Illumio Core®

Version 22.5.32

What's New in This Release

April 2024

14000-200-22.5

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: 22.5.32

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

Contents

Chapter 1

Welcome to Illumio Core 22.5.*x*

This chapter contains the following topics:

Illumio is pleased to announce the general availability of version 22.5.*x* 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 22.5.*x* release.

> IMPORTANT:
> Illumio Core 22.5.*x* is available for Illumio Core On Premises customers.

Product Versions

PCE Version: 22.5.32 (LTS)

VEN Version: 22.5.33 (LTS)

FlowLink Version: 1.2.0, 1.1.x

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

NEN Version: 2.6.10. 2.6.1, 2.6.0, 2.5.2, 2.5.1, 2.5.0, 2.4.10, 2.4.0, 2.3.10

C-VEN Version: 22.5.13 and 22.5.20

Standard versus LTS Releases

22.5.32-PCE and 22.5.33-VEN are LTS 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 “22.5”
- “.c”: Maintenance release number, for example “.0”
- “-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.

Supported Operating Systems

The 22.5.32 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 this release. 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 version22.5.32.

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

Feature Change

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 22.5.0 and 22.5.10, Illumio removed the Explorer feature from the PCE web console main menu.

> IMPORTANT:
> In Illumio Core 22.5.10+UI2, Illumio returned the Explorer feature to the PCE web console for customers who still want to use the functionality in that area of the GUI.
>
> To access the original Explorer feature, upgrade from 22.5.*x* to Illumio Core 22.5.10+UI2.

In all Illumio Core 22.5.*x* releases, the functionality for the Explorer feature is available in the Table View and Mesh View in Illumination Plus. See Illumination Plus Table View and Illumination Plus Mesh View in the *Visualization Guide* to learn how to use these features, which provide the functionality formerly provided in the Explorer feature.

> IMPORTANT:
> When you use the original Explorer feature, the functionality 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.

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.

What's New and Changed in This Release

This chapter contains the following topics:

Before upgrading to Illumio Core22.5.32, 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 22.5.32

IMPORTANT:
Illumio Core 22.5.32.32-PCE is available for Illumio Core On-Premises customers only.

22.5.32.33-VEN is available for Illumio Core On-Premises customers only.

22.5.32.32-VEN is available for both Illumio Core On-Premises customers and Cloud customers.

Illumio Core 22.5.32-PCE Maintenance Release

Released October 2023

Illumio Core 22.5.32.32 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 22.5.32.32 solved software and security issues for the PCE to refine the software and improve its reliability and performance.

For the complete list of improvements and enhancements to the PCE, see "Resolved Issue in 22.5.32.32-PCE" in the Illumio Core Release Notes 22.5.

Illumio Core 22.5.33-VEN Maintenance Release

Released April 2024

Illumio Core 22.5.32.32 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 22.5.32.33-VEN solved software and security issues for the VEN to refine the software and improve its reliability and performance.

For the complete list of improvements and enhancements to the VEN, see "Resolved Issue in 22.5.32.33-VEN" in the Illumio Core Release Notes 22.5.

Illumio Core 22.5.32-VEN Maintenance Release

Released February 2024

Illumio Core22.5.32.32 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 Core22.5.32.32-VEN solved software and security issues for the VEN to refine the software and improve its reliability and performance.

For the complete list of improvements and enhancements to the VEN, see "Resolved Issue in 22.5.32.32-VEN" in the Illumio Core Release Notes 22.5.

What's New and Changed in Release 22.5.30

Illumio Core 22.5.30 Maintenance Release

Illumio Core22.5.32.30 includes an updated version of the PCE and VEN software.

IMPORTANT:
Illumio Core22.5.32.30-PCE is available for Illumio Core On-Premises customers only.

22.5.32.30-VEN is available for both Illumio Core On-Premises customers and Cloud customers.

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 22.5.30 solved software and security issues for the PCE and VEN to refine the software and improve its reliability and performance.

For the complete list of improvements and enhancements to the PCE and VEN, see "Resolved Issue in 22.5.30" in the Illumio Core Release Notes 22.5.

Changes in Release 22.5.30

Documentation Change

The procedure for preparing to deploy PCEs into a Supercluster is updated in this release to reflect clarified requirements for the PCE member deployments. See the topic "Documentation Updates for Illumio Core 22.5.30" in the Illumio Core 22.5.30 Release Notes.

Terminology Update in PCE Web Console UI

In this release, the following terminology changed in the filter fields in Illumination Plus:

Previous Terminology	New Terminology
External	External (Non-Corporate)

The Networks page, Illumination Plus Table view, and the Classic Explorer feature used the terminology "External (Non-Corporate)" in their list views; however, the filters for these areas used the terminology "External" to search by type of network.

In this release the filters now use the terminology "External (Non-Corporate)" to match the rest of the list view pages in the PCE UI.

What's New and Changed in Release 22.5.20

Illumio Core 22.5.20 Maintenance Release

Illumio Core22.5.32.20 includes an updated version of the PCE and VEN software.

> IMPORTANT:
> Illumio Core22.5.32.20-PCE is available for Illumio Core On-Premises customers only.
>
> 22.5.32.20-VEN is available for both Illumio Core On-Premises customers and Cloud customers.

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 22.5.20 solved software and security issues for the PCE and VEN to refine the software and improve its reliability and performance.

For the complete list of improvements and enhancements to the PCE and VEN, see “Resolved Issue in 22.5.20” in the Illumio Core Release Notes 22.5.

Changes in Release 22.5.20

Deprecated non-C-VEN Deployment on Kubernetes

In previous releases, Core VEN software could be deployed on Kubernetes nodes, and in conjunction with Kubelink could provide visibility and enforcement of containerized workloads in a Kubernetes cluster. As of this Core 22.5.20 release this configuration is no longer supported. The only way to get visibility and enforcement of containerized workloads in a Kubernetes cluster is to use the Illumio Core for Kubernetes product.

Illumio Core REST API in 22.5.30

The Illumio Core REST API v2 has changed in 22.5.30 in the following ways.

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

In this release no new or changed APIs are introduced to support new features. However, many new and changed APIs are covered in this document to help users understand where to look for changes and what these changes represent.

Changed Public APIs

In release 22.5.30, there is only one minor change to the existing REST APIs.

`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`
- `per_rule_flow_log_setting`
- `labels_editing_warning_for_enforcement_mode`

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

Illumio Core REST API in 22.5.20

The Illumio Core REST API v2 has changed in 22.5.20 in the following ways.

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

In this release no new or changed APIs are introduced to support new features. However, many new and changed APIs are covered in this document to help users understand where to look for changes and what these changes represent.

New Public APIs

common ip_list.schema.json

This new common schema offers a list of URIs with the time/user data about a ruleset creation, updating, or deletion.
It is referenced from sec_policy_rule_sets_sec_rules_consumers_get.

common label_group_optional_key_value.schema.json

This new common schema offers information about the label URi and key and value in the key-value pair.

Rulesets and Rules for Consumers and Providers

sec_policy_rule_sets_sec_rules_consumers

This schema is replaced by the following two new APIs:

sec_policy_rule_sets_sec_rules_consumers_get

There are changes to some of the properties, such as:

- `ip_list`: description is substituted with the reference to `common/ip_list.schema.json`
- `label`: description substituted with a reference to `common/label_optional_key_value.schema.json`
- `label_group`: removed "additionalProperties": false
- `workload`: removed "additionalProperties": false.

Added:

- `items`: removed "additionalProperties": false.

sec_policy_rule_sets_sec_rules_consumers_put

- `ip_list`: description is substituted with the reference to `/common/href_object.schema.json`
- `label`: description substituted with the reference to `/common/href_object.schema.json`

sec_policy_rule_sets_sec_rules_providers

This schema is replaced by the following two new APIs:

sec_policy_rule_sets_sec_rules_providers_get

There are changes to some of the properties, such as:

- `ip_list`: description is substituted with the reference to `/common/ip_list.schema.json`
- `label`: description substituted with the reference to `/common/label_optional_key_value.schema.json`
- `virtual_service`: Added the property `name`(Name of virtual service)

sec_policy_rule_sets_sec_rules_providers_put

`label`: description substituted with the reference to `common/href_object.schema.json`

Security Principals

common consuming_security_principals

This schema is replaced by the following two new APIs:

common consuming_security_principals_get

- Several new properties have been added: `href`, `sid`, `name`, `description`, `deleted`, and `used_by_ruleset`(Flag to indicate if this security principal is being used by a ruleset)

common consuming_security_principals_put

- One additional propery is added: `href`, URI of security principal

IP Tables

common ip_tables_rule_actors

This schema is replaced by the following two new APIs:

common ip_tables_rule_actors_get

The property label is now described with a reference to a schema:

- `label` is referencing `label_optional_key_value.schema.json`

common ip_tables_rule_actors_put

These properties are now described using references:

- `label` is referencing `href_object.schema.json`
- `label_group` is referencing `href_object.schema.json`
- `workload` is referencing `href_object.schema.json`

Scopes

common rule_set_scope

This schema is replaced by the following two new APIs:

common rule_set_scope_get

These properties are now described using references:

- `label` is referencing `label_optional_key_value.schema.json`
- `label_group` is referencing `label_group_optional_key_value.schema.json`

common rule_set_scope_put

These properties are now described using references:

- `label` is referencing `href_object.schema.json`
- `label_group` is referencing `href_object.schema.json`

common rule_set_scopes

This schema is replaced by the following two new APIs:

common rule_set_scopes_get

The property `items` is now described with a reference to a schema:

- `items` is referencing `rule_set_scope_get.schema.json`

common rule_set_scopes_put

The property `items` is now described with a reference to a schema:

- `items` is referencing `rule_set_scope_put.schema.json`

Changed Public Experimental APIs

Global changes for the APIs in this release have been summarized in the following overview:

Common IP Tables

common-ip_tables_rules_get

Property

- Added properties are: `created_at`, `updated_at`, `deleted_at`, `created_by`, `updated_by`, `deleted_by`, `update_type` (with an added type `null`)
- For the property `actors`, the schema `common/ip_tables_rule_actors.schema.json` was replaced with `ip_tables_rule_actors_get.schema.json`

common-ip_tables_rules_post

- For the property `actors`, the reference to the schema `common/ip_tables_rule_actors.schema.json` was replaced with `ip_tables_rule_actors_get.schema.json`

rule_search_post_response_rule_set

- For the property `scopes`, the reference to the schema `common/rule_set_scopes.schema.json` was replaced with `ip_tables_rule_actors_put.schema`

Firewall Settings

sec_policy_firewall_settings_get

These properties have been changed:

- `static_policy_scopes`
  Reference to `common/rule_set_scopes.schema.json` is replaced with `common/rule_set_scopes_get.schema.json`
- `containers_inherit_host_policy_scopes`
  Reference to `common/rule_set_scopes.schema.json` is replaced with `common/rule_set_scopes_get.schema.json`
- `blocked_connection_reject_scopes`
  Reference to `common/rule_set_scope.schema.json` is replaced with `common/rule_set_scope_get.schema.json`
- `loopback_interfaces_in_policy_scopes`
  Reference to `common/rule_set_scope.schema.json` is replaced with `common/rule_set_scope_get.schema.json`

sec_policy_firewall_settings_put

These properties have been changed:

- `static_policy_scopes`
  Reference to `common/rule_set_scopes.schema.json` is replaced with `common/rule_set_scopes_put.schema.json`
- `containers_inherit_host_policy_scopes`
  Reference to `common/rule_set_scopes.schema.json` is replaced with `common/rule_set_scopes_put.schema.json`
- `blocked_connection_reject_scopes`
  Reference to `common/rule_set_scope.schema.json` is replaced with `common/rule_set_scope_put.schema.json`
- `loopback_interfaces_in_policy_scopes`
  Reference to `common/rule_set_scope.schema.json` is replaced with `common/rule_set_scope_put.schema.json`

Rules and Rulesets

sec_policy_rule_search_post

- For the property consuming_security_principals:
  Reference to common/consuming_security_principals.schema.json is replaced with common/consuming_security_principals_put.schema.json

sec_policy_rule_search_post_response

These substitutions are introduced:

- For the property providers:
  Reference to sec_policy_rule_sets_sec_rules_providers.schema.json is replaced with sec_policy_rule_sets_sec_rules_providers_get.schema.json
- For the property consumers:
  Reference to sec_policy_rule_sets_sec_rules_consumers.schema.json is replaced with sec_policy_rule_sets_sec_rules_consumers_get.schema.json
- For the property consuming_security_principals:
  Reference to common/consuming_security_principals.schema.json is replaced with common/consuming_security_principals_get.schema.json

rule_search_post_response_rule_set

- For the property scopes:
  Reference to common/rule_set_scopes.schema.json is replaced with common/rule_set_scopes_get.schema.json.

sec_policy_rule_sets_get

For the API sec_policy_rule_sets_get, the changes are as follows:

- The property rules is not required anymore and has a reference to sec_policy_rule_sets_sec_rules_get.schema.json
- The property update_type has a reference to common/sec_policy_update_type.schema.json

- The property scopes has a reference to common/rule_set_scopes_get.schema.json instead of to common/rule_set_scopes.schema.json

sec_policy_rule_sets_post

- The property scopes has a reference to common/rule_set_scopes_put.schema.json instead of common/rule_set_scopes.schema.json

sec_policy_rule_sets_put

- For the property scopes: common/rule_set_scopes.schema.json is replaced with common/rule_set_scopes_put.schema.json
- For the property rules: sec_policy_rule_sets_sec_rules_providers.schema.json is replaced with sec_policy_rule_sets_sec_rules_providers_put.schema.json
- For the property consumers: sec_policy_rule_sets_sec_rules_consumers.schema.json is replaced with sec_policy_rule_sets_sec_rules_consumers_put.schema.json
- For the property consuming_security_principals: common/consuming_security_principals.schema.json is replaced with common/consuming_security_principals_put.schema.json
- For the property ip_tables_rules: common/ip_tables_rule_actors.schema.json is replaced with common/ip_tables_rule_actors_put.schema.json

sec_policy_rule_sets_sec_rules_get

The following properties are added:

- created_at: Timestamp when this rule set was first create
- updated_at: Timestamp when this rule set was last updated
- deleted_at: Timestamp when this rule set was deleted
- created_by: User who originally created this rule set
- updated_by: User who last updated this rule set

- deleted_by: User who deleted this rule set
- For the property providers:
  Reference to sec_policy_rule_sets_sec_rules_providers.schema.json is replaced with sec_policy_rule_sets_sec_rules_providers_get.schema.json
- For the property consumers:
  Reference to sec_policy_rule_sets_sec_rules_consumers.schema.json is replaced with sec_policy_rule_sets_sec_rules_consumers_get.schema.json
- For the property consuming_security_principals:
  Reference to common/consuming_security_principals.schema.json is replaced with common/consuming_security_principals_get.schema.json
- For the property update_type:
  Reference is added to common/sec_policy_update_type.schema.json

sec_policy_rule_sets_sec_rules_post

- For the property providers:
  Reference to sec_policy_rule_sets_sec_rules_providers.schema.json, replaced by sec_policy_rule_sets_sec_rules_providers_put.schema.json
- For the property consumers:
  Reference to sec_policy_rule_sets_sec_rules_consumers.schema.json replaced by sec_policy_rule_sets_sec_rules_consumers_put.schema.json
- For the property consuming_security_principals:
  Reference to common/consuming_security_principals.schema.json replaced by common/consuming_security_principals_put.schema.json

sec_policy_rule_sets_sec_rules_put

References have been changed as follows:

- For the property providers:
  sec_policy_rule_sets_sec_rules_providers.schema.json, is replaced by sec_policy_rule_sets_sec_rules_providers_put.schema.json
- For the property consumers: sec_policy_rule_sets_sec_rules_consumers.schema.json replaced by sec_policy_rule_sets_sec_rules_consumers_put.schema.json
- For the property consuming_security_principals:
  common/consuming_security_principals.schema.json is replaced by common/consuming_

security_principals_put.schema.json

Traffic Flows

traffic_flows_async_queries_post

In this release, the API `traffic_flows_async_queries_post` was changed so that the new properties are added for the property `boundary_decisions`:

- `override_deny_rule`: Overridden deny rule
- `blocked_non_illumio_rule`: Deny rule not written by Illumio

explorer_filters

These same properties,

- `override_deny_rule`: Overridden deny rule
- `blocked_non_illumio_rule`: Deny rule not written by Illumio

have been added to `explorer_filters.`

What's New and Changed in Release 22.5.10+UI2

Illumio Core 22.5.10+UI2 Maintenance Release

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 22.5.10+UI2 solved software and security issues to refine the software and improve its reliability and performance.

For the complete list of improvements and enhancements to the PCE, see "Resolved Issue in 22.5.10+UI2" and "Known Issues in 22.5.10+UI2"in the Illumio Core Release Notes 22.5.

Changes in Release 22.5.10+UI2

In Illumio Core 22.5.10+UI2, Illumio returned the Explorer feature to the PCE web console for customers who still want to use the functionality in that area of the GUI. To access the original Explorer feature, upgrade to Illumio Core 22.5.10+UI2.

IMPORTANT:
When you use the original Explorer feature, the functionality does not support the new Illumio Core 22.5 flexible labing features, 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. See Illumination Plus Table View and Illlumination Plus Mesh View the *Visualization Guide* to learn how to use these features, which provide the functionality formerly provided in the Explorer feature.

What's New and Changed in Release 22.5.12

Illumio Core 22.5.12 Maintenance Release

Illumio Core 22.5.32 includes an updated version of the PCE and VEN software.

IMPORTANT:
Illumio Core 22.5.32.12-PCE and 22.5.32.12-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 22.5.12 solved software and security issues for the PCE and VEN to refine the software and improve its reliability and performance.

For the complete list of improvements and enhancements to the PCE, see “Resolved Issue in 22.5.12-PCE” and “Resolved Issue in 22.5.12-VEN”in the Illumio Core Release Notes 22.5.

Documentation Updates for Core 22.5.12

The *PCE Installation and Upgrade Guide* for Core 22.5 no longer includes documentation for the `kernel.shmmax` parameter. In prior releases, the guide recommended that you set `kernel.shmmax` to 60000000. As of Postgres13, which was added in Core 21.5.0, you no longer need to change the `kernel.shmmax` value.

What's New and Changed in Release 22.5.10

New Features in the Release 22.5.10

The following new features were added in Illumio Core 22.5.10.

VEN Dashboard

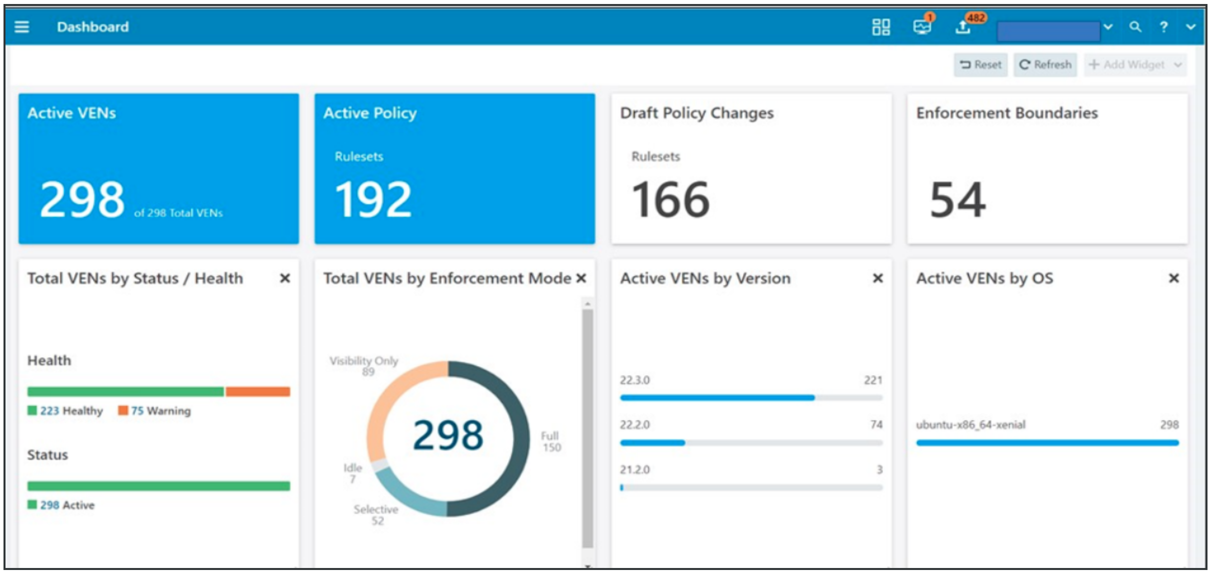
Illumio now provides a dashboard to give you broad, visualized information about VEN statistics.

The Dashboard aggregates various data from the system and helps you focus on the data you are interested in.

In this release, only two user roles are allowed to use the Dashboard:

- Global Org Owners
- Global Administrators

The Dashboard contains several widgets to display summary statistics or status information.



For more information, see VEN Dashboard in the *Visualization Guide*. For information about the REST APIs for this feature, see VEN Dashboard in the *REST API Developer Guide*.

VEN Tampering Protection

In Illumio Core and Illumio Endpoint 22.5.10 and later releases, you can protect the following types of VENs from unintended actions and tampering:

- Windows and Linux VENs running on servers
- Windows VENs running on endpoints

This feature protects the VEN itself from tampering. The VEN also has an existing capability to protect the workload host that the VEN is running on from being tampered with. For information about how the VEN detects tampering with the host firewall, see VEN Firewall Tampering Detection.

The new VEN tampering protection feature protects VENs from unintended, accidental invocation of VEN CLI actions and installer commands that impact VEN functionality, and malicious attempts (including from System Administrators) to disable or uninstall the VEN, or otherwise render the VEN unusable. This tampering protection restricts VEN CLI commands issued by all users, including the users who have administrative or root access to the VEN hosts (servers and endpoints).

> NOTE:
> Not all VEN actions support using a maintenance token for tampering protection. See About Tampering Protection in the VEN Administration Guide for the list of supported actions.

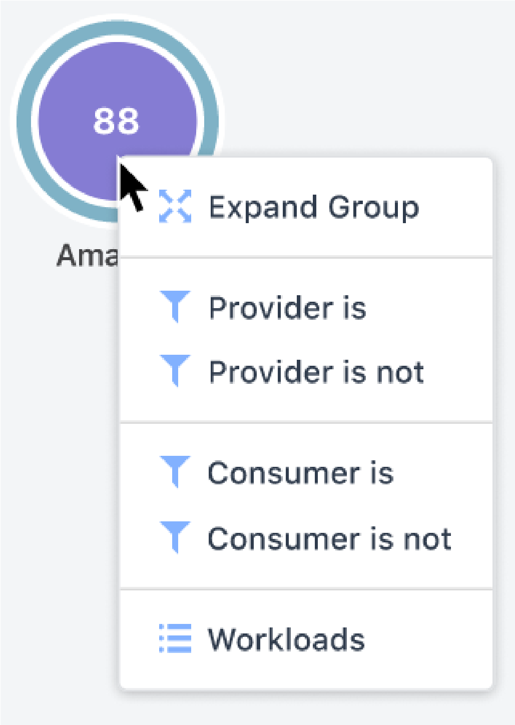
Show Amount of Data Transfer GA

In this release, the Show Amount of Data Transfer feature is now generally available. This feature first appeared in the Illumio Core 20.2 release. For more information about using this feature in your production environment, see Enhanced Data Collection in the *Security Policy Guide*.

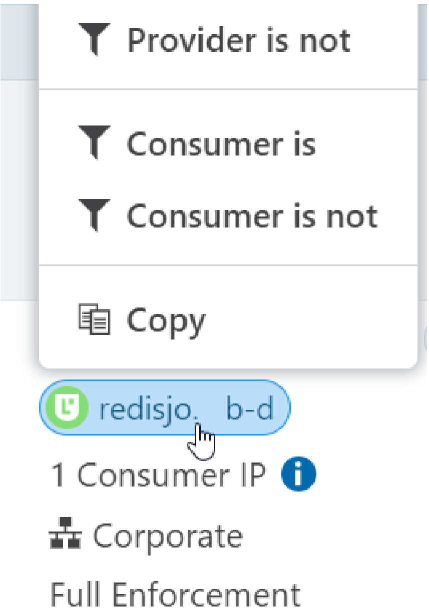
Context Menus in Illumination Plus

Illumination Plus now provides context menus in the following locations:

- In the Map view:



- In the Table view:



This menu includes a copy, cut, paste and other options like copy and paste objects into a specific field. For example, you can select an option to “Include in Consumers,” or add an object as a search query.

For information about Illumination Plus, See Illumination Plus in the *Visualization Guide.*

Changes in the Release 22.5.10

Support for Additional Operating System

Starting from this release, support for Mac OS was added for the on-premises installations. For information about the Endpoint for macOS, see the Endpoint Installation and Usage Guide.

Chapter 2

What's New and Changed in Release 22.5.0

Illumio Core 22.5.0 was an unreleased version of the Illumio Core software.

New Features in 22.5.0

The following new features were added in Illumio Core 22.5.0.

Flexible Label Types

In this release, Illumio has introduced user-defined label types in addition to the previous four types (REAL). Now, administrators can create their own label types such as for operating system, business unit, and compliance.

You can define custom label types to reflect additional characteristics of the workloads in your installation. Create any label type that meets your organization's business needs. For example, you might want to label workloads according to their operating systems.

Flexible labeling provides for tighter, more granular policies. You can visualize larger deployments more efficiently.

New label types are supported throughout Illumio Core, including pairing profiles, container workload profiles, rules and rulesets, enforcement boundaries, and so on.

For more details about flexible labeling, see Labels and Label Groups in the Security Policy Guide.

Illumination Plus

Illumination Plus supports additional label types, as well as writing rules for these labels. It provides a unique new way to reveal the traffic flows in your network and to help you configure policies to secure your applications using filtering.

New features in Illumination Plus are:

- Illumination Plus feature provides functionality from the classic map and the functionality from the former Explorer feature.

  You can still access the classic Illumination feature in this release because Illumination Plus has limitations working with the new flexible labeling feature. However, the previous Explorer feature is replaced by Illumination Plus and no longer available in this release. The functionality in the former Explorer feature is now available in Illumination Plus in the Table View and Mesh View.

  > NOTE:
  > In Illumio Core 22.5.10+UI2, Illumio returned the Explorer feature to the PCE web console for customers who still want to use the functionality in that area of the GUI. To access the original Explorer feature, upgrade to Illumio Core 22.5.10+UI2.
  >
  > When you use the original Explorer feature, the functionality does not support the new Illumio Core 22.5 flexible labing features, which allows you to create custom labels. The original Explorer feature only supports the standard Core RAEL labels.

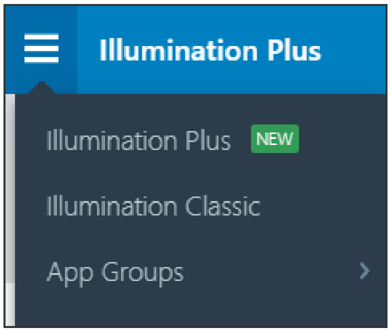
  See Illumination Plus Table View and Illlumination Plus Mesh View the *Visualization Guide* to learn how to use these features, which provide the functionality formerly provided in the Explorer feature.

- Illumination Plus Map View and Table View support the new label types.
- Workloads are stacked in groups, without being confined to the previous label ordering. These are options for grouping:
  - Auto grouping, which is currently configured, allows for cleaning up the view and gives the appropriate level of grouping.
  - Grouping by role, application, environment, or location (REAL), as it was available previously in Illumination Classic
  - Grouping by other defined criteria such as BU (business units), ST (special symbol test), C (currencies), and so on. Grouping can be done flexibly as you run your queries.
- New layout options for maps:
  - Circular Layout, which enhances the space use on the screen.

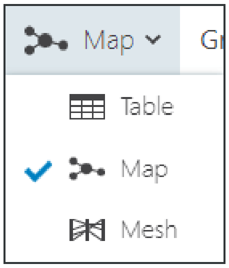
    - Organic Layout, which reduces overlaps in label sets, groups, and traffic lines. It groups things that are highly connected and avoids crossing of the links.
    - Tiered Layout, which highlights source or destination relationships and gives you the overview of traffic flows from top to bottom. This layout type works better with smaller data sets.
- Ability to increase the VEN traffic update frequency:

  By default, VENs update traffic on the Illumination map every 10 minutes. An option on the Summary tab (which displays when you click a Workload in the Map) allows you to temporarily increase the update frequency to once per minute. After 10 minutes, the default update rate of once every 10 minutes resumes.
- Reported vs. Draft View. Reported view categories are:
    - All Draft
        - Draft View: Allowed
        - DraftView: Potentially Blocked
        - Draft View: Blocked
    - Quick Draft Rules, which determine policy decisions using label-set rules only'
    - Deep rule analysis, which performs deep analysis to determine policy
- Results Settings:
    - If you increase the maximum number of connections, the result will be more complete and the performance slower.
    - If the number of connections returned from the database exceeds the maximum displayed in Illumination Plus, all connections can be viewed by stepping through the results.

To start working with Illumination Plus, select it from the menu:

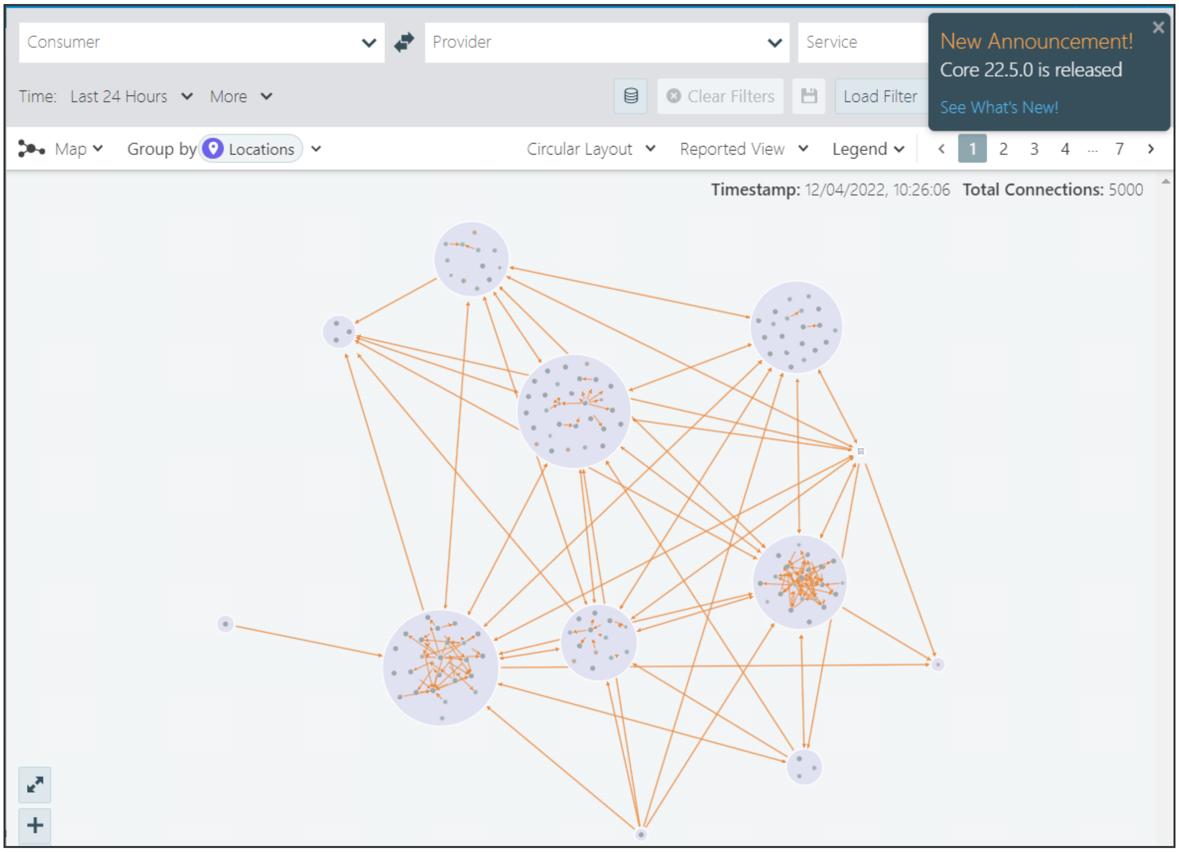


Once in the Illumination Plus screen, select the view from the dropdown menu:



Select the time frame you want to include to view the results:

- Last Hour
- Last 24 Hours
- Last Week
- Last Month
- Anytime
- Custom (using the supplied pop-up calendar)



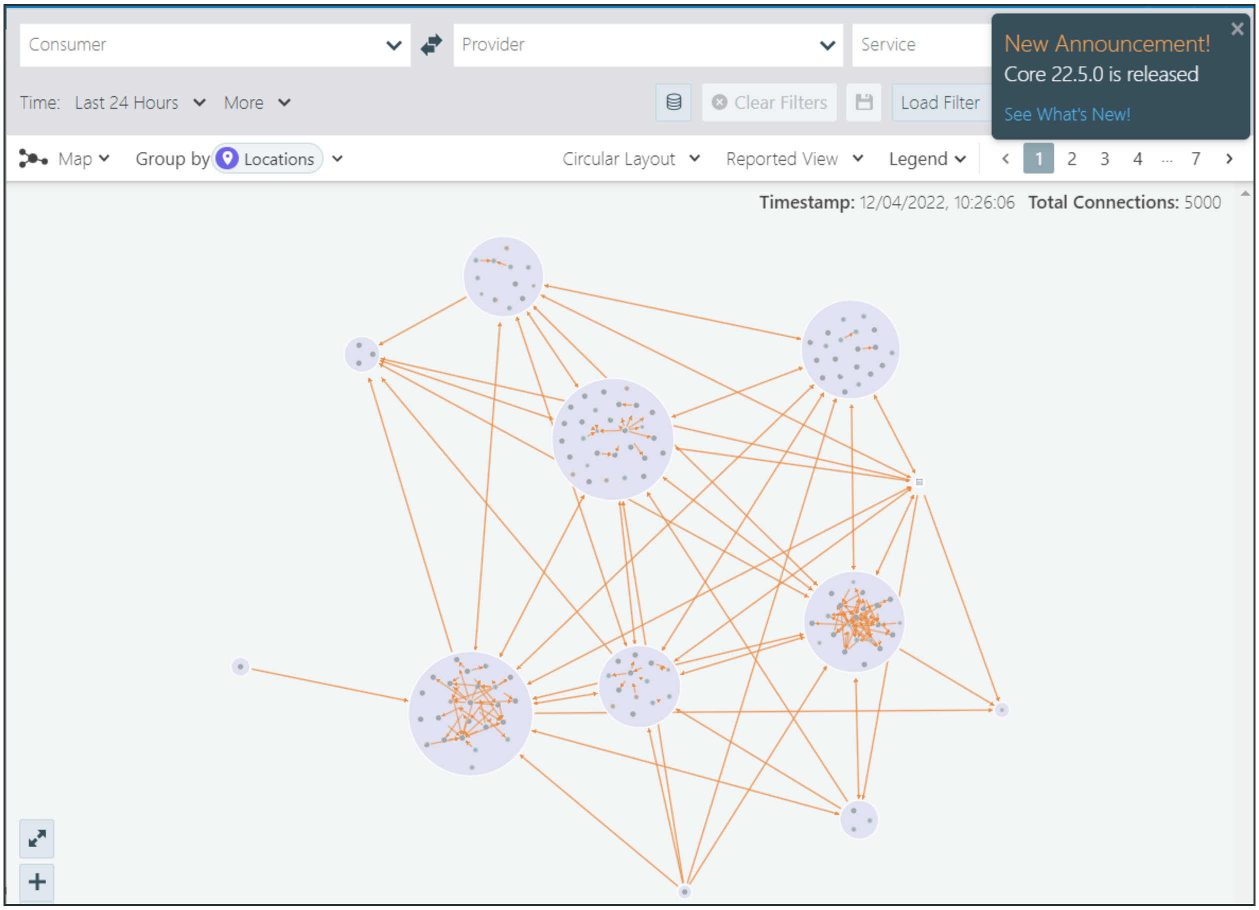
New Announcement!
Core 22.5.0 is released
See What's New!

Time: Last 24 Hours

Group by Locations

Timestamp: 12/04/2022, 10:26:06 Total Connections: 5000

It is convenient to use cashed results, which are run in the last 24 hours.



New Announcement!
Core 22.5.0 is released
See What's New!

Timestamp: 12/04/2022, 10:26:06 **Total Connections:** 5000

For more details about Illumination Plus, see the Visualization Guide.

Enhancements in 22.5.0

The following enhancements were added to existing features in Illumio Core 22.5.0:

Enabling Container Inherit Host Policy on nftables

For Core VEN running standalone containers, the Container Inherit Host Policy (CIHP) provides a mechanism to get visibility and enforcement for traffic between containers and the outside world.

With CIHP, containers running on the workload inherit the policy sent down by the PCE to the VEN. As a result, the containers can be considered part of the host workload.

In RHEL/CentOS/Oracle Linux/etc. 8+, the default firewall type has changed from iptables to nftables: starting in 22.5.0 VEN, CIHP rules will now be properly applied on these platforms

Removing a PCE from a Supercluster

A new command is provided for removing a PCE from a Supercluster. Unpair any VENs from the PCE, then run this command on the PCE to be removed:

```
$ sudo -u ilo-pce illumio-pce-ctl supercluster-leave
```

For the complete procedure, see Remove PCE from Supercluster in the PCE Supercluster Deployment Guide.

New APIs for Checking Draft Policy Impact Before Provisioning

The new API `sec_policy_impact_post` contains the name of the method on existing resources, which is **impact**. It is used to see the policy impact before provisioning.

This new schema is referencing `sec_policy_change_subset`, which contains the property `change_subset`:

- If `change_subset` is provided, the impact will be calculated only on this property.
- If `change_subset` is missing, the impact will be calculated on all of the pending items.

src_ip in Collector Traffic Filters

This feature enables users to filter traffic based on the source IP address.

Scanners can generate a lot of frequent traffic, flooding the Core’s traffic database and resulting in shorter than expected traffic data horizon. Using the predefined source IP, users can eliminate traffic from the data pipeline and database and reduce PCE host resources utilization.

In this release, filtering by source IP is supported only via API.

UI changes for both source port and IP are planned in a future release.

For the `settings_traffic_collector` APIs, there are two IP addresses that are defined for search:

- The new single-source IP address (`src_ip`), which was added to all three APIs
- The updated single destination IP address (`dst_ip`), which is now renamed from "single IP address or CIDR" to "single destination IP address or CIDR".

For more details, see Settings Traffic Collector.

VEN Uninstall Timer

The configurable VEN uninstall timer was introduced to assist customers who ran into issues when mass-unpairing of VENs, either via API or UI. It will ensure that the VEN cleanly unpairs from the hosts over a certain time frame.

In previous releases, the VEN unpair request would time out after 7 days . If the VEN heartbeats within the 7 days, the VEN was instructed to uninstall itself but after 7 days the VEN record was completely purged from the PCE.

In such case:

- User had to manually get onto the host and uninstall the VEN.
- PCE did not send an instruction to the VEN to uninstall itself.
- VEN would send a heartbeat to the PCE every four hours and receive the 401 error from the PCE.

In this release, the 7-day VEN Uninstall Timer is adjustable in both directions. The timer can be set for a short time such as one hour, all the way to 30 days to allow for the longest possible time for the hosts to come back, and then gracefully uninstall themselves.

Distinguishing Among Idle, Unmanaged, and No Port Exposure in VES

When querying vulnerability summary, the UI cannot differentiate between vulnerabilities that are still calculating and the ones that are N/A (not applicable), which stands for unmanaged workloads and idle workloads. As a result, the UI returns a Null value.

The new field `vulnerability_computation_state` was added to the `vulnerability_summary` and defines three computation states:

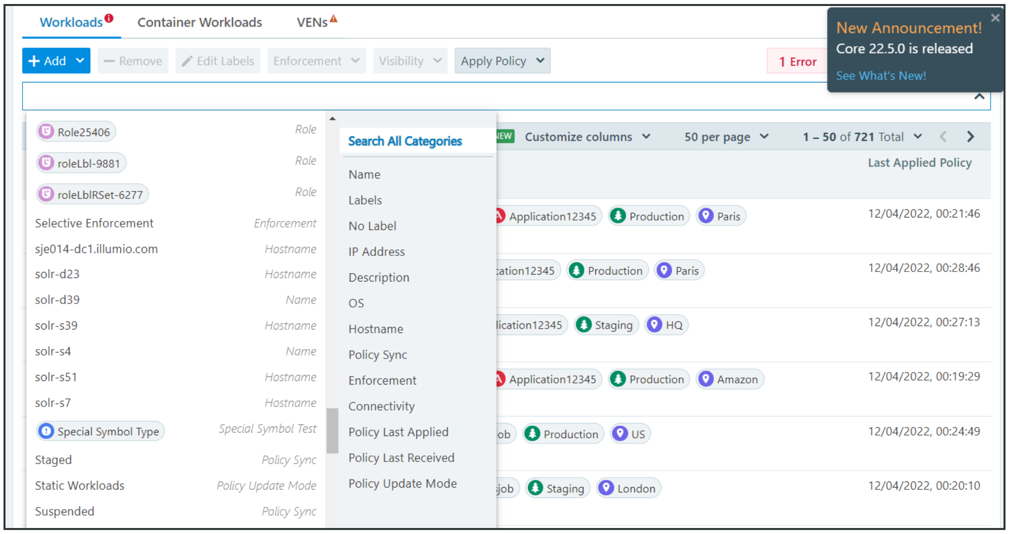
- `not_applicable`
- `syncing`
- `in_sync`

For more details, see vulnerability_summary.schema.json.

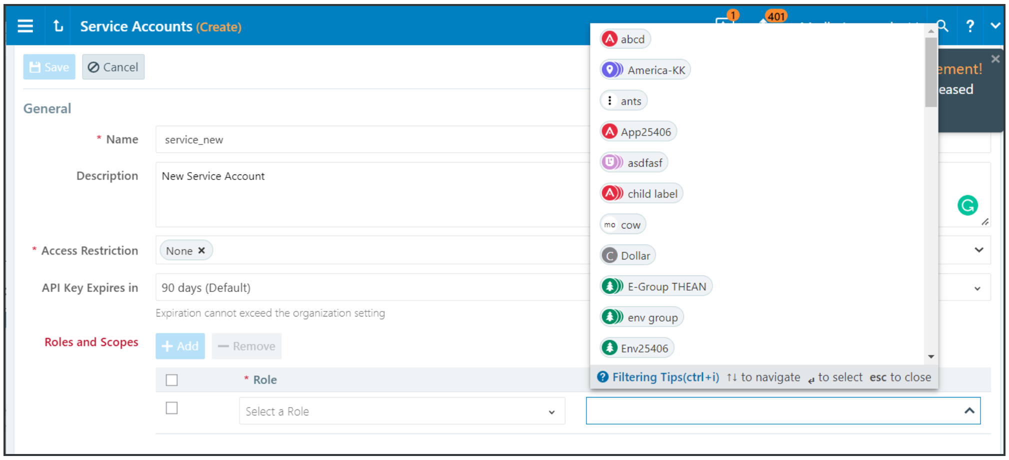
RBAC Changes

The following changes have been introduced:

- Support for the `role` dimension along with other custom dimensions for user scopes and service accounts



- Code that was restricting RBAC dimensions to four dimensions has been removed



* Name: service_new

Description: New Service Account

* Access Restriction: None ×

API Key Expires in: 90 days (Default)

Expiration cannot exceed the organization setting

- Changes to the autocomplete/facet APIs to support the new UI filter.

The common schema `rbac_permission_types.schema.json` is referenced from other APIs to indicate the RBAC permission that is used: `write` or `provision`.

In the case of Illumination Plus and with the new property `caps`, the type `provision` is not used to avoid additional delays when checking the permissions of each flow. Therefore, only permission `write` is used and further verification is handled on the UI side.

For more details, see RBAC Permissions.

Illumio Core REST API in 22.5.0

The Illumio Core REST API v2 has changed in 22.5.0 in the following ways.

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

New Public Stable APIs

Vulnerability APIs

vulnerability_summary.schema.json

The new vulnerability summary schema looks as follows:

```
{
"$schema": "http://json-schema.org/draft-04/schema#",
"type": "object",
"description": "Vulnerabilities summary associated with the workload",
"additionalProperties": false,
"required": ["num_vulnerabilities", "max_vulnerability_score"],
"properties": {
       "num_vulnerabilities": {
               "description": "Number of associated vulnerabilities",
               "type": "integer"
               },
       "vulnerability_score": {
               "description": "The aggregated vulnerability score of
                the workload across all the vulnerable ports.",
               "type": "integer"
               },
       "max_vulnerability_score": {
               "description": "The maximum of all the vulnerability
                scores with the detected_vulnerabilities on the workload.",
               "type": "integer"
               },
       "vulnerable_port_exposure" : {
               "description" : "The aggregated vulnerability port exposure
                score of the workload across all the vulnerable ports",
               "type" : ["integer", "null"]
               },
       "vulnerable_port_wide_exposure" : {
               "additionalProperties" : false,
               "properties" : {
               "any" : {
                       "description" : "The boolean value representing if at least
                        one port is exposed to internet (any rule) on the
workload",
                       "type" : ["boolean", "null"]
               },
               "ip_list" : {
                       "description" : "The boolean value representing if at least
                        one port is exposed to ip_list(s) on the workload",
                       "type" : ["boolean", "null"]
               }
           }
       },
       "vulnerability_exposure_score": {
               "description": "The aggregated vulnerability exposure score of
                the workload across all the vulnerable ports.",
               "type": ["integer", "null"]
               },
       "vulnerability_computation_state": {
               "description": "Indicates the computation state for the
                vulnerability exposure score for the workload.",
               "type": "string",
               "enum": ["not_applicable", "syncing", "in_sync"]
               }
       }
}
```

where

vulnerability_computation_state

is the new field added for all APIs that return the namespace. It defines three computation states:

- `not_applicable`: N/A (not applicable) ndicates that the vulnerability exposure score cannot be calculated and happens in the following cases:

  - Unmanaged workloads
  - Idle workloads
  - Vulnerabilities that have no port associated with them.
- `syncing`: For managed workloads, when the vulnerability exposure score hasn't been calculated yet and the value is not available.
- `in_sync`: For managed workloads, when the workload with the VES value is calculated and available.

The following APIs have been updated to return vulnerability_computation_state:

- `workloads` (get collection)
- `workloads/detailed_vulnerability`
- `workloads` (get instance)
- `workloads/:uuid/detected_vulnerabilities`
- `aggregated_detected_vulnerabilities`

Examples of Computation States:

`syncing`: Workload is in syncing state (VES is calculable but hasn't been calculated yet)

```
"vulnerability_summary": {
        "num_vulnerabilities": 30,
        "max_vulnerability_score": 88,
        "vulnerability_score": 1248,
        "vulnerable_port_exposure": null,
        "vulnerable_port_wide_exposure": {
                "any": null,
                "ip_list": null
        },
        "vulnerability_exposure_score": null,
        "vulnerability_computation_state": "syncing"
},
```

`not_applicable`:Unmanaged workload with applied vulnerabilities

```
"vulnerability_summary": {
        "num_vulnerabilities": 30,
        "max_vulnerability_score": 88,
        "vulnerability_score": 1248,
        "vulnerable_port_exposure": null,
        "vulnerable_port_wide_exposure": {
                "any": null,
                "ip_list": null
        },
        "vulnerability_exposure_score": null,
        "vulnerability_computation_state": "not_applicable"
},
```

`in_sync`:Managed (non-idle) workload with applied vulnerabilities and computed vulnerability exposure score

```
"vulnerability_summary": {
        "num_vulnerabilities": 30,
        "max_vulnerability_score": 88,
        "vulnerability_score": 768,
        "vulnerable_port_exposure": 6,
        "vulnerable_port_wide_exposure": {
                "any": true,
                "ip_list": true
        },
        "vulnerability_exposure_score": 52,
        "vulnerability_computation_state": "in_sync"
},
```

common/aggregated_detected_vulnerability.schema.json

The new schema `aggregated_detected_vulnerability` applies to multiple workloads. The rules for resolving the aggregated computation state are as follows:

- If any of the workloads referencing the label(s) in the request is in the state `syncing`, the aggregated state is `syncing`.
- For the aggregated value to be in the `N/A` state ALL workloads must be in the state `N/A`.
- For all the other cases, the aggregated state is `in_sync`.

  For example:

- all workloads are managed and are not idle (eliminating `N/A`)
- all workloads have at least one valid vulnerable port (the port is not `NULL` and the prototype is not `NULL` for vulnerability)

```
{
"$schema":"http://json-schema.org/draft-04/schema#",
"type": "object",
"required": [ "aggregated_detected_vulnerabilities",
            "aggregated_detected_vulnerability_summary"],
"properties": {
       "aggregated_detected_vulnerability_summary": {
               "$ref": "vulnerability_summary.schema.json"
       },
       "aggregated_detected_vulnerabilities": {
           "type":"array",
            "items":{
            "type" : "object",
            "required" : [
               "vulnerability_exposure_score",
               "num_workloads",
               vulnerability"
            ],
               "additionalProperties" : false,
               "properties" : {
                  "port" : {
                     "description" : "The port which is associated with
                                     the vulnerability",
                      "type" : "integer"
                 },
                  "proto" : {
                        "description" : "The protocol which is associated
                                          with the vulnerability",
                        "type" : "integer"
                   },
                   "vulnerable_port_exposure" : {
                         "description" : "The aggregated exposure of the port
                                          across all the requested workloads
                                          based on the current policy",
                         "type" : ["integer", "null"]
                   },
                   "vulnerable_port_wide_exposure" : {
                   "additionalProperties" : false,
                   "properties" : {
                          "any" : {
                          "description" : "The boolean value representing if the
                           port is exposed to internet (any rule) on at least one
of
                           the workloads in the requested group",
                          "type" : ["boolean", "null"]
                   },
                   "ip_list" : {
                          "description" : "The boolean value representing if the port
                           is exposed to ip_list(s) on at least one of the
workloads
                           in the requested group",
                          "type" : ["boolean", "null"]
                       }
                 }
                 },
                 "vulnerability_exposure_score" : {
                          "description" : "The aggregated vulnerability exposure score
                           of the port across all the requested workloads based on
the
                           current policy",
                          "type" : ["integer", "null"]
                  },
                  "num_workloads" : {
                          "description" : "The number of workloads within the requested
                           group where the vulnerability exists on the specified
port
                           and protocol",
                          "type" : "integer"
                  },
                  "vulnerability" : {
                  "type": "object",
                  "additionalProperties": false,
                      "required": ["href", "score", "name"],
                          "properties": {
                          "href": {
                          "description": "The URI of the vulnerability class
                            to which this vulnerability belongs to",
                          "type": "string"
                  },
                  "score": {
                          "description": "The normalized score of the vulnerability
                            within the range of 0 to 100",
                          "type": "integer",
                             "minimum": 0,
                             "maximum": 100
                          },
                  "name": {
                          "description": "The title/name of the vulnerability",
                          "type": "string"
                  },
                  "cve_ids": {
                          "description": "The cve_ids for the vulnerability",
                          "type": "array",
                          "items": {
                          "type": "string"
                  }
            }
        }
   }
}
```

common/workloads_detected_vulnerabilities.schema.json

This schema specifies workload detected vulnerability, references the `vulnerability_summary.schema.json` for the summary information, and specifies the collection of the `workload_detected_vulnerabilities`. It is referenced by the following schema files:

- `workloads_detected_vulnerabilities_get.schema.json`
- `v1/workloads_get.schema.json`
- `v2/workloads_get.schema.json`

```
{
"$schema":"http://json-schema.org/draft-04/schema#",
"type": "object",
"required": ["detected_vulnerability_summary", "workload_detected_
vulnerabilities"],
"properties": {
       "detected_vulnerability_summary": {
               "$ref": "vulnerability_summary.schema.json"
       },
       "workload_detected_vulnerabilities": {
               "type":"array",
               "description": "Collection of the detected vulnerabilities
                 associated with the workload",
               "items":{
                       "type" : "object",
                       "required" : [
                       "ip_address",
                       "vulnerability"
                       ],
               "additionalProperties" : false,
                       "properties" : {
                       "ip_address" : {
                          "description" : "The ip address of the host where
                            the vulnerability is found",
                          "type" : "string"
                       },
               "port" : {
                          "description" : "The port which is associated
                            with the vulnerability",
                          "type" : "integer"
                       },
               "proto" : {
                          "description" : "The protocol which is associated
                            with the vulnerability",
                          "type" : "integer"
                       },
               "port_exposure" : {
                          "description" : "The exposure of the port based
```

```
             on the current policy",
           "type" : ["integer", "null"]
        },
 "port_vulnerability_exposure_score" : {
           "description" : "The vulnerability exposure score
                calculated for the port, based on the port
                 exposure and vulnerability",
           "type" : ["integer", "null"]
        },
"port_wide_exposure" : {
           "additionalProperties" : false,
           "properties" : {
           "any" : {
           "description" : "The boolean value representing
                if the port is exposed to internet (any rule).",
           "type" : ["boolean", "null"]
        },
"ip_list" : {
           "description" : "The boolean value representing if the
                port is exposed to ip_list(s)",
           "type" : ["boolean", "null"]
      }
    }
},
"workload" : {
  "type": "object",
  "additionalProperties": false,
  "required": ["href"],
  "properties": {
        "href": {
        "description": "The URI of the workload to which this
                vulnerability belongs to",
        "type": "string"
       }
   }
 },
 "vulnerability" : {
  "type": "object",
                 "additionalProperties": false,
                 "required": ["href"],
                 "properties": {
                       "href": {
                       "description": "The URI of the vulnerability class to
                        which this vulnerability belongs to",
                       "type": "string"
                       },
                "score": {
                 "description": "The normalized score of the vulnerability
                       within the range of 0 to 100",
                 "type": "integer",
                          "minimum": 0,
                          "maximum": 100
                        },
                       "name": {
                           "description": "The title/name of the vulnerability",
                           "type": "string"
                         }
                    }
                 },
                  "vulnerability_report" : {
                 "type": "object",
                 "additionalProperties": false,
                 "required": ["href"],
                 "properties": {

                 "href": {
                    "description": "The URI of the report to which this
                       vulnerability belongs to",
                    "type": "string"
               }
         }
     }
}
```

Other Common Schemas

These are the other new schemas in the `common` directory:

- common/sec_policy_update_type.schema.json
- common/label_optional_key_value.schema.json
- common/nfc_dvs_service_checks.schema.json
- common/nullable_href_object.schema.json

They are referenced by other schemas and have been added to this directory to eliminate duplication in the schema definitions.

New Public Experimental APIs

Security Policy

sec_policy_impact_post.schema.json

This API contains the name of the method on existing resources, which is `impact`. It is used to see the policy impact before provisioning.

```
{
        "$schema": "http://json-schema.org/draft-04/schema#",
        "type": "object",
        "properties": {
                "change_subset": {
                "$ref": "sec_policy_change_subset.schema.json"
                }
        }
}
```

This new schema is referencing `sec_policy_change_subset.schema.json`, which contains the property `change_subset`:

- If `change_subset` is provided, the impact will be calculated only on change_subset.
- If `change_subset` is missing, the impact will be calculated on all of the pending items.

sec_policy_impact_post_response.schema.json

The new API endpoint `POST /api/v2/orgs/1/sec_policy/impact` requires a schema to define it.

```
{
"$schema": "http://json-schema.org/draft-04/schema#",
"type": "array",
"items": {
       "type": "object",
       "properties": {
       "dependency": {
               "type": "object",
               "properties": {
               "label_groups": {
               "$ref": "../common/href_object.schema.json"
               },
       "services": {
               "$ref": "../common/href_object.schema.json"
               },
       "rule_sets": {
               "$ref": "../common/href_object.schema.json"
               },
       "ip_lists": {
               "$ref": "../common/href_object.schema.json"
               },
       "virtual_services": {
               "$ref": "../common/href_object.schema.json"
               },
       "firewall_settings": {
               "$ref": "../common/href_object.schema.json"
               },
       "secure_connect_gateways": {
               "$ref": "../common/href_object.schema.json"
               },
       "virtual_servers": {
               "$ref": "../common/href_object.schema.json"
               },
       "enforcement_boundaries": {
```

```
                "$ref": "../common/href_object.schema.json"
                }
        }
        },
        "required_by": {
                "type": "object",
                "properties": {
                        "label_groups": {
                        "type": "array",
                        "items": {
                        "$ref": "../common/href_object.schema.json"
                }
        },
        "services": {
                "type": "array",
                "items": {
                "$ref": "../common/href_object.schema.json"
                }
        },
        "rule_sets": {
                "type": "array",
                "items": {
                "$ref": "../common/href_object.schema.json"
                }
        },
        "ip_lists": {
                "type": "array",
                "items": {
                "$ref": "../common/href_object.schema.json"
                }
        },
        "virtual_services": {
                "type": "array",
                "items": {
                "$ref": "../common/href_object.schema.json"
                }
        },
        "firewall_settings": {
                "type": "array",
                "items": {
                "$ref": "../common/href_object.schema.json"
                }
        },
        "secure_connect_gateways": {
                "type": "array",
                "items": {
                "$ref": "../common/href_object.schema.json"
                }
        },
        "virtual_servers": {
                "type": "array",
                "items": {
                "$ref": "../common/href_object.schema.json"
                }
        },
        "enforcement_boundaries": {
                "type": "array",
                "items": {
                "$ref": "../common/href_object.schema.json"
                }
          }
     }
 }
```

Each of the allowed properties such as `ip_lists`, `label_groups`, and `services` can be included in the request body of the POST API endpoint call but the new schema defines the format and values of this API request for the example in the request body.

The response schema of that endpoint is `sec_policy_impact_post_response.schema.json` and if defines what the endpoint returns, such as the count of affected workloads, affected sets, and so on.

The response schema looks as follows:

```
{
"$schema": "http://json-schema.org/draft-04/schema#",
"type": "object",
"required": ["num_sets", "num_managed_workloads", "num_container_workloads",
                "num_unmanaged_workloads"],
       "properties": {
       "num_sets": {
               "description": "number of affected sets",
               "type": "integer"
               },
       "num_virtual_servers": {
               "description": "number of affected virtual servers",
               "type": "integer"
               },
       "num_managed_workloads": {
               "description": "number of affected workloads of type Workload",
               "type": "integer"
               },
       "num_container_workloads": {
               "description": "number of affected workloads of type ContainerWorkload",
               "type": "integer"
               },
       "num_unmanaged_workloads": {
               "description": "number of affected unmanaged workloads",
               "type": "integer"
               },
       "all_workloads_optimization": {
               "description": "flag to indicate if all-workloads-optimization
                       has been used",
               "type": "boolean"
               }
       }
}
```

RBAC Permissions

rbac_permission_types.schema.json

This common schema `rbac_permission_types.schema.json` is referenced from other APIs to indicate the RBAC permission that is used: `write` or `provision`.

```
{
        "$schema":"http://json-schema.org/draft-04/schema#",
        "type": "string",
                "description": "RBAC Permission types",
                "enum": ["write", "provision"]
        }
```

In the case of Illumination Plus and with the new property `caps`, the type `provision` is not used to avoid additional delays when checking the permissions of each flow. Therefore, only permission `write` is used and further verification is handled on the UI side.

Example

`GET /api/v2/orgs/:xorg_id/traffic_flows/async_queries/:uuid/download`

```
{
"dst": {
        "ip": "10.244.0.1",
        "workload": {
                "href": "/orgs/1/workloads/35d8efea-f230-4027-a8ee-5f20626c4d21",
                "name": "wl3",
                "labels": [
                {
                        "key": "env",
                        "href": "/orgs/1/labels/7",
                        "value": "Production"
                },
                {
                        "key": "loc",
                        "href": "/orgs/1/labels/11",
                        "value": "Amazon"
                },
                {
                        "key": "role",
                        "href": "/orgs/1/labels/3",
                        "value": "API"
                },
                {
                        "key": "B-label",
                        "href": "/orgs/1/labels/15",
                        "value": "b_label_2"
                }
        ],
        "managed": false,
                "os_type": "linux",
                "endpoint": false,
                "hostname": "",
                "enforcement_mode": "visibility_only"
                }
        },
"src": {
        "ip": "10.0.2.15",
        "workload": {
                "href": "/orgs/1/workloads/fc3801b8-05ec-4954-a957-7f5673123389",
                "name": "wl2",
                "labels": [
                {
                        "key": "env",
                        "href": "/orgs/1/labels/7",
                        "value": "Production"
                },
                {
                        "key": "loc",
                        "href": "/orgs/1/labels/11",
                        "value": "Amazon"
                },
                {
                        "key": "role",
                        "href": "/orgs/1/labels/3",
                        "value": "API"
                }
                ],
        "managed": false,
                "os_type": "linux",
                "endpoint": false,
                "hostname": "",
                "enforcement_mode": "visibility_only"
                }
        },
        "caps": [],
                "state": "snapshot",
                "dst_bi": 0,
                "dst_bo": 0,
                "seq_id": 2,
                "network": {
                        "href": "/orgs/1/networks/fbeeb98d-4ed6-428d-9f71-69f542bfd8fd",
                        "name": "Corporate"
                },
                "service": {
                        "port": 3306,
                        "proto": 6
                },
                "flow_direction": "outbound",
                "num_connections": 1,
                "policy_decision": "unknown",
                "timestamp_range": {
                "last_detected": "2022-09-01T20:35:22Z",
                "first_detected": "2022-09-01T20:35:22Z"
                }
        }
```

Report Schedules APIs

report_schedules_post_response.schema.json

This new schema is referencing report_schedules_get, which is used to return the user's choice to send by mail.

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

Deleted Public Stable APIs

detected_vulnerability_get.schema.json

workloads_detected_vulnerabilities_get.schema.json

For information where the functionality fro these deleted APIs was transferred, see common/workloads_detected_vulnerabilities.schema.json.

Changed Public Stable APIs

Workloads

workloads_get

In this schema:

The whole section on `vulnerabilities_summary` was replaced with a reference to the new schema `common/vulnerability_summary.schema.json`.

The reference to `workloads_detected_vulnerabilities_get.schema.json` was replaced with a reference to `common/workloads_detected_vulnerabilities.schema.json`, or the same schema that was moved to the `common` directory.

Settings Traffic Collector

For the settings_traffic_collectorAPIs:

- **settings_traffic_collector_get**
- **settings_traffic_collector_post**
- **settings_traffic_collector_put**

there are two IP addresses that are defined for search:

- The new single-source IP address (`src_ip`), which was added to all three APIs
- The updated single destination IP address (`dst_ip`), which is now renamed from "single IP address or CIDR" to "single destination IP address or CIDR".

Oracle flows are currently filtered via a `runtime src_ip/dst_ip` (CIDR) setting and this feature is not available in SaaS. Runtime changes also require a PCE restart, while API settings do not.

The collector filters now support `src_ip` (CIDR) so that various filters can be created per organization without restarting the PCE.

```
"properties": {
        "target": {
        "properties": {
                "src_ip": {
                        "type": "string",
                        "description": "single source ip address or CIDR"
                },
                "dst_ip": {
                        "description": {
                        "single destination ip address or CIDR"
                }
        }
};
```

The collector filters now support `src_ip` (CIDR) so that various filters can be created per organization without restarting the PCE.

Example POST Curl command:

```
curl -i -u api_
10415cd5bcc0e14cc:'2ac31cbee8cd3e8fa7ca79d32d39a0249636624ada675965dd2ec239e3ea8af
0' --request POST --data '{"action":"drop","transmission":"unicast","target":
{"proto":6,"src_ip":"10.1.2.3"}}'
https://2x2testvc360.ilabs.io:8443/api/v2/orgs/2/settings/traffic_collector --
header "Content-Type: application/json"
```

Virtual Services

sec_policy_virtual_services_get

The Properties section was updated with new references to the common schemas:

- for the property created_by, the reference to common/href_object.schema.json is replaced with a reference to common/nullable_href_object.schema.json.
- for the property updated_by, the reference to common/href_object.schema.json is replaced with a reference to common/nullable_href_object.schema.json.
- for the property deleted_by, a new reference was added: common/nullable_href_object.schema.json.
- for the property update_type, a new reference was added: common/sec_policy_update_type.schema.json.
- for labels, a reference to common/labels.schema.json is replaced with a reference to common/label_optional_key_value.schema.json.

virtual_service_service_ports

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

               "$ref": "../common/service_ports_protocol_numeric.schema.json",
               "type": "integer",
               "enum": [
               6,
               17
               ]
           }
       }
}
```

For this schema, a reference to common/service_ports_protocol_numeric.schema.json was deleted.

Changed Public Experimental APIs

Virtual Servers and Virtual Services

discovered_virtual_servers_get

- Two properties have been deleted:
  - `snat_type`: SNAT source IP type
  - `snat_pool_ips`: NAT source IPs of virtual server in ipv4 format
- For the property `service_checks`, the reference to common/service_ports_protocol_numeric.schema.json was removed
- For the property virtual_server, the reference to common/sec_policy_update_type.schema.jsonwas added.

sec_policy_virtual_servers_get

For this API:

- For the property `labels`, the reference to `labels.schema.json` was replaced with a reference to `common/label_optional_key_value.schema.json`.
- For the property `providers`, the reference to `common/href_object.schema.json` was replaced with a reference to `common/label_optional_key_value.schema.json`.
- Properties `mode`, `discovered_virtual_server`, and `deleted_at` the additional type `NULL`.
- For the property `deleted_by`, the reference to `common/href_object.schema.json` was replaced by the reference to `common/nullable_href_object.schema.json`.

Settings

For this API, both for the GET and PUT methods a new property was added:

- `ven_maintenance_token`: This token identifies if the tampering protection for the VEN and endpoints is enabled. The default is `not enabled`.

settings_get

settings_put

```
{
        "properties": {
        "ven_maintenance_token_required": {
                "description": "Identifies if the tampering protection for
                        the VEN and endpoints is enabled or not.",
                "type": "boolean",
                "default": false
                }
        }
}
```

Traffic Flows

traffic_flows_async_queries_download_get

```
{
        "$schema": "http://json-schema.org/draft-04/schema#",
        "description": "The list of traffic flows matching the query",
        "type": "array",
        "items": {
                "type": "object",
                "required": [
                        "src",
                        "dst",
                        "service",
                        "num_connections",
                        "policy_decision",
                        "flow_direction",
                        "timestamp_range",
                        "caps"
                ],
                "properties": {
                ------------------------------------
```

```
       },
       "caps": {
               "description": "Array of permissions for the
                       flow for the current user",
               "type": "array",
               "items": {
               "$ref": "rbac_permission_types.schema.json"
       }
    }
}
```

The new required property caps was added, which represents an array of permissions for the current user's flow.

The caps info is added to support UI for the Illumination Plus feature. It shows whether a user has read and/or write access to the individual flow.

traffic_flows_traffic_analysis_queries_post

traffic_flows_traffic_analysis_queries_post_response

These two synchronous traffic query APIs have been deprecated and replaced with an async version.

Rather than removing the API entirely in release 22.5.0, they return a 410 error.

Other Changed Experimental APIs

slb_device_config.schema.json

```
 },
       "credential": {
       "description": "credential",
       "type": [
               "string",
               "null"
       ]
},
```

This schema provides management configuration information for SLB devices and the credential property was changed so that it can also be NULL.

optional_features_put

```
{
"$schema": "http://json-schema.org/draft-04/schema#",
"type": "array",
"items": {
       "oneOf": [
       {
               "type": "object",
               "additionalProperties": false,
               "required": [
                       "name",
                       "enabled"
               ],
               "properties": {
                       "name": {
                       "description": "Name of the feature",
                       "type": "string",
                       "enum": [
                       "ip_forwarding_firewall_setting",
                       "ui_analytics",
                       "illumination_classic"
               ]
       },
```

The property illumination_classic was added to PUT /api/v2/orgs/:xorg_id/optional_features, which is used to manage user analytics.

To set or clear the optional feature, use

```
{
name: "illumination_classic", enabled: false|true
}
```