Illumio® Core

Version 22.4.*x*

Release Notes

11/01/2022

14000-100-22.4

illumio

Contents

Welcome

These release notes describe the resolved issues and known issues for the Illumio Core 22.4.*x* releases.
Illumio Core 22.4 is available for Illumio Core On Premises customers.

Document Last Revised: November 2022
Document ID: 14000-100-22.4.1

What's New in This Release

To learn what's new and changed in 22.4, see the **What's New in This Release** guide.

Product Version

PCE Version: 22.4.1 (Standard)

Release Types and Numbering

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

- "a.b": Standard or LTS release number, for example, "22.4"
- ".c": Maintenance release number, for example, ".1"
- "-d": Optional descriptor for pre-release versions, for example, "preview2"

Resolved Issues in 22.4.1

- **Draft mode incorrectly marking corporate traffic as allowed due to non-corporate rules** (E-96916)
  In Explorer/Illumination's draft mode, traffic on the corporate network was erroneously marked as "allowed" due to rules that apply only to non-corporate networks. This issue occurs when there are rules on the non-corporate network to broad IP lists. The issue only affected Draft mode and had no impact on policy correctness. This issue is resolved.
- **Slow Explorer queries** (E-96770)
  When running a query in Explorer, the results screen was not displayed. This issue was caused by an error in one of the internal queries used to populate data.

This issue is resolved. The query SQL has been fixed, and the Explorer query results screen is displayed properly.

Resolved Issues in 22.4.0

PCE Web Console

- **Unable to scroll and select scope in Ruleset Add Modal** (E-93985)
  User was not able to scroll and select scope in Ruleset Add modal dialog. This issue is resolved.
- **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.
- **Ruleset UI Issues** (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.
- **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.
- **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.

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 than 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 remained 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.

Data Visualization

- **Slow App Group queries in Explorer** (E-96860)
  When running queries on App Groups in Explorer, the results took longer than expected to load and sometimes caused the browser to hang. This issue is resolved. Performance improvements have been made to the data aggregation function and other aspects of Explorer.
- **Query results freeze in Explorer** (E-96770)
  When running a query in Explorer, the results screen was not displayed. This issue was caused by an error in one of the internal queries used to populate data. This issue is resolved. The query SQL has been fixed, and the Explorer query results screen is displayed properly.
- **Could not update VEN rate from the workload command panel** (E-95269)
  Could not update the VEN rate from the workload command panel, so it could not be updated when workloads were outside of groups. The rate could only be updated as part of a group. This issue is resolved.
- **Existing rulesets not used by default even when applicable scoped rulesets exist** (EYE-95143)
  Sometimes a previously selected ruleset would cause a new ruleset to be created even though other rulesets with the correct scope already existed. This issue is resolved.
- **Under policy generator IP List Rule Preview, IP lists were incorrectly merged** (E-94685)
  When merging multiple rules for a common provider port, the multiple IP lists for the selected rules were incorrectly merged. The resulting rules were missing some of the applicable IP lists. This issue is resolved.
- **Adding rules from Explorer but proposed deletion other unrelated rules in the ruleset** (E-94684)
  Sometimes when adding a rule to an existing ruleset in Explorer, a completely unrelated rule would be 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.

- **Traffic Database Summary was showing Zero for PCE Health** (E-93648)
  Traffic Database Summary was showing Zero for PCE Health by mistake. This issue is resolved, and the summary is displayed properly.
- **Service information missing for essential services inbound rules** (E-93633)
  In the View Policy dialog, service information was missing for essential service inbound rules. This issue is resolved.
- **Unable to download reports** (E-93405)
  When clicking any Download button on the **Reports** page, sometimes no reports would be downloaded, and the error "This site cannot be reached" would be displayed. This issue is resolved. Reports can be downloaded as expected.
- **No data in illumination / app group maps / explorer** (E-93384)
  Data was sometimes completely missing from Illumination maps, App Group maps and lists, and Explorer. Also, queries would sometimes be very slow, or would completely hang. This issue is resolved.
- **Enforcement Boundary Panel does not show service with same port and different protocol** (E-93371)
  In the Illumination Map, the Enforcement Boundary Panel Service column showed only a given TCP port number but did not show the UDP equivalent. This issue is resolved.
- **Illumination incorrectly defaulted to creating a Windows Service** (E-93295)
  When creating a flow in Illumination to a Windows workload, the PCE would by default incorrectly create a new Windows Service, even when a Windows-based service already existed. This only occurred for Windows services, not Linux ones. This issue is resolved. Illumination now properly uses a matching existing Windows Service, and creates an 'all operating system' service if no matching service exists.
- **Explorer: pills in the 'services' filters get replaced by an empty pill** (E-93125)
  When a saved Explorer filter specified services, they got removed when a user clicked the button to switch between fields. This issue could not be reproduced. 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.
- **Blocked traffic showing in the VRRP protocol** (E-89842)
  Filtering for ports and protocols by number in Illumio Explorer would display 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.
- **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.

- **Drop-down lists and buttons were 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.
- **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 displays the previous Add Rule panel for other selected traffic. This issue is resolved.

PCE Platform

- **Explorer & reporting failures when using user account with IP access restriction** (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 restriction can now view traffic data.
- **PCE support bundle UI - custom time filter** (E-93267)
  A boundary bug incorrectly subtracted a day from the date filter for February, April, June, September, or November when the last day of the month was requested using the support bundle custom time filter. This issue is resolved.
- **Editing scopes for Access Management displayed Role label group as option in menu** (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 scopes for access management. This issue is resolved.
- **PCE UI Health page not alerting on disk issue** (E-80080)
  The PCE Health page did not display a warning when disk information was inaccessible. This was inconsistent with the system health log file where the warning level was properly set and a '?' was used to indicate an issue obtaining disk status. This issue is resolved.

Known Issues in 22.4

PCE Web Console

- **Explorer pagination jumps to the last page of Label Based Connections in some cases** (E-93223)
  In the **PCE Web Console > Explorer**, clicking the right arrow above the connections list to advance to the next page unexpectedly redirects you to the last page in the following circumstances:

a. Select multiple connections in Explorer.
b. Click **Allow Selected Connections**. The **Proposed Ruleset** page opens.
c. Click **Cancel** in the **Proposed Ruleset** page.

Workaround: none currently

- **In Explorer, parameter drop-down list is duplicated in some cases** (E-93206)
  In the **PCE Web Console > Explorer**, after selecting to include **All Workloads** in Consumers, the drop-down list is duplicated such that a second menu appears atop the initial menu.
  Workaround: none currently; users should ignore the duplication and select parameters on the visible menu.
- **Filtered searches for workloads on the Virtual Servers page return incorrect results** (E-82414)
  The following happens when you search for workloads on the Virtual Servers page:
  - After searching for workloads by label, the search doesn't work and the full list of workloads continues to display regardless of your search criteria.
  - In searches that don't return any matching results, the reported page count is erroneous.
- **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 do 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 and will be resolved in a future release.
- **No error message is displayed after typing in an invalid port** (E-68255)
  When you enter an invalid port number while editing a service, the PCE still displays options to select from. When you move to another field without making a selection, the entered letters/digits are not cleared to reflect that the entered value was not selected. It can appear that the value you entered was accepted even though invalid.
  Workaround: Press ENTER after entering text. When the combination was valid, it will be selected. Otherwise, it will be cleared.
- **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: There is no workaround but this is only a cosmetic issue.
- **Filtering by an invalid port in the Services List page displays an error** (E-68249)
  When you filter the Services list using an invalid port, you receive the 406 error: "Port value out of range." The port filter category is a free search and your input is passed to the PCE

without validation.
Workaround: Clear the entered port number and filter the list with a value in the valid port range.

- **Wildcard in workloads filter not working** (E-65232)
  "The PCE web console Workloads page supports filtering using special characters such as an asterisk (*). However, instead of displaying an error message when *only* special characters are used, the Workloads page neither filters the result nor gives an error message.
- **Filter doesn't handle the percentage symbol** (E-64904)
  When users select a filter option from the drop-down list, the selected value is added to the URL. If the selected value contains the percentage symbol (%), the UI throws an error, and a blank page shows up. There is no workaround, but this is a rare situation because the % symbol is not used often in values.
- **API call to switch multi_enforcement_instructions_request returns error** (E-59518)
  A REST API call to switch `multi_enforcement_instructions_request` returns an incorrectly handled error. This issue will be resolved in a future release.
- **Pressing Enter doesn't select the default option in the dialog box** (E-53831)
  When the PCE web console displays a dialog box, pressing **Enter** might select an action other than the default.
  Workaround: Use your mouse to click the required button in the dialog.
- **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.

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)
  When creating and provisioning a rule set (for example, ruleset A, renaming it ruleset B, then creating ruleset A and reverting modifications to ruleset B), the UI displays an incorrect “500” error instead of an error message stating that the ruleset name is already in use.
- **Policy restore impacts the virtual services of a container cluster** (E-73979)
  The issues are as follows:
  - When policy is restored to a version before the creation of a container cluster’s virtual services, the container cluster’s virtual services are marked for deletion in the draft change.
  - When a container cluster is deleted, restoring its virtual services is possible through policy restore.
- **Inconsistencies in rule coverage for the Windows process-based rules** (E-71700)
  The draft view of Illumination and Explorer could show an incorrect draft policy decision for traffic covered by a rule using a service with a Windows process or service name. This generally happens when there is a port/protocol specified in the rule in addition to the process/service name, or when a non-TCP/UDP protocol is used in the rule. In these cases, the reported view provides the correct policy decision as reported by the VEN based on the active policy.
- **Rule search with virtual service and labels returns an incorrect rule** (E-65081)
- When a rule is written with a virtual service whose labels conflict with the ruleset scope, and a rule search is done for the virtual service, the rule search could return the rule even though the rule does not apply due to the scope conflict.
  Workaround: use rule search to ensure that the rule applies to the virtual services and the scope labels separately.
- **Unable to select multiple protocols in Rule Search** (E-57782)
  If you try to select multiple protocols in Rule Search, you cannot select a second protocol after selecting a protocol once. For example, if you select TCP and then want to select UDP, the UI does not display the protocol option again.
  Workaround: This issue is only an issue in the PCE web console. Using the REST API, you can select multiple protocols and obtain the correct search results.

Data Visualization

- **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; E-73277)
  The Total V-E score indicated on the Vulnerabilities page is higher than the sum of the values in the V-E score column. For example, in a given case the sum of the values in the V-E scores column was 69.8 but the Total V-E score was 71 instead of 70.
  Workaround: Not available.
- **VES and E/W exposures wrong for the internet and other workloads** (E-73023)
  If a rule provides a service on a vulnerable port/protocol to the internet and to some set of workloads, the workloads in the port exposure are not counted. This leads to a VES of 0 instead of larger than 0. The exposure calculation is correct if the internet is not provided as a consumer.

PCE Platform

- **VENs on RHEL8 potentially subject to OpenSSL CVEs** (E-93205)
  VENs installed on RHEL 8 use the OpenSSL package that is installed as part of the OS. There are known security vulnerabilities on several OpenSSL versions.
  Workaround: Upgrade to the latest OpenSSL package v3.0.5 or v1.1.1q or later. Please note that based on its usage of OpenSSL, VENs are not impacted by CVE-2022-1292, CVE-2022-2068, and CVE-2022-2274.

- **Power off, then on a member region, core nodes are stuck in PARTIAL** (E-92384)
  After powering off and powering on a PCE, the run fails, and core nodes remain in partial states. Restarting the databases do not fix the issue.
  Workaround: Restart all core and database nodes. This issue is rare and not easily reproducible.
- **Created By field in CEF events not working** (E-91151)
  The Created By field for events is not working because Illumio events return the integer primary key of the creator as a `duid` in the CEF events. The CEF field should return HREF and not the primary key. Returning the `duid` does not work for container clusters or Illumio Service Accounts because they use the `uuid` and not integer IDs for this field; therefore, they do not populate the `created_by_id` field.
  Workaround: Not available
- **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.
- **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`.

REST API

- **Vulnerability APIs should distinguish between 0/syncing/NA Exposure scores** (E-71689)
  Users might get confused when the workload list page shows as Syncing and the workload vulnerability tab shows as N/A.
  Workaround: This is a cosmetic issue and no workaround is available.

VEN

> ⚠ Illumio Core 22.4.1 does not include a 22.4.x VEN release. These issues apply to the latest released version of the VEN.

- **Process-based rule not showing properly in Explorer** (E-89749)
  A process-based rule was defined but was shown as "no rule" in Explorer. The workaround is to not specify the service name in the process-based rules.

- **On CentOS 8, VEN can't load the FTP and TFTP modules** (E-85127)
  On CentOS 8, the VEN can't load the `nf_conntrack_ftp` and `nf_conntrack_tftp` modules, which blocked the workload from uploading and managing files. Due to this issue, customers can't upgrade the VEN on CentOS 8 workloads.
- **[CentOS 8] Custom IPtables rule does not work with -j REDIRECT** (E-80818)
  After creating a custom rule on the PCE with -j REDIRECT in the nat table, the CentOS 8 VEN enters an error state because the VEN could not correctly handle the -j REDIRECT part of the rule. The custom rule performs a NAT operation that requires a different chain type therefore, nftables does not allow the VEN to perform the redirect in our chains.
  Workaround: remove the custom Iptables rule and restart the VEN. This brings the VEN back to a healthy state.
- **Established connections are not removed when the VEN is restarted** (E-63072)
  After the VEN is paired and restarts using the Illumio-ven-ctl options, it dumps suspicious log entries into vtap.log twice per minute. The log type is INFO and they appear to be caused by an error related to the restart of the VEN. This issue is observed on the global zone and the exclusive IP zone.
  Workaround: Not available; however, this issue has no major impact except for vtap.log receiving these log entries.

Security Information

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

- **OpenSSL upgraded to address CVE-2022-1292 and CVE-2022-2068**
  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.
- **Simple_form upgraded to address CVE-2019-16676**
  The simple_form package was upgraded to 5.1.0 to address CVE-2019-16676. The PCE is not impacted by this vulnerability.
- **Rack upgraded to address CVE-2020-8184, CVE-2022-30122 and CVE-2022-30123**
  The rack package was upgraded to 2.2.3.1 to address CVE-2020-8184, CVE-2022-30122 and CVE-2022-30123. The PCE is not impacted by these vulnerabilities.
- **Curl upgraded to address CVE-2022-32206, CVE-2022-32207 and CVE-2022-32208**
  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.
- **Redis upgraded to address several non-impacting vulnerabilities.**
  The redis package was upgraded to 6.2.7 to address several non-impacting vulnerabilities. For more information, see Redis 6.2 Release Notes.

Legal Notices