Illumio® Core

Version 24.1.4

Release Notes

06/14/2024
14000-100-24.1.4

Contents

Welcome

These release notes describe the resolved issues and known issues for Illumio Core 24.1.*x* releases.

Illumio Core 24.1.4 is available for Illumio Core Cloud customers only, depending on the version of the Illumio Core running in their environments. You can verify your version in the PCE web console.

Document Last Revised: June 2024
Document ID: 14000-100-24.1.4

What's New in This Release

To learn what's new and changed in 24.1.*x* see the **What's New in This Release** guide.

Product Version

PCE Version: 24.1.4 (Illumio Cloud customers only)

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, "24.1"
- ".c": Maintenance release number, for example, ".0"
- "-d": Optional descriptor for pre-release versions, for example, "preview2"

Resolved Issue in Release 24.1.4

- **Kubernetes Workload service network interfaces are unnecessarily updated upon every Node update** (E-116631)
  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 redeployed at the same time (via unpair/pair) while there were Kubernetes Workloads already present.

Resolved Issues in Release 24.1.3

PCE updates to support ECC Ciphers

The Illumio PCE has been updated to support elliptic-curve cryptography (ECC) cipher suites, including:

ECDHE-ECDSA-AES128-GCM-SHA256

ECDHE-ECDSA-AES256-GCM-SHA384

Resolved Issues in Release 24.1.0+UI3 PCE

- **AND operator appeared between labels of the same type in Traffic query fields** (E-115653)
  On the Traffic page, in the include and exclude (e.g., Is Not) query fields, an AND operator was inserted automatically between labels of the same type. Labels of the same type should always be joined by OR because workloads cannot have more than one label of the same type. This was a text defect only; the actual query functioned correctly because, on the back end, an OR joins labels of the same type.
- **Writing rules using Illumination Plus** (E-115225)
  Users have been unable to write rules based on port numbers using Illumination Plus. This issue is fixed.
- **Unable to create new service from within rules and 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 for Upgrade customers** (E-115189)
  Since SCP2, upgrade users have been unable to save Filters in Illumination Plus. This issue is fixed

Resolved Issues in Release 24.1.0+UI2 PCE

- **Rule provisioning from the Map** (E-115047)
  The issue with rule provisioning from the map is resolved.

Resolved Issues in Release 24.1.0

Enterprise Server

- **Traffic results were inconsistent when using Reported View and filters** (E-113043)
  This issue is resolved. Additional connections show up without rerunning or modifying the initial query; only the filters are manipulated.
- **Provisioning a Virtual service from the Details page was not working** (E-112697)
  This issue is resolved and works as expected.
- **An error was thrown during the bulk Import of Workload labels when the labels contained double-byte characters** (E-112278)
  This issue is fixed, and users can import double-byte characters.
- **GET pairing profile encountered an error in an invalid release** (E-112026)
  The issue is fixed.
- **Received an empty response when navigating to the CWP (Container Workload Profile) page on the PCE UI** (E-111845)
  If the default container workload profile is deleted, users will see a blank page when navigating to the CWP page.
- **ERROR: cannot DROP TABLE "event_bus_changes" was triggered with pending trigger events** (E-111745)
  This regression was caused by an optimization introduced to drop a temp table to avoid vacuum buildup.
  This issue is resolved.
- **Garbled characters shown in App Group Summary report** (E-111687)
  The font used for the App Group Summary report in PDF (Roboto) was causing problems because it doesn't support double-byte characters.
  It was replaced with the font Noto, and this issue is resolved.
- **The Merge option for Proposed rules was merging Existing rules** (E-111593)
  This issue is resolved.
- **Upgrade PostgreSQL to address CVE-2023-5869 and CVE-2023-5868** (E-111556)
  PostgreSQL was upgraded to mitigate exposure to two CVEs: CVE-2023-5868 and CVE-2023-5869. As the PCE uses PostgreSQL internally and does not offer external user access the likelihood of this exploit is low without additional access privileges.
  PostgreSQL was upgraded as a cautionary measure to address two CVEs.
- **Added unmanaged workloads from Explorer no longer use hostnames** (E-111363)
  When unmanaged workloads are created from Illumination Plus (Explorer), the priority for the workload name is the hostname followed by the IP Address.
  IP Address will be taken into account when the hostname for a workload doesn't exist.

- **Policy decision reported as potentially blocked for deleted workloads but not calculated in UI rules** (E-110145)
  The draft policy decision returned from the backend is incorrect, it should be labeled as 'unknown' for flows with deleted workloads.
- **Vulnerability data shows on the map only upon interaction** (E-111087)
  Vulnerability data was shown on the Vulnerability Map only when users interacted with it. This issue is resolved.
- **The Reported view was not showing if a flow was blocked** (E-111058)
  The reported view did not show if a flow was blocked by a source or destination in Illumination Plus.
  This issue is resolved and works as expected.
- **Traffic query not showing blocked DHCPDISCOVERING flows** (E-110940)
  Traffic query did not show blocked DHCPDISCOVERING flows with FlowCollection set to aggregate broadcast traffic.
  This is resolved and works as expected.
- **Global Viewer was able to click on Edit Rulesets** (E-110220)
  This issue is resolved and now works as expected.
- **Saving filter with a duplicate name did not give an error** (E-110132)
  When a filter containing a duplicate name was saved, no error was triggered.
  This issue is resolved and saving a duplicate name for a filter gives an error: "A filter with that name already exists. This will overwrite the existing filter".
  This issue is resolved and now works as expected.
- **Vulnerability data was showing on the map only upon interaction** (E-111087)
  Vulnerability data was shown on the Vulnerability Map only when users interacted with it.
  This issue is resolved.
- **Explorer page bug** (E-108585)
  When the policy was changed, the traffic view grid pagination in the draft view did not reset to page 1. This issue has been resolved.
- **IP list traffic not appearing in searches** (E-108490)
  The IP list traffic was not appearing in searches due to the inclusion of iplist containing an fqdn in query parameters.
  This leads to the inclusion of region_id in the sql query executed in each region. However, the region_id being passed is the leader's region id. The issue happens only on a supercluster.
- **Creating a traffic report for the Default Graph results in an endless loop** (E-108203)
  This issue is resolved and works as expected.
- **Blank space in IP address causes a query to fail** (E-106290)
  When filtering by an IP address in Explorer > Traffic, if a blank space appeared after an IP address in the filter criteria, the query failed. This issue is resolved.

Ransomware Dashboard

- **The "Recommended Actions" tab was showing only 16 instead of all risky services** (E-113193)
  This issue is closed and the count of risky services in the Recommended Actions list is accurate. The risky services count included the services with no associated workloads, which lack the protection coverage score. Services without a protection score are labeled as "No workload associated with the service" for clarity.
- **The Ransomware Dashboard was displaying the same port/processes multiple times** (E-112055)
  This issue is fixed.

PCE-Explorer

- **Explore Traffic was showing traffic for labels that did not match the query** (E-112968)
  When running an Explore traffic query for a particular label combination, the results show traffic from a different query.
  This issue is resolved, and the results match the labels specified in the filters.

Illumination Plus

- **UI in Illumination Plus defaulted to "search all categories"** (E-107347)
  In Illumination Plus, the UI always defaulted to "search all categories" in Explore > Traffic.
  This issue is resolved and works as designed.
- **Explorer/Illumination Plus filter was interpreting incorrectly the 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.
- **Traffic query was returning unexpected results** (E-112418)
  This issue is fixed, and the generated SQL queries for all scenarios look as expected.

PCE Platform

- **PCE remained in a partial state after the upgrade to 23.5.10** (E-113574)
  PCE remained in a partial state for a long time after the upgrade to 23.5.10, which sometimes caused intermittent test failures. This issue is resolved.
- **Changes to system_health events after upgrade to 23.2.20** (E-112922)
  After upgrading to PCE 23.2.20, system health events were including "illumio_pce/cli" rather

than "illumio_pce/system_health".
This issue is resolved.

- **The PCE failed to initialize in FIPS mode on RHEL 8.3 or higher with Ruby 3.1.2** (E-111825)
  When operating in FIPS mode on EL 8.3 or higher the PCE would be unable to start on an initial install. This issue was introduced by a change in the runtime environment and has now been fixed.

Known Issues in Release 24.1.0

Enterprise Server

- **Refused to connect 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.
- **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
- **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 the 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.

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.

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.

- **libssl upgraded to v3.1.3**
  libssl upgraded to v3.1.3 to address CVE-2023-0464. This CVE did not impact Illumio PCE.
- **postgreSQL upgraded to v13.13**
  postgreSQL upgraded to v13.13 to address CVE-2023-5869. This CVE did not impact Illumio PCE.
- **ruby upgraded to v3.1.4**
  ruby upgraded to v3.1.4.

Legal Notices