Legal Notice

Resources

- Legal information
- Trademarks statements
- Patent statements
- License statements

Contact Information

- Contact Illumio
- Contact Illumio Legal
- Contact Illumio Documentation