TECHNICAL
DOCUMENTATION

Illumio Core What's New and Release Notes 22.5

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

Table of Contents

What's New in 22.5

What's New and Changed in This Release

Before upgrading to Illumio Core 22.5, familiarize yourself with the following new and modified features in this release.

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

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: 22.5.35 (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

22.5.35-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 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.

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.

You have the option to upgrade the VENs in your environment at any time.

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.

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.

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.

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.

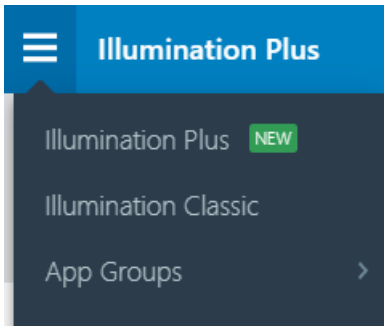
  When you use the original Explorer feature, the functionality does not support the new Illumio Core 22.5 flexible labing features, which allows you to create custom labels. The original Explorer feature only supports the standard Core RAEL labels.

- 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.

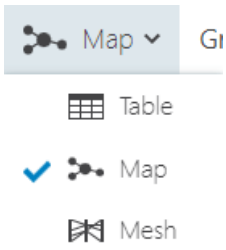
- New layout options for maps:
  - Circular Layout, which enhances the space use on the screen.
  - Organic Layout, which reduces overlaps in label sets, groups, and traffic lines. It groups things that are highly connected and avoids crossing of the links.
  - Tiered Layout, which highlights source 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:



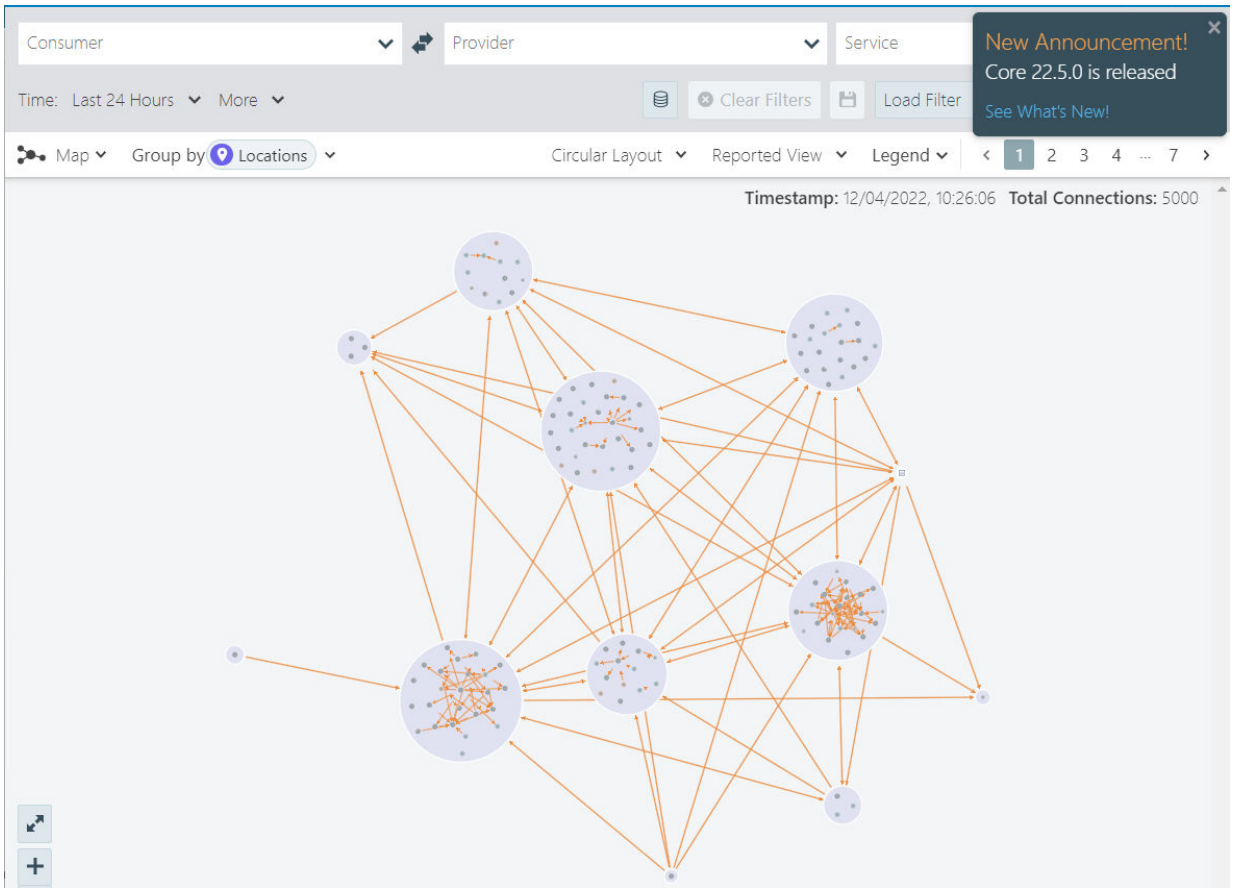
Once in the Illumination Plus screen, select the view from the dropdown menu:



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)

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



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
```

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".

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.

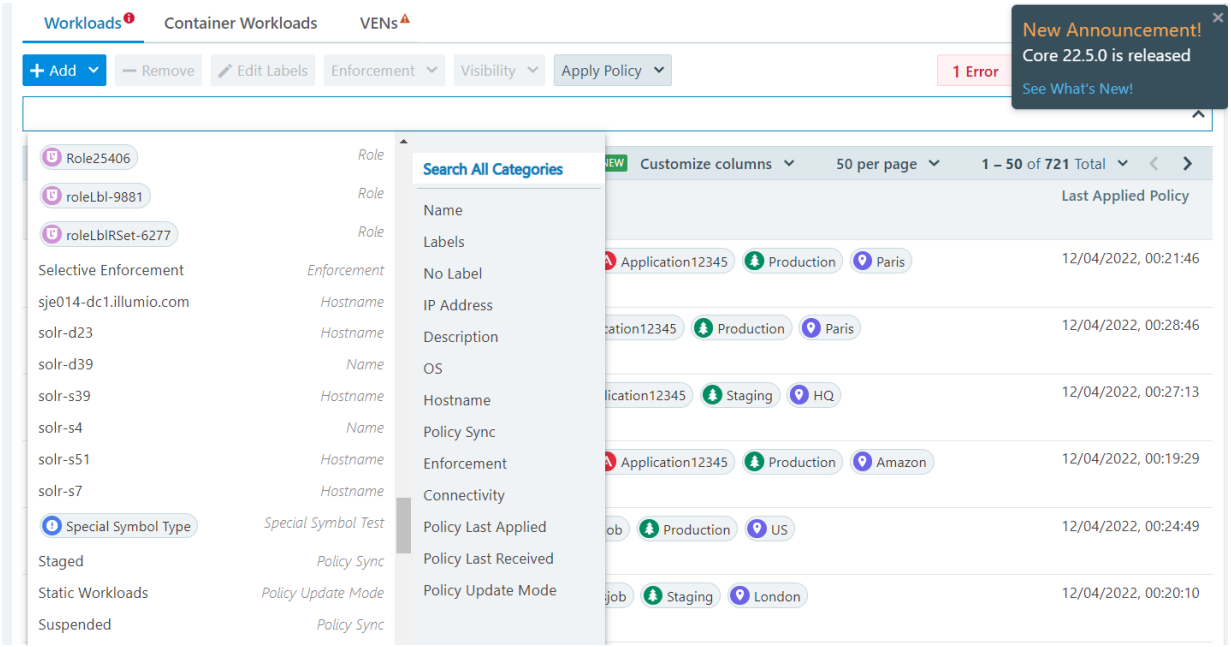
The new field `vulnerability_computation_state` was added to the `vulnerability_summary` and defines three computation states:

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

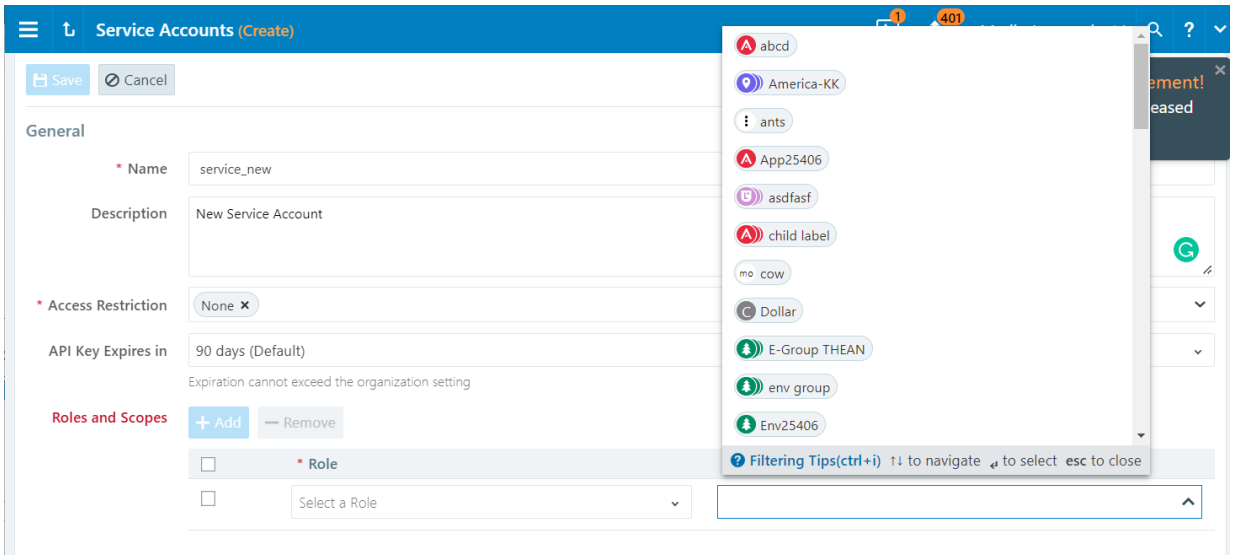
RBAC Changes

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



- 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.

Illumio Core REST API in 22.5.0

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

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 [19].

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:'2ac31cbee8cd3e8fa7ca79d32d39a0249636624ada675965dd2ec
239e3ea8af0' --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
}
```

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

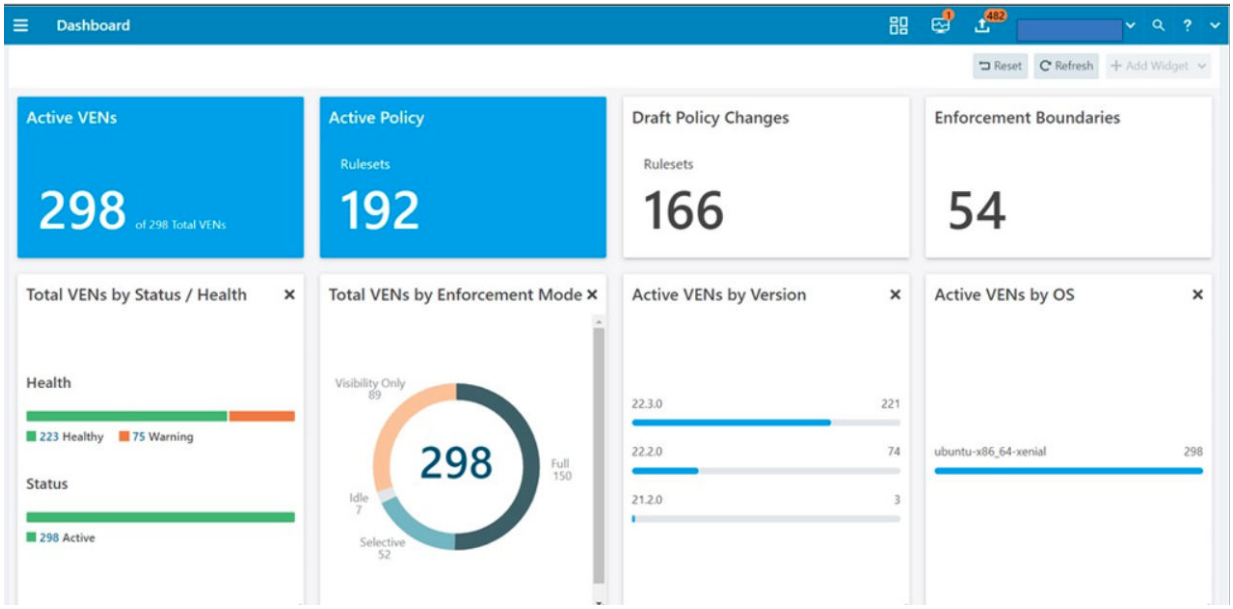
Illumio now provides a dashboard to give you broad, visualized information about VEN statistics.

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.



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.

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.

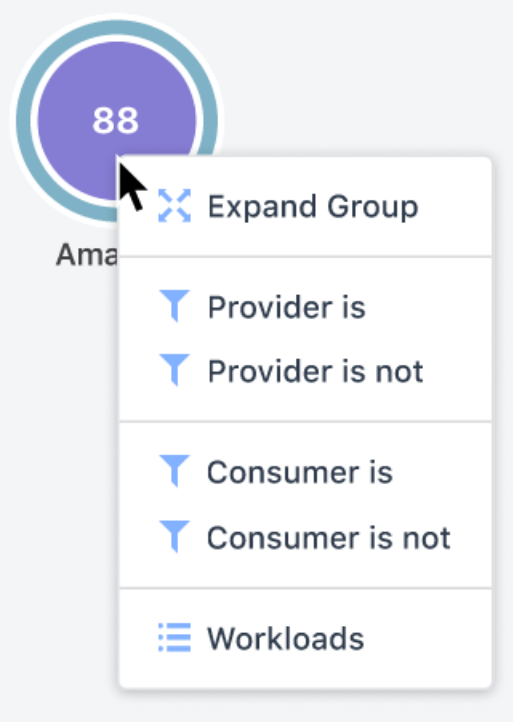
Show Amount of Data Transfer GA

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.

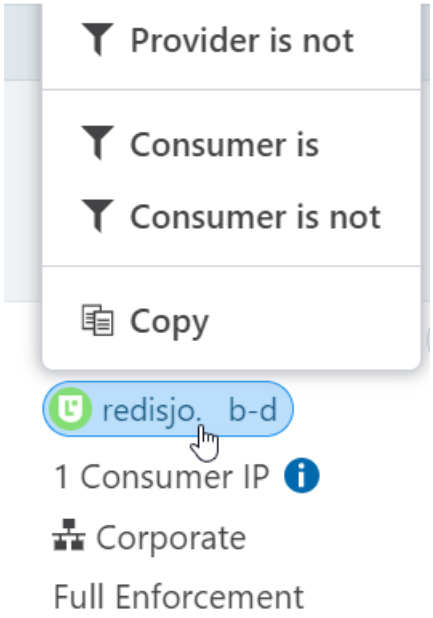
Context Menus in Illumination Plus

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.

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.

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.

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.

What's New and Changed in Release 22.5.12

Illumio Core 22.5.12 Maintenance Release

Illumio Core22.5 includes an updated version of the PCE and VEN software.

IMPORTANT

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

Illumio provides regular maintenance updates for reported bugs and security issues, and to add support for new operating system versions. As a maintenance release, Illumio Core 22.5.12 solved software and security issues for the PCE and VEN to refine the software and improve its reliability and performance.

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 22.5.20

Illumio Core 22.5.20 Maintenance Release

Illumio Core22.5.20 includes an updated version of the PCE and VEN software.

IMPORTANT

Illumio Core22.5.20-PCE is available for Illumio Core On-Premises customers only.

22.5.20-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.

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 22.5.20

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

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 22.5.30

Illumio Core 22.5.30 Maintenance Release

Illumio Core22.5.30 includes an updated version of the PCE and VEN software.

IMPORTANT

Illumio Core22.5.30-PCE is available for Illumio Core On-Premises customers only.

22.5.30-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.

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.

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.

Illumio Core REST API in 22.5.30

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

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"
        ]
```

What's New and Changed in Release 22.5.32

IMPORTANT

Illumio Core22.5.32-PCE is available for Illumio Core On-Premises customers only.

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

22.5.32-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 Core22.5.32 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 Core22.5.32 solved software and security issues for the PCE to refine the software and improve its reliability and performance.

Illumio Core 22.5.33-VEN Maintenance Release

Released April 2024

Illumio Core22.5.32 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 Core22.5.33-VEN solved software and security issues for the VEN to refine the software and improve its reliability and performance.

Illumio Core 22.5.32-VEN Maintenance Release

Released February 2024

Illumio Core22.5.32 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-VEN solved software and security issues for the VEN to refine the software and improve its reliability and performance.

What's New and Changed in Release 22.5.35

Illumio Core 22.5.35-PCE LTS Maintenance Release

Illumio Core 22.5.35 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 22.5.35-PCE solved software and security issues for the PCE to refine the software and improve its reliability and performance. For details, see Resolved Security Issue in 22.5.35-PCE [46].

Illumio Core Release Notes 22.5

Welcome

These release notes describe the resolved issues and known issues for Illumio Core 22.5.*x* releases.

Illumio Core 22.5 is available for Illumio Core Cloud customers depending on the version of the Illumio Core Cloud running in their environments. Illumio Core Cloud customers can verify their version in the PCE web console.

Document Last Revised: March 2025

Document ID: 14000-100-22.5.35

MSI to EXE package format

Starting with the Illumio Core 21.2.1 release, the Windows VEN installer switched from the MSI to the EXE package format. Customers upgrading their VENs by using the PCE-based VEN deployment (the VEN Library) must take an extra step for the transition.

Illumio Core customers running older MSI-based Windows VENs must upgrade to 19.3.6+H1-VEN or 21.2.0+H2-VEN before upgrading their VENs to 21.2.1 or a later version. The 21.2.0+H2-VEN release contains the necessary VEN changes to handle the transition in the VEN packaging from MSI to EXE format.

Product Version

PCE Version: 22.5.35 (LTS)

VEN Version: 22.5.34 (LTS)

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

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

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

Resolved Security Issue in 22.5.35-PCE

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

Resolved Security Issue in 22.5.34-PCE

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

Illumio Core 22.5.34-VEN

Resolved Issue in 22.5.34-VEN

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

Known Issue in 22.5.34-VEN

- **Bug in nftables versions pre-0.9.2 may prevent policy application** (E-116635)
  Policy may fail to load on VENs installed on RHEL Linux 8 workloads with a version of nftables earlier than 0.9.2. Workaround: upgrade to nftables 0.9.2+.

Illumio Core 22.5.33-VEN

Resolved Issues in 22.5.33-VEN

- **VEN Installation Fails on Amazon Linux 2023** (E-113934)This issue was caused by a change Amazon made to the format of the release name in the system release file. This issue is fixed.
- **Windows VEN over-restricted cipher suites selection for Event Channel** (E-113245)
  When the PCE was set to disable weak ciphers, a service on the VEN restricted the selection of some TLS cipher suites on the Event Channel. This prevented the PCE from updating policy on Windows VENs using Lightning Bolts (event service), meaning policy could be updated only during scheduled heartbeats (5 minutes). This issue is resolved: Lightning Bolt communication now works as designed.
- **Support for pairing VENs on AWS Workloads with IMDS v2** (E-109528)
  VEN release 22.5.33 provides support for pairing VENs on AWS workloads with Instance Metadata Service Version 2 (IMDS v2). This update was necessary to support IMDS v2 session-oriented authentication.

Known Issues in 22.5.33-VEN

There are no known issues in this release.

Resolved Security Issue in 22.5.33-VEN

OpenSSL is upgraded from **3.0.12** to **3.0.13** to address CVE-2024-0727, CVE-2023-5678, and CVE-2023-3446. The VEN is not impacted by this vulnerability.

Illumio Core 22.5.32-VEN

Resolved Issues in 22.5.32-VEN

- **Generating an individual maintenance token failed** (E-111662)
  When the Agent Tampering Detection feature was enabled and a user generated a token for a specific VEN (not tokens for all VENs), in some cases it wasn't possible to perform a protected `illumio-ven-ctl` action such as `stop` (example shown below):
  `PS C:\Program Files> .\Illumio\illumio-ven-ctl.ps1 stop --maintenance-token <token for a specific VEN> Failed to verify maintenance token`
- **C-VENs failed to synchronize policy** (E-108536, E-111490)
  C-VENs running 21.5.33 showed "Error" for the Policy Sync state with the message "Failed to load policy line." Concurrent threads (`MsgHandler` and `downloadPolicyFromPCE`) caused a race condition because of shared variables. This issue is resolved.
- **VEN failed to process FQDN rules and caused blocked traffic** (E-111486, E-108639)
  After upgrading VENs from version 19.3.5 to version 22.5 and greater, some VENs failed to process FQDN rules, causing traffic to be blocked. Due to a transient error, the VEN may fail to detect the DNS server(s) on the workload and fail to program FQDN rules correctly. This issue is resolved. Now VENs will continue trying to detect a DNS server after the initial detection fails.

Known Issues in 22.5.32-VEN

- **SecureConnect only logs the "E" on the provider** (E-101229)
  Works as designed. There is no way to tell whether SecureConnect is in the egress path.
- **Windows 11 shows as Windows 10 on the workload/VEN page** (E-100844)
  Workaround: Verify the Windows version through the workload operating system.

Resolved Security Issues in 22.5.32-VEN

- OpenSSL is upgraded from **3.0.8** to **3.0.12** to address CVE-2023-3446. The VEN is not impacted by this vulnerability.
- cURL is upgraded from **7.88.1** to **8.4.0** to address CVE-2023-38545 and CVE-2023-38546. The VEN is not impacted by these vulnerabilities.
- SQLite is upgraded from **3.41.0** to **3.45.0** to address CVE-2023-7104. The VEN is not impacted by this vulnerability.

Illumio Core 22.5.30

Documentation Updates for Illumio Core 22.5.30

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

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

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

1. On the new PCE, edit its `runtime_env.yml` file so that its value for `service_discovery_encryption_key` is identical to the value set in the `runtime_env.yml` files of all other Supercluster nodes.
2. Reset all nodes:
   ```
   $ sudo -u ilo-pce illumio-pce-ctl reset
   ```
3. Start services at runlevel 1 on all nodes:
   ```
   $ sudo -u ilo-pce illumio-pce-ctl start --runlevel 1
   ```

   NOTE

   If a node gets stuck in the PARTIAL state, reboot the node.
4. On any node, set up the database:
   ```
   $ sudo -u ilo-pce illumio-pce-db-management setup
   ```
5. On any node, set runlevel 5:
   ```
   $ sudo -u ilo-pce illumio-pce-ctl set-runlevel 5
   ```

Resolved Issues in Illumio Core 22.5.30

Illumination Plus

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

  Illumination Plus and reports pages were displaying blank when users created a custom time-saved filter in different timezone formats.

  This issue is resolved.
- **Illumination Plus - Filtered Objects lists are not displayed properly** (E-102466)

  When users add a filter after the PCE has generated two columns of objects, the first column (workloads) stays empty and the second one (container workloads) contains the filtered object. This issue is resolved.
- **Change the network name "External" to "External (Non-Corporate)"** (E-102368)

  The name External was changed to External (Non-Corporate) in Explorer, in Illumination Plus Traffic Tables, and on the Networks page.

- **Default view to go straight to the table view from the classic UI** (E-102364)
  Configure the default view on Illumination Plus to go straight to the table view from the classic UI. This issue is resolved.
- **Delete icon not visible when a filter has a long name** (E-102359)
  The Delete icon was not properly visible in Illumination Plus and Explorer if a filter with a lengthy name was saved. This issue is resolved.
- **Illumination Plus Deep Rule Analysis showed Allowed Traffic as Blocked** (E-101506)
  A rule created to allow traffic was shown as Blocked when viewed in **Deep rule analysis**. The same rule was correctly shown as Allowed in Quick Draft Rules and in Explorer. This issue is resolved.
- **Provider/Consumer order mismatched between filters and column headers** (E-101156)
  Configuring the provider/consumer order in the Policy Settings did not control the filters and the column headers in the table view of Illumination Plus. Instead, the filters and column headers were displayed in the opposite order. This issue is resolved.
- **Illumination Plus - Reports page displaying with a blank page when upgrading from v22.4.x to v22.5.0** (E-99327)
  When users who had two-label app group filters upgraded from 22.4.x to 22.5.0, a Java-Script error caused reports to display as a blank page. This issue is resolved.

Endpoint

- **VEN services restarted unnecessarily** (E-106136)
  On some Windows workloads, VEN services were restarted unnecessarily after waking up from sleep. This issue is resolved.
- **Double colons in FQDNs with quad A records caused a policy sync error** (E-104996)
  A policy sync error affecting multiple VENs occurred in the following circumstances:

  1. The PCE policy included rules specifying FQDNs, and . . .
  2. The customer environment had FQDNs that contained AAAA (IPv6) records ending in double colons (::). For example, `2603:1037:1:60::`

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

Enterprise Server

- **VEN doesn't capture local DNS properly** (E-106370)
  On systems that use local DNS resolution (such as `systemd-resolved`), DNS capture packets did not properly match DNS responses for processing in userspace. This issue is resolved.
- **On-Prem 21.5.34 Workload Filter Inconsistency** (E-106223)
  Using multiple filters for the workload page that includes IP addresses might have produced an inaccurate result set. This issue is resolved.
- **Workloads filter returned an incomplete list** (E-105920)
  Specifying a particular subnet when filtering for workloads returned an incomplete list if any of the workloads had more than one interface in that subnet. This issue is resolved.
- **After upgrade, the VEN could lose connectivity to the PCE** (E-105022)
  After upgrading the VEN to 22.5.10, it could lose connectivity with the PCE. This issue only occurred with PCEs that were part of a Supercluster deployment. This issue is resolved. After upgrading the VEN to 22.5.22, the VEN can connect with PCEs in a Supercluster.
- **Kubelink could restart when container cluster services were deleted** (E-104786)
  Kubelink could restart due to an unexpected PCE error when reporting to the PCE that container cluster services were deleted. This issue occurred when PCE port separation was enabled. This issue is resolved.

- **Traffic worker not coming up after stop/start** (E-104519)
  After operations involving changes in the runlevel and/or service restart, in rare circumstances, the app gateway service generated duplicate proxy ports. This resulted in the failure of services, such as traffic worker, to connect to redis related services, with a "wrong password" exception. This issue is resolved.
- **Data in exported CSV files didn't match policy decision data in Explorer** (E-104439)
  When exporting policy data from Explorer, the content in the CSV file didn't match the policy data in the Explorer page. This issue occurred because the PCE exported the aggregate traffic flows and not the individual connections, which the Explorer page displays. This issue is resolved. In this release, exporting policy data from Explorer correctly exports the individual connections. The CSV file now matches the data displayed in the PCE web console Explorer page.
- **Scopes not appearing on User Activity details and Local user details screen** (E-104175)
  In automated environments, labels can be created or can exist with invalid label types. Labels in grids will not appear if their label types are invalid, but they will appear in other places such as edit/detail pages. Currently, no workaround is available.
- **Warn when changing labels of enforced workloads** (E-102907)
  Net admins needed to be informed when they change labels used by workloads so that they are aware these changes will impact policies. This issue is resolved and admins receive appropriate warnings

PCE Platform

- **PCE upgrade fails from PCE 22.2.x and earlier to 22.5.0 and later with endpoint VENs** (E-105999)
  The PCE upgrade failed in the `illumio-pce-db-management migrate` step when upgrading from PCE version 22.2.x and earlier to 22.5.20 and later when endpoint VENs were present before the PCE upgrade. This issue is resolved.

Policy Platform

- **Deadlocks in Container Workload Purging** (E-106907)
  There is a background job in the PCE to remove decommissioned container workloads from the database. This background job could fail in highly dynamic container environments due to PostgreSQL deadlocks. This job has been made resilient to this and other failures.
- **Potential PCE performance impact in highly dynamic container environments** (E-106906)
  When C-VENs acknowledged to the PCE that policy had been applied, the PCE in turn updated all records associated with the C-VENs, including records for previously-deleted container workloads still in the PCE database. While this caused no functional issues, it could possibly result in a large number of writes with the potential to degrade performance in highly dynamic container environments where containers were being created and deleted very quickly.
  This issue is resolved.
- **Workloads page did not update on external IP changes** (E-106847, E-106806)
  When VENs are deployed on VMs in certain well-known public clouds (such as AWS), the PCE attempts to detect the public NAT address (e.g. elastic IP) of those workloads and use them in policy. The logic that updates the NAT address upon a VEN heartbeat was not working properly. When the NAT address of a public cloud VM changed, the PCE did not program the new address in the policy unless there was an interface change on that VM. This issue is now resolved.
- **Events page showing repeated `clone.detected` messages** (E-106579)
  After upgrading from the release 21.5 to 22.5, the Events page was flooded with `clone.detected` messages up to 5 times per second. This issue is resolved.

- **Supercluster PCE upgrade failure from PCE version 22.2.x with endpoint VENs** (E-106479)

  The supercluster PCE upgrade failed in the `illumio-pce-db-management migrate step when upgrading from PCE version 22.2.x to 22.5.x when endpoint VENs were present before the PCE upgrade. This issue is resolved.
- **Keys were missing from** `agent_missed_heartbeats_check` **event detail page** (E-97912)

  When viewing a `system_task.agent_missed_heartbeats_check` event in the UI, the "resource changes" and "notifications" fields were missing from the UI. The data existed in the API JSON but these values didn't appear in the UI. This issue is resolved.

UI Components

- **Backport: Application labels absent in the workload's Blocked Traffic tab** (E-105383)

  UI did not display application labels for Consumer/Provider in the workload's Blocked Traffic tab. This issue is resolved.
- **Unable to add CIDR range to unmanaged workload interfaces** (E-104729)

  In certain conditions, a CIDR could not be applied to an unmanaged workload interface. Note that the CIDR is used for informational purposes only to encode information about a subnet mask, and does not add the entire IP range to the unmanaged workload. This issue is resolved.
- **Virtual server rules weren't displayed in the Rules tab** (E-103687)

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

  This issue is resolved. In this release, the virtual server rules appear in the **Rules** tab when navigating from the **Summary** tab.
- **A rule copy appears to modify the original rule** (E-103604)

  Deleting a virtual service on a rule copy makes it look as if the change will also apply to the original rule.

  If the rule copy is saved with the change, the original rule remains unchanged. This issue is mostly cosmetic and is closed as such.

VEN

- **On Windows, VEN fails to add an AUS rule for a logged-in user** (E-106773)

  This resulted in the user not being able to connect to the provider protected by the AUS rule. The issue is resolved.
- **VEN pairing fails with certain macOS updates** (E-106229)

  A recent security update from Apple caused the macOS VEN pairing to fail. An error appears, "Could not set environment: 150: Operation not permitted while System Integrity Protection is engaged." This has been resolved.
- **Incomplete static policy caused VENs to go offline** (E-105833/E-105138)

  In some circumstances, VENs went offline after the PCE sent an incomplete static policy to VENs. This issue is resolved.
- **Unexpected Port Scan Results** (E-104213)

  During a port scanning test, a Windows server protected by Illumio VENs in Enforcement mode was able to respond to ports that had no listeners. This issue stemmed from unexpected behavior from the Windows Firewall Stealth filter. This issue is resolved.
- **Allowed traffic reported as dropped** (E-103701)

  After an upgrade, VENs temporarily reported allowed flows as dropped. The issue is resolved.
- **ilo_ipsets load: ipset v6.36: Error in line 6975: The set with the given name does not exist** (E-103250)

On Linux and AIX operating systems, VEN still inserted IPv6 elements into IPv6 FQDN ipsets, which were not created when IPv6 was disabled. This issue is resolved. In this release, if IPv6 is disabled, the VEN will not create the IPv6 FQDN ipset, nor will the VEN insert elements into the FQDN ipset.

- **Disabled boundary rules causing potentially blocked by boundary flows in Explorer** (E-98104)

  Explorer displays traffic that is potentially blocked by a boundary even if there are no active boundary rules.

  Workaround: Not available.
- **VEN on Solaris 10 fills up space with the large** `ippool-extra debug` file (E-92538)

  An OS bug exists whereby the IP Filter `ippool` OS utility may generate repetitive/unlimited output under the `/opt/illumio_ven_data` directory. This fix mitigates the OS bug by terminating `ippool` as needed.

Illumio Core 22.5.23-PCE

- **PCE upgrade from the 22.2.x and earlier releases to 22.5.20 and later releases could fail** (E-105999)

  When the PCE had paired endpoint VENs, upgrading the PCE from Core 22.2.x and earlier releases to 22.5.20 and later releases could fail during the `illumio-pce-db-management migrate` step. This issue is resolved.

Illumio Core 22.5.22

This release is available for both the Core PCE and VEN.

What's New in This Release

Starting in Illumio Core 22.5.22, the VEN supports Amazon Linux 2 on the ARM64 architecture.

Resolved Issues in 22.5.22-PCE

- **High memory consumption on Supercluster data nodes could occur** (E-105671, E-104608)

  Due to a memory leak in the database replication process, the memory consumption on data nodes of a Supercluster could gradually increase. This issue is resolved. In this release, a memory leak no longer causes memory consumption by the PCE to continuously increase.
- **Traffic worker not coming up after stop/start** (E-105637, E-104519)

  After operations involving changes in the runlevel and/or service restart, in rare circumstances, the app gateway service generated duplicate proxy ports. This resulted in the failure of services, such as traffic worker, to connect to Redis-related services, with a "wrong password" exception. This issue is resolved.
- **Illumination Plus could show allowed traffic as blocked** (E-105554, E-101506)

  When selecting “Deep rule analysis” from the **View** menu, Illumination Plus could show traffic was blocked for flows that had `allow` rules. However, when you selected “Quick Draft Rules” from the **View** menu in Illumination Plus, or used the classic version of Explor-

er, you saw that the traffic was allowed. This issue is resolved. Using Deep Rule Analysis to view traffic that has `allow` rules now correctly shows that the traffic is allowed.

- **Data in exported CSV files didn't match policy decision data in Explorer** (E-104439)
  When exporting policy data from Explorer, the content in the CSV file didn't match the policy data on the Explorer page. This issue occurred because the PCE exported the aggregate traffic flows and not the individual connections, which the Explorer page displays. This issue is resolved. In this release, exporting policy data from Explorer correctly exports the individual connections. The CSV file now matches the data displayed in the PCE web console Explorer page.

Resolved Issue in 22.5.22-VEN

- **After an upgrade, VEN could lose connectivity to the PCE** (E-105022)
  After upgrading the VEN to 22.5.10, the VEN could lose connectivity with the PCE. This issue only occurred with PCEs that were part of a Supercluster deployment. This issue is resolved. After upgrading the VEN to 22.5.22, the VEN can connect with PCEs in a Supercluster.

Resolved Issues in 22.5.20

Core Services

- **In Traffic Pattern Mode detection, clicking the button won't show traffic** (E-102906)
  There should be no information icon for detected Scanner Core service in Recommended and Accepted Grid.
  This issue is resolved.

PCE Platform

- **Potential PCE DOS caused by malicious IF-None-Match header** (E-102567)
  This issue is resolved.
- **Data node stuck in PARTIAL state during regression test** (E-89797)
  This PCE Platform issue applies to Illumio Core On-Premises customers only. It does not apply to Illumio Core Cloud customers.
  In rare cases, if application metrics are enabled the data node could be seen in the PARTIAL state both from the `illumio-pce-ctl` cluster-status and `illumio-pce-ctl` status. In those cases, if `metrics_database_service/influxdb` is not running, move the influxdb bolt file located in `PERSISTENT_DIR/influxdb/meta/influxd.bolt` to any directory outside this InfluxDB directory.
  This issue is closed and does not require a fix.

Platform

- **Validation error when changing IPv6 settings on SC PCE** (E-102469)
  When using a supercluster, 406 input_validation_errors occurred when changing IPv6 settings on the UI. This issue is resolved.

- **PCE should stop requesting client cert** (E-93147)
  The PCE tried to request a client certificate every time and allowed it even if the client did not send a certificate. It was an extra handshake that could have caused delays. This issue is resolved.

UI Components

- **Unable to use 0.0.0.0/0 in iplist** (E-102198)
  When users entered 0.0.0.0/0 to create an IP list, the values were rejected. This issue is resolved.
- **'No X Label' filters are not working when selected from 'Search All Categories'** (E-102000)
  When users chose a filter like 'No Application' or 'No Location' on the Workloads and VENs page, the page did not refresh with the filtered results. This issue is resolved.

UI Platform

- **Couldn't duplicate rules in a ruleset** (E-101114)
  In Illumio Core 22.5.x, you couldn't duplicate extra-scope rules or custom iptables rules because the **Edit** menu for those types of rules didn't include the **Duplicate** option. Duplicating an intra-scope rule was still available. Instead, the **Edit** menu included the **Reverse** option, which wasn't applicable. This issue is resolved. In Illumio Core 22.5.20-PCE, you can now duplicate extra-scope and custom iptables rules when editing a ruleset.
- **Large IP list or FQDNs made IP List page non-responsive** (E-101167)
  In the **Policy Objects > IP Lists** page, editing either a large number or a large range of IP addresses or FQDNs in the **IP List** field caused the page to become non-responsive. This occurred because the PCE Web Console's attempt to validate the data impacted performance. This issue is resolved. The PCE now automatically disables address/FQDN validation when the list exceeds 300.
- **Unable to distinguish between unmanaged workload and managed in Illumination Plus** (E-101069)
  Illumination Plus icons for managed and unmanaged workloads were misleading.
  As a result, it was impossible to distinguish between the unmanaged "Router" and the managed "WIN10-225" workload. This issue is resolved.
- **Autocomplete not filtering labels based on user scope** The VEN page displayed all labels instead of solely the ones applicable to scoped users. This issue is resolved.
- **Browser unresponsive while editing a huge IP list** (E-96832)
  Browsers were unresponsive when users edited large IP lists for policy objects. IP list validation is now disabled above a certain threshold, mitigating the load on browsers. This issue is resolved.

Data Experience

- **Context menu moved out of view when close to Map edge** (E-101545)
  When right-clicking on a node near the edge of the screen in Map view, the context menu went out of view. This issue is resolved. The entire context menu is now visible in this situation.
- **Incorrect mapping to Container Network** (E-99193)
  In Illumination Plus and Explorer table, we used to display the network name in consumer and provider columns, which made users associate the network name to both the consum-

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

- **Illumination Plus - Add dragging icons for the Mesh axis** (E-98339)

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

RBAC

- **Reports show in the main menu for the user with the global administrator role** (E-102127)

  Global Administrator Role users were able to see a Reports option in the hamburger menu, causing an error when selected. This issue is resolved.
- **Problem with VEN local install where the command is in one line** (E-101820)

  This issue is resolved. VEN services now start automatically when VEN auto-activation is required.
- **Policy Sync Error** (E-101510)

  VEN fails to apply policy if a file named "0" is present in the root directory.

  The VEN uses heuristics to detect whether IPtables on the machine support the `--wait` option. This heuristics breaks down if a file named "0" is present in the root directory and the VEN incorrectly assumes that the `--wait` option is supported.

  This issue is resolved.
- **Solaris policy generation looks broken** (E-102189)

  The VEN does not support fully qualified domain name (FQDN) rules for packet filter firewalls. When customers defined an FQDN rule for Solaris 11.4+ workloads, the VEN generated an FQDN rule, which was erroneously applied to a packet filter firewall. This issue is resolved.
- **Unauthorized VENs are causing frequent events related to interface_statuses/update** (E-101795)

  When a VEN is unpaired from the PCE, it is possible for the VEN to not receive the unpair message. This can happen, for example, if the host is down for an extended time. When the host comes back up, VEN requests to the PCE is rejected, and the PCE emits `request.authentication_failed events`. This issue has been resolved. The VEN no longer makes frequent requests to the PCE after receiving consistent authentication errors.
- **Support CloudLinux for VEN** (E-101473)

  This release of the VEN adds support for a new distribution of Linux. CloudLinux versions 6, 7, 8, and 9 are now supported.

Policy Platform

- **Constant policy churn due to "All Workloads" with "Use Workload Subnets"** (E-102250)

  When either the provider or consumer of a rule is set to "all workloads" and the "use workload subnets" option was enabled for that side of the rule, the PCE did get into a state where VENs are almost always in "Active (Syncing)".

  This issue is resolved.
- **Rule coverage for endpoints is timing-dependent** (E-96488)

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

Production

- **Pairing Profile VEN version drop-down list is not in any discernable order** (E-102162)
  The version list did not display in a discernible order. The UI was corrected, and the version list was put in numerical order. This issue is resolved.

Common Criteria

- **Change default and minimum password length to 16 characters** (E-101249)
  When the common criteria (CC) feature is enabled, set the password policy for local user accounts as follows: the minimum length is now 16 characters and the maximum is 64 characters.

Resolved Issue in 22.5.12-PCE

IMPORTANT
Illumio Core 22.5.12-PCE is available for Illumio Cloud customers only.

- **PCE performed validation checks for certain reserved IP subnets** (E-102540)
  In previous releases, the PCE had built-in validation checks for some reserved IP address subnets (such as 0.0.0.0/8) and rejected updates from those interfaces with these special IP addresses. This behavior could disrupt some customer applications during disaster recovery events. This issue is resolved. In this release, the PCE no longer performs validation checks for IP addresses in the ranges 240.0.0.0/4 and 0.0.0.0/8, which means that the PCE now accepts practically all IP address ranges.

Resolved Issue in 22.5.12-VEN

- **VEN changed system default actions in Firewall Coexistence primary mode** (E-102504, E-101773)
  When pairing a VEN with a workload in Firewall Coexistence Primary mode, the VEN inadvertently changed the firewall system default to ALLOW. As a result, the VEN overwrote the existing workload firewall. This issue only occurred when the PCE was configured to use Primary mode for Firewall Coexistence. This issue is resolved. The VEN no longer changes the firewall system default to ALLOW under these circumstances.

Illumio Core 22.5.10+UI2

Feature Announcement

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

By the end of 2023, Illumio plans to deprecate the Explorer feature and encourages customers to use the equivalent functionality 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.

Resolved Issue in 22.5.10+UI2

- **Saved workloads filter returns no results following the upgrade** (E-99346)
  After upgrading from Core version 22.4.0 to 22.5.0, loading an existing saved filter in Illumination Plus to filter by workloads returned no results.
  This issue is resolved.

Resolved Issues in 22.5.10

Data Experience

- **Illumination Plus displayed incorrect information for database usage** (E-101252)
  In the PCE web console, the bar graph in Illumination Plus for the traffic database status displayed the wrong percentage. This issue is resolved. The bar graph now displays the correct percentage for database usage.
- **Unable to edit and save a filter with a previous name** (E-100853)
  In the PCE web console, users couldn't save a filter when it had the same name as an existing filter. This issue is resolved. In this release, the PCE web console warns the user that it will overwrite the existing filter when the user tries to save a filter that has the same name as an existing one.
- **Save Filter button in Illumination Plus was disabled after running a query** (E-100824)
  In the PCE web console, the **Save Filter** button in Illumination Plus was still disabled after you ran a query. This issue is resolved. In this release, the **Save Filter** button is clickable after you run a query. Users can now test the results of their queries before saving them.
- **Any user/service account can view/download any PCE report via API** (E-100645)
  Reports created by org owners were visible to scoped users. This issue is resolved.
- **Emailed reports from PCE include the wrong default port** (E-100523)
  Emailed Reports had the wrong port in the URL for on-prem PCE 8443 and when users change `https_port` in the runtime variables, they notice it doesn't reflect well on the reports link in emails.

As a solution, a different port is pointed for the reporting link, and respective changes were made to properly direct users to the correct reporting URL even when runtime environment ports are modified.

- **Emailed reports from PCE included invalid text in the subject** (E-100514)

  Reporting Email subject header contained the invalid text "translation missing."

  As a solution, the previously missing proper text translation was added for the subject headers into the reporting web service. Users do not see the invalid text anymore.
- **GET location_summary returned a 503 error** (E-99632)

  The wrong password was remembered for the Redis cache, preventing it from being initialized. This issue is resolved.
- **Attempting to save a proposed rule that includes ICMP service failed** (E-98898)

  If a user with the Ruleset Manager role selected Blocked traffic in Illumination Plus and tried to save a proposed rule that included a new service (for example, ICMP), the action failed with a 403 error. This occurred because Ruleset Managers don't have permission to create new services, even though the "new" service appears in the Providing Services column. These users can only save such a rule if the ICMP service was already created by a Global Organization Owner. This issue is resolved.
- **Illumination Plus:`set_flow_reporting_frequency` API throwing 403 error with increased VEN update rate** (E-98886)

  This issue only happened when there were over 50 workloads. The Increase VEN update rate button will not appear if there are more items than that in a group. This issue is resolved.
- **The Create Unmanaged Workloads button was available to global viewers** (E-98532)

  The **Create Unmanaged Workloads** button was available from the **Summary** tab to users with the Global Viewer role even though that role lacks permissions to create workloads. An error occurred after these users clicked the **Confirm** button in the **Assign Labels** dialog box. This issue is resolved. The **Create Unmanaged Workloads** button is no longer available to Global Viewers.
- **Illumination Plus stops working after disabling the old Illumination map** (E-98496)

  Illumination Plus stopped working when Illumination was disabled from PCE runtime. This issue is resolved.
- **Illumination Plus - Run button progress completed but query remains in working state** (E-97966)

  The RUN progress will stop as soon as the first page is available, but the query will still be working on the other pages. This behavior is expected and works as designed
- **Explorer returns results with incorrect labels** (E-96438)

  If there are multiple virtual services from different container networks with the same ip+port+proto in the PCE when the user queries with the labels of one virtual service, the flows from other container networks under other virtual services can come into the results and be shown as different labels. Users should ignore the flows with labels different than the query labels in this case.

UI Platform

- **22.5 Pending Rules do not show what was changed** (E-101337)

  The changes in rules were not correctly displayed for a draft Ruleset. This issue is resolved. Now the UI properly highlights the changed elements of the rule.

Policy and Workloads

- `workload_interfaces.update` **wasn't capturing network changes** (E-96188)
  This issue is resolved. When a workload interface is added or removed, the network name (usually Corporate or External networks; External networks apply only to endpoints) is included in the event.

Platform

- **Validation error when changing IPv6 settings on SC PCE** (E-102469)
  When using a supercluster, 406 input_validation_errors occurred when changing IPv6 settings on the UI. This issue is resolved.
- **Scoped Ruleset Manager role didn't provide correct access for users** (E-101513)
  Users who were members of the Scoped Ruleset Manager role couldn't access labels provided by the autocomplete feature on the Rulesets page. The PCE was filtering out labels from dimensions that weren't part of those users' scopes. This issue is resolved. Users can now view labels that belong to dimensions that are not part of their user scopes.
- **Failed to deploy the VEN bundle on PCE** (E-99725)
  The 22.2.40 VEN bundle cannot be installed in the VEN library on a PCE earlier than 22.2.40 due to a limitation in the allowed VEN bundle size. The VEN can still be installed from the host or VM's command line (e.g. via RPM). The 22.2.40 PCE allows the installation of the 22.2.40 VEN bundle.
- **Consul messages not sent to internal syslog** (E-99715, E-90286)

  IMPORTANT
  This PCE Platform issue applies to Illumio Core On-Premises customers only. It does not apply to Illumio Core Cloud customers.

  This issue is resolved. Messages from the PCE consul service are no longer sent to the internal syslog. Messages do not appear in consul.log. Instead, they appear in `/var/log/messages` and `/var/log/illumio-pce/consul`.
- **Limit simultaneous Login** (E-99304)
  A newly created local user doesn't log in again after being logged out for 15 minutes and receiving a Logout error. This issue is resolved.
- **Illumination Plus was showing deleted workloads** (E-97955)
  Since deleted workloads do not provide useful information to a customer, these workloads do not show in the graph anymore. This issue is resolved.
- **Supercluster Restore issues in corner cases** (E-97847)
  In a case when a PCE has already joined a supercluster, it detects when it joins another supercluster and raises an exception. Users need to reset and shut down all PCEs in the previous supercluster, and then retry the command. This issue is resolved.

VEN

- **[Centos 7] Connectivity blocked after VEN upgrade from 21.5.0 to 22.5.10** (E-100683)
  Upgrading the VEN to 22.5 could result in an incorrect policy rendering the workload unreachable. This issue is resolved.
- **Windows DC's PRF: Policy process high CPU on Platform Handler** (E-100410)
  FQDN in the policy could result in high CPU usage by the VEN Platform Handler service. This issue is resolved.

- **Tampering events after upgrading VEN** (E-100296)

  When upgrading from a previous version of the VEN on RHEL8 or its variants (CentOS/Oracle, Rocky, etc.), a tampering event might occur and be sent to the PCE. This is a false positive firewall tampering event and can safely be ignored. This issue is resolved.
- **Unauthorized VENs are causing frequent events related to interface_statuses/update** (E-98612)

  When a VEN is unpaired from the PCE, it is possible for the VEN to not receive the unpair message. This can happen, for example, if the host is down for an extended time. When the host comes back up, VEN requests to the PCE are rejected, and the PCE emits `request.authentication_failed` events. This issue is resolved. The VEN no longer makes frequent requests to the PCE after receiving consistent authentication errors.
- **(Windows) Policy sync error** (E-97013)

  Older endpoint VENs might not report PPP VPN adapters correctly, including Microsoft Always-On VPN. This issue is resolved.
- **venPlatformHandler error** (E-96180)

  Sometimes, the Windows OS API (`WTSQuerySessionInformationW`) returns the session information with an invalid logon time. The invalid logon time made some runtime library functions fail. This issue is resolved. The invalid time is no longer passed into these runtime library functions.
- **Unauthorized VENs are causing frequent** `request.authentication_failed` **events** (E-90627)

  When a VEN is unpaired from the PCE, it is possible for the VEN to not receive the unpair message. This can happen, for example, if the host is down for an extended time. When the host comes back up, VEN requests to the PCE are rejected, and the PCE emits `request.authentication_failed` events. This issue is resolved. The VEN no longer makes frequent requests to the PCE after receiving consistent authentication errors.

Resolved Issues in 22.5.2

- **Running saved Illumination Plus table view queries failed after upgrade** (E-100693)

  After upgrading from a previous version of 22.5.x (for example, 22.5.1) to 22.5.2, users couldn't run their saved queries in the Table view of Illumination Plus. (For Illumio Core Cloud customers, Illumio operations perform platform upgrades.) This issue is resolved. Upgrading the Illumio Core 22.5.2 no longer impacts running saved Illumination Plus queries.
- **Cannot view vulnerability details for workloads when the Vulnerability Map feature is enabled** (E-100637)

  After adding a Vulnerability Map license to the PCE and uploading vulnerability data for the feature, you cannot view vulnerability details for workloads in the PCE web console. All detected vulnerabilities for workload ports and protocols are empty. To view vulnerability details for a workload, from PCE web console main menu, go to **Workloads and VENs** > **Workloads** > *workload* > **Vulnerabilities** tab. This issue is resolved.

Resolved Issue in 22.5.1-VEN

In this release, the following security issue was resolved for the VEN.

- **Improper certificate validation on macOS VEN** (E-100532)

  Certificate validation was improperly performed on the macOS VEN, impacting traffic between the VEN and the PCE. This issue is resolved.

Resolved Issue in 22.5.1-PCE

- **Upgrade to 22.5.0 could be slow** (E-100088)

  Upgrading from a prior release to 22.5.0 could take a long time (sometimes more than an hour). The cause was PCE database caching. This issue is resolved. To upgrade the PCE, go directly to 22.5.1 instead of 22.5.0.

Resolved Issues in 22.5.0

PCE Web Console

- **Filtered searches for workloads on the Virtual Servers page return incorrect results** (E-82414, E-75711)

  When searching for workloads on the Virtual Servers page by label, the full list of workloads continued to display regardless of search criteria and the reported page count was erroneous for searches that don't return any matching results. This issue is resolved.
- **Specifying multiple labels within each label type is not supported** (E-73039)

  You can filter one label per Role, Application, Environment, or Location label type. While you have the ability to indicate multiple labels in your search filter within each type, you do not receive any results. This issue is resolved.

Policy and Workloads

- **Draft mode incorrectly marking corporate traffic as allowed due to non-corporate rules** (E-96916)

  In Explorer/Illumination's draft mode, traffic on the corporate network was erroneously marked as "allowed" due to rules that apply only to non-corporate networks. This issue occurs when there are rules on the non-corporate network to broad IP lists. The issue only affected Draft mode and had no impact on policy correctness. This issue is resolved.
- **Container updates do not trigger policy updates in other PCEs in a Supercluster** (E-95714)

  Under certain conditions, changes to container workloads in one PCE in a Supercluster would not lead to policy updates on workloads paired with other PCEs in the Supercluster. This issue is resolved.
- **Incorrect policies on workloads for Avi load balancers** (E-95516)

  Workloads that were paired to a PCE other than the leader PCE of a supercluster did not receive the correct policies to communicate with Avi load balancers. This issue is resolved.

Data Visualization

- **Illumination Plus: At scale, the Workload tab is showing empty** (E-98808)

  At scale, only the top 500 most vulnerable workloads in a group will show the vulnerabilities in the workloads tab of the group panel. This issue is resolved.
- **Rule coverage not called after switching to the "Allowed" filter or clicking on "Refresh Draft Policy"** (E-97210)

  As a workaround, click on the Go button or switch to "Individual Connections". No other fixes are planned.

- **App group Explorer is extremely slow** (E-96860)
  This issue is closed because the old Explorer became obsolete in release 22.4.0.
- **SaaS SCP2 slow Explorer queries** (E-96770)
  When running a query in Explorer, the results screen was not displayed. This issue was caused by an error in one of the internal queries used to populate data.
  This issue is resolved. The query SQL has been fixed, and the Explorer query results screen is displayed properly.
- **410 error when downloading async_queries** (E-96043)
  The error 410 was thrown when users performed an Explorer query on an organization that returned empty results. A query that returned some results was not causing errors. This issue is resolved.
- **Provide a GUI option in the Explorer to perform "exclude_workloads_from_ip_list_query":false** (E-94737, E-94408)
  Starting with the release 22.2.20, the Explorer page in the PCE web console includes the **Exclude Workloads from IP List Query** option.
  To select the option, go to the PCE web console **Settings** menu. This setting applies to Explorer queries that contain an IP list in the Consumer or Provider fields. It specifies whether known managed and unmanaged workloads are excluded from the search results. When selected (the default setting), Explorer excludes managed and unmanaged workloads from the results when their IP addresses exist in one of the query's IP lists. When not selected, Explorer does not exclude workloads from the results. This issue is resolved.
- **Proposed Enforcement Boundary rulesets do not match existing service port/protocol** (E-93641)
  Service names have not been mapped in the enforcement boundaries blocked connection page. This issue is resolved.
- **Explorer pagination jumps to the last page of Label based connections in some cases** (E-93223)
  In the **PCE Web Console > Explorer** , clicking the right arrow above the connections list to advance to the next page unexpectedly redirects you to the last page in these circumstances:

  1. Select multiple connections in Explorer.
  2. Click **Allow Selected Connections**. The **Proposed Ruleset** page opens.
  3. Click **Cancel** on the **Proposed Ruleset** page.

  This issue is resolved and no other fix is planned.
- **In Explorer, the parameter drop-down list is duplicated in some cases** (E-93206)
  In the PCE Web Console > Explorer, after selecting to include All Workloads in Consumers, the drop-down list is duplicated such that a second menu appears atop the initial menu.
  Users should ignore the duplication and select parameters on the visible menu. This issue is resolved.
- **Clearing the traffic counters for virtual services doesn't remove the links in the Illumination map** (E-81658)
  Clicking the **Clear Traffic Counters** link in the Illumination control panel for virtual services doesn't clear the traffic links between the virtual services in the map.
  After clearing the traffic counters for virtual services, click the refresh icon to recalculate the map data. This issue is resolved and no other fix is planned.

PCE Platform

- **Agent background service CRITICAL alerts in PCE Health page** (E-96420)
  Execution of background jobs could cause the PCE Health page to continually display alerts that the agent background service was in a critical state. This was caused by orphan

records in database tables that caused background job queries to take longer or fail. The workaround was to schedule downtime and manually remove the orphan database entries. This issue is resolved. Orphan records are now automatically removed when detected. Manual intervention is no longer necessary.

- **Update events are not generated in SaaS for actions using agent service as a proxy call to the login cluster** (E-96186)

  When the user tried to update the password policy for a local user, authentication settings, SAML configuration, or LDAP configuration, it was supposed to generate an update event, which failed to generate. This issue is resolved.
- **PCE showing plaintext password for login** (E-96079)

  If the PCE was misconfigured, such as when `pce_fqdn` was unreachable and/or is resolving to the wrong IP address, passwords could be written to logs in plaintext. This issue is resolved.
- **Created By field in CEF events didn't work** (E-91151)

  The **Created By** field for certain events wasn't properly translated to `duid` when exported using the CEF format. The `duid` didn't work for events created by container clusters or Illumio Service Accounts because they don't expose integer IDs; therefore, they didn't populate the `duid` in CEF events. This issue is resolved. If an entity has an `uuid`, it will be returned for the CEF `duid`.
- **Consul messages not sent to internal syslog** (E-90286)

  Messages from the PCE consul service are no longer sent to the internal syslog. Messages do not appear in consul.log. Instead, they appear in `/var/log/messages` and `/var/log/illumio-pce/consul`. This issue is resolved.

UI Platform

- **Pairing profiles reporting a white page after clicking Generate Key** (E-98414)

  This issue is resolved, and the white page is not showing anymore.
- **Providing Services/Ports are indistinct in the Rule Search CSV export** (E-98045)

  Users could not see or identify the ports or services from the Rule Search export. This issue is resolved.
- **Changes to enforcement mode of multiple workloads not showing in the event log** (E-97878)

  When enforcing a group of workloads, the event that was logged did not contain enough information to determine what had changed. The "Changes" field was blank. This issue is resolved.
- **PCE UI - Workloads Processes tab doesn't load** (E-97109)

  When Illumination was disabled by the Illumio administrator, the Workloads Processes tab did not load and displayed an error. This issue is resolved.
- **When a ruleset is copied, the replica doesn't carry over the rule notes** (E-96154)

  When a ruleset was duplicated, the replica did not contain the rule notes. This issue is resolved.
- **Clicking Add Ruleset or Rules displayed an empty page** (E-95948)

  When you performed either of these steps, the PCE web console displayed an empty page:
  - Go to the Rulesets page and click the **Add** button.
  - Go to the Rules page and click **Add** > **Add Intra-Scope Rule** or **Add** > **Add Extra-Scope Rule**.

  This issue is resolved. In this release, the PCE web console now refreshes the page with the fields to add a ruleset or rule.
- **Too many labels available for a scoped user** (E-95564)

The ruleset filter previously only ever returned app, env, loc labels, because the ruleset scope was artificially limited to those labels. With MT4L there could be labels of all types in the scope, but the filtering options did not adjust accordingly. This issue is resolved.

- **An unexpected arrow pointer is displayed when selecting exclusion in a rule with Virtual Service** (E-95283)

  When users tried to select an exclusion in a rule with a Virtual Service, they observe that a weird pointer was displayed. This issue is resolved.
- **Ruleset changes didn't appear after navigating away and returning** (E-95103)

  If a user changed the scope of a Ruleset, navigated away, and then returned to the Ruleset, the changes didn't appear unless the user refreshed the browser. This issue is resolved. Scope changes now appear after navigating away without the need to refresh the browser tab.

VEN

- **On Oracle RAC RHEL 7.7, VEN reported multiple tampering events** (E-97636)

  The VEN incorrectly reported tampering events when coexistence mode was used. This issue is resolved.
- **Abrupt shutdown of RedHat VEN causing issues with aggressive tampering detection** (E-91763)

  On Red Hat Enterprise 7.9, 21.2.4-7978, in extremely rare cases, an abrupt shutdown of the VEN (for example. manual `kill -9`) might prevent the VEN from cleaning up kprobe configuration. This could lead to errors enabling aggressive tampering detection when the VEN is restarted. System administrators are advised to use only documented methods of shutting down the VEN (for example, `illumio-ven-ctl stop`).

  This issue is closed because it works as designed. In addition, there is a knowledge base article available named "LINUX VEN goes to Error State when Installed on a SYMLINK".

Known Issues in 22.5.30 and Earlier Releases

Enterprise Server

- **Blank space in IP address causes a query to fail** (E-106290) When filtering by IP address in **Explorer > Traffic**, if a blank space appears after an IP address in the filter criteria, the query fails. Explorer doesn't auto-correct blank spaces in this circumstance, which may be unexpected. Workaround: If your query fails, examine the filter criteria and ensure that no blank spaces appear after IP addresses.
- **Explorer/Illumination Plus misinterpret flows with the label group "Empty"** (E-105503)

  Workaround: none
- **Mesh: Re-renders repeatedly. Interactions are not working** (E-105167)

  Hover and brush interactions on Mesh are not working. Images re-render repeatedly. No workaround is available.
- **Proposed Rules - Status information is being hidden** (E-105098)

  The Proposed Rules status information is hidden by the Ruleset Summary page.
- **App Group is not showing for Workload Manager in New UI** (E-105068)

  Workload manager cannot see the **App Group** menu in the New UI. If you navigate from the Old UI to the App Group page, and then switch to the New UI, you can see the data for the App Group, but still cannot see an **App Group** option in the menu.

- **Fedramp: Removal of inactive accounts ignores API use** (E-103316)
  In PCE release 22.4.1+A3, user accounts that have been inactive for more than 90 days are removed automatically. However, the active status is determined based only on whether the account has logged in to the web console UI. If the account is used only to issue API requests, it is counted as inactive and removed after 90 days.

Illumination Plus

- **Updating max results in Illumination Plus (10K) updates the Explorer max results** (E-102742)
  The maximum connection number in Explorer gets updated to the same maximum number as the update in Illumination Plus. However, the max number in Illumination Plus is 10,000 while in Explorer it is 100,000. Workaround: Update the max results setting in Explorer to get more than 10K results.
- **Reported policy decision is incorrect when the flow is blocked by boundary** (E-102588)
  Draft policy decision should show as 'By Boundary' if the traffic is 'blocked by a boundary'.
  Workaround: not available.
- **Illumination Plus and reports pages display blank when users create a custom time-saved filter in different time zone formats** (E-102528)
  Workaround: Remove the created custom-time saved filter in Explorer.
- **Recent filters become empty in Illumination Plus when users run a query from Explorer** (E-102525)
  Workaround: None
- **When users load saved filters in Explorer, more than four labels are showing up** (E-102438)
  The explorer results are not filtered based on the custom labels.
  Workaround: Not available.
- **After creating a new organization, users are unable to load saved filters in Illumination Plus** (E-102268)
  Workaround: Create the Save filter once you issue a new query from Explorer or Illumination Plus.
- **Saved filter for Explore and Loading showing empty data by default** (E-102257)
  The created Saved filter for Explore and Loading is showing reported policy decisions with empty data by default.
  Workaround: None
- **Enforcement boundaries filters showing after boundaries are deleted** (E-102251)
  Enforcement boundaries filters are still showing after enforcement boundaries are deleted.
  Workaround: Not available.
- **(App Group Map): Tooltips are not showing for connected app groups** (E-96033)
  When users expand (right-click) a traffic link between connected app groups and then hover around any of the expanded links, the tooltip does not show up.
  Users can still click on the link and display the Summary and Connections panel with details.
  No workaround is available.
- **Refresh Draft Policy is not working after enabling or disabling rules** (E-95410)
  Refreshing a draft Policy is sometimes not correctly displayed in Illumination Plus after enabling or deleting rules. No workaround is available.

Data Experience

- **Context menu moves out of view when close to Map edge** (E-101545) When right-clicking on a node that is near the edge of the screen in Map view, the context menu goes out of view.

  Workaround: Drag the map so that the node is no longer close to the edge of the screen, then right-click again to see the context menu.
- **Existing policy with label group not displayed in the UI** (E-101505)

  In Illumination Classic, when adding a new rule from the App Group Map view, label groups are not displayed in the auto-populate window.

  Workaround: none.
- **Provider and Consumer order is mismatched between filters and column headers** (E-101156)

  This issue is resolved in Explorer and is still unresolved in Illumination Plus.
- **Saved Workloads filter returns no results following an upgrade** (E-99346)

  After upgrading from Core version 22.4.0 to 22.5.0, loading an existing saved filter in Illumination Plus to filter by workloads returns no results.

  Workaround: To filter by workload, specify the filter parameters manually instead of using a saved filter.
- **Non-default display options don't persist in some cases** (E-99125)

  In Illumination Plus, if you select a display option from the **More** menu (for example, **Show Reported Policy Decision Filter**), don't choose any parameters from the filters, and then click **Run** or refresh the browser, the selected display option doesn't persist and no filtered results are returned.

  Workaround: You'll need to re-select the display option, choose parameters from the filters, and then re-run the filter.
- **Special character in Label Type Key causes the app to crash when resized** (E-98984)

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

  Workaround: Avoid using special characters when specifying the Label Type Key.
- **Users not automatically redirected to the Extra-Scope tab** (E-98507)

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

  Workaround: Click the Extra-Scope tab to go there manually.
- **Explorer returns results with incorrect labels** (E-96438)

  If there are multiple virtual services from different container networks with the same ip+port+proto in the PCE, when the user queries with the labels of one virtual service the flows from other container networks under other virtual services can come into the results and be shown as different labels. Users should ignore the flows with labels different than the query labels in this case.
- **Total V-E (Vulnerability) score is slightly inaccurate** (E-75418/E-73277)

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

  No workaround is available.

Policy Platform

- **Keys missing from `agent_missed_heartbeats_check` event detail page** (E-97912)
  When viewing a "system_task.agent_missed_heartbeats_check" event in the UI, the "resource changes" and "notifications" fields are missing from the UI. The data exists in the API JSON but the UI no longer shows these values.
- **Flow timestamp incorrect in Illumination for inbound-only or outbound-only reported flows** (E-96595)
  The flow timestamp that is shown in Illumination is not reliable for ingress-only or egress-only reported flows.
  Workaround: Use Explorer to see the correct timestamp.

Data Platform

- **NodePort - CVEN: Illumination map arrows are not correct** (E-97387)
  Traffic sent from an external client to a NodePort Service in a Kubernetes Cluster appears destined for the backing pod or host workload rather than for the service in the Illumination Map. No workaround is available.
- **Flow timestamp incorrect in Illumination for inbound-only or outbound-only reported flows** (E-96595)
  The flow timestamp that is shown in Illumination is not reliable for ingress-only or egress-only reported flows.
  Workaround: Use Explorer to see the correct timestamp.
- **A large app_stats log file (8GB and more) is continuing to grow** (E-95636)
  On some systems, logrotate for the internal log files is sometimes not successful, which causes these files to continue to grow in size. No workaround is available.

PCE Web Console

- **No error message is displayed after typing in an invalid port** (E-68255)
  When you enter an invalid port number while editing a service, the PCE still displays options to select from. When you move to another field without making a selection, the entered letters/digits are not cleared to reflect that the entered value was not selected. It can appear that the value you entered was accepted even though invalid.
  Workaround: Press ENTER after entering text. When the combination was valid, it will be selected. Otherwise, it will be cleared.
- **Filtering by an invalid protocol in the Services List page displays all services** (E-68251)
  When you type an invalid protocol and press ENTER, the protocol appears as a filter item but the list page is not refreshed. The PCE web console validates the entered protocol and refreshes the page only when the protocol is valid.
  No workaround is available but this is only a cosmetic issue.
- **Filtering by an invalid port in the Services List page displays an error** (E-68249)
  When you filter the Services list using an invalid port, you receive the 406 error: "Port value out of range." The port filter category is a free search and your input is passed to the PCE without validation.
  Workaround: Clear the entered port number and filter the list with a value in the valid port range.
- **Wildcard in workloads filter not working** (E-65232)
  The PCE web console Workloads page supports filtering using special characters such as an asterisk (*). However, instead of displaying an error message when *only* special characters are used, the Workloads page neither filters the result nor gives an error message.

No workaround is available.

- **Filter doesn't handle the percentage symbol** (E-64904)
  When users select a filter option from the drop-down list, the selected value is added to the URL. If the selected value contains the percentage symbol (%), the UI throws an error, and a blank page shows up.
  There is no workaround, but this is a rare situation because the % symbol is not used often in values.
- **A REST API call to switch** `multi_enforcement_instructions_request` **returns an error** (E-59518)
  A REST API call to switch `multi_enforcement_instructions_request` returns an incorrectly handled error.
  This issue will be resolved in a future release.
- **Pressing Enter doesn't select the default option in the dialog box** (E-53831)
  When the PCE web console displays a dialog box, pressing **Enter** might select an action other than the default.
  Workaround: Use your mouse to click the required button in the dialog.
- **PCE web console doesn't provide warning for out-of-scope Rule entities** (E-29502)
  You are incorrectly allowed to select a workload as a provider for a rule, even if the provider's labels do not match the labels of the specified scope.
  No workaround is available.

Policy and Workloads

- **Container workload profile updates could generate a PCE error** (E-84624) Occasionally, updating the labels or enforcement mode of a container workload profile fails with a 500 Internal Server Error. This is caused by concurrent C-VEN and Kubelink background activity.
  Workaround: The update should succeed by retrying the PUT request.
- **Tunnel IP appears on VM's inbound port unnecessarily in Illumio policy** (E-84081)
  In a policy managing traffic between a Kubernetes pod (Consumer) and an external managed Virtual Machine (Provider), the managed VM has both the Host IP and the Tunnel IP on the inbound port. Illumio needs only the pod's Host IP on the external VM; the host's tunnel IP address is unnecessary.
  While this situation doesn't impact functionality, Illumio plans to correct this in a future release.
- **Enforcement Boundary filter returns Potentially Blocked flows mislabeled "no Rule"** (E-83415)
  Enforcement Boundaries filtered by IP Lists and displayed in the Draft View include Potentially Blocked flows that are labeled "no Rule" instead of "Blocked by Boundary." As it's not possible to enforce a boundary on flows with no rules, the "no Rule" status appears in error.
  Workaround: If you see the "no Rule" status in these circumstances, assume that the flows are "Blocked by Boundary."
- **Virtual Server Mode does not map directly to the management state in the Web Console** (E-78370)
  Any virtual server discovered on an SLB is considered to be in the “Managed” state when it has a corresponding entry in the virtual server list page. A managed virtual server could be either Not Enforced or Enforced. The `virtual_servers` object in the API returns a “Managed: Not Enforced” virtual server as “unmanaged.”
  No workaround is available.
- **Incorrect error message displayed when ruleset named to a name that's in use** (E-74498)
  When creating and provisioning a rule set (for example, ruleset A, renaming it ruleset B, then creating ruleset A and reverting modifications to ruleset B), the UI displays an

incorrect "500" error instead of an error message stating that the ruleset name is already in use.

- **Policy restore impacts the virtual services of a container cluster** (E-73979)

  The issues are as follows:

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

  No workaround is available.
- **Inconsistencies in rule coverage for the Windows process-based rules** (E-71700)

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

  No workaround is available.
- **Rule search with virtual service and labels returns an incorrect rule** (E-65081)

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

  Workaround: Use rule search to ensure that the rule applies to the virtual services and the scope labels separately.
- **Unable to select multiple protocols in Rule Search** (E-57782)

  If you try to select multiple protocols in Rule Search, you cannot select a second protocol after selecting a protocol once. For example, if you select TCP and then want to select UDP, the UI does not display the protocol option again.

  Workaround: This issue is only an issue in the PCE web console. Using the REST API, you can select multiple protocols and obtain the correct search results.

Data Visualization

- **After creating a new organization, users are unable to load saved filters** (E-102268)

  Workaround: Create the save filter once you issue a new query from Explorer or Illumination Plus.
- **Time filter not working properly for weekly rollup tables in some cases** (E-97491)

  When users put the start date in Explorer as later than Monday in a week, the flow that happened after Monday is not returned for that week, making the query invalid.

  No workaround is available.
- **User column remains empty in Explorer by mistake** (E-89313)

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

  No workaround is available.
- **Problem when running multiple Explorer queries in separate tabs** (E-82385)

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

  No workaround is available.
- **Time between two traffic flow events might be misreported** (E-79204)

  In Explorer, when viewing a traffic flow allowed by FQDN rules that was initially dropped and then allowed, the time between the drop and the allow events might be reported

erroneously. The actual time between the two events could be only a matter of seconds (as expected), but the reported time could be more than one minute, which would be erroneous.

No workaround is available.

- **Vulnerability - V-E score is not showing correctly** (E-75418, E-73277)

  The Total V-E score indicated on the Vulnerabilities page is higher than the sum of the values in the V-E score column. For example, in a given case the sum of the values in the V-E scores column was 69.8 but the Total V-E score was 71 instead of 70.

  No workaround is available.
- **VES and E/W exposures wrong for the internet and other workloads** (E-73023)

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

  No workaround is available.

PCE Platform

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

  The setup of a syslog server can be performed only from the leader PCE.
- **PCE application log files are not rotated** (E-105659)

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

  Workaround: none.
- **VENs on RHEL 8 potentially subject to OpenSSL CVEs** (E-93205)

  VENs installed on RHEL 8 use the OpenSSL package that is installed as part of the OS. There are known security vulnerabilities on several OpenSSL versions.

  Workaround: Upgrade to the latest OpenSSL package v3.0.5 or v1.1.1q or later. Please note that based on its usage of OpenSSL, VENs are not impacted by CVE-2022-1292, CVE-2022-2068, and CVE-2022-2274.
- **XFF not working properly** (E-88891)

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

  No workaround is available.
- **The `agent.activate` events are not always classified correctly** (E-74682)

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

  No workaround is available.

UI Platform

- **Intermittent error "Unable to Edit Enforcement Boundaries Rule"** (E-94530)

  Users are unable to edit Enforcement Boundaries blocked connection count while the query is running.

  No workaround is available.
- **Service ports are no longer shown in rules** (E-94476)

After upgrading the PCE to 22.x, service ports are no longer shown in rules -- only the name of the service. Note that ports are shown as expected in rule searches.

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

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

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

VEN

- **VEN should not ask for maintenance token on unsupported OSes for tampering protection** (E-101470)

  When VEN tampering protection is enabled, Solaris and macOS workloads (where VEN tampering protection is not yet supported) might also ask for a maintenance token for CLI commands. CLI commands other than suspend will succeed if a valid maintenance token is provided. However, the suspend command does not work even if a valid token is provided. There is no workaround. If you will enable the VEN tampering protection feature, do not upgrade Solaris or macOS workloads to 22.5.10.
- **SecureConnect only logs the "E" on the provider** (E-101229)

  Works as designed. There is no way to tell whether SecureConnect is in the egress path.
- **Workload (CentOS 7) keeps emitting agent.tamper error events after configured custom iptables rule** (E-101029)

  A firewall policy with a custom iptables rule might get dumped in a different format than the one it was in when ingested. When using `-key value` arguments to iptables such as `--k2 v2 --k1 v1`, it does not matter which order you add them in for correctness in the system. However, if the Linux kernel dumps the arguments back to the VEN in a different order, the VEN falsely considers it a tamper. For example, if the kernel always dumps "`-k1 v1 --k2 v2`" even if you give "`-k2 v2 --k1 v1`", then the VEN will think somebody has changed the firewall. A workaround is to order the custom iptables rules the same way that the Linux kernel dumps them in.
- **Windows 11 shown as Windows 10 on workload/VEN page** (E-100844)

  Workaround: not available.
- **VEN 22.2.30 failure to restart at boot was holding up critical processes** (E-100416)

  In some cases, when Solaris cluster nodes were restarted due to a storage issue with the underlying hardware devices, Illumio Core processes appeared to block the rest of the node processes from starting. The reboot did not work. Workaround: Place the VEN into suspend mode and then reboot the hardware again,
- **Compatibility report (problem 2) - nftables /RHEL8** (E-91481)

  The customer installs the missing packages and reruns the compatibility report from the Web Console but is unable to run the report.

  Workaround: Either restart the VEN (`sudo /opt/illumio_ven/illumio-ven-ctl restart`) or rerun the script that manually generates the report (`sudo /opt/illumio_ven/bin/.agent_qualify.sh`).

  Works as designed.
- **Process-based rule not showing properly in Explorer** (E-89749)

  A process-based rule was defined but was shown as "no rule" in Explorer. The workaround is to not specify the service name in the process-based rules.
- **On CentOS 8, VEN can't load the FTP and TFTP modules** (E-85127)

On CentOS 8, the VEN can't load the `nf_conntrack_ftp` and `nf_conntrack_tftp` modules, which blocked the workload from uploading and managing files. Due to this issue, customers can't upgrade the VEN on CentOS 8 workloads.

No workaround is available.

- **[CentOS8] Custom Iptables rule does not work with -j REDIRECT** (E-80818)

  After creating a custom rule on the PCE with -j REDIRECT in the nat table, the CentOS 8 VEN enters an error state because the VEN could not correctly handle the -j REDIRECT part of the rule. The custom rule performs a NAT operation that requires a different chain type therefore, nftables does not allow the VEN to perform the redirect in our chains.

  Workaround: remove the custom Iptables rule and restart the VEN. This brings the VEN back to a healthy state.
- **Established connections are not removed when the VEN is restarted** (E-63072)

  After the VEN is paired and restarts using the `Illumio-ven-ctl` options, it dumps suspicious log entries into vtap.log twice per minute. The log type is INFO and they appear to be caused by an error related to the restart of the VEN. This issue is observed in the global zone and the exclusive IP zone.

  Workaround: Not available; however, this issue has no major impact except for vtap.log receiving these log entries.

REST API

- **Vulnerability APIs should distinguish between 0/syncing/NA Exposure scores** (E-71689)

  Users might get confused when the workload list page shows as Syncing and the workload vulnerability tab shows as N/A. This is a cosmetic issue and no workaround is available.

Security Information

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

22.5.32

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

  cgi-0.3.2.gem upgraded to v0.3.6 to address CVE-2021-33621. This CVE did not impact Illumio PCE.
- **globalid upgraded to v1.0.1**

  globalid upgraded to v1.0.1 to address CVE-2023-22799.
- **google-protobuf upgraded to v3.22.5**

  google-protobuf upgraded to v3.22.5 to address CVE-2022-3171 and CVE-2021-22569.
- **rack upgraded to v2.2.7**

  rack upgraded to v2.2.7 address CVE-2022-44572, CVE-2022-44571, CVE-2023-27530, CVE-2023-27539, and CVE-2022-44570.
- **rails, actionpack, activerecord, activesupport and related gems upgraded to v6.1.7.4**

  rails, actionpack, activerecord, activesupport and related gems upgraded to v6.1.7.4 to address multiple CVEs including CVE-2023-28120, CVE-2023-23913, CVE-2023-28362, CVE-2023-22792 CVE-2023-22795 CVE-2022-3704, CVE-2023-22794 CVE-2022-44566, and CVE-2023-22796.

22.5.30

- **OpenSSL was upgraded to v3.0.8**
  OpenSSL was upgraded to v3.0.8 on the Illumio VEN to address CVE-2022-3996, CVE-2022-4203, CVE-2022-4304, CVE-2022-4450, CVE-2023-0215, CVE-2023-0216, CVE-2023-0217, CVE-2023-0286, and CVE-2023-0401. Illumio VENs were not impacted by these CVEs.
- **curl was upgraded to v7.88.1**
  curl was upgraded to v7.88.1 on the Illumio VEN to address CVE-2022-22576, CVE-2022-27774, CVE-2022-27775, CVE-2022-27776, CVE-2022-27779, CVE-2022-27780, CVE-2022-27781, CVE-2022-27782, CVE-2022-30115, CVE-2022-32205, CVE-2022-32206, CVE-2022-32207, CVE-2022-32208, CVE-2022-35252, CVE-2022-32221, CVE-2022-42915, CVE-2022-43551, CVE-2022-43552, CVE-2022-42916, CVE-2023-23914, CVE-2023-23915, and CVE-2023-23916. Illumio VENs were not impacted by these CVEs.
- **sqlite was upgraded to v3.41.0**
  sqlite was upgraded to v3.41.0 to address CVE-2022-46908. Illumio products were not impacted by this CVE.
- **ua-parser-js was upgraded to 0.7.35**
  ua-parser-js was upgraded to 0.7.35 to address sonatype-2018-0272. Illumio products were not impacted by this vulnerability.

22.5.20

- **rails upgraded to v6.1.7.2**
  The rails gem has been upgraded to v6.1.7.2 to address CVE-2023-22795
- **activerecord upgraded to v6.1.7.1**
  The activerecord gem has been upgraded to v6.1.7.1 to address CVE-2023-22792
- **nokogiri updated to v1.13.10**
  The nokogiri gem has been upgraded to v1.13.10 to address CVE-2022-23476
- **sinatra upgraded to v2.2.4**
  The Sinatra gem has been upgraded to v2.2.4 to address CVE-2022-45442
- **rails-html-sanitizer upgraded to v1.4.4**
  The rails-html-sanitizer gem has been upgraded to v1.4.4 to address CVE-2022-23520, CVE-2022-23519, CVE-2022-23518 and CVE-2022-23517
- **loofah upgraded to v2.19.1**
  The loofah gem has been upgraded to v2.19.1 to address CVE-2022-23516
- **fluentd upgraded to v1.15.3**
  The fluentd gem has been upgraded to v1.15.3 to address CVE-2022-39379
- **curl upgraded to v7.86.0**
  The curl package has been upgraded to v7.86.0 to address CVE-2022-32221, and CVE-2022-35252

22.5.10

- **The rails gems are upgraded to v6.1.7**
  The rails gems including `activestorage`, `activerecord`, `actionaview`, and `actionpack` have been upgraded to v6.1.7 in order to address CVE-2022-21831, CVE-2022-32224, 27777 and CVE-2022-22577.
- **SQLite is upgraded to v3.40.0**
  SQLite is upgraded to v3.40.0 to address CVE-2021-20227.

- **Improper certificate validation on macOS VEN**
  Certificate validation was improperly performed on the macOS VEN, impacting traffic between the VEN and the PCE. This issue is resolved.

22.5.0

- **OpenSSL upgraded to v3.0.7 on Core 22.5.0 VEN**
  The openssl package has been upgraded to v3.0.7 in order to address CVE-2022-3786 and CVE-2022-3602. For additional information on the affected versions of the VEN, review the Security Advisory here.
- **devise-two-factor upgraded to v4.0.2**
  The devise-two-factor gem has been upgraded to v4.0.2 in order to address CVE-2021-43177.
- **jquery-rails upgraded to v4.5.0**The jquery-rails gem has been upgraded to v4.5.0 in order to address CVE-2020-11023.
- **rails-html-sanitizer upgraded to v1.4.3**
  The rails-html-sanitizer gem has been upgraded to v1.4.3 in order to address CVE-2022-32209.
- **yajl-ruby upgraded to v1.4.3**
  The yajl-ruby package has been upgraded to v1.4.3 in order to address CVE-2022-24795
- **consul upgraded to v1.13.2**
  The consul package has been upgraded to v1.13.2 in order to address CVE-2022-29153, CVE-2022-24687, CVE-2021- 41805, CVE-2021-38698, and CVE-2021-37219.
- **PostgreSQL upgraded to v13.8**
  The postgresql package has been upgraded to v13.8 in order to address CVE-2022-2625.
- **zlib upgraded to v1.2.12**
  The zlib package has been upgraded to v1.2.12 in order to address CVE-2018-25032.
- **netaddr upgraded to v1.5.3**
  The netaddr gem has been upgraded to v1.5.3 in order to address CVE-2019-17383.
- **Misconfigured PCE could lead to sensitive information being disclosed within log files**
  If the PCE was misconfigured, such as when pce_fqdn was unreachable and/or resolving to the wrong IP address, passwords could be written to logs in plaintext. This issue is resolved.

Illumio Core for Kubernetes Release Notes 4.3.0

What's New in Kubernetes 4.3.0

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

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

Here are the new and changed items in this release:

- **New Kubelink 3.3.1**
  This Kubernetes 4.3.0 release includes an upgraded Kubelink component, version 3.3.1 .
- **New C-VEN 22.5.14**
  This Kubernetes 4.3.0 release includes an upgraded C-VEN component, version 22.5.14.

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

Security Information

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

Base Image Upgraded

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

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

Product Version

Compatible PCE Versions: 22.5.0 and later releases

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

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

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

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

Updates for Core for Kubernetes 4.3.0

C-VEN

Resolved Issues

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

Known Issue

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

Kubelink

Resolved Issue

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

Known Issue

- **Kubelink does not properly apply label mappings with PCE using two-sided management ports** (E-105391)
  Label mappings are not properly applied when using the LabelMap CRD if the PCE uses two-sided management ports.

Workaround: Use the label map feature only with a PCE that uses only one management port.

Legal Notice

Resources

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

Contact Information

- Contact Illumio
- Contact Illumio Legal
- Contact Illumio Documentation