Illumio Core Release Notes 24.2

Table of Contents

Legal Notice

Resources

- Legal information
- Trademarks statements
- Patent statements
- License statements
- Open Source Licensing Disclosures

Contact Information

- Contact Illumio
- Contact Illumio Legal
- Contact Illumio Documentation

Welcome

These release notes describe the new features and known limitations for Illumio Core 24.2.x releases.

- Illumio Core 24.2.10 is available for Illumio Core On-Premises customers.
- Illumio Core 24.2.0 is available for Illumio Core Cloud customers.

Document Last Revised: September 2024

Document ID: 14000-100-24.2.10

Product Version

PCE Version: 24.2.10 (Illumio On-Premises customers only)

VEN Version: 24.2.10

LW-VEN Version: 1.1.0

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

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

Security Information

This section provides important security information. 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.

- **Resolved Security Issue in Release 24.2.10**
  - **ruby-saml**

    ruby-saml, a third-party component in the PCE, was impacted by CVE-2024-45409. It is now fixed, as the impacted component was upgraded.
- **Resolved Security Issue in Release 24.2.0**
  - **postgreSQL**

    postgreSQL was upgraded to v15.7.

Resolved Issues in Release 24.2.10-PCE

- **Last updated policy timestamp for C-VENs reflects Kubernetes Workload policy changes** (E-118372)

  The last updated policy timestamp on C-VENs now updates after a C-VEN successfully updates the policy for its pods.
- **Navigation error while navigating to Authentication Settings > SAML: Not Found** (E-118183)

  In PCEs running 22.5.32, sometimes going to Authentication Settings > SAML resulted in the attempted navigation being cancelled, and a "Navigation error details" popup appearing.
- **PCE sending partial IPP instructions** (E-117863)

  PCE was sending partial IPP instructions, which was causing instruction replacement due to the current Kubelink's inability to receive partial instructions. This issue is resolved.
- Erroneous Ransomware Exposure status for AIX and Solaris workloads (E-117858)

  Solaris and AIX workloads have always showing the Ransomware Exposure status as Protected. This issue is resolved.
- **Unmanaged workloads created incorrectly** (E-117637)

  Unmanaged workloads created via the Deny Rules menu were incorrectly created with the previous creation's Name and hostname. This issue is fixed.
- **Policy generator throwing an error when saving rules** (E-117499)

  When users tried to save the rule with custom iptables rules, the Policy generator was throwing an "Unexpected input validation error". This issue is resolved.
- **"Duplicate key value" error occurs during database migration phase of PCE upgrade** (E-117235)

  When upgrading the PCE from 22.5.32 to 23.2.21, during database migration the following error occurred: `ERROR: duplicate key value violates unique constraint "flow_process_references_7_org_id_region_id_value_idx`.
- **Missing app-tiers label on pod using annotation** (E-117004)

  In non-CLAS (legacy) container clusters, when applying Illumio labels through Kubernetes annotations, a label key containing a dash is not properly assigned to Container Workloads. For example, a pod annotation of `annotation.com.illumio.app-tiers` with a label value of AT_A is not created with label type `App-Tiers` nor the label `AT_A`. This issue is now resolved for new Container Workloads created on this release. However, upgrading the PCE to this release does not fix existing Container Workloads that have labels containing a dash character. To fix such existing Container Workloads, you can edit the Container Workload Profile to add another possible value for the dash-containing label. After saving this edit, existing Container Workloads get relabelled correctly to their assigned annotation values.
- **NEN 2.6.20 is stuck in "ACL generation pending"** (E-116805)

  In a configuration with a 2.6.20 NEN paired with a supercluster member on PCE Version 22.5.32-12, running "Generate ACLs" never completed, and only showed the "ACL Generation Pending" message without ever producing an ACL.
- **CLAS - Rules are not created for Kubernetes Workloads and VIPs** (E-116721)

  In CLAS-enabled deployments, rules created between a Kubernetes Workload and a VIP (from a virtual server, for example a F5 Virtual Server) are not created even after provisioning. These rules fail to appear in the PCE Web Console. This issue is resolved. The new runtime environment variable `clas_workloads_ipset_only_changes_enabled` must be set to `false` in the PCE `runtime_env.yml` file (under `agent_service`:) for the PCE to correctly send Virtual Server instructions to Kubernetes Workloads.
- **UI fields fail to occasionally load under Rulesets and Rules** (E-116648)

Sometimes when writing a rule in 24.1.3-PCE, the Sources or Destination fields never properly loaded or were populated with labels that were chosen. This could occur when viewing a grid layout in smaller screen sizes, which reduced the source/destination selector drop-down height and caused options to be improperly displayed or hidden completely with a scroll.

- **Last updated policy timestamp for C-VENs reflects Kubernetes Workload policy changes** (E-116258)

  The last updated policy timestamp on C-VENs now updates after a C-VEN successfully updates the policy for its pods.
- H**eader manipulation issue fixed** (E-116114)

  Appropriate validation for host header was added to avoid any host header manipulation.
- **curl upgraded to v8.8.0** (E-115842)

  curl was upgraded to v8.8.0 to address CVE-2024-7264, CVE-2024-6197, CVE-2024-2466, CVE-2024-2398, CVE-2024-2379, and CVE-2024-2004.
- **External users with multiple scopes reporting PCE slowness** (E-109314)

  External users with many scopes in their RBAC permission have been reporting PCE UI slowness, especially when browsing the VENs tab and querying traffic. This issue is resolved.

Resolved Issues in Release 24.2.10-VEN

CAUTION

Maintain VEN Operating System Support

Compatibility and performance issues can occur if the operating system version running on your workloads and endpoints is upgraded to a version that is not supported by the VENs on those machines. Before upgrading the operating system on workloads and endpoints, first make sure that the VENs installed on these machines support the new OS version. For workload VENs, see VEN OS Support Package Dependencies. For Endpoint VENs, see Endpoint VEN OS Support Package Dependencies.

- **False positive IPSec tampering error in platform.log** (E-118562)
  After disabling rules with SecureConnect options, the error IPSec policy tampered nonetheless appeared in the platform.log every 10 minutes. This issue is resolved. The error no longer appears in this circumstance.
- **VEN misinterpreted flow direction** (E-118007)
  Linux VENs could fail to determine the flow direction correctly in some circumstances, (for example, for UDP packets sent to a broadcast IP address), resulting in the VEN reporting an inbound flow as an outbound flow. This issue is fixed.
- **Transient environmental variable could prevent applying policy** (E-117699)
  While upgrading any VEN version on Solaris workloads, it was possible for VEN processes to inherit transient environment variables from the OS pkgadd command (for example, `$TMPDIR`). This issue could've prevented the VEN from applying policy until the VEN was manually restarted. This issue is resolved.
- **Policy application failed in some circumstances** (E-117246)
  Some earlier VEN versions failed to apply policy if the workload on which it was installed had multiple valid IPv6 DNS addresses. This issue is fixed.
- **Bug in nftables versions pre-0.9.2 prevented policy application** (E-116635)
  Policy failed to load on VENs installed on RHEL Linux 8/9 workloads with a version of nftables earlier than 0.9.2. This issue is resolved.
- **Issue affecting the persistent connection between PCE and VEN** (E-116177)
  A regression was introduced into 22.5.33 and 23.2.23 Windows VEN, which could cause the Event Channel between VEN and PCE to stop functioning, resulting in a policy convergence delay. This issue is resolved.
- **PCE didn't recognize external IP address of external Azure VM** (E-115935)
  Unix VENs failure to correctly detect Azure environment prevented the PCE from recognizing the external IP addresses of the workloads. This issue is resolved. VENs now correctly detect when they're operating in an Azure environment,
- **ICMP code misinterpretation caused false positive tampering error** (E-113439)
  After misinterpreting a rule specifying the ICMP protocol, the VEN generated a false positive tampering error. This issue was resolved by updating the VEN to normalize ICMP code.
- **Improper VM shutdowns caused VEN data file corruption** (E-113231, E-109231)
  If a workload was shut down improperly, such as by a sudden loss of power, and the kernel crashed, some critical VEN data files could've gotten corrupted, preventing the VEN from

loading policy. This issue is resolved. Critical VEN data files are now more resilient if the workload is shut down improperly.

- **Support for pairing VENs on AWS Workloads with IMDS v2** (E-109528)

  This VEN release provides support for pairing VENs on AWS workloads with Instance Metadata Service Version 2 (IMDS v2). This update was necessary to support IMDS v2 session-oriented authentication.
- **Improper VM shutdowns caused VEN data file corruption** (E-109231)

  If a workload was shut down improperly, such as by a sudden loss of power, and the kernel crashed, some critical VEN data files could've gotten corrupted, causing the VEN to lose connectivity with the PCE. This issue is resolved. Critical VEN data files are now more resilient if the workload is shut down improperly.

Resolved Issues in Release 1.1.0-LW-VEN

- **LW-VEN activation failed on non-UTF-8 legacy Windows workloads** (E-119190)
  LW-VEN activation failed on workloads configured for non-US languages. This happened because LW-VEN version 1.0.1 doesn't support non-UTF-8 strings. This issue is fixed. Support for non-UTF-8 was added in LW-VEN 1.1.0.
- **Activate option appeared during "non-fresh" LW-VEN installation** (E-118952)
  When installing an LW-VEN on a supported legacy Windows machine on which an LW-VEN is already activated, the option **Start + Activate** appeared, which was unexpected. As this wasn't a fresh installation, only the **Start** option should've appeared, not **Start+Activate**. This issue is resolved. Now, only **Start** appears during non-fresh installations.
- **Users weren't prompted during LW-VEN activation if activation command was run without options** (E-118764)
  Attempting to activate LW-VEN failed if users issued the illumio-lwven-ctl activate command without options. A command prompt appeared but no prompts displayed and the activation hung. This issue is fixed.
- **LW-VEN 1.0.1 failed to apply 2008 firewall policy that contained very large port range** (E-118600)
  The Windows Firewall rejected Illumio security policy rules that specified extremely large port ranges, resulting in policy not being applied. This issue is resolved. Rules exceeding 1000 ports are now split into multiple rules, and rules with large port ranges are no longer rejected. **Note:**Customers should keep in mind that applying a policy with a large port range may cause the Windows firewall to become unresponsive and take a long time to respond to any firewall command.

Known Issue in Release 24.2.10-VEN

- **AIX / Solaris 10 policy update fails in some circumstances** (E-118539)
  Updating policy on AIX and Solaris 10 workloads fails if the workloads are in Full Enforcement mode and flow visibility is turned off. This issue is caused by some incorrectly generated syntax. This is a known issue. Workaround: Go to **Servers & Endpoints > Workloads**, select AIX/Solaris 10 workloads that are in Full Enforcement mode, and then in the Visibility drop-down menu enable flow visibility by making sure the setting isn't **Off**.

UI improvements in Release 24.2.0+UI2

This release provides user interface updates for Extra-Scope and Intra-Scope rules.

- The separate tabs that contained Intra-Scope and Extra-Scope options in previous releases are removed and a new column called **Scope Type** appears in the Allow rules section of the Policies page.
- Extra-Scope and Intra-Scope rules occupy different sections within Allow Rules, separated by a grey line.
- You can move rules up or down but only within their respective section.
- Extra-Scope rules are now distinguished by an icon.

Resolved Issues in Release 24.2.0

Enterprise Server

- **Bug in nftables versions pre-0.9.2 preventing policy application** (E-116635)
  The policy would fail to load on VENs installed on RHEL Linux 8/9 workloads with a version of nftables earlier than 0.9.2. This issue is fixed.
- **On occasion, ransomware dashboard widgets were not updating or populating** (E-116603)
- **App Group's enforcement state shows as "Mixed" by mistake** (E-116536)
  The enforcement state of the App Group incorrectly displays 'Mixed' when a workload has 'Selective' enforcement along with unmanaged workloads. To accurately define the enforcement state as 'Mixed' for an app group, the issue was resolved by excluding the state of unmanaged workloads.
- **High latency was observed when loading an app group list page** (E-116521)
  This issue is fixed.
- **Traffic queries would fail when the "Source OR Destination" field had an APP label** (E-116365)
  Traffic searches failed when the search type was set to "Source OR Destination" and when an APP label was used.
  This issue is fixed.
- **Issue affecting the persistent connection between PCE and VEN** (E-116177)
  A regression was introduced into 22.5.33 and 23.2.23 Windows VEN, which could cause the Event Channel between VEN and PCE to stop functioning, resulting in a policy convergence delay.
  This issue is fixed.
- **FQDN missing from the "Connections with unknown IP" view** (E-116077)
  This issue is fixed.
- **Different behavior of filters was observed in the map versus traffic views** (E-115933)
  Works as designed.
- **AND operator showing between labels of the same type** (E-115653)
  The AND operator was showing between labels of the same type in Traffic query fields (UI display only).
  This issue is fixed.
- **In Illumination Plus, users were unable to write rules based on port numbers** (E-115225)
  This issue is fixed.
- **Unable to create new service from within rules ad ruleset page** (E-115210)
  Users experienced slow performance, resulting in a long time to create a new service from the rules and rulesets page.
  This issue is resolved.
- **Saving filters in Illumination Plus** (E-115189)
  Since the SCP2 upgrade, a customer was unable to save filters in Illumination Plus. This issue is fixed.
- **Save and Provision for a rule fails** (E-115047)
  After performing Save and Provision for the rule, the Comment field did not show up and the rule was not provisioned.
  This issue was fixed.
- **Upgrade json-jwt-1.13.0.gem to N/A or higher to address CVE-2024-51774** (E-114939)

The json-jwt (aka JSON::JWT) gem version 1.16.3 for Ruby sometimes allows bypass of identity checks via a sign/encryption confusion attack.

This issue is resolved after upgrading json-jwt to version 1.16.6.

- **Script needed for default profile recreation and sync migration** (E-113855)

  A script was needed for default profile recreation and sync migration with release 23.2 and later.

  This issue is fixed.
- **Upgrade rails-6.1.7.4.gem to 6.1.7.7, 7.0.8.1, or higher to address CVE-2024-26144** (E-114138)

  Starting with Rails version 5.2.0, there was a possible sensitive session information leak in Active Storage. This vulnerability was fixed in Rails releases 7.0.8.1 and 6.1.7.7 and this issue will not be addressed.
- **The `ilo-pce` command should not require sudo access** (E-113745)

  Remove 'sudo' in `services/cron_perfmon/bin/avn_perfmon.sh` and then test. It is not critical to know the program name of processes users don't own.
- **Script needed for default profile recreation and sync migration** (E-113855)

  A script was needed for default profile recreation and sync migration with release 23.2 and later.

  This issue is fixed.
- **App Group Rule Listing is missing Rulesets** (E-113259)

  Intra-scope rules were not showing up in the App Group rules menu. This issue is fixed.
- **Policy check not properly showing Rules Pending status** (E-112974)

  The Policy check did not show that Rules Pending was disabled. This issue is fixed.
- **Lookup by external_data_reference not working** (E-111950)

  When a label was created using the API and later edited in the UI, the lookup by external_data_reference did not work. This issue is fixed.
- **Unresponsive web page when writing rules** (E-110946)

  When users were writing a rule in the PCE, the webpage became unresponsive. This issue is fixed.

Containers

- **Kubernetes Workload service network interfaces are unnecessarily updated upon every Node update** (E-114962)

  On every network interface update of a cluster node, the network interfaces of every Kubernetes Workload of type Service were getting updated. This caused a large amount of `workload_ip_address_change` event creations when used with thousands of services. This behavior worsened when many nodes were re-deployed at the same time (unpair/pair) while there were Kubernetes Workloads already present.
- **Container cluster reporting "Virtual service is still active on a workload" after upgrading to "clusterMode: migrateLegacyToClas"** (E-114727)

  After a non-CLAS (legacy) deployment was upgraded to CLAS mode, existing container clusters running multiple ClusterIP virtual services each went into an Error Status, with each cluster detail page also displaying a "Virtual service is still active on a workload" message.

LW-VEN

- **Unexpected 404 error during LW-VEN deactivation** (E-117731)

Issuing the deactivation command while the LW-VEN was either receiving/applying policy or sending a heartbeat to the PCE caused a 401 error. The LW-VEN wasn't deactivated and continued trying to get policy from the PCE. This was unexpected behavior. This issue is resolved. Issuing the deactivation command in this circumstances now works as expected.

- **LW-VEN activation failed if a NIC lacked a default gateway** (E-117318)

  When trying to activate an LW-VEN on a legacy Windows server with at least one network interface lacking a default gateway, activation failed and the following error message was thrown: `error undefined method `strip' for nil:NilClass` . This issue is resolved.

Known Issues in Release 24.2.0

Enterprise Server

- **Creating same name workloads from the ip address contextual menu** (E-116711)
  On the main workloads component (WorkloadEdit) users are able to create workloads with the same name.
  Workaround: none
- **Refused connection to the Support portal with Segmentation Templates > sign in** (E 113084)
  Clicking on **segmentation templates > sign in** the support portal returns an error.
  Workaround: none.
- **Unable to select a workload inside an open combo node** (E-112344)
  Clicking on a workload inside a combo node does not select a workload and the traffic links connected to it are not showing.
  Workaround: none
- **The Explorer page is not loading and redirects to the Traffic page** (E-111574)
  Workaround: The Explorer page loads if users enable both Explorer and Classic Illumination.
- **Deleted Workload traffic link shows a policy decision** (E-110143)
  A deleted workload traffic link shows a policy decision by mistake.
  Workaround: None
- **Ransomware Dashboard always shows high Protection coverage score** (E-106996)
- **Global admin prompted to update Ransomware "Workloads Requiring Protection" but not authorized to do so** (E-105756)
- **PCE application log files are not rotated** (E-105659)
  Some PCE application log files (agent, collector, haproxy) are not rotated, while the other files are rotated correctly.
  Workaround: none.
- **Standalone PCE not starting up after service_discovery_encryption_key change** (E-104880)
  Workaround: none
- **Removal of inactive accounts ignores API use** (E-103316)
  In PCE release 22.4.1+A3, user accounts that have been inactive for more than 90 days are removed automatically. However, the active status is determined based only on whether the account has logged in to the web console UI. If the account is used only to issue API requests, it is counted as inactive and removed after 90 days.
- **Updating max results in Illumination Plus (10K) updates the Explorer max results** (E-102742)
  The maximum connection number in Explorer gets updated to the same maximum number as the update in Illumination Plus. However, the maximum number in Illumination Plus is 10,000, while in Explorer, it is 100,000.
  Workaround: Update the max results setting in Explorer to get more than 10K results.
- **Recent filters become empty when users run a query from Explorer** (E-102525)
  Workaround: None
- **When users load saved filters in Explorer, more than four labels are showing up** (E-102438)
  Workaround: None

- **After creating a new organization, users are unable to load saved filters** (E-102268)
  Workaround: Create the save filter once you issue a new query from Explorer or Illumination Plus.
- **Enforcement boundaries filters are still showing after enforcement boundaries are deleted** (E-102251)
  Workaround: None
- **SecureConnect only logs the "E" on the provider** (E-101229)
  Works as designed. There is no way to tell whether SecureConnect is in the egress path.
- **Windows 11 shows as Windows 10 on workload/VEN page** (E-100844)
  Workaround: none.
- **Flow timestamp incorrect in Illumination for inbound-only or outbound-only reported flows** (E-96595)
  The flow timestamp shown in Illumination is unreliable for ingress- or egress-only reported flows.
  Workaround: Use Explorer to see the correct timestamp.

Illumination Plus

- **Explorer/Illumination Plus filter was incorrectly interpreting flows with an empty label group** (E-105503)
  When using an empty Label Group as a filter in Explorer or Illumination, the same result was returned as expected if the filter criteria were "Any Workloads."
  This issue is resolved and works as designed.
- **Saved filter for Explore and Loading showing empty data by default** (E-102257)
  The created Saved filter for Explore and Loading is showing reported policy decisions with empty data by default.
  Workaround: None

PCE Platform

- **chronyd usage failure** (E-111664)
  - 'illumio-pce-env check' cmd relies on 'chronyc' for checking the clock drift.
  - There is a STIG (Security Technical Implementation Guide) security advisory which recommends users disable access to chronyd.
  - As of today, on implementing the STIG directive, 'illumio-pce-env check' results in a warning message: '506 Cannot talk to daemon error'.
  - Federal customers/government agencies are more likely to follow the STIG advisories.

Data Platform

- **Missing vulnerability data in the Workloads Export** (E-114354)
  The Workload export feature does not include vulnerability data.
  Workaround: none.

PCE Web Console UI

- **Proposed Rules - Status information is being hidden** (E-105098)
  The Proposed Rules status information is hidden by the "Add to Ruleset" page.
  Workaround: The information is shown on the Ruleset Summary page.