Illumio Core®

Version 23.5.10

What's New in This Release

June 2024

14000-200-23.5

Legal Notices

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

Product Version

PCE Version: 23.5.10

For the complete list of Illumio Core components compatible with Core PCE, see the Illumio Support portal (login required).

For information on Illumio software support for Standard and LTS releases, see Versions and Releases on the Illumio Support portal.

Resources

Legal information, see https://www.illumio.com/legal-information

Trademarks statements, see https://www.illumio.com/trademarks

Patent statements, see https://www.illumio.com/patents

License statements, see https://www.illumio.com/eula

Open source software utilized by the Illumio Core and their licenses, see Open Source Licensing Disclosures

Contact Information

To contact Illumio, go to https://www.illumio.com/contact-us

To contact the Illumio legal team, email us at legal@illumio.com

To contact the Illumio documentation team, email us at doc-feedback@illumio.com

illumio

Contents

Chapter 1

Welcome to Illumio Core 23.5.10

This chapter contains the following topics:

Illumio is pleased to announce the general availability of version 23.5.10 of the Illumio Core for the PCE. This new release contains many improvements and changes as described in this document.

About This Release

This documentation portal describes the new features, enhancements, platform support, and new and modified REST APIs for the Illumio Core 23.5.10 release.

> IMPORTANT:
> Illumio Core 23.5.10.1 is available for Illumio Core Cloud customers. Illumio Core 23.5.10.10 is available for Illumio Core On-Premises customers.

Product Versions

PCE Version: 23.5.10.1 (Cloud) and 23.5.10.10 (On Premises)

VEN Versions: 18.2.4; 19.3.1 and above; 21.%.0 except for 21.1.0; 22.%.0 except for 22.2.40; 22.5.0 (Standard), 22.5.10, 22.5.12 (Cloud only)

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

FlowLink Versions: 1.2.1, 1.2.0, 1.1.x

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

Standard versus LTS Releases

23.5.10.1 and 23.5.10.10 are Standard releases.

For information on Illumio software support for Standard and LTS releases, see Versions and Releases on the Illumio Support portal.

Release Types and Numbering

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

- “a.b”: Standard or LTS release number, for example “23.5”
- “.c”: Maintenance release number, for example “.1”
- “-d”: Optional descriptor for pre-release versions, for example “preview2”

General Advisories

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

Updated Minimum Browser Versions for the Core PCE UI

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

For current information about the browser versions supported by the PCE, see the supported browsers section in PCE OS Support and Package Dependencies.

Supported Operating Systems

The 23.5.10 PCE is supported on operating systems detailed on the Illumio Support portal.

For information, see PCE OS Support and Package Dependencies.

Open Source Package Updates

Illumio updated several open source packages for the PCE in 23.5.10.1. See the “Change History” in Illumio Open Source Licensing Disclosures for information.

The Upgrade to This Release

As part of the upgrade process, Illumio strongly encourages you to review the prior release notes from your previously installed version of Illumio Core to version 23.5.10.

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

Announcements

End of Support Announcements, Deprecations, Compatibility

Classic UI Removed

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

In 23.5, the toggle option is removed. The classic UI is no longer available. For more information, see Welcome to the New Illumio Experience

End of Support

Illumio REST API v1

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

Internet Explorer 11

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

Organization Events

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

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

Customers should upgrade to the latest version of Illumio Adaptive Security and take advantage of the newly designed auditable events. See the *Events Administration Guide* for information.

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 23.4.0, Illumio deprecated the PCE classic UI.

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

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

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

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

What Are the Primary Benefits?

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

Why is Illumio making these changes?

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

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

- Easily work in the PCE with a simplified look-and-feel found in the UI headers, map, and selected pages.
- Achieve faster access to key features with updated navigation, including simplified terms.
- Learn key information about your environment by reviewing dashboards for Ransomware Protection and VEN statics, both with styling updates.

- Use Illumio maps more effectively due to significant usability enhancements.
- Start your work faster by using integrated quick search in the left navigation.

What is Changing?

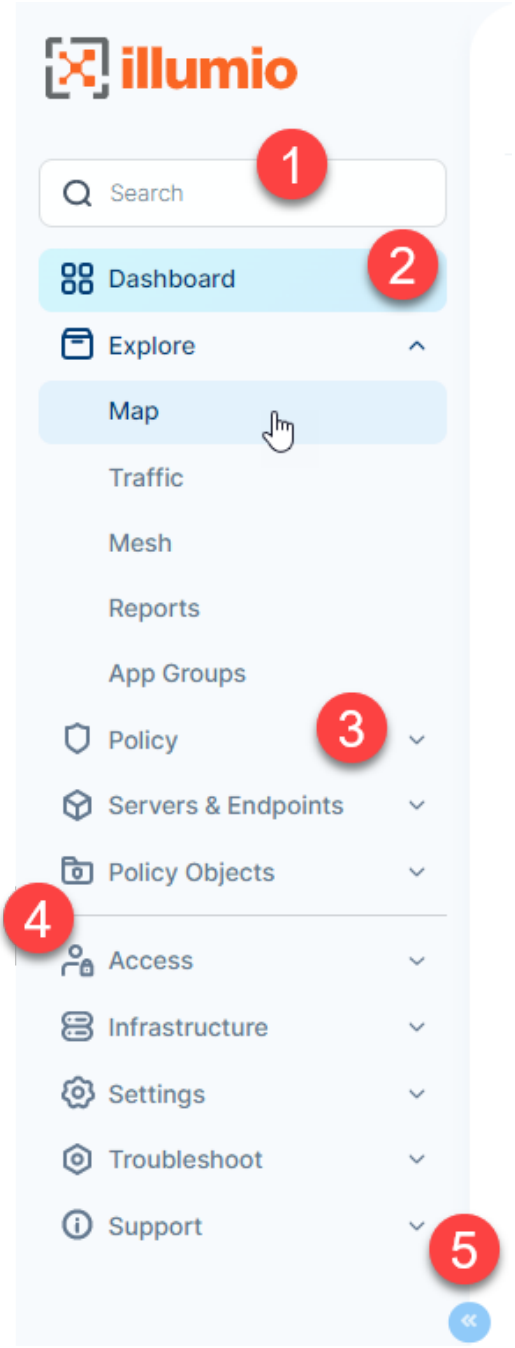
These changes include redesigned navigation, simplified naming, and an updated look-and-feel.

Redesigned Navigation

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

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

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



(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.

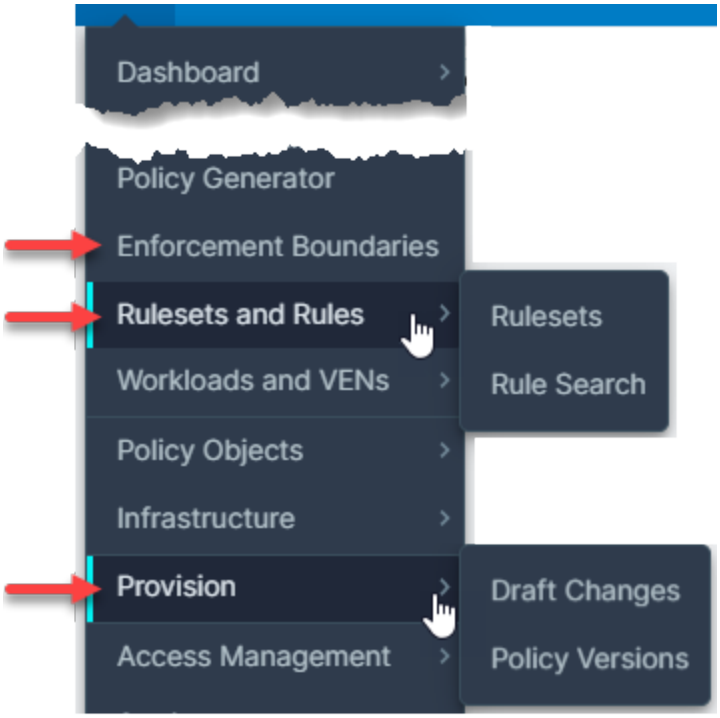
Navigation Changes at a Glance

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

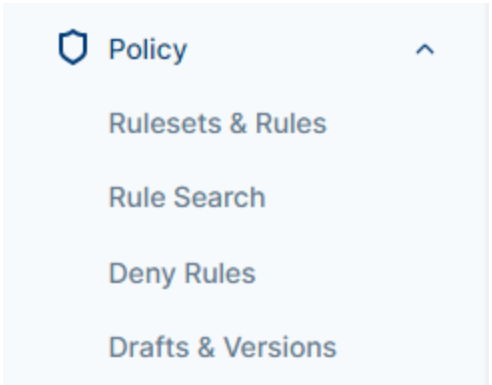
However, much of the navigation from the Classic UI carries forward into the New UI. Illumio Administrative categories that are clearly accessible in the Classic UI haven't changed, such as Infrastructure, Settings, Access Management, and Troubleshooting.

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

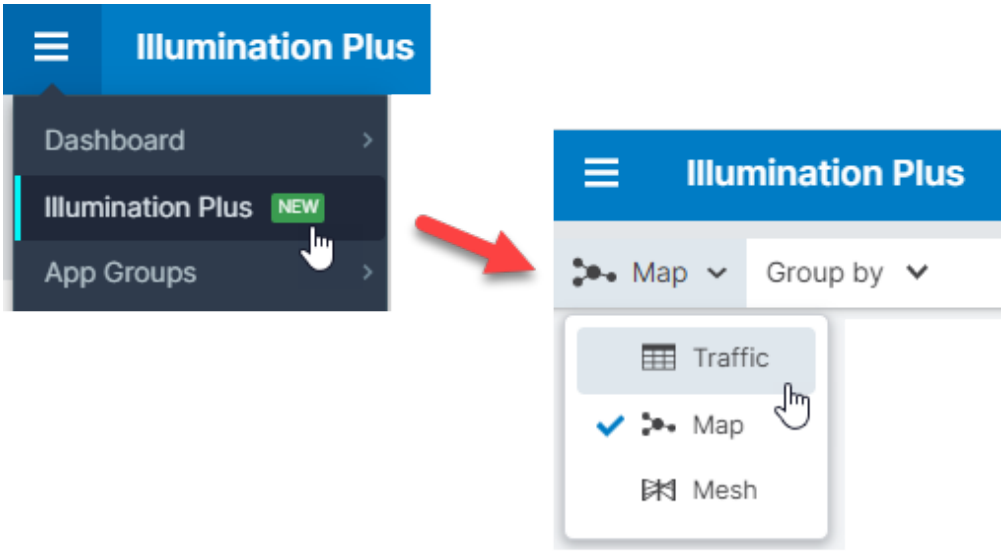


New UI

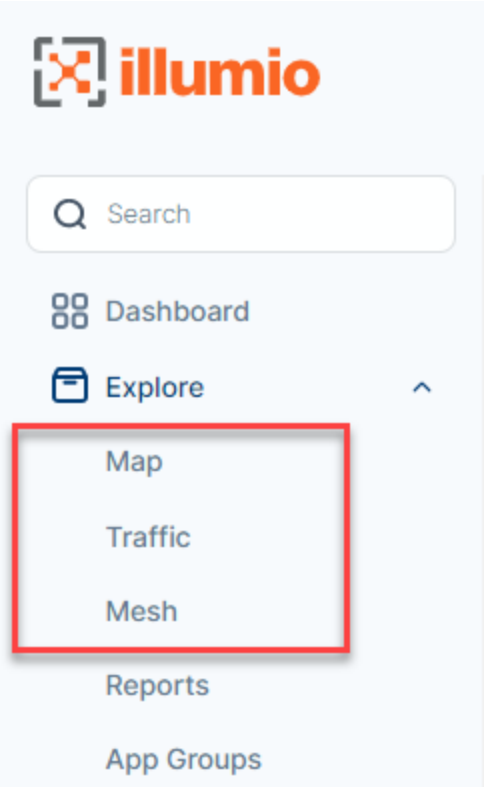


The New UI also centralizes all tasks related to visualization under the new Explore category. The Illumination Plus views (Map, Traffic, and Mesh) are easily accessible in the Explore category:

Classic UI



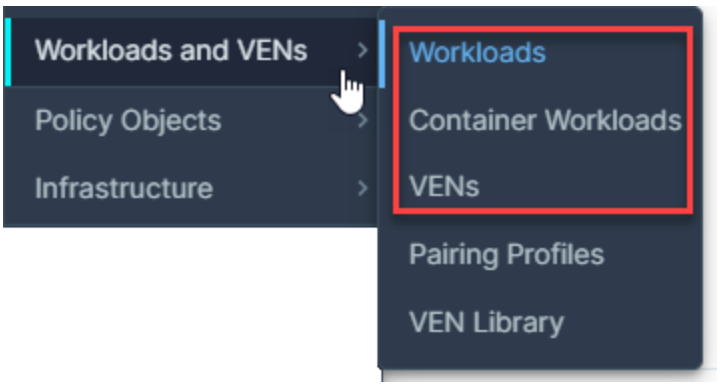
New UI



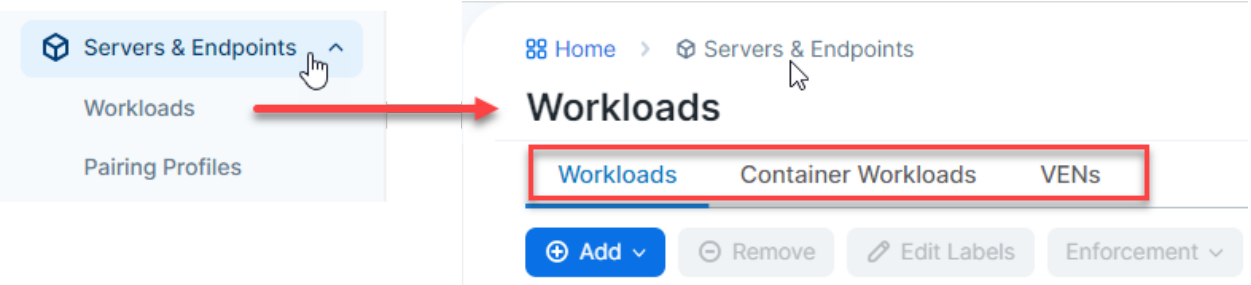
The **Workloads and VENs** category from the Classic UI is simplified and renamed in the New UI.

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.

(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
- Labels
- Label Groups
- Virtual Services
- Virtual Servers
- Segmentation Templates

Infrastructure

- Core Services
- Load Balancers
- Container Clusters
- SecureConnect Gateways
- Networks
- CloudSecure

Provision

- Draft Changes
- Policy Versions

Access Management

- Global Roles
- Scopes
- External Groups
- External Users
- Local Users
- Service Accounts
- User Activity
- Authentication
- Access Restrictions

Settings

- Corporate Public IPs
- Event Settings
- Flow Collection
- Label Settings
- Security
- Core Services
- Essential Service Rules
- VEN Operations
- Trusted Proxy IPs
- Policy Settings
- API Key Settings
- Global Roles
- Scopes
- External Groups
- External Users
- Local Users
- Service Accounts
- User Activity
- Authentication
- Access Restrictions

Infrastructure

- Core Services
- Load Balancers
- Container Clusters
- SecureConnect Gateways
- Networks
- CloudSecure

Settings

- Corporate Public IPs
- Event Settings
- Flow Collection
- Label Settings
- Security
- Core Services
- Essential Service Rules
- VEN Operations
- Trusted Proxy IPs
- Policy Settings
- API Key Settings
- Offline Timers

Troubleshoot

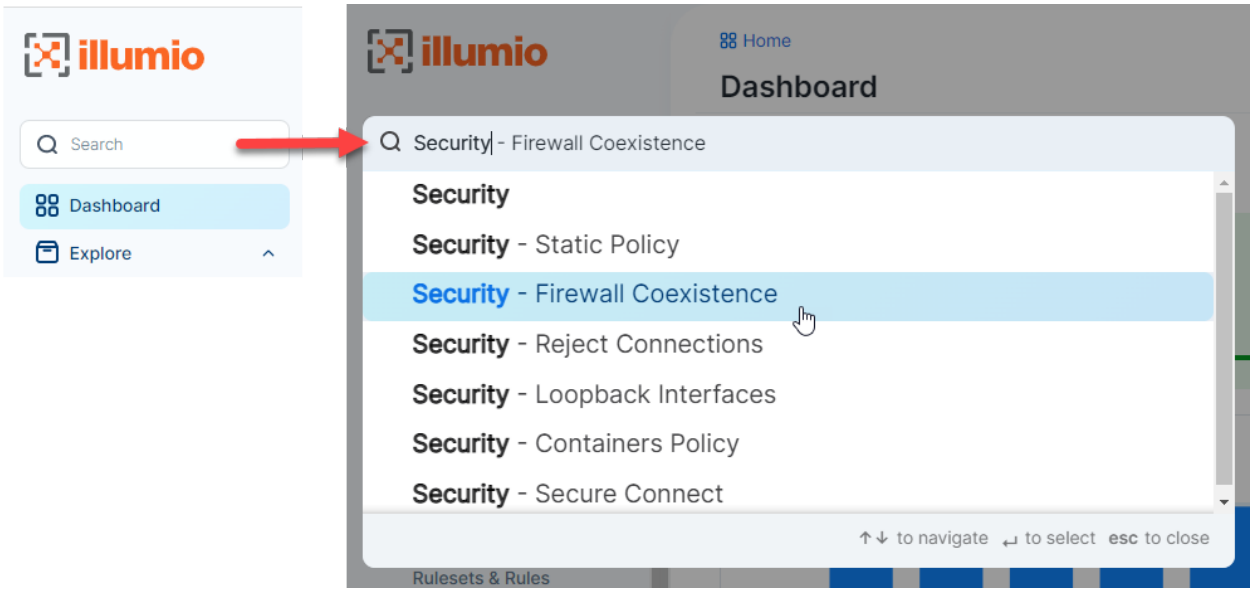
- Blocked Traffic
- Events
- Exports
- VEN Support Bundles
- PCE Support Bundles
- Policy Check
- Product Version

Support

- Offline Timers
- **Troubleshooting**
  - Blocked Traffic
  - Events
  - Exports
  - VEN Support Bundles
  - PCE Support Bundles
  - Policy Check
  - Product Version
- **Support**
  - VEN Library
  - Support Portal

Easy to Use Quick Search

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



Additional Context through Breadcrumbs

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

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

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

Simplified Naming

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

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

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

Full List of Changed Terms

22.5.x	23.5.10 Classic UI	23.5.10 New UI
Illumination Plus	Illumination Plus	Explore
Illumination Plus Table view	Illumination Plus Table view	Explore > Traffic
Enforcement Boundaries	Enforcement Boundaries	Deny Rules
Label-Set Connections	Label-Set Connections	Connections with common labels
Connections	Traffic	Traffic
Consumer and Provider	Consumer and Provider	Source and Destination

Updated Look-and-Feel

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

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

Deprecated Features in the New UI

The New UI deprecates the following features:

- Illumination Classic
- Explorer
- Policy Generator
- Segmentation Templates

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

Illumination Classic

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

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

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

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

Original Explorer

Illumio Core introduced the Explorer feature as a preview in Illumio Core 17.2.0. In Illumio Core 18.1.0, this feature became generally available. In Illumio Core 22.5, Illumio integrated the Explorer feature with Illumination Plus. The functionality for the

Explorer feature was available in the Table view and Mesh view in Illumination Plus in the Classic UI.

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

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

Chapter 2

What's New and Changed in This Release

This chapter contains the following topics:

Before upgrading to Illumio Core 23.5.10, 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.

Illumio Core REST API in 23.5.20

The Illumio Core REST API v2 has changed in 23.5.20 in the following ways.

See the *REST API Developer Guide* for more information.

Changed APIs

Two APIs,

sec_policy_firewall_settings_put

and

sec_policy_firewall_settings_get

have the added property `ip_forwarding_enabled_scopes`:

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

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

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

What's New and Changed in Release 23.5.10

The following new feature was added in Illumio Core 23.5.10.

CLAS Architecture in Illumio Core for Kubernetes and OpenShift

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

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

For complete details on new CLAS improvements, including how to migrate existing clusters to CLAS mode, see Illumio Core for Kubernetes and OpenShift.

Illumio Core REST API in 23.5.10

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

See the *REST API Developer Guide* for more information.

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

- Organization Access
- Cluster Mode for Container Cluster

Organization Access

Changes to the organization access introduced a new common schema:

common ipv4_ipv6_subnet

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

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

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

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

- orgs_access_restrictions_post
- orgs_access_restrictions_put

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

settings_trusted_proxy_ips_put

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

Cluster Mode for Container Cluster

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

container_clusters_get

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

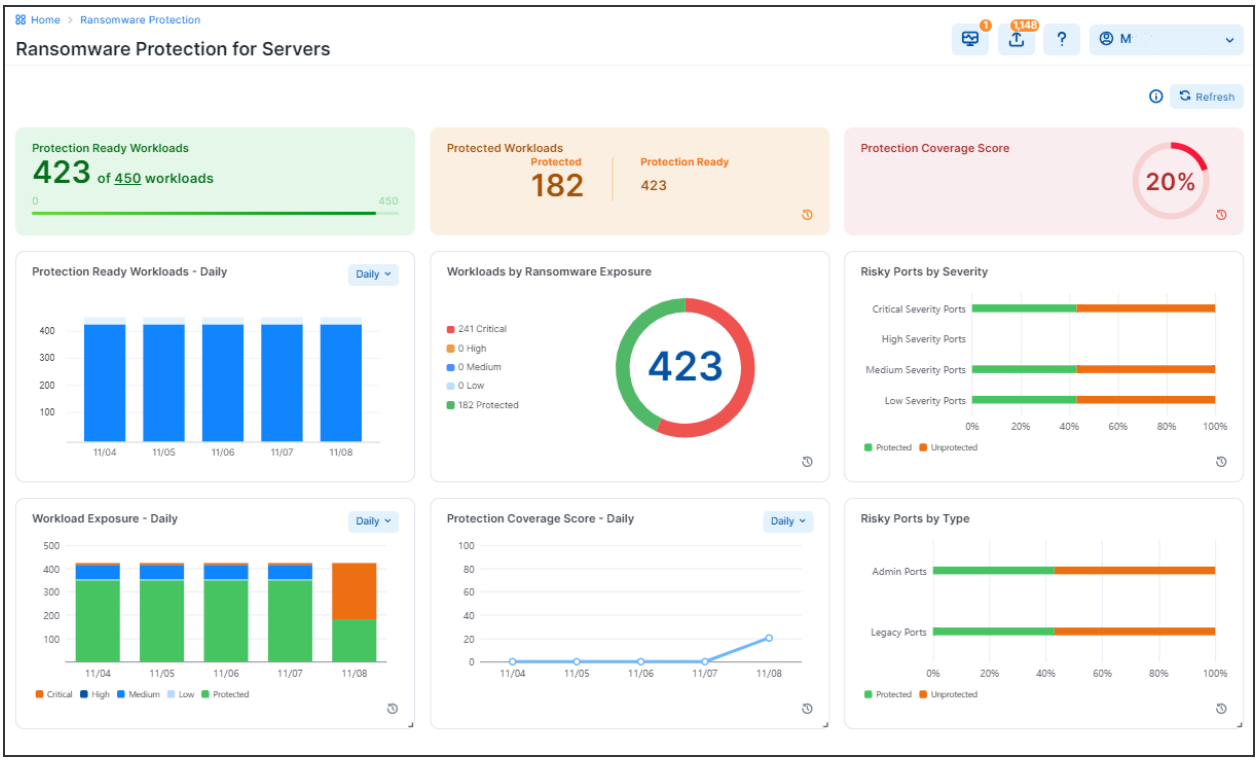
What's New and Changed in 23.5

The following new features were added in Illumio Core 23.5.

Policy Templates

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

Ransomware Protection Dashboard Changes



New Widgets

> NOTE:For all widgets see detailed explanations in Ransomware Protection Dashboard in the *Visualization Guide*.

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

- **Workloads Exposure (Daily, Weekly, Monthly, Quarterly)**

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

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

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

  The Protection Coverage Score is a metric used to measure the effectiveness of security policies in protecting workloads. It indicates the percentage of the entire possible attack surfaces that are actively protected by security policies. For example, a policy that allows all workloads as source will have a lower coverage score compared to a policy that only allows a small number of source workloads.
  Protection coverage score takes all the protection-ready workloads into consideration across the organization.
  The color of the widget changes from red to yellow and then to green as the protection coverage score increases.

- **Risky Ports by Type**

  This widget shows the percentage of risky ports by type: administrative vs. legacy ports.
  Each port type is presented with a bar that depicts the percentage of protected (green) and unprotected (orange) ports.
  To help visualize the protection coverage by port type, five percentage data points are used: 20%, 40%, 60%, 80%, and 100%.

Existing Widgets

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

- **Protected Workloads**

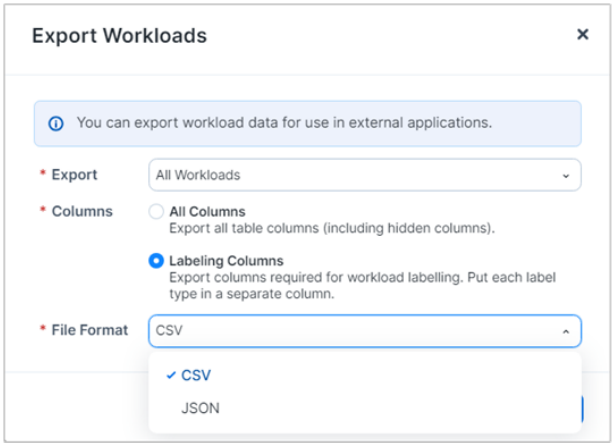
  For the widget Protected Workloads, a list of services that are at risk of ransomware penetration and lateral movement is provided to help customers assess ransomware exposure on their Enterprise Service.

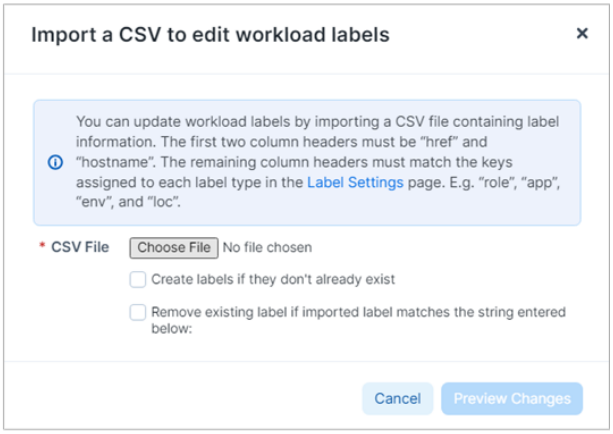
- **Protection Coverage Score**

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

Bulk Export/Import of Workload Labels

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

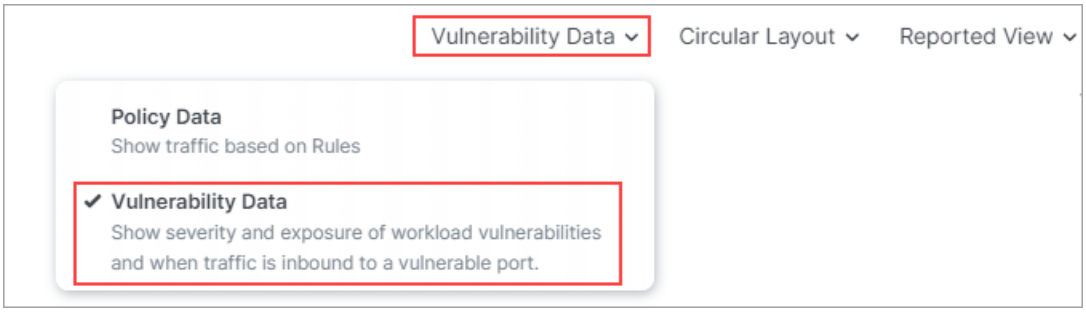


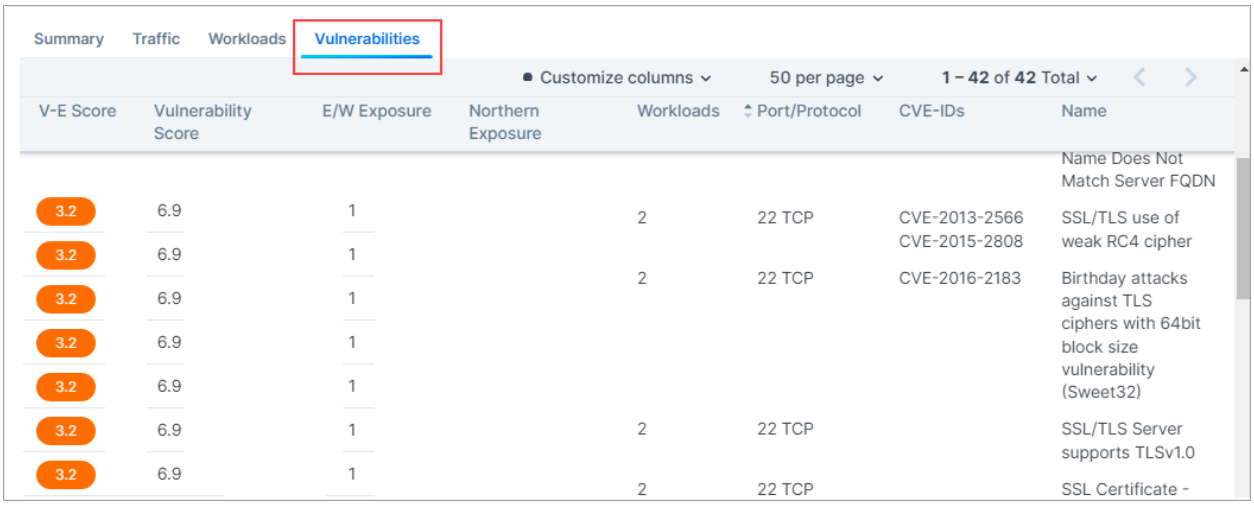


Enhancements in the Visualization Tools

Vulnerability Data Option

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

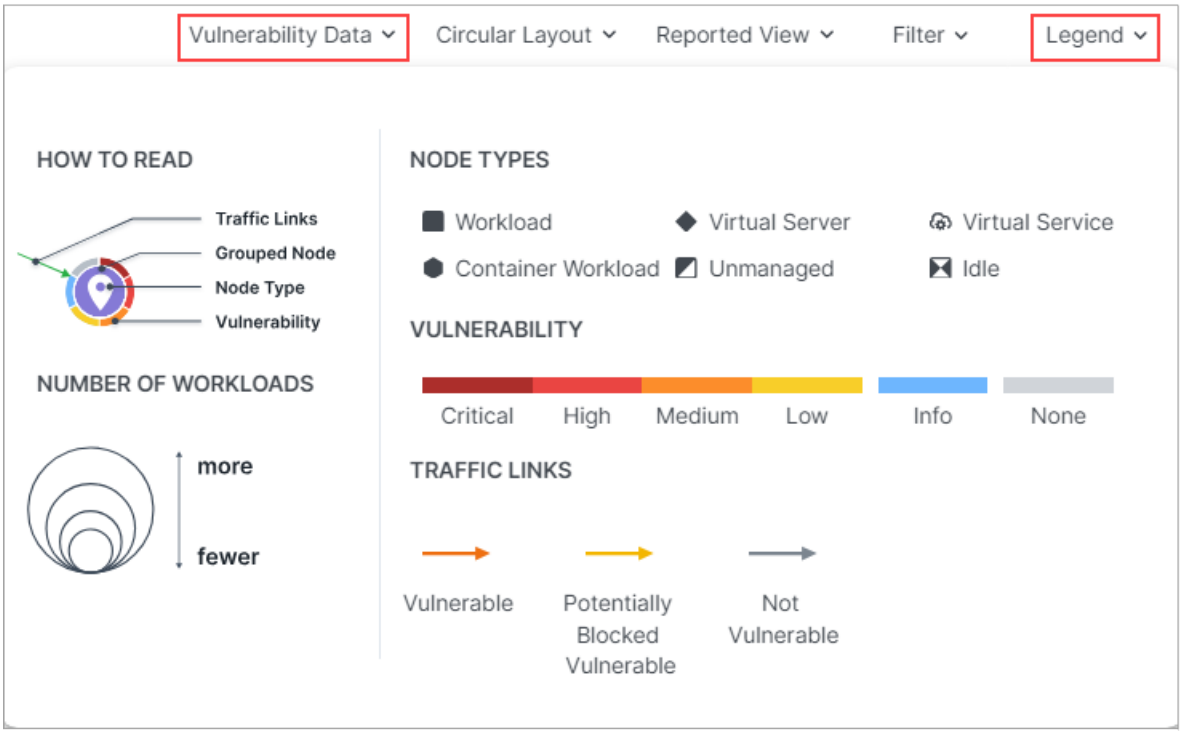




Legend for the New Vulnerability Data Option

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

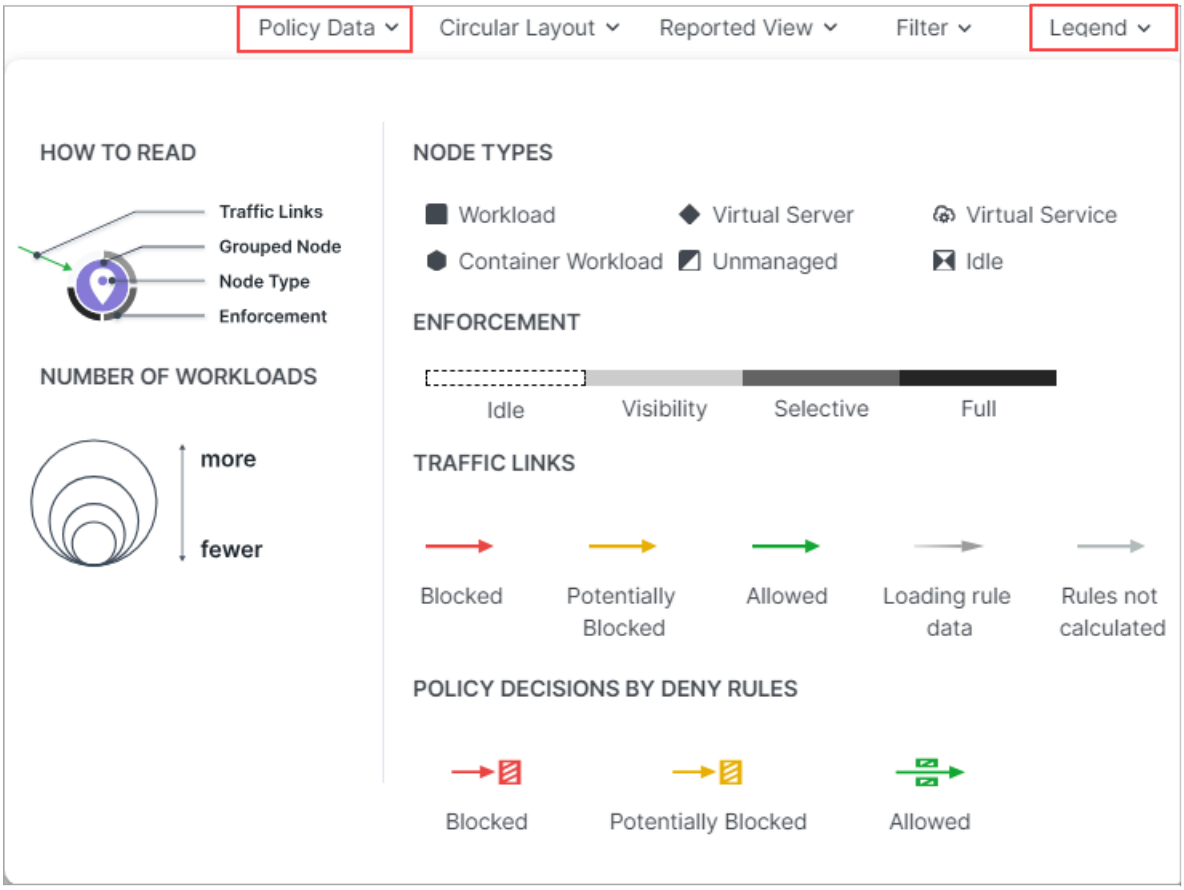
- The relative size of each node indicates the number of workloads in the node.
- The outer ring may be continuous or comprised of segments. The color of the segments shows the vulnerability level of workloads; segment sizes show the proportion of workloads assessed to be at the indicated vulnerability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



Updated Legend for the Policy Data option

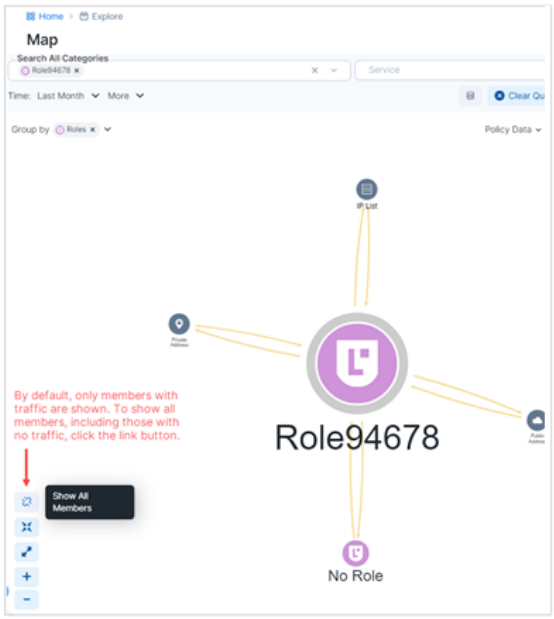
The Policy Data option in the Illumination Map features an updated legend.

- The relative size of each node indicates the number of workloads in the node.
- The outer ring may be continuous or comprised of segments. The shade of the segments shows the enforcement level of workloads; segment sizes show the proportion of workloads under the indicated enforcement level.

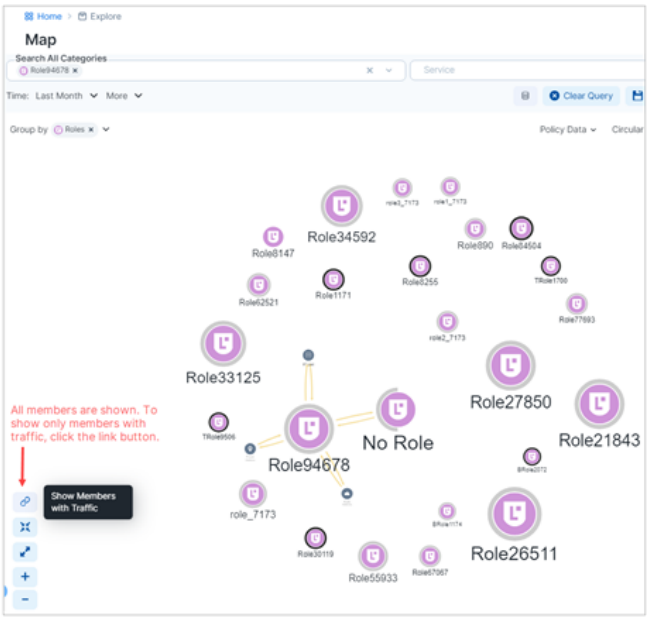


Show Members with No Traffic

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



Only workloads with traffic are shown (default)

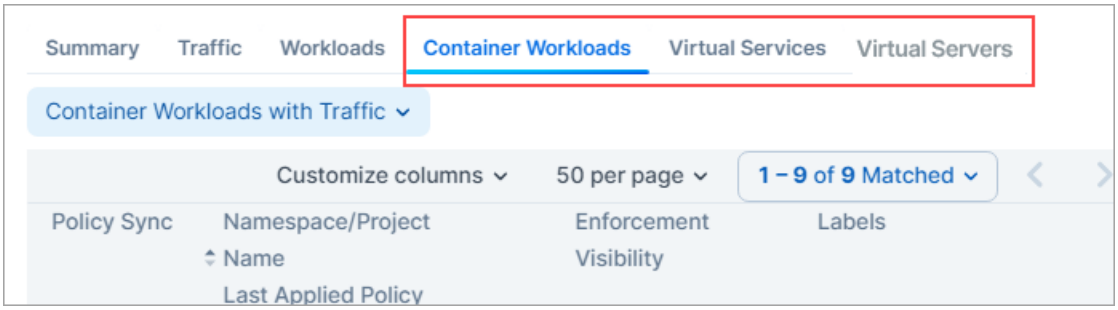


All workloads are shown

New Group Member Tabs

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

- Container Workloads
- Virtual Services
- Virtual Servers



Windows Outbound Process: A New Object Type

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

Limits on Flowlink Traffic Data

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

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

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

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

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

Splunk Integration Version Upgrade

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

Traffic from Unpaired VENs

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

Classic UI Removed

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

There are two parts of the classic UI that are exceptions to this removal. The Explorer and Illumination Plus can be enabled with a setting in the user's Profile page. For more information, see Configure Visibility Display in the PCE Web Console.

Illumio Core REST API in 23.5.0

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

See the *REST API Developer Guide* for more information.

New APIs

There are two new APIs in this release:

reports_risk_summary_ransomware_timeseries_statistics_post

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

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

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

workloads/bulk_import

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

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

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

common kubernetes_workloads_metadata

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

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

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

Exposure and Authorization Changes

Network Enforcement Nodes Changes

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

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

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

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

API	Exposure Change	New Authorization Change
		ager", "Ruleset Provisioner", "Ruleset Viewer", "Workload Manager"
`network_enforcement_nodes_network_devices_post`	YES	"Workload Manager"
`network_enforcement_nodes_put`	YES	NO

Other Exposure Changes

supported_devices

API being made available to integrators.

Changed APIs

Ransomware Dashboard API Changes

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

reports_risk_summary_get

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

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

reports_time_series_statistics_post

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

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

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

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

reports_time_series_statistics_post_response

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

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

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

This API is now referencing the schema `num_workloads_by_exposure_time_series`.

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

workload_ransomware_services

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

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

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

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

Other API Changes

sec_policy_rule_coverage_post_response

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

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

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

optional_features_put

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

```
       "properties": {
              "name": {
              "description": "Name of the feature",
              "type": "string",
              "enum": [
                     "ip_forwarding_firewall_setting",
                     "ui_analytics",
                     "illumination_classic",
```

```
                    "ransomware_readiness_dashboard",
                    "per_rule_flow_log_setting",
                    "lightning_default",
                    "collector_scanner_filters",
                    "corporate_ips_groups",
                    "labels_editing_warning_for_enforcement_mode",
                    "label_based_network_detection",
                    "cloudsecure_enabled",
                    "windows_outbound_process_enforcement"
                ]
            },
```

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

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

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

kubernetes_workloads_get

For this API, these changes have been made:

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

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

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