TECHNICAL
DOCUMENTATION

# Illumio Core What's New and Release Notes 22.2

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

# Table of Contents

# What's New in 22.2

## What's New and Changed in this Release

Before upgrading to Illumio Core 22.2.*x*, familiarize yourself with the following new and modified features in this release.

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

## What's New and Changed in Release 22.2.0

Illumio Core 22.2.0 introduces the following new features and enhancements.

### Installation Change

In the name of the Illumio Core PCE installation RPM file, c6 has changed to c7. This reflects the change in CentOS support to CentOS version 7, which was made in an earlier PCE version. In the PCE Installation and Upgrade Guide, this file is referred to as `illumio_pce_rpm`.

### New Features in This Release

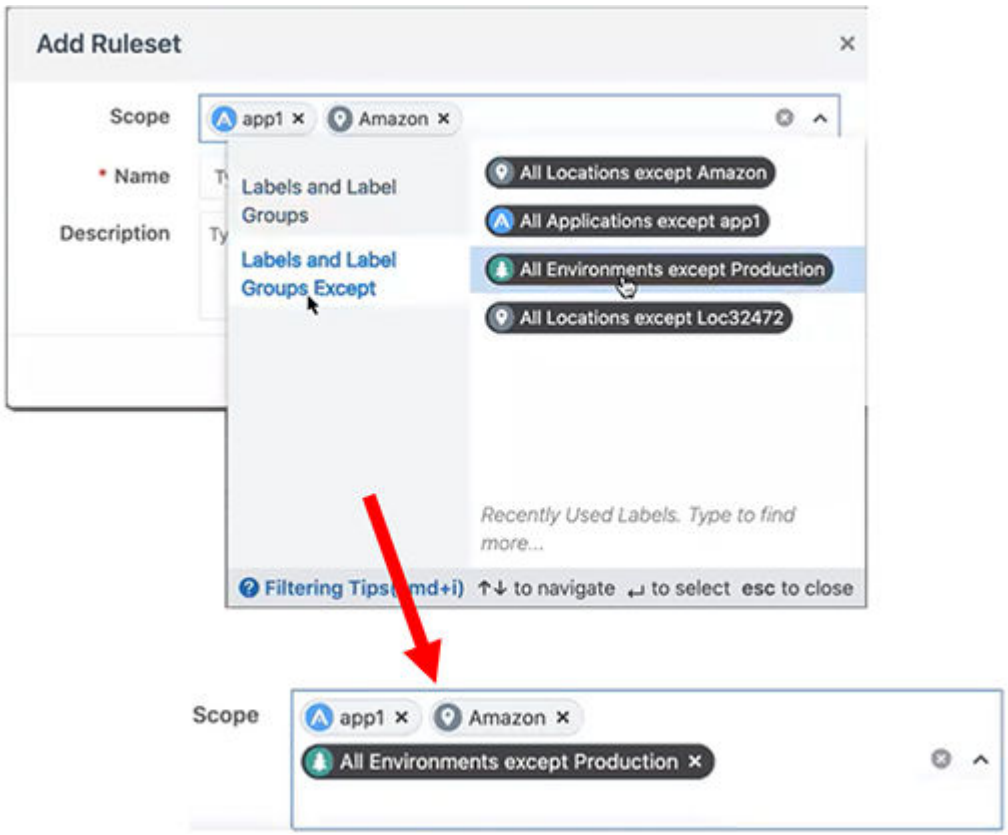
The following new features were added in Illumio Core 22.2.0.

### Policy Exclusions

Illumio Core 22.2.0 delivers policy exclusions as a new feature. In particular, the PCE supports including policy exclusions in ruleset scopes and rules.

Using policy exclusions in your Illumio Core policy can greatly simplify the rule writing process. Specifically, using a policy exclusion in a ruleset scope or in rules allows you to replace the inclusion of a large number of required labels with the exclusion of a small number of unwanted labels. Security policy written with policy exclusions can be easier to read and definitely easier to maintain.

Using a policy exclusions gives you a way to state in your security policy that you want a ruleset or rule to apply to "all except *X*," where *X* can be both labels and label groups. To state this another way, "all except *X*" means "All labeled workloads except X."




## Scopeless Rulesets

In this release, you have the option to create basic or scoped rulesets. You can choose whether you want to include scopes when creating new rulesets. The **Scope** field appears in the **Add Ruleset** dialog box only when the PCE is configured to display scopes in rulesets. When the PCE is configure to create scopeless rulesets, you create simple rules that do not apply to specific environments, locations, or applications. These rules are scopeless rules because they do not belong to a ruleset that uses scopes.

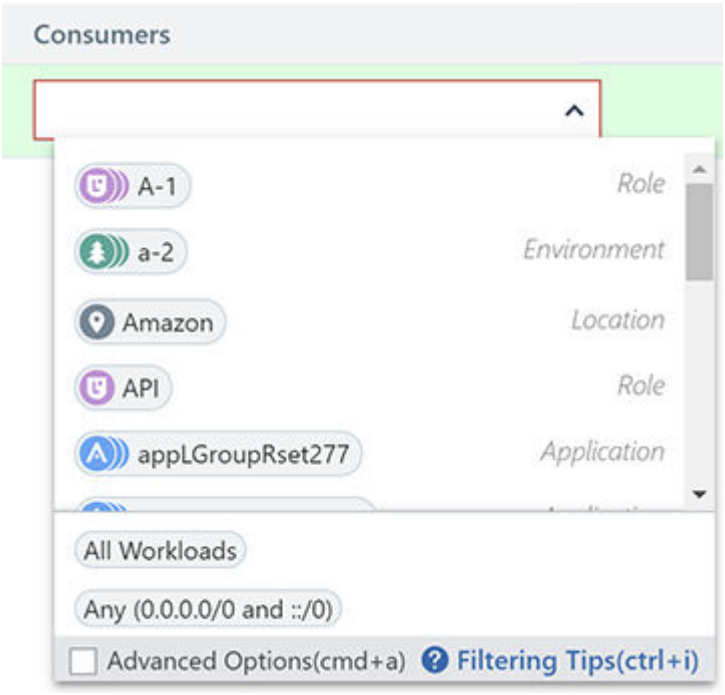
You might want to create these basic rules when you are new to using Illumio Core and you are creating your first security policy rules. For example, you might want to create a simple rule to control SSH traffic for all your workloads. As you become more familiar with Illumio Core or you need to create more complicated rules, you can choose to create scoped rules; namely intra-scope, extra-scope, and custom iptables rules. Creating scoped rules allows you to create rulesets and rules that are defined for specific environments, locations, and applications (typically larger environments).

When the PCE is configured create scopeless rulesets, you can still add a scope to a ruleset after saving the ruleset. From the **Ruleset Actions** menu at the top right corner of the **Ruleset** page, select **Add Scope**.

## Simplified Rule Writing

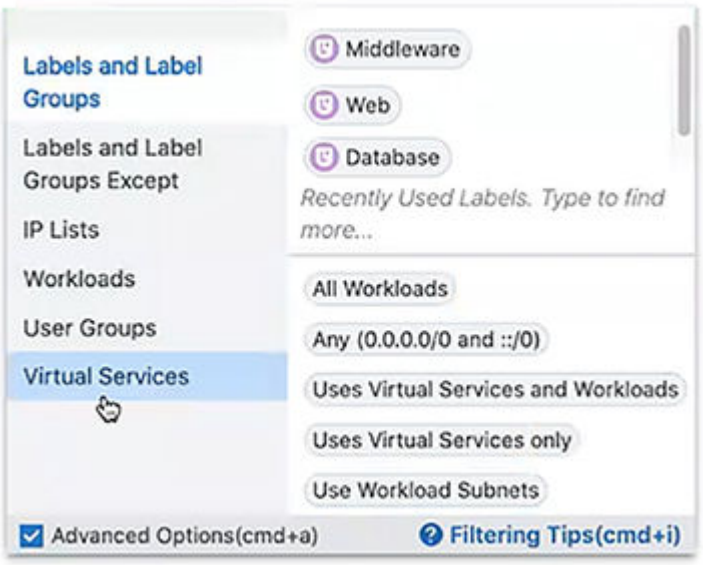
In this release, the dialog boxes in the PCE web console are split into a simple mode and an advanced mode.

In the simple mode, you can select labels and label groups for your rules. Your most recently used labels appear in this screen, then as you type, the UI auto-completes the names to find labels in the PCE.




To access the Advanced Options for rules, select the **Advanced Options** checkbox:

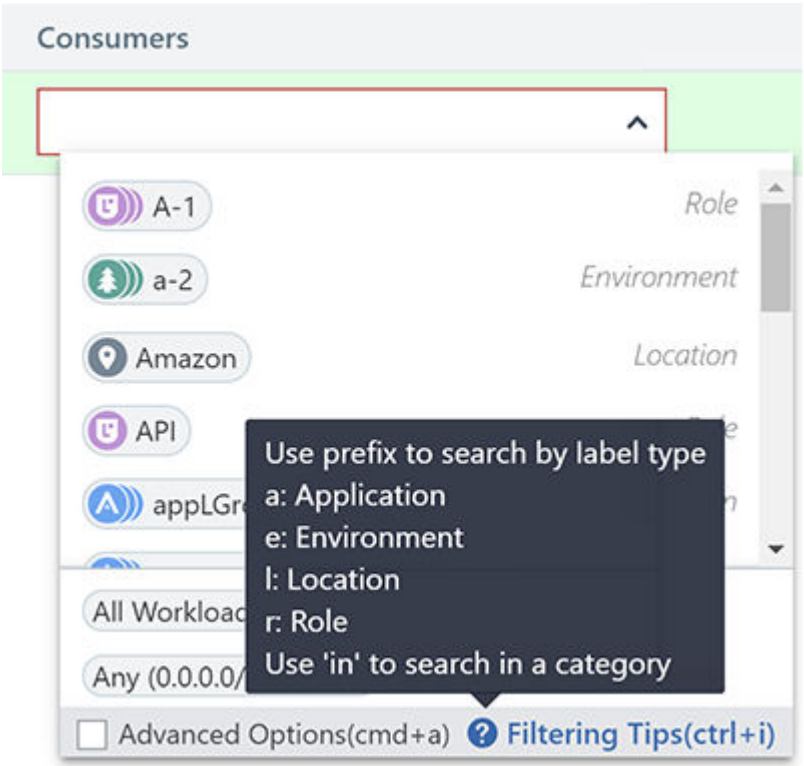

A panel appears on the left providing the following policy objects that you can add to your rules:



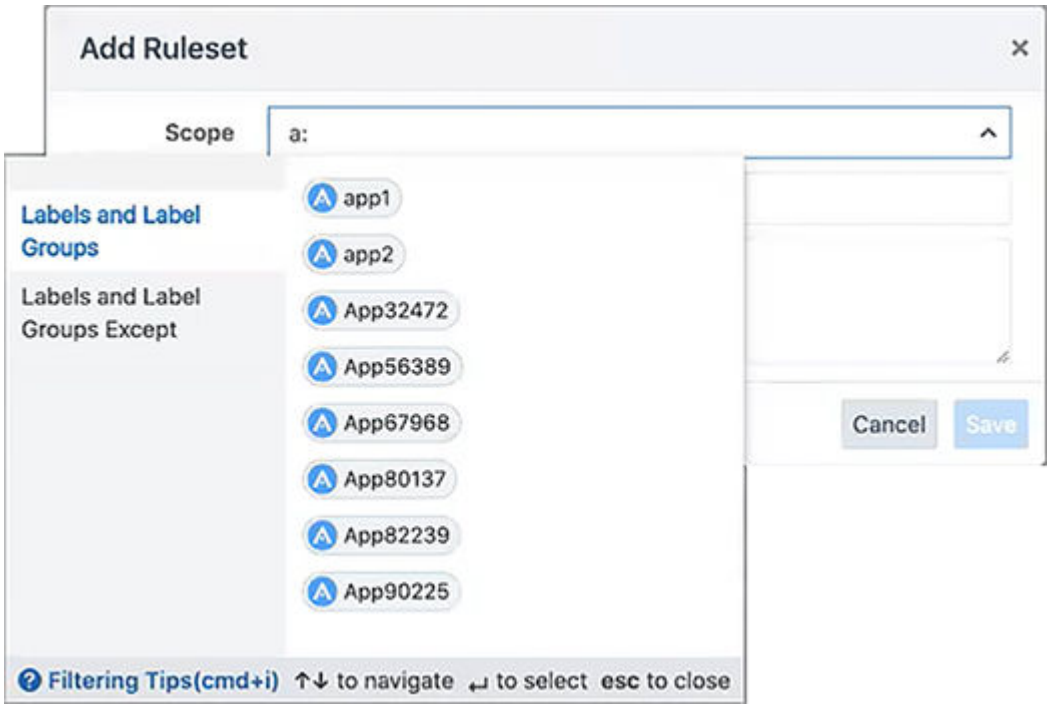

In Advanced Options, you can also select *Use Workload Subnets* and *Container Host* options for Consumers and *Use Workload Subnets* and *Virtual Servers* for providers.

## Enhanced Filtering Support for Labels

It's not uncommon in customer environments to find an Application label and a Role label, for example, with the same name. To provide added usability, the PCE web console in this release includes icons before the label types.




In addition, you can be more explicit in what you want to specify by prefacing what you're typing with an "a," "e," "l," or "r" and a colon before you start typing in names.




## Enforcement Boundaries in the Illumination Map

The Illumination map now displays traffic blocked by Enforcement Boundaries.

In previous releases, you could detect that traffic was blocked in Illumination; however, the map did not distinguish between traffic that was blocked because of full enforcement or because an Enforcement Boundary was in place.

## Single Pane of Glass and Scale

The Single Pane of Glass and Scale feature is a method of writing policy for endpoints so the PCE can scale its support of workloads from 5,000 (1,000 servers and 2,000 endpoints) to 25,000 workloads. In previous releases, Illumio Core supported up to 5,000 VENs for the Single Pane of Glass Feature.

## Traffic Flow Query Report

You can generate, schedule, and email reports which are based off saved and recent filters from Explorer for reporting. The report can be downloaded as a CSV file.

## Configurable Time for Heartbeat Warning Events

You can change the 15-minute threshold for the time the VEN goes without a heartbeat and goes into the Warning state.

## VEN Firewall Script Logging

Before this release, logging scripts did not log much information which resulted in unnecessary time to debug environmental issues. In this release, the Illumio scripts log all errors and other key information into `platform.log`. This will reduce the amount of time it takes Illumio to debug issues.

## PCE Platform Enhancements

The following enhancements were added to existing features in Illumio Core 22.2.0.

## Disable and Enable Enforcement Boundaries

In the Enforcement Boundaries list page and the Enforcement Boundary detail page, Enable and Disable buttons have been added. You can enable or disable one or more enforcement boundary rules by selecting them on these pages and clicking the button.

## Illumio Core REST API in 22.2.0

The Illumio Core REST API v2 has changed in 22.2.0 in the following ways.

## New Public APIs

### New Schema to Workload Notifications

Customers asked to be able to control when they get alerted about missing agents, as well as to have this control be separate from the policy offline timer. They might have a relatively high offline timer but a short warning threshold.

This change allows the customers to set explicit thresholds when they want a warning sent as well as its severity.

- `settings_workload_notifications.schema.json`: This new schema has additional properties: `info` and `error`.

Here is the new schema part that defines warning and error:

```
["end_user_private_perm"]
    },
    "warning": {
      "description": "Workload disconnect warning timeout",
      "type": "integer",
      "minimum": -1,
      "maximum": 2147483647
    },
    "error": {
      "description": "Workload disconnect error timeout",
      "type": "integer",
      "minimum": -1,
      "maximum": 2147483647,
"expose_to": ["end_user_private_perm"]
```

## Changed Public APIs

### SAML Configuration Changes

### GET /api/v2/authentication_settings_saml_config

Changes to this API apply to two properties, where `issuer_url` was deleted and replaced with the `issuer` property.

```
"properties": {
    "issuer": {
    description": "The URL for the Illumio login server.
    Some identity providers might need this to establish the
    identity of the service provider requesting authentication.",
    "type": "string"
```

The two properties have the same meaning.

### Reports Changes

The APIs for the endpoints

- `/api/v2/orgs/:xorg_id/report_schedules`
- `/api/v2/orgs/:xorg_id/reports`

have been changed for saved query explorer reports as follows:

### GET /api/v2/report_schedules

This API has two new properties:

- `scheduled_at`: which provides the timestamp to return the scheduled time.
- `send_by_email`: which defines whether to send the report via email.

Here are the two new properties:

```
{
    "properties": {
    "scheduled_at": {
      "description": "Timestamp in UTC for report generation",
      "type": "string",
      "format": "date-time"
    },
    "send_by_email": {
      "description": "Flag for whether to send user report by email",
      "type": "boolean"
    }
}
```

### POST /api/v2/report_schedules

This API has three new properties:

- `send_by_emai`l: defines whether to use email)
- `cheduled_at`: timestamp for report generation at a specific time
- `report_generation_frequency`: in addition to daily, weekly, monthly, and quarterly reports, you can schedule to receive the report only once.

Here are the new properties:

```
properties": {
    "send_by_email": {
    "description": "Flag for whether to send user report by email",
```

```
    "type": "boolean"
    },
    "scheduled_at": {
    "description": "Timestamp in UTC for report generation",
    "type": "string",
    "format": "date-time"
    },
    "report_generation_frequency": {
    "enum": [
    ..............................
    "once"
    ]
    ]
}
```

### GET /api/v2/reports

and

### POST /api/v2/reports

These two APIs have a new property `send_by_email`, which defines whether to use email for sending reports.

Here is the new property:

```
{
    "properties": {
    "send_by_email": {
    "description": "Flag for whether to send
user report by email",
    "type": "boolean"
    }
}
```

### Security Policy Changes

### Enable or Disable Enforcement Boundaries

Security policy APIs have an additional property that enables or disables updating of a request executed against the specific enforcement boundary object. These changes provide an ability to enable/disable an enforcement boundary rule, which is used for troubleshooting and to add a baseline capability for pre-packaged boundary rules.

The following schema files are updated by adding a description for the new `enabled` boolean field.

- `/api/v2/orgs/:xorg_id/sec_policy/:version/enforcement_boundaries`
- `/api/v2/orgs/:xorg_id/sec_policy/:version/enforcement_boundaries/:id`

The only change is the additional enabled field in the response.

### POST /api/v2/orgs/:xorg_id/sec_policy/:version/enforcement_boundaries

The optional enabled boolean field can be provided in the payload. If it is not provided, the newly created enforcement boundary object is enabled by default.

### PUT /api/v2/orgs/:xorg_id/sec_policy/:version/enforcement_boundaries/:id

A single change to provide the optional boolean value for the enabled field in the payload is: `"enabled": true`

The new property `enabled` looks as follows:

```
{
    "properties": {
    "enabled": {
    "description": "Enabled flag",
    "type": "boolean"
    }
}
```

### Settings Changes

### settings_get.schema.json

### settings_put.schema.json

These APIs have been changed so that a new property `advanced_ruleset_display` was added, which can display rulesets in advanced mode.

```
{
    "properties": {
    "advanced_ruleset_display": {
    "description": "When true, the UI will display rulesets
in advanced mode. This means that scopes will be displayed
for any unscoped rulesets, including newly added rulesets.",
        "type": "boolean",
        "default": true
        }
    }
}
```

### settings_workloads_get.schema.json

### settings_workloads_put.schema.json

These APIs have been changed so that a new property `workload_disconnected_notification_seconds` was added:

```
{
    "properties": {
    "workload_disconnected_notification_seconds": {
    "$ref": "settings_workload_notifications.schema.json"
    }
    }
}
```

### Other Changed APIs

### slbs_get.schema.json

A new property `status` was added, which describes the SLB status that can be `error`, `pending connection`, or `active`.

The SLB get_collection API can be filtered by the following:

- `name`
- `description`
- `has_virtual_server`
- `status`: this is a new property that can be `active`, `pending`, or `error`.
  For the HA pair case, if either one device is in `error`, then the SLB has the status `error`. If neither device is in `error` and one device is `pending`, the SLB has the status `pending`. The SLB has the status `active` if neither device is in `error` or `pending` connection state.
- device type - this is a dynamic list of values (requires facet API)

- number of devices

```
{
    "properties": {
    "status: {
    "description": "Status of the SLB: error, pending
connection, or active. In an HA pair, the status will be
pending connection or error if either device is pending
connection or error.",
    "type": "string"
    }
    }
}
```

### resource_canonical_representations.schema.json

Three new properties have been added to describe `LOG_INFO` level notification, `LOG_WARNING` level notification, and `LOG_ERR` level notification for workloads going offline.

When a VEN does not contact the PCE within a set time interval, it is marked as being offline. Previously, before that happened, a notification was created when the VEN was AWOL (missing) for 25% of the offline time.

These three new optional settings generate different levels of notifications at different intervals so the user can customize the timing and levels of notification.

```
{
"oneOf": [
.....................................
    {
    "workload_setting": {
    "type": "object",
    "properties": {
    "workload_disconnected_timeout_seconds":
{
    "description": "Disconnected timeout in seconds",
    "type": "integer"
    },
    "workload_goodbye_timeout_seconds": {
    "description": "Goodbye timeout in seconds",
    type": "integer"
    },
    "workload_disconnect_notification_info": {
```

```
    "description": "Threshold in seconds for LOG_INFO
level notification of a workload going offline",
    "type": "integer"
    },
    "workload_disconnect_notification_warning": {
    "description": "Threshold in seconds for LOG_WARNING
level notification of a workload going offline",
    "type": "integer"
    },
    "workload_disconnect_notification_error": {
    "description": "Threshold in seconds for LOG_ERR
level notification of a workload going offline",
    "type": "integer"
    }
   }
}
.........................................
```

## What's New and Changed in Release 22.2.1

Illumio Core 22.2.1 introduces the following new features and enhancements.

**IMPORTANT**

Illumio Core 22.2.1-PCE is available for Illumio Core On-Premises customers.

### Illumio Core 22.2.1 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 22.2.1 solved software and security issues to refine the software and improve its reliability and performance.

For more information about the Illumio software release types and software support, see Versions and Compatibility on the Illumio Support portal (login required).

## What's New and Changed in Release 22.2.10

Illumio Core 22.2.10 introduces the following new features and enhancements.

**IMPORTANT**

Illumio Core 22.2.10-PCE is available for Illumio Core On-Premises customers only.

The 22.2.10-VEN is available for both Illumio Core On-Premises customers and Illumio Core Cloud customers.

## Illumio Core 22.2.10 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 22.2.10 solved software and security issues to refine the software and improve its reliability and performance.

For more information about the Illumio software release types and software support, see Versions and Compatibility on the Illumio Support portal (login required).

## New Features in Illumio Core 22.2.10

### PCE Replication and Failover

To increase reliability, you can set up replication and failover for PCEs. Having a PCE on "warm standby," ready to take over if the active PCE fails, contributes to a resilient disaster recovery (DR) plan.

For PCE replication and failover, set up PCEs in pairs. Each pair has an active PCE and a standby PCE. A combination of continuous real-time replication and periodic synchronization is used to keep the standby PCE's data up to date with the active PCE. If the active PCE fails, the standby PCE can take over and become the new active PCE.

### Reassign a NEN from one PCE to Another in a Supercluster through CLI or API

You can move a NEN from one PCE to another PCE in the same supercluster using either a command line or through the API. When a NEN is moved in this way, associated Server Load Balancers maintain policy for managed virtual servers. After the PCE database is restored, the moved NEN remains connected to the new PCE. For details on reassigning a NEN from one PCE to another in a Supercluster using either method.

## Enhancements in the Illumio Core REST APIs

Illumio Core 22.2.10 introduced the following new public experimental REST API.

### Update the NEN with a New Target PCE hostname

`/api/v2/orgs/<org-id>/network_enforcement_nodes/<uuid>`

Use the following payload:

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "description": "Update a NEN's target PCE.",
  "type": "object",
  "additionalProperties": false,
  "properties": {
    "target_pce_fqdn": {
      "description": "cluster FQDN for target PCE",
      "type": "string"
    }
  }
}
```

## What's New and Changed in Release 22.2.20

Illumio Core 22.2.20 introduces the following enhancements.

**IMPORTANT**

Illumio Core 22.2.20-PCE is available for Illumio Core On-Premises customers only.

The 22.2.20-VEN is available for both Illumio Core On-Premises customers and Illumio Core Cloud customers.

### Illumio Core 22.2.20 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 22.2.20 solved software and security issues to refine the software and improve its reliability and performance.

For more information about the Illumio software release types and software support, see Versions and Compatibility on the Illumio Support portal (login required).

## What's New and Changed in Release 22.2.3

Illumio Core 22.2.3 introduces the following new features and enhancements.

**IMPORTANT**

Illumio Core 22.2.3-PCE was initially available for Illumio Core Cloud customers only. However, the issues resolved in this release are available in later 22.2.x releases for Illumio Core On Premises customers.

### Illumio Core 22.2.3 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 22.2.3-PCE solved software and security issues to refine the software and improve its reliability and performance.

For more information about the Illumio software release types and software support, see Versions and Compatibility on the Illumio Support portal (login required).

## What's New and Changed in Release 22.2.30

Illumio Core 22.2.10 introduces the following enhancements.

**IMPORTANT**

Illumio Core 22.2.30-PCE is available for Illumio Core On-Premises customers only.

The 22.2.30-VEN and 22.2.31-VEN are available for both Illumio Core On-Premises customers and Illumio Core Cloud customers.

### Illumio Core 22.2.30 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 22.2.30 solved software and security issues to refine the software and improve its reliability and performance.

For more information about the Illumio software release types and software support, see Versions and Compatibility on the Illumio Support portal (login required).

## What's New and Changed in Release 22.2.40

Illumio Core 22.2.40 introduces the following enhancements.

**IMPORTANT**

Illumio Core 22.2.40-PCE is available for Illumio Core On-Premises customers only.

The 22.2.40-VEN is available for both Illumio Core On-Premises customers and Illumio Core Cloud customers.

### Illumio Core 22.2.40 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 22.2.40 solved software and security issues to refine the software and improve its reliability and performance.

For more information about the Illumio software release types and software support, see Versions and Compatibility on the Illumio Support portal (login required).

### New Feature in 22.2.40

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

### Documentation Update for Core 22.2.40

The PCE Installation and Upgrade Guide for Core 22.2 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 22.2.44

### Illumio Core 22.2.44-PCE LTS Maintenance Release

Illumio Core 22.2.44-PCE includes an updated version of the PCE. 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 22.2.44-PCE solved a security issue for the PCE to refine the software and improve its reliability and performance.

For the complete list of improvements and enhancements to the PCE in Illumio Core 22.2.44, see Resolved Security Issue in 22.2.44-PCE [21].

# Illumio Core Release Notes 22.2

## Welcome

These release notes describe the resolved issues and known issues for the Illumio Core 22.2.*x* releases.

Illumio Core 22.2 is available for Illumio Core-PCE On-Premises customers. Illumio Core-VEN is available for both Illumio Core Cloud and On-Premises customers.

**Document Last Revised:** May 15, 2024

**Document ID:** 14000-100-22.2.45

## 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.

## What's New in This Release

To learn what's new and changed in 22.2, see the What's New in This Release guide.

**PCE Version:** 22.2.42

**VEN Version:** 22.2.45

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 Issue in 22.2.45+A1-VEN

- **Combination of factors caused policy sync failure on REHL 9.x OS VENs** (E-115693)
  Policy sync failed and an error was thrown when the PCE applied custom iptable rules to VENs installed on REHL 9.X OS (or later) workloads with iptables-nft-1.8.10 package. The issue stemmed in part from invalid syntax introduced by iptables-nft-1.8.10. This issue is resolved on 22.2.45-9201 VENs and later.

## Resolved Issues in 22.2.45-VEN

- **VENs fail to communicate after VEN upgrade in some cases** (E-109759)
  When a VEN paired to a 22.5.30, 22.5.31, 23.2.10, or 23.2.11 PCE is upgraded to a previous 22.2.x VEN version, the VEN loses connectivity with the PCE. This is resolved in this VEN version. For additional important details, log in to Illumio Support and see the Knowledge Base article Upgraded VENs fail to communicate with the PCE due to an API version mismatch issue .
- **False nftables firewall tampering error** (E-109623)
  In some cases, on operating systems using nftables, a false positive firewall tampering error is reported on enforced workloads with FQDN rules. This issue is fixed.
- **Agent Manager process crash on VENs using Kerberos** (E-109606)
  When Kerberos was used for VEN-PCE authentication, a VEN process (Agent Manager) could crash after the VEN was upgraded from an older version, or after the VEN was restarted. The crash occurred due to a defect in the VEN code, due to which a NULL pointer was dereferenced. This issue has been fixed in this release of the VEN.

## Resolved Security Issue in 22.2.44-PCE

### Illumio Core 22.2.44-PCE LTS Maintenance Release

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 Core 22.2.42-PCE

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

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

## Issue Resolved in 22.2.43-VEN

- **VENs using Kerberos authentication couldn't sync with the PCE after a policy change** (E-107799, E-107367)
  Kerberos authentication of the VEN with the PCE could fail and the VEN couldn't sync after a policy change or when the PCE refreshed the agent token. The PCE rotates the agent token every 7 days. The VEN logged 401 errors for a token mismatch when this occurred. This issue is resolved. VENs using Kerberos authentication with the PCE no longer fail to sync with the PCE after a policy change or when the PCE refreshes the agent token.

## CloudLinux support in 22.2.42-VEN

Illumio Core 22.2.42-VEN is a limited availability (LA) release for Illumio Core Cloud only.

This LA release introduces CloudLinux support for the VEN. The VEN now supports CloudLinux OS 6, 7, 8, and 9.

## Resolved Issues in 22.2.40

### PCE Platform

- **Agent background service CRITICAL alerts in PCE Health page** (E-100083)
  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.
- **Misconfigured PCE could cause sensitive information to be disclosed in log files** (E-96079)
  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 security 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 do not expose integer IDs; therefore, they did not populate the `duid`in CEF events. This issue is resolved. If an entity has a UUID, it will be returned for the CEF `duid.`
- **Consul messages not sent to internal syslog** (E-90286)
  This PCE Platform issue applies to Illumio Core On-Premises customers only. It does not apply to Illumio Core Cloud customers. 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`.

### Data Experience

- **Adding rules from Explorer but proposed deletion of other unrelated rules in the ruleset** (E-99603, E-94684)

Sometimes when adding a rule to an existing ruleset in Explorer, a completely unrelated rule was proposed for deletion. This issue is resolved. Illumination properly creates by default a new Windows Service only if a mapped service is not already provisioned.

- **Time filter not working 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 was not returned for that week, making the query invalid. This issue is resolved.

## PCE Web Console

- **Workloads Processes tab did not 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 did not carry over the rule notes** (E-96154)
  When a ruleset was duplicated, the replica did not contain the rule notes. This issue is resolved.
- **Filtered searches for workloads on the Virtual Servers page returned 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.

## REST API

- **Workloads list page and Vulnerability tab showed different values for Syncing and N/A** (E-71689) Users might get confused when the workload list page showed as Syncing and the workload vulnerability tab showed as N/A. This issue is resolved. The UI now reads the state from the response and properly presents it.

## UI Platform

- **Changes to enforcement mode of multiple workloads were not shown in the event log** (E-98343, 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.
- **Intermittent Error "Unable to Edit Enforcement Boundaries Rule"** (E-94530) The blocked connection count query was taking a long time and customers started editing the rule before the query was done. This issue is resolved. Queries that are still not finished are repeatedly checked in the background and deleted after they finish, so it doesn't affect using the application for a client.

## Policy

- **Rule coverage for endpoints was timing-dependent** (E-96488)
  Endpoints did not correctly display allowed connections. This was caused by the transient nature of the endpoint's network affiliation. Rules are evaluated if two workloads are co-resident on a network. This issue is resolved. A missing network on an endpoint is now interpreted as being on the same network.

- **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 did not lead to policy updates on workloads paired to other PCEs in the Supercluster This issue is now resolved.
- **Incorrect policies on workloads for Avi load balancer** (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

- **Adding rules from Explorer but proposed deletion of other unrelated rules in the ruleset** (E-94684)

  Sometimes when adding a rule to an existing ruleset in Explorer, a completely unrelated rule was proposed for deletion. This issue is resolved. Illumination properly creates by default a new Windows Service only if a mapped service is not already provisioned.
- **Add Rule panel didn't update on right-click for each traffic selection** (E-89343)

  After it was opened for a traffic selection, the Add Rule Panel didn't refresh for another traffic selection. This issue is resolved.

## VEN

- **Frequent nft table tampering warnings** (E-100010)

  On VENs using nftables 1.0.0 or later, tampering events occurred every 10 minutes, even though no actual tampering occurred. This was caused by a change in nftables 1.0.0. This issue is resolved. The VEN now responds correctly, no matter whether the nftables version is earlier or later than 1.0.0.
- **Failure 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 command line (for example. using RPM). The 22.2.40 PCE allows the installation of the 22.2.40 VEN bundle.
- **Endpoint VEN in IDLE mode reported tampering event** (E-98389)

  When the Windows VEN was switched to Idle mode, it could incorrectly report firewall tampering events. This issue is resolved in the 22.2.32 Preview build.
- **(Solaris) VEN could incorrectly report firewall tampering** (E-96755)

  The VEN used basic optimization (the default) to load the firewall rules into packet filter. As a result, the rule order could be unpredictable and the VEN could incorrectly detect and report firewall tampering. This issue is resolved. In this release, the VEN no longer uses basic optimization to load firewall rules. Without optimization, the original rule order is maintained. The optimization no longer causes the VEN to incorrectly detect firewall tampering.
- **(Solaris) VEN failed to apply policy on workloads running ICMPv6 services** (E-95140)

  Due to an issue with the way the VEN processed ICMPv6 services on Solaris workloads, the VEN couldn't apply policy from the PCE to those workloads. This issue is resolved. In this release, the VEN can now process ICMPv6 types correctly. Applying policy from the PCE with these workloads is no longer an issue.
- **Compatibility report (problem 2) nftables / RHEL 8** (E-91481, E-92482)

  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.

## 22.2.32-VEN Release

### Resolved Issues in 22.2.32-VEN

PCE 22.2.32-VEN is available for both Illumio Core Cloud customers and Illumio Core On-Premises customers.

- **(Windows) Issue with VEN deactivate command** (E-98628)
  The VEN `deactivate` command could fail when run under certain conditions, such as the VEN had pending flow data to send to the PCE when the command was run. This issue is resolved.
- **Endpoint VEN in IDLE mode reported tampering event** (E-98389)
  When the Windows VEN was switched to Idle mode, it could incorrectly report firewall tampering events. This issue is resolved.
- **On Oracle RAC RHEL 7.7, VEN reported multiple tampering events** (E-97636)
  The VEN incorrectly reported tampering events when co-existence mode was used. This issue is resolved.

### Security Issue in 22.2.32-VEN

- **OpenSSL upgraded to address CVE-2022-3602 and CVE-2022-3786**
  The openssl package was upgraded to 3.0.7 to address CVE-2022-3602 and CVE-2022-3786 (https://www.openssl.org/news/secadv/20221101.txt).

## Resolved Issues in 22.2.31-VEN

**IMPORTANT**

PCE 22.2.31-VEN is available for both Illumio Core Cloud customers and Illumio Core On-Premises customers.

- **(Windows) WMI subsystem could consume more CPU** (E-97713, E-97451, E-96841, E-88784)
  Known issues in Windows applications can cause handle leaks in the WMI provider (wmiprvse.exe) process and CPU consumption to raise. This behavior is expected. However, a VEN feature introduced in Illumio Core 21.5.0 can exacerbate this situation. The feature "Run As as a Different User" for Illumio Adaptive User Segmentation can increase CPU consumption even more when handle leaks occur. This issue is resolved. In this release, Illumio has disabled the "Run As a Different User" feature on Windows workloads.

# 22.2.30+A2 Release

This release is intended for customers who want to adopt the Illumio Core with Common Criteria certification. No new product features have been added in this release. Some changes were made for security purposes, which are listed below.

## Security Information

- **Default minimum password length increased to 16 characters**
  For the Common Criteria enabled version of the PCE, the default minimum required password length is increased to 16 characters from the previous 8 characters, with an acceptable length of 16-64 characters.
- **activerecord upgraded to v6.1.7.1**
  Rails gems including activerecord were upgraded to v6.1.7.1 to address CVE-2023-22792.
- **consul upgraded to v1.13.2**
  consul was upgraded to v1.13.2 to address CVE-2021-41803 and CVE-2022-40716.
- **curl upgraded to v7.87.0**
  curl was upgraded to v7.87.0 to address CVE-2022-32221 and CVE-2022-35252.
- **fluentd upgraded to v1.15.3** fluentd was upgraded to v1.15.3 to address CVE-2022-39379.
- **loofah updated to v2.19.1** loofah was upgraded to v2.19.1 to address CVE-2022-23516.
- **nokogiri upgraded to 1.13.10**
  nokogiri was upgraded to 1.13.10 address CVE-2022-23476.
- **rails-html-sanitizer upgraded to v1.4.4** rails-html-sanitizer was upgraded to v1.4.4 to address CVE-2022-23520, CVE-2022-23519, CVE-2022-23518, and CVE-2022-23517.
- **sinatra upgraded to v2.2.4**
  sinatra was upgraded to v 2.2.4 to address CVE-2022-45442.

# Resolved Issues in 22.2.30

## PCE Web Console

- **Clicking Add Ruleset or Add Rules displayed an empty page** (E-95948)
  When you performed either of these steps, the PCE web console displayed an empty page:
  - Go to **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.
- **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.
- **Scopes unselectable in Add dialog if scrolling occurred** (E-93985)
  When adding a Ruleset and attempting to select a scope through the **Add** dialog box, users couldn't select scopes if they scrolled within the list, though it was possible to select scopes if no scrolling occurred. This issue is fixed and users can now both scroll and select scopes as expected.
- **Filtering issues in Rulesets** (E-93402)

It was not always possible to filter for certain labels in the consumer or provider fields. For example, searching for "R: Web" provided many results, but not the label "R: Web". In this example, R:Web was only available in recent searches but not in the search list. This issue is resolved.

- **Incorrect Group Label count is displayed while editing a group for a workload** (E-68691)
  This issue is resolved.

## Data Experience

- **Existing rulesets not used by default even when applicable scoped rulesets exist** (E-95143)
  Sometimes a previously selected ruleset caused a new ruleset to be created even though other rulesets with the correct scope already existed. This issue is resolved.
- **Explorer UI updated to include option to exclude IP list** (E-94737, E-94408) In this UI release, the Explorer page in the PCE web console now includes this option: **Exclude Workloads from IP List Query**. 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.
- **Drop-down lists and buttons are misaligned on the Explorer page** (E-81916)
  When selecting Draft View for an Explorer query, the drop-down lists and buttons above the query results were not correctly aligned with the columns in the results table. This issue is resolved.
- **Add Rule panel not displaying for selected traffic with right-click actions** (E-68548)
  When right-clicking on selected traffic and clicking Add Rule, the Add Rule panel should display for selected traffic. Instead of the current selection, it displayed the previous Add Rule panel for other selected traffic. This issue is resolved.

## Policy and Workloads

- **Unable to pair VEN with UI error "Invalid URI"** (E-95672) A customer was unable to unpair a VEN and was getting the UI error "Invalid URI". This issue is resolved.
- **Passenger error on `generate_exclusion_sets` when called from EM thread** (E-94452)
  In rare cases, the PCE returned a 502 error code when label exclusions were used in rules. This issue is resolved.
- **NEN: Multiple API requests to load balancers even when policy did not change** (E-93330) In some cases, the NEN received policy updates from the PCE and program them on the load balancers even if the policy did not change. This issue is resolved.

## PCE Platform

- **Leader PCE and cluster UI not responsive** (E-96151, E-95586)
  When logging in, the PCE was unresponsive and the PCE web console displayed the following error message:
  ```
  The PCE server seems busy to be reached, you could try again later or use another page in the meantime.
  ```

In large-scale deployments and dependent on customer usage patterns, Supercluster replication could slow down database performance and affect general PCE responsiveness. This issue is resolved. Illumio updated the Supercluster replication logic to address this performance issue.

- **A large`app_stats` log file (8GB and more) was continuing to grow** (E-95636)

  In some cases, frequent rotation of the app_metrics_stats files is preventing the rotation of the `app_stats/perflog` files.

  This issue is resolved.
- **Explorer and reporting failures when using user accounts with IP address restrictions** (E-94035) When a user with IP access restriction opened the Explorer page and performed a query, no traffic data was returned. This issue occurred in all areas of the UI that displayed traffic data, such as Explorer.

  This issue is resolved. Users with IP access restrictions can now view traffic data.
- **Curl upgraded to address CVE-2022-32206, CVE-2022-32207, and CVE-32208** (E-93416) The curl package was upgraded to 7.84.0 to address CVE-2022-32206, CVE-2022-32207, and CVE-2022-32208.

  The PCE is not impacted by these vulnerabilities.
- **Editing scopes for Access Management displayed Role label group as a menu option** (E-90529)

  When editing the labels for scopes for access management (also called "role-based access control"), the menu incorrectly displayed the Role label group in addition to Application, Environment, and Location. The Role label group wasn't added to scope for access management. This issue is resolved.

## VEN

- **VEN loses connectivity after upgrade over VPN** (E-96155, E-94942)

  After upgrading to 21.5.30 and 22.5.0, the VEN lost connectivity, and all traffic was blocked. Due to the upgrade, the local policy format of the VEN changes and the upgraded VEN was unable to recognize the old policy. The VEN needs to communicate with the PCE to refresh the policy. Because the upgrade was performed over a VPN (the PCE is only accessible over the VPN), when the VEN applies the old policy incorrectly, the local firewall dropped/blocked the VPN connection. Therefore, the VEN was unable to refresh the policy. This issue is resolved.
- **Compatibility report does not detect nftables rules** (E-94962, E-95407)

  After VENs with existing nftables set up for port forwarding were switched from Idle to Test mode, existing nftables (and port-forwarding rule) were removed. This issue is resolved. For systems with nftables, the compatibility report now displays the correct firewall rules counter.
- **Abrupt shutdown of RedHat VEN might cause 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 can 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 was labeled as "working as designed". Additionally, Knowledge Base article #3744 was provided with the title "LINUX VEN GOES TO ERROR STATE WHEN INSTALLED ON A SYMLINK".
- **(AIX) Workload process page not reporting all ports** (E-89116)

  Previously, the VEN only reported services listening on IPv4 sockets. The PCE web console did not display services listening on IPv6 sockets in the Workload Process page. This issue

is resolved. In this release, the VEN reports services listening on IPv6 sockets and the PCE now displays them in the UI.

### REST API

- **Events API: Missing information for Access Restriction** (E-82044) Exception error reporting, which was causing the UI not to receive the bad/invalid IP in the response, was resolved.

## Resolved Issues in 22.2.20

### PCE Web Console

- **Enforcement Boundaries page not showing EB rules** (E-93640)
  The Enforcement Boundaries page did not show the Enforcement Boundaries rules when the filter "No Label Type" was applied on Workloads or VENs (such as when "No Application Labels" or "No Rule Labels" were applied in workload/ven). This issue is resolved.
- **RBAC Rule manager is broken in 22.2.x** (E-93575)
  In release 22.2.x, if RBAC users had both a global and a scoped role then they were unable to create a ruleset because the scope must be specified and this field was hidden when creating a ruleset.
- **Ctrl+left-click not opening a tab in Firefox** (E-92978)
  The ctrl+left-click action on a link did not open a tab in the background when using Firefox. This issue is resolved.
- **Rulesets and Rules: Unable to add "Location" or "Environment" label in Scope** (E-92557)
  While editing the scope of the ruleset, users were unable to add the labels of a label type that was used in the consumers of an extra-scope rule. This issue is resolved. Labels of a label type that is used in the consumers of an extra-scope rule now are available to add in scope.
- **Issues with Recently Used Objects in Selector** (E-89969) The Recently Used objects in Selector did not work properly. This issue is resolved.
- **UI not displaying metric entries properly** (E-89362)
  The UI did not display entries of the same metric in a different row. This issue is resolved.

### Data Visualization

- **Explorer UI updated to include option to exclude IP list** (E-94737, E-94408)
  In this UI release, the Explorer page in the PCE web console now includes this option: **Exclude Workloads from IP List Query**. 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.
- **Explorer is not responsive with JS errors. No explorer flows displayed** (E-93720, E-93674)

If a flow was reported as 'Unknown' (usually for the first packet of an FQDN flow) but there was also an enforcement boundary that matched the flow, Explorer was displaying an error. This issue is resolved.

- **Explorer query results were not correctly sorted by last seen timestamp** (E-93705, E-93678)

  Sometimes the flow data in Explorer query results were not correctly ordered by time. This issue is resolved.
- **Traffic Database Summary Showing Zero for PCE Health** (E-93648)

  The Traffic Database Summary was showing Zero for PCE Health by mistake.

  This issue is fixed and the summary is displayed properly.
- **Add support for `src_port` collector filters** (E-93509)

  It was requested to add support for the src-port collector filters:
  - To extend the current collector filters to support the scr_port
  - To provide API-only support initially, with UI support to follow.

    This issue is resolved.
- **Missing labels when creating rules with app group maps** (E-92929)

  Some labels were missing when a user created rules using the app group maps. This issue is resolved after the system in extra-scope cases stopped removing the duplicate labels from the scope of the ruleset.
- **Incorrect value for the number of flow days available during rollups** (E-92042)

  When weekly rollups were enabled, and there was data with only a partial week in it, the number of flow days was incorrectly calculated. This issue is resolved.
- **Remove count value from scope** (E-88833)

  In rules with multiple scopes, label count no longer appears. Previously in Explorer Proposed Rules, in rules with multiple scopes, Illumio displayed a tally of the number of labels specified in the rule. The tally has been removed, in part because if Policy Exclusions are defined, an accurate tally is impossible to calculate.

## Policy and Workloads

- **Removing FQDNs from IP list does not remove FQDN from policy** (E-94243)

  If an FQDN address was removed from an IPList, the FQDN incorrectly still remained in policy and the VEN still was programmed with the FQDN address. This issue is resolved.
- **IP Exclusion calculated incorrectly with fully overlapped inclusion IPs** (E-93830)

  In some cases, when a subnet or IP range in an IPList was fully contained within another subnet or IP range in the same IPList -- and exclusion IPs, ranges, or subnets were also specified -- the exclusion might not take effect. This issue is resolved.
- **SecureConnect failed** (E-90747)

  Connections using SecureConnect did not work between VENs versions before 21.2.*x* and after versions 21.2.*x*. This issue is resolved. SecureConnect connection between VENs with these release versions work in this release.
- **Policy revert of a VS without underlying DVS should be prevented** (E-87830)

  If a discovered virtual server was managed (that is, a virtual server policy object was created against it), and the DVS was removed from the device independently of the PCE, the VS changed to a deletion pending state. The VS deletion should be provisioned at this time. But if the VS was instead reverted, issues could occur because both VS and DVS were assumed to exist. This issue is resolved. These VS deletions are now prevented.
- **Discovered Virtual Servers are in pending deletion state on PCE** (E-83175)

  In rare cases in which the NEN received an unexpected error from the load balancer device during Virtual Server discovery, the Virtual Server could remain in the “Deletion Pending” state on the PCE even after the device did not return an error. This issue is resolved.

Now, on the next successful Virtual Server discovery loop, the “Deletion Pending” state is removed from the Virtual Server on the PCE if the device remains present.

## PCE Platform

- **Support Bundle download gives 502 error** (E-91480)
  This issue is now fixed.
- **Support report used configuration files instead of the PCE for reporting limits** (E-91348)
  The PCE support report previously reported limits based on configuration files instead of the PCE. The PCE support reports now report limits as seen by the PCE itself. This issue is resolved.
- **PCE Health page displayed confusing warnings about PCE node disk size** (E-91283)
  The **PCE Health** page displayed warnings that the disk sizes of the PCE nodes were below the minimum PCE requirements and the **Node** tab indicated that the node specs were below requirements. For example, the page could display a warning that a data node didn't have the expected 51200MB minimum data disk size when the data disk was actually 32748MB. This issue is resolved. The PCE health check wasn't correctly taking into account all disk partitions when calculating the minimum disk sizes. This issue is resolved. The PCE Health page now calculates the PCE node disk sizes based on all device partitions.

## VEN

- **Support for OpenVPN to VEN** (E-94079)
  Before this fix, Windows VEN only reported interfaces of the type `IF_TYPE_ETHER-NET_CSMACD`. This issue has been resolved. With this change, VEN reports on interfaces as long as the media type is 802.3.
- **EventService connection not working when using Self-Signed Cert** (E-93870)
  The EventService connection does not work when using the Self-Signed Certificate. This issue is resolved, and the EventService connection works as expected.
- **Intermittent drops to FQDN** (E-93564)
  FQDN-based rule with nftable failed to rehydrate when a policy was updated. This issue is resolved.
- **RHEL 8.4 and 8.5 VEN reporting continuous tampering alerts** (E-93264)
  When the VEN firewall mode is changed from exclusive to primary coexistence, numerous tampering alerts may be triggered when the VEN checks the firewall every 10 mins. This issue has been resolved. VEN now compares the NFT ruleset to the correct table.
- **VEN reporting ignored interfaces immediately** (E-93135)
  In 20.x release and in an enforced Microsoft cluster, IPv6 traffic for a clustering service became blocked when IPv4 traffic with the same specifications was also allowed by the rules. To ignore tunnel interfaces in an enforced Microsoft cluster, you must allow enforcement. Unfortunately, after a reboot, the ignored interfaces temporarily blocked traffic, and the cluster temporarily went offline. This issue has been resolved. The VEN-ignored interfaces are reported to the PCE as soon as they are connected to the VEN.
- **Tampering events appear in RHEL 6 after upgrade to 21.2.0** (E-88718)
  Upgrading VEN into 20.2.0 or later may trigger firewall tampering events. This issue is resolved.
- **Avoid use of symbolic links for generating support reports** (E-85348)
  To avoid consuming unnecessary disk space on the VEN, the support report generation logic has leveraged symbolic links to represent many of the files included in the final zipped report. While the report is generated, until it is zipped, there exists a temporary "write-through" hazard by which a third party might execute the `chown` or `chmod` commands

against the filesystem where the VEN resides. This might result in unintended changes in ownership/ACL of the targets of the symbolic links. In rare cases, the support report can be aborted, leaving it unzipped, thereby making the temporary hazard long-lived. This issue is resolved.

### Supercluster

- **Moving VENs between regions caused data inconsistency** (E-93594)
  When VENs on Region A were moved to Region B, such as for a VEN migration or DNS move, data inconsistency issues could occur if there was a significant delay in replication from Region A to Region B. Changes from Region A were not replicated to Region B, and the VENs created missing changes in Region B. Later, when pending replication data from Region A was sent to Region B, data conflicts could occur, because duplicate data may have been created in both regions. Supercluster replication did not deal with conflict resolution correctly. This issue is resolved. Such a conflict is now resolved by supercluster replication.
- **Replication lag kept increasing** (E-95136)
  In a PCE supercluster, the replication lag between the leader PCE and member PCE for the policy database sometimes kept increasing. This issue arose because supercluster replication can encounter a conflict when it tries to synchronize data across multiple regions. To resolve such a conflict, the PCE makes queries on the local data to compare it to the incoming data from another region. The issue with increasing replication lag occurred because the query buffer size was fixed, which could cause a buffer overflow. This issue is resolved. Dynamic buffer size is now used.
- **OpenSSL upgraded to address CVE-2022-1292 and CVE-2022-2068** (E-93128) The OpenSSL package was upgraded to 1.1.1q to address CVE-2022-1292 and CVE-2022-2068. The PCE is not impacted by this vulnerability.

## Resolved Issues in 22.2.10

**IMPORTANT**

Illumio Core 22.10-PCE is available for Illumio Core On-Premises customers only.

### PCE Web Console

- **Enter key on Add New Service option not working** (E-91063)
  The Enter key on Add New Service option in the service selector did not work. This issue is resolved.
- **Rulesets and Rules: Change not reflected after editing the draft ruleset** (E-90218)
  Changes did not reflect after users edited the fields 'Name' and 'Description' of the Draft Ruleset. This issue is resolved.
- **Selector was not expanding or scrolling correctly** (E-90188)
  The selector tool did not expand or scroll correctly when many labels were selected at a lower screen resolution. This issue is resolved.
- **Deletion Pending Rule: Checkbox and Edit drop-down enabled by mistake** (E-90077)

Deletion Pending Rule had the checkbox and Edit drop-down enabled by mistake. This issue is resolved.

- **New service was not showing in the Service selector** (E-89974)
  While editing a rule that contains "All Services," the newly-created service did not show in the Service selector, and the field "All Services" was not replaced. This issue is resolved.
- **'Idle' enforcement option displayed when adding a new container workload profile** (E-89899) 'Idle' enforcement option was displayed when users tried to add a new container workload profile. This issue is resolved.
- **UI filter for workloads with staged policy calls API incorrectly** (E-89324)
  The policy cannot be pushed to individually staged workloads in release 19.3.x. Upgrade to 21.5.x or later, including this release, where it is resolved.
- **VEN library filtering and sorting broken** (E-88577) VEN library filtering and sorting were broken and did not work permanently. This issue is resolved.

## Data Visualization

- **Explorer queries were slower in previous release** (E-91133)
  Some Explorer queries took a long time to complete after upgrading to release Core PCE 21.5.2. This issue is resolved, and queries now execute in the expected time.
- **In Explorer, an extraneous line appeared below some column headings** (E-90753) When viewing Explorer through the PCE Web Console, an extraneous underline appeared under headings in columns with multiple query parameters. This issue is resolved, and these lines no longer appear.
- **App Group workload count wasn't updated following refresh** (E-90693)
  In the **PCE Web Console > App Group Map**, after expanding a Connected App group and then refreshing the map, the Workload count wasn't recalculated as expected. It was necessary to collapse the group and refresh the map a second time for the Workload count to recalculate accurately. This issue is resolved. The map is recalculated as expected in these circumstances.
- **Explorer filters with OR provide inconsistent results** (E-90367)
  Explorer IPlist queries using OR incorrectly provided zero results. This issue is resolved. IPlist Explorer queries now produce proper results.
- **Traffic disappeared in App Group Map after map refresh** (E-90281)
  In the App Group Map, after expanding a connected app group and refreshing the map, traffic was no longer being displayed. This issue is resolved.
- **Scopes appear when advanced rule writing is off** (E-90266)
  In Illumination and Explorer, when advanced rule-writing mode is turned off, scopes were still visible even though they were not expected to be visible. This issue is resolved. The scopes no longer appear.
- **Core Services Detection couldn't run** (E-90231)
  A transient error prevented a data wrapper from being set up correctly; subsequently, the core services generator was not restarted because of faulty detection. These issues are resolved.
- **Clicking on the View Rule Link sometimes throws an error** (E-90143)
  When users clicked on the **Workload Traffic** panel > **IP Lists** > **View Rules**, the console sometimes threw an unexpected error. The workaround was to refresh. This issue is resolved. The error no longer appears.
- **Error when querying the IPList traffic** (E-90112)
  Explorer queries failed when using only IPLists in filters. This issue is resolved.
- **App Group V-E Scores reported erroneously** (E-89960) In some cases, the App Group list displayed a Vulnerability Exposure Score (V-E Score) greater than zero for app groups that had no vulnerabilities in the ports/protocols associated with the App Group's workloads.

This issue is resolved. App groups without vulnerabilities tied to specific ports/protocols in the group will report a V-E Score of 0.

- **View Rule panel not displayed properly** (E-89574)
  When users right-click to open the View Rule panel at the group level, the View Rule panel did not open as expected. This issue is resolved. The View Rule panel opens as expected.
- **Group Details panel showing an error** (E-89558)
  When two labels are assigned to a group and the user right-clicked Enforcement Boundary, the Group Details panel showed. This issue is resolved. The Enforcement Boundary panel now appears as expected.
- **The number of workloads reported was inconsistent** (E-88766)
  The number of workloads reported on the App Group Map sometimes differed from the number of workloads shown in the detailed popup window when the App Group was clicked. This issue is resolved. The detail panel always shows the first 500 of the total workloads that match the set of labels, whereas the count in the connected role is only the number of workloads connected to the focused app group. Clicking the 'Expand Connected Group' link loads all the details of the connected group, and the count in the role properly includes all workloads with the labels, matching the detail panel.
- **Extra Scope rules appear unexpectedly in App Group Rules tab** (E-87833)
  Extra scope rules defined only by a particular role appeared in the Rules tab of App Groups which didn't themselves contain the same role. This behavior was unexpected for some customers. This issue is resolved. Now, Extra Scope rules defined by a role will only appear in App Groups that contain the same role.
- **Save and Provision buttons appeared in error** (E-87243)
  For users with the Ruleset Manager role viewing a Ruleset in the PCE Web Console, the **Save** and **Provision** buttons were available and active. Because Ruleset Managers lack permission to save or provision ruleset changes, these buttons should not have appeared to them. This issue is resolved. The **Save** and **Provision** buttons no longer appear to users with the Ruleset Manager role.

## Policy and Workloads

- **Concurrent workload label updates caused errors** (E-90427)
  In rare cases, if the labels of the same workload were updated by concurrent requests, some update attempts might have received a 500 error. This issue is resolved.
- **PCE Health no longer includes authentication failures in failure percentage** (E-90325)
  The Health page in the PCE web console and the PCE Health API included authentication failures in heartbeat and policy failure percentages. This led to unnecessary alarm, as these requests do not put a significant load on the PCE. This issue is resolved. The status codes 401 and 403 are now excluded from failure percentages.
- **Unmanaged workload creation/deletion didn't always trigger policy changes** (E-89874)
  Under certain conditions, workload policy was not updated in response to changes to unmanaged workloads, including unmanaged workload creation and deletion. Usage of containers or other workloads with a short lifespan increased the likelihood of encountering this issue. This issue is resolved.
- **Labels were incorrectly marked as unused and could be deleted** (E-89189) Labels could be incorrectly marked as not in use by the workload, based on the status of the VEN. As a result, it was possible to delete the label if the VEN had a status other than Active. This issue is resolved.
- **Container Workload to Internet showed enforcement boundary in Illumination** (E-88534)
  In Illumination, when displaying traffic between container workloads and the Internet, an enforcement boundary was sometimes displayed even though the enforcement boundary was not being enforced on the container workload. This issue is resolved.

- **Filtering enforcement boundaries returns the 500 error** (E-88230) Filtering enforcement boundaries by name and service (by HREF) was returning the 500 error. This issue is resolved.
- **Workload object limit for unmanaged workloads not respected** (E-88160)

  The PCE did not respect the workload object limit when using bulk APIs to create unmanaged workloads. This issue is resolved.
- **Workloads synchronizing banner not working properly** (E-87593)

  In rare cases when the PCE is under load or PCE services were restarting, the banner showing the number of Workloads synchronizing did not work. This issue is resolved.

## PCE Platform

- **The remaining core node shut down in split cluster condition** (E-91893)

  Although it is rare, an invalid PID check of a service discovery process by service discovery monitor has caused service discovery to restart. This caused consul to lose quorum, which eventually caused the remaining core node to stop all the services. This prevented the system administrator from performing the split cluster repair procedure; see" Site Failure (Split Clusters)". This issue is resolved. The PID check has been fixed in the service discovery monitor.
- **PCE Support bundle failure with 21.5.21** (E-91132)

  When the database fails over, support bundle generation could go offline. Customers are advised to restart each node in order to reset the support bundle service.
- **Incorrect node spec messages displayed when features disabled** (E-90901, E-88248)

  When certain features were disabled, the PCE incorrectly displayed messages like "node specs are below PCE requirements." This indicated (incorrectly) that PCE nodes did not have sufficient resources to meet minimum requirements. This issue is resolved. The incorrect node spec messages are no longer generated.
- **Unvalidated redirect through the Referrer header** (E-89344)

  There was an unvalidated redirect through a Referrer header in `/login/users/password/update` which resulted in cross-domain Referrer leakage. This issue is resolved. The referrer header and other user inputs are now validated by the server that only allows headers coming from a PCE cluster. The Referrer header is a request header that indicates the site which the traffic originated from.
- **".public" workload interfaces should not be ignorable** (E-89290) Previously, the PCE allowed users to ignore PCE-generated `.public` interfaces on Workloads, which could cause unwanted behavior on the VENs. This issue is resolved. All PCE-generated interfaces are filtered from the ignored interface list before it is sent to the VEN.
- **Harmless time-drift threshold warning on the Health page for the PCE** (E-87425)

  If the local node clock was out-of-sync with the NTP time server beyond a threshold, then the health page displayed an appropriate warning on the PCE. The threshold value was too low and caused false alarms. This issue is resolved. The system has been reconfigured to increase the threshold to 384 ms to minimize the occurrences of these warning messages.
- **Trusted Proxy IP was not always used** (E-83012)

  The trusted proxy IP feature did not work for the initial VEN pairing. The VEN's actual IP address did not appear in the Public IP property of the workload and in the `agent.activated` event. Instead, the IP address of the load balancer, proxy, or whatever entity was performing NAT appeared. This issue is resolved. The VEN's actual IP address appears in all the appropriate places and events.
- **UPDATE calls that made no changes still generated events** (E-81227)

  In the REST API, an UPDATE call that did not make any change to resource data generated an event. This issue is resolved. These events are no longer generated.

## Supercluster

- **VENs did not fail back when original region recovered** (E-86195)
  When a region that had VENs paired went offline in a supercluster, and the load balancer configuration was updated to resolve the offline region to another region, the VENs continued sending heartbeats to the new region even after the original came back online. This issue is resolved. Now, unless action is taken to permanently migrate the VENs to the new region permanently, the VENs once again send heartbeats to the original region once it comes back online and the load balancer is reconfigured. VENs do not permanently move to a new region during failover.

## VEN

**IMPORTANT**
Illumio Core 22.2.10-VEN is available for both Illumio Core On-Premises customers and Illumio Core Cloud customers.

- **Support for OpenVPN to VEN** (E-94079)
  Before this fix Windows VEN only reported interfaces of type IF_TYPE_ETHERNET_CSMACD. This issue is resolved. With this change, VEN reports on interfaces as long as the media type is 802.3.
- **Replaced /opt/illumio_ven with INSTALL_PATH in openssl.cnf** (E-91789)
  The Core 22.2.0-VEN did not support installing or upgrading into a non-standard directory which prevented the VEN from configuring OpenSSL successfully. This issue is resolved. The VEN has been reconfigured with the installation paths to the OpenSSL configuration and the FIPS module configuration file. RHEL8 and Windows VENs were not affected by this issue.
- **Unauthorized VENs are causing frequent `request.authentication_failed` events** (E-98612, 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 is rejected, and the PCE emits `request.authentication_failed` events. This issue is resolved. The VEN no longer makes frequent requests to the PCE after receiving consistent authentication errors.
- **SQL cluster fails when enforced** (E-89580)
  When you set a Windows workload's network interface from being Managed to Ignored, the setting did not take effect. The interface was still being treated as Managed. This issue is resolved. The change from Managed to Ignored takes effect as expected.
- **Store the VEN certificate in a specific directory** (E-86768)
  Illumio supported the customer to specify the CA bundle/directory, but the `runtime_env.yml` file is no longer a safe public file for customers on Linux systems, AIX, Solaris, and SunOS system. This issue is resolved. Users can specify a trusted CA bundle/directory in `/etc/default/illumio-agent`. The `runtime_env.yml` file is no longer a place to store the path of the trusted CA bundle/directory.
- **[CentOS 8] Custom IPtables rule doesn't work with -j RETURN** (E-81317)
  After creating a custom rule on the PCE, the CentOS 8 VEN entered an error state because the VEN could not correctly handle the `-j RETURN` part of the command. This issue is resolved. The VEN now recognizes custom rules with the `RETURN` command.

## Resolved Issue in Core PCE 22.2.3+UI3

**IMPORTANT**

Illumio Core PCE 22.2.3+UI3 is available to Illumio Core Cloud customers only. However, not all Illumio Core Cloud environments are upgraded to this release. To locate your Cloud release version, go to the drop-down menu in the top-right bar of the PCE web console and view the About Illumio page.

- **Slow Explorer performance in 22.x** (E-95198, E-92070)
  Explorer slowed down after upgrading to a release 22.x. This issue is resolved.

## Resolved Issue in Core PCE 22.2.3+UI2

**IMPORTANT**

Illumio Core PCE 22.2.3+UI2 is available to Illumio Core Cloud customers only. However, not all Illumio Core Cloud environments are upgraded to this release. To locate your Cloud release version, go to the drop-down menu in the top-right bar of the PCE web console and view the About Illumio page.

- **Core Services Detection error when adding unmanaged workload** (E-92625)
  When adding an unmanaged workload to Core Services (**PCE web console > Core Services > Accept**), the PCE displays the message "Error: Workload does not exist." This issue is resolved.

## Resolved Issue in 22.2.3-PCE

**IMPORTANT**

Illumio Core 22.3-PCE is available to Illumio Core Cloud customers only. However, not all Illumio Core Cloud environments are upgraded to this release. To locate your Cloud release version, go to the drop-down menu in the top-right bar of the PCE web console and view the About Illumio page.

- **Explorer filters with OR provide inconsistent results** (E-92289, E-90367)
  Explorer IPlist queries using OR incorrectly provided zero results. This issue is resolved. IPlist Explorer queries now produce proper results.

# Resolved Issues in 22.2.1-PCE

- **Removing/Creating an unmanaged workload doesn't always trigger policy update** (E-89874)

  Under certain conditions, workload policy was not updated in response to changes to unmanaged workloads, including unmanaged workload creation and deletion. Usage of containers or other workloads with a short lifespan increased the likelihood of encountering this issue. This issue is resolved.
- **Spurious traffic and rules showing as blocked post-upgrade** (E-90685)

  Sometimes Explorer showed spurious reports of traffic blocked to non-existent services based on non-existent rules. This issue is resolved. When a Windows process-based rule allows traffic, the traffic is allowed outbound (off the client workload) regardless of the resulting destination process. Draft view in Explorer has been fixed to reflect this behavior.
- **Some flows do not report the Windows service and show Blocked for Windows service rules** (E-91016)

  Explorer sometimes showed incorrect Windows service information for some flows. This issue is resolved. When the VEN does not report complete information, Explorer now infers the Windows service name based on other observed flows.
- **Services in Explorer are mapped based on the port regardless of the process** (E-91017)

  Services in Explorer were being mapped incorrectly. This issue is resolved.

# Resolved Issues in 22.2.0

## PCE Web Console

- **In Firefox v98+, a group bubble border would not appear after certain actions** (E-88630)

  When viewing the Illumination Map using Firefox version 98 or higher, a group bubble border did not appear properly when navigating to the Group Details page and then back to the Illumination Map. This issue is resolved.
- **After selecting a non-default filter in Workloads and then typing, the default filter sometimes appeared instead** (E-87834)

  In the Workloads page, after selecting a non-default filter, and then starting to type, the filter occasionally reverted back to the default name filter. This issue is resolved.
- **Clicking traffic workload arrow displayed wrong panel** (E-86930)

  When right-clicking on a traffic workload arrow to Internet or IPList, the traffic panel was being shown instead of the expected Add Rule panel. This issue is resolved.
- **Surface last pairing key generation information** (E-83761)

  Previously, the PCE Web Console did not expose pairing information in the pairing profile API and UI. Now, for each pairing profile, the PCE Web Console shows on the pairing profile details page the following details:
  - The last time a pairing key was generated using this pairing profile
  - The last time a VEN was paired using this pairing profile
- **Warning message about discarding pending changes didn't always appear** (E-82420) If you clicked your browser's Back button when creating or editing a ruleset, the warning message "Are you sure? Leaving this page will discard pending changes" didn't appear. However, the message did appear if you attempted to navigate away from the page by clicking options in the PCE web console. This issue is resolved.
- **OPTIONS http verb sometimes failed authentication with 403 error** (E-79747)

When sending an http OPTIONS verb with a proper authorization header, authorization could fail on occasion with response status error 403. This issue is resolved.

- **PCE user interface displays the Program Name and Service Name on the same ports** (E-77450) Typically, as soon as the VEN is paired, on certain connections, the PCE user interface displayed both the Program Name and Service Name as using the same ports. For example, both the service name, `svchost.exe`, and the program name, TermService, seemed to be using port 3389. This issue is resolved.
- **Clicking deleted ruleset in Policy Versions showed "Resource Not Found"** (E-62929)
  In the PCE web console Policy Versions page, when you clicked the name of a deleted ruleset, the message "Resource Not Found" appeared. The message was correct but not very informative. With this release, instead of displaying a message to users, users are redirected to the deleted ruleset's details page where the **Provision Status** indicates **Deleted**.
- **Could not create a rule with a label type defined in the Scope** (E-59100)
  In the UI, you could not create a Rule with a label type that had also been used in the Scope. This issue is resolved. You can now select a label type (label/label group) which is used in scope.

## Data Visualization

- **Blocked traffic showing in the VRRP protocol** (E-89842) Filtering for ports and protocols by number in Illumio Explorer displayed potentially confusing results. For example, the VRRP (Virtual Router Redundancy Protocol) uses the unique protocol number 112. Filtering for it in Explorer omitted protocol 112, showing only 112 TCP and 112 UDP. Explorer still has this issue, but the new Illumio UI feature, Illumination Plus, fixes this by showing ports and protocols (such as 112) in addition to their TCP and UDP counterparts.
  This issue is resolved.
- **In rules with multiple scopes, label count no longer appears** (E-88833)
  Previously in **Explorer Proposed Rules**, in rules with multiple scopes, Illumio displayed a tally of the number of labels specified in the rule. Illumio has removed the tally because if Policy Exclusions are defined, it's not possible to calculate an accurate tally.
- **Specifying filter parameters in Explorer didn't work as expected** (E-88536)
  When specifying filter parameters in Explorer to find IP lists, entering only a single value returned IP lists with complex names that included the value but didn't return the IP list named simply with the single value. For example, entering "NCR" in the field returned multiple IP lists with names that included "NCR" as a prefix but not the IP list named simply "NCR." This issue is resolved.
- **Overlapping rules with Addition Pending status weren't merged** (E-87871)
  When an App Group has several consumers communicating with a specific provider, the Policy Generator is supposed to merge all the consumers into one rule for easy readability and better scalability. In this case, when an existing Addition Pending rule was edited such that it overlapped with another Addition Pending rule, merging didn't occur as expected. This issue is resolved.
- **Enforcement Boundaries Rule Merging Issues** (E-87849)
  When a rule was saved with port and port range found, that port range was not saved into the rule. This issue is resolved.
- **View Policy dialog box contained Enforcement Boundary details** (E-87812)
  In Explorer, if you clicked a fully-enforced workload in the Policy Decision column while in Draft View, the View Policy dialog box erroneously contained Enforcement Boundary details as though an enforcement boundary was in place. This issue is resolved.
- **Renaming labels not updating App Group List or App Group map** (E-87632)
  Renaming labels within the PCE did not immediately update the name in the App Group List or App Group Map. This issue is resolved.

- **Edited Extra-Scope rules disappeared after saving** (E-87613) If you edited the **Consumers** and **Providers** parameters of proposed **Extra-Scope** rules to include **All Workloads** and then saved the changes, all of the **Extra-Scope** rules disappeared. This issue is resolved.
- **Reported status of merged flows was incorrect** (E-87471)

  When filtering flows in Explorer, **Label-Based Connections** view, an allowed and a blocked flow that were merged were reported as "Blocked by Boundary" instead of "Blocked." The Reported Policy Decision should've been "Blocked." This issue is resolved and the merging of such flows is now correctly reported as "Blocked."
- **Label edits didn't appear unless the Explorer page was refreshed manually** (E-87237)

  In Explorer, after selecting a flow and editing any of its labels, the list of flows didn't refresh automatically, so a manual refresh was required for the changes to appear. This issue is resolved. The list of flows now refreshes automatically after labels are edited.
- **Label truncations in Illumination** (E-86960)

  Captions were truncated on the Illumination and App Group map pages. This issue is resolved.
- **Hover-over menu didn't appear in Explorer** (E-86794)

  When hovering over any port/process of a workload in Explorer, the contextual menu didn't appear. This issue is resolved.
- **Policy Generator failed to suggest a rule for blocked DNS traffic** (E-84298)

  Policy Generator didn't suggest a rule for blocked DNS traffic even though it was shown as **Blocked** in the App Group map and Explorer. This issue is resolved by the Essential Services feature. Traffic covered by essential service rules now appears green in Illumination and Explorer and doesn't appear in Policy Generator as requiring a rule to be written.
- **Unexpected and Incorrect "Permission Denied" alert in the GUI** (E-83445)

  A user without Global Org Owner permissions got the 'Permission Denied' error when they tried to use to Explorer page, even though they were able to perform the required action. This issue is resolved and the incorrect error was removed.
- **Drop-down lists and buttons misaligned in the Explorer page** (E-81916)

  When selecting Draft View for an Explorer query, the drop-down lists and buttons above the query results were not correctly aligned with the columns in the results table.

  This issue is resolved and drop-down lists are aligned properly.

## Policy and Workloads

- **Rule Optimization for rules with IP lists** (E-89091, E-89066)

  In this release, Illumio has optimized rules that have only IP lists on one side of the rule.
- **Filtering Workloads and VENs by IPv6 IP Address failed in some circumstances** (E-87543)

  In Workloads & VENs, attempting to filter workloads or VENs by IP Address by specifying part of an IPv6 address that included double colons (::) returned faulty matching results. This issue is resolved, and filtering in this way now works as expected.
- **Labels disappeared when editing one of the labels in a virtual server** (E-87402)

  When changing a label of a virtual server, all the other labels were removed automatically. This issue is resolved.
- **Wrong error code generated when trying to remove an already-deleted workload** (E-87048)

  Attempting to remove an already-deleted unmanaged workload through the API generated a **404 Not Found** error, which was incorrect. This issue is resolved and the action now throws a **406 Not Acceptable** error with a token/message response body indicating that the workload was already deleted.
- **Virtual Servers could be marked as pending deletion when unexpected F5 errors occur** (E-83175)

In rare cases in which the NEN receives an unexpected error from the F5 device during Virtual Server discovery, the Virtual Server appeared in the “Deletion Pending” state on the PCE. This issue is resolved.

- **Container Workload Profile allowed an invalid combination of configuration options** (E-81371)

  When adding or editing a Container Workload Profile in a container cluster, it was possible to configure **Management** as *Managed* and **Enforcement** as *Idle*, which is an invalid combination. This issue is resolved, and now the *Idle* **Enforcement** option is no longer available if *Managed* is selected in **Management**.
- **Rule search incorrectly calculated label groups in Scopes** (E-72318) Rule search calculated label-groups in Scopes incorrectly when the rule search was performed with both providers and consumers and the resulting Ruleset had either multiple Scopes or label groups in the Scope. This issue is resolved.

## PCE Platform

- **PCE response header names were lower case** (89767) HTTP response header names from the PCE could sometimes be sent in lower case. This could affect scripts that were written for earlier PCE versions, which expected mixed-case headers. For example, Content-Length in the response header of a previous PCE version might be content-length in a later version. This issue is resolved. The PCE will continue to provide mixed-case header names for the moment. However, any tooling that parses the HTTP headers should be changed to allow case-insensitive header name matching in order to retain compatibility with future PCE releases. Refer to RFC 7230, section 3.2, "Header Fields," which states that field names should be case insensitive.
- **Exposure charts in Executive Summary report did not show data** (E-89032)

  **IMPORTANT**

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

  In the Executive Summary report, the sections Vulnerability Exposure (All App Groups) and Vulnerability (All App Groups) showed the message NO DATA AVAILABLE, even when data existed. The cause was an inter-service permissions issue. This issue is resolved. The services can now upload the data, so that it appears correctly in the Executive Summary report.
- **Database migration failed during upgrades** (E-88273)

  **IMPORTANT**

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

  When upgrading Illumio Core on a Supercluster, an error message like the following appeared during the database migration step: " 'id' column is missing. A multimaster table requires an INSERT statement to provide 'id' column explicitly." Data being generated during the migration required an explicitly specified database primary key to verify Supercluster region ownership. The migration involving the `clone_detected` state triggered this restriction. This issue is resolved. The migration involving the `clone_detected` state no longer triggers this restriction.
- **Logs did not rotate** (E-86588)

**IMPORTANT**

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

Log files such as collector.log and agent.log became very large, because they were not rotated in a timely way. The log rotation error was caused by a damaged status file. This issue is resolved. The status file is now cleared when any such errors occur.

## VEN

**IMPORTANT**

The following resolved Core 22.2.0-VEN issues in this topic apply to both Illumio Core On-Premises customers and Illumio Core Cloud customers.

- **IPSets failed checks during upgrade** (E-89656)
  IPSets have FAILED checks when upgrading a machine that uses NFT (CentOS 8) from an old version of the VEN to 21.5.0+ VEN. Only NFT platforms were affected. This issue is resolved.
- **Aggressive tampering on Ubuntu 20 not working** (E-89180)
  Aggressive tempering on Ubuntu 20 is expected but was not working. This issue is resolved.
- **Container workloads continuously syncing policy with the PCE** (E-88967)
  Environments with high rates of container workload changes could cause all VENs to continuously sync policy. This issue is resolved.
- **Accessing APIs hosted by non-agent web service using expired service account API keys** (E-88696)
  Users were able to obtain a valid response with an expired service account API key for the APIs on a non-agent web service. This issue is resolved.
- **VEN is stuck in "policy sync" after upgrading to 21.5.10** (E-88386)
  VENs running on Windows get stuck in policy sync mode after upgrading to 21.5.10. This issue is resolved. The workaround is to manually create the file, C:\ProgramData\Illumio\etc\platform_handler_config.yml, and restart VEN.
- **VEN created unlimited number of debug/history subdirectories** (E-88345, E-88309)
  When you provisioned more than 10 policy changes with the PCE, the affected VENs could create more than 10 of the following subdirectories:
  `/opt/illumio_ven_data/etc/firewall/debug/history`
  This issue occurred because the VEN did not enforce the `firewall_history_count` option in the `/opt/illumio_ven/runtime_env.yml` file. This issue is resolved. In this release, the VEN now enforces the firewall_history_count option and won't generate more than 10 debug/history subdirectories even then you provision more than 10 policy updates.
- **Running the Linux pair script does not activate the VEN** (E-87853)
  Running the Linux `pair.sh` script on a system with the VEN already installed and not activated, fails to activate the VEN. Running the pairing line on a machine where a VEN is already installed, but not activated, successfully activates the VEN.
- **Forward Port: Optimized policy application to workloads** (E-87625)

The VEN used to take a long time to process policies with a large number of empty IP sets, usually caused by label group usage. This has been optimized.

- **Windows 10 Endpoint OS displaying as a Server (win-x86_64-server)** (E-87179)

  This issue is resolved. VENs running on endpoint operating systems now report win-x86_64-client. Other versions of operating systems that primarily host clients (e.g. VDI) could also report `win-x86_64-client`. Illumio continues to recommend using a pairing profile with a dedicated Endpoint label for pairing endpoints and searching for endpoints using the Endpoint label.
- **VENs flooding the DNS server with DNS queries of PCE FQDN** (E-86835)

  VENs were performing multiple DNS queries and flooding their DNS server instead of performing such queries as expected (every 5 minutes). This issue is resolved.
- **AIX VEN: Getting "cp" error when trying to upgrade** (E-86233)

  A VEN, running on AIX OS version 7.2, fails an upgrade from a 18.2.4 to release 21.2.4-7978 with the following error: `cp: Not a recognized flag: a.`

  The AIX VEN must be installed in the default /opt/illumio_ven and /opt/illumio_ven_data, and installing the AIX VEN in a custom directory is not supported. Do not change the default installation directory for the AIX VEN.
- **Windows 2016 VEN needed a reboot for policy sync** (E-86183)

  Persistent errors with policy sync on a workload occurred and required regular reboots of the VEN. This issue is resolved.
- **VEN processes making call to PDC Emulator on remote server** (E-85319)

  In idle mode, systems were experiencing many errors for `GetGPOFirewallInfo` which appeared to cause slowness of GPO downloads. After multiple tests, the test systems could not duplicate the issue. This issue is resolved.
- **Upgrading VENs in some cases generated tampering events** (E-85145)

  After upgrading to VEN 21.2.3-7944 to resolve CentOS 8.4 issues with nftables, multiple firewall tampering events were generated. This in turn caused the VEN's firewall tampering protection to fetch the current security policy stored on the PCE and return the host firewall to its pre-tampered security policy state. The tampering attempt, though false, was reported to the PCE as an `agent.tampering` event.
- **Policy that includes wrong PCE IP address failed in Illumination** (E-84709)

  While in Illumination mode, if you tried to apply a policy that specifies the wrong IP address for the PCE, the policy failed, which was not expected. The VEN now tolerates such a policy while in Illumination mode (but not while in Enforcement mode). This issue is resolved.
- **UDP traffic flows in Illumination can be confusing** (E-84615)

  How the PCE displayed UDP traffic flows in Illumination could be confusing because of the way the VEN evaluated flows for UDP (which is connectionless). For example, Illumination could display false positive flows for the syslog service. Syslog listens on local UDP ports while acting as a client (sending only outbound packets from those ports). This issue is resolved. In this release, Illumio adjusted VEN heuristics for determining UDP flow directions. The VEN now accounts for local and remote UDP port numbers. If local UDP port numbers are ephemeral (>= 1024) and remote UDP port numbers are privileged (< 1024), the VEN doesn't treat these UDP flows as inbound even when a service is listening on the local port.
- **VEN does not try to pair with the PCE except for 426 error** (E-84563)

  When the customer installed VEN and tried to pair it for the first time, the pair failed. The VEN did not seem to retry to pair with the PCE until a service restart using `illumio-ven-ctl restart` was issued. Workarounds were available; including the following steps. Before pairing the VEN: If the user wanted to use the Squid proxy, they needed to configure Squid to allow port 443, and unset the Squid proxy variable to allow `pce_port` through TCP 8443 by issuing: `unset http_proxy` and `unset https_proxy`.After pairing the VEN failed: the user had to restart VEN using `/opt/illumio_ven/illumio_ven_ctl restart`, which allowed the VEN to retry to pair with the PCE and bypass the Squid proxy server. This issue is resolved.

- **19.3.1 VEN on Red Hat 6.10 fails to update policy or revert tampering** (E-82610)
  Failed policy changes failed to revert policy tampering for multiple VENs: `IPv4iptables-restore v1.4.7: Couldn't load target `ILO-NAT-INPUT':/lib64/xtables/libipt_ILO-NAT-INPUT.so: cannot open shared object file: No such file or directory.` This issue is resolved. Root cause was due to tampering at the OS level where one or more `/sbin/iptables`* or `/sbin/ip6tables`* symlinks were removed.
- **VEN continues to run testscript.ps1 after activation** (E-80431)
  For a certain scenario, the VEN was retrying immediately and continuously to retrieve the master config which caused a spike in CPU usage. This issue is resolved. The fix was to ensure that the VEN exponentially increases the cadence of retries to retrieve the master config.

## Known Issues in 22.2.45

**IMPORTANT**

Unless otherwise noted, the following known issues apply to both Illumio Core On-Premises customers and Illumio Core Cloud customers, because they are also known issues in Core 22.2.3-PCE.

### PCE Web Console

- **Specifying multiple labels within each label type is not supported** (E-73039, E-72388)
  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 will not receive any results.
- **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.
- **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.
  Workaround: Not available. However, 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)

  In the Workloads page of the PCE web console, the asterisk (*) wildcard is intended to be supported in a filter expression for filtering the workload list. However, while the UI accepts the asterisk as a valid character, the filter will always return zero results, even if there are workloads that should match the filter expression.
- **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.

  Workaround: Not available; however, this is a rare situation because the % symbol is not used much in values.
- **API call to switch** `multi_enforcement_instructions_request` **returns an errorAPI call to switch** (E-59518)

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

## Data Visualization

- **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.
- **User column remains empty in Explorer by mistake** (E-89313)

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

  Workaround: After clearing the traffic counters for virtual services, click the refresh icon to recalculate the map data. The links disappear after refreshing the Illumination map.
- **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 seconds (as expected), but the reported time could be more than one minute, which would be erroneous.

  Workaround: Not available.

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

  V-E score is not correct when compared with V-E score column and Total V-E score. For example, when adding V-E score column showing as a 69.8 the Total is showing as 71 instead of 70.

  Workaround: Not available.
- **Vulnerability - V-E score is not showing correctly** (E-73277)

  V-E score is not correct when compared with V-E score column and Total V-E score. For example, when adding V-E score column showing as 69.8, the Total is showing as 71 instead of 70.
- **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.

## 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.”
- **Incorrect error message displayed when ruleset renamed to a name that's in use** (E-74498)

  On creating and provisioning rule set, for example, rule set A, renaming it to B, then creating ruleset A and reverting modifications to ruleset B, the UI displays an incorrect “500” error instead of an error message informing 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.
- **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 will provide the correct policy decision as reported by the VEN based on the active policy.
- **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.

## PCE Platform

- **Data node stuck in PARTIAL during regression test** (E-89797)

  **IMPORTANT**

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

  In rare cases, if application metrics is enabled the data node could be seen in PARTIAL state both from the `illumio-pce-ctl` cluster-status and `illumio-pce-ctl` status. In those cases, if `metrics_database_service/influxdb` is not running, move the `influxdb`bolt file located in `PERSISTENT_DIR/influxdb/meta/influxd.bolt` to any directory outside this `InfluxDB`directory.
- **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.
- **PCE node stop command fails** (E-84227, E-84719)

  **IMPORTANT**

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

  Running `illumio-pce-ctl stop` to stop a PCE node sometimes fails, with the node stuck in the PARTIAL state.

  Workaround: Run the `stop` command again if it fails.

- **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`.
- **The `agent.log` in a Supercluster deployment can include an undefined method** (E-66998)

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

  When a Supercluster configuration fails to load, the `agent.log` for that Supercluster deployment can include an undefined method `external_fqdn` exception.

### VEN

- **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 may occur and be sent to the PCE. This is a false positive firewall tampering event, and can safely be ignored.
- **Process-based rule not showing properly in Explorer** (E-89749)

  A process-based rule was defined but was shown as "no rule" in Explorer.

  Workaround: Do not specify the service name in the process-based rules.
- **On CentOS 8, VEN can't load the FTP 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.
- **[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. The workaround is to 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 restarted 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 on the global zone and the exclusive IP zone.

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

## Security Information

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

## 22.2.40

- **OpenSSL upgraded to v3.0.7 on Core 22.2.40 VEN**
  OpenSSL has been upgraded to v3.0.7 to address CVE-2022-3786 and CVE-2022-3602. Some versions of the VEN were affected by this vulnerability. Review the Security Advisory on the Illumio Knowledge Base for more information.
- **devise-two-factor upgraded to v4.0.2**
  devise-two-factor has been upgraded to v4.0.2 to address CVE-2021-43177.
- **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.

## 22.2.30

- **Redis updated to address multiple CVEs**
  Redis was updated to 6.2.6 to address CVE-2021-32626, CVE-2021-32627, CVE-2021-32628, CVE-2021-32687, CVE-2021-41099, CVE-2021-32675, CVE-2021-32762, and CVE-2021-32672. These CVEs do not impact the PCE.
- **Action Pack upgraded to address CVE-2022-23633**
  The actionpack gem was updated to 6.1.4.6 to address CVE-2022-23633.
- **Content Security Policy header fixed**
  A misconfiguration of the Content Security Policy header allowed loading of scripts and other content from arbitrary sources over HTTPS. This issue is resolved.

## 22.2.0

- **OpenSSL upgraded to address CVE-2022-0778**We upgraded to OpenSSL 3.0.2 in 22.2.0 to address CVE-2022-0778. The PCE is not impacted by this vulnerability.

# Legal Notice



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

Resources

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

Contact Information

- Contact Illumio
- Contact Illumio Legal
- Contact Illumio Documentation