Illumio® Core

Version: 21.5.30

Release Notes

06/06/2022

14000-100-21.5.30

illumio

Contents

Welcome

These release notes describe the resolved issues and known issues for the Illumio Core 21.5.*x* releases.

Document Last Revised: June 2022
Document ID: 14000-100-21.5.30

What's New in This Release

To learn what's new and changed in 21.5, see the What's New in This Release guide.

Product Version

PCE Version (On Premises): 21.5.30 (LTS)
VEN Version (On Premises and Saas): 21.5.30 (LTS)

Release Types and Numbering

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

- "a.b": Standard or LTS release number, for example, "21.5"
- ".c": Maintenance release number, for example, ".1"
- "-d": Optional descriptor for pre-release versions, for example, "preview2"

Resolved in 21.5.30-PCE

⚠ PCE 21.5.30 is only available for Illumio On-Premises customers. The VEN is available both for Illumio Core Cloud customers and for Illumio Core On-Premises customers.

PCE Web Console

- **Workload UI page filter reverts back to name while typing** (E-87834)
  After a user selects a non-default filter and then starts typing, the filter reverts back to the default name filter. This issue is resolved.

Policy and Workloads

- **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.
- **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.
- **Rule Optimization for rules with IP lists** (E-89091)
  In this release, Illumio has optimized rules that have only IP lists on one side of the rule.
- **Container workloads could continuously sync policy with the PCE** (E-88967)
  Environments with high rates of container workload changes and container policy changes could experience a condition where all VENs were constantly syncing policy and PCE performance significantly degraded. This issue is resolved.
- **Unmanaged workload creation/deletion didn't always trigger policy changes** (E-89874)
  Under certain conditions, workload policy would not be 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.
- **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.
- **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.

Data Visualization

- **Explorer filters with OR provide inconsistent results** (E-90367)
  Explorer IPlist queries using OR would incorrectly provide 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.
- **SCP4 Core Services Detection couldn't run** (E-90231)
  A transient error prevented a data wrapper from being set up correctly on SCP4, and subsequently, the core services generator was not being restarted because of faulty detection. These issues are resolved.
- **Error when querying the IPlist traffic** (E-90112)
  Explorer queries failed when using only IPLists in filters. This issue is resolved.
- **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.
- **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 that value as a prefix but didn't return the IP list named just with that single value. For example, entering "NCR" in the field returned multiple IP lists with names that include "NCR" as a prefix but not the IP list named simply "NCR." 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.

PCE Platform

- **PCE response header names were lower case** (E-90166, E-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.

- **haproxy maxconn is not large enough** (E-89638)
  haproxy maxconn was not large enough to handle a spike of policy requests. This issue is resolved and it now accommodates a queue of 15,000 requests.
- **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.
- **Exposure charts in Executive Summary report did not show data** (E-89032)
  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.
- **Expired service-account API keys accessing non-agent endpoint** (E-88696)
  The expired service-account API keys were able to access a few endpoints. This issue is resolved. The API queries using an expired key will respond with the expected unauthorized error.
- **Database migration failed during upgrade** (E-88273)
  When upgrading Illumio Core on a Supercluster, an error message like the following appeared during the database migration step: " 'id' column is missing. A multi-master table requires an INSERT statement to provide 'id' column explicitly." Data 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.
- **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. The system has been reconfigured to increase the threshold to 384 ms to minimize the occurrences of these warning messages.

VEN

- **(Windows) "Ignore" setting not working on network interfaces** (E-89580)
  When you set a Windows workload's network interface from being Managed to Ignored, the setting does not take effect. The interface is still treated as Managed.
- **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.
- **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 has been resolved. The root cause was due to tampering at the OS level where one or more `/sbin/iptables*` or `/sbin/ip6tables*` symlinks were removed.
- **Running the Linux pairing script on a system with an unactivated VEN already installed failed to activate the VEN** (E-87853)
  After installing a VEN and then running the pairing line, the pairing script noticed an installed VEN and immediately exited, failing to successfully activate the VEN. This issue is resolved. Running the paring line on a machine that has already installed a VEN now successfully activates it.

Resolved in 21.5.21-PCE

> ⚠ Illumio Core 21.5.21 was available only for Illumio Core PCE On-Premises customers.

- **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.
- **Container workloads could continuously sync 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.

- **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.

Security Information for 21.5.21-PCE

- **OpenSSL upgraded to address CVE-2022-0778**
  The OpenSSL package was upgraded to 1.1.1n to address CVE-2022-0778 (https://www.openssl.org/news/secadv/20220315.txt). **The PCE is not impacted by this vulnerability.**

Resolved in 21.5.20

> ⚠ Illumio Core 21.5.20 was available for both Illumio Core Cloud customers and Illumio Core On-Premises customers. Illumio Operations has upgraded Illumio Core Cloud customers to later releases.

Policy and Workloads

- **Labels disappear 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 automatically removed. This issue is resolved
- **In some cases, blocked traffic was erroneously shown to be allowed in Explorer and Illumination Draft View** (E-86181)
  Given a rule that allows traffic on a specific port/protocol using a specific Windows service (for example, `135 TCP %SystemRoot%\System32\lsass.exe`):
  - Under certain query conditions, **Draft View** erroneously showed traffic to be allowed over the same port/protocol but using a different Windows service (for example, `135 TCP %SystemRoot%\System32\svchost.exe`).
  - **Reported View** correctly showed such traffic to be blocked and traffic was blocked in Enforcement Mode, but this was unexpected for customers who relied on Draft View.

  This issue is resolved. The PCE now checks the rule for Windows service properties, and Draft View in Explorer and Illumination correctly reports when such traffic is allowed or blocked.
- **Rule search incorrectly calculates label groups in Scopes** (E-72318)
  Rule search was calculating 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 Web Console

- **Events "Today" preset filter failed to return results** (E-86124)
  Clicking the **Timestamp: Today** preset filter returned no results when filtering events on the PCE (**Troubleshooting > Events**. This occurred even though events were generated on the current day. This issue is resolved and the **Today** preset now returns events generated on the current day.
- **Event forwarding UI rejects FQDNs containing underscores** (E-86061)
  When configuring the PCE to forward syslogs to an external server (**Settings > Event Settings**, addresses that include the underscore character (_) were disallowed and the message **Invalid address** appeared below the **Address** field. This issue is resolved. The Address field now accepts addresses that contain underscores.

Data Visualization

- **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.
- **Rule merging not working with multiple same-type labels** (E-87731, E-87531)
  Rule merging was not working for rules with multiple labels of the same type. 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.
- **Draft view in Full Enforcement mode showing boundaries by mistake** (E-87594)
  Explorer, in draft view, is showing boundary information for Workloads in full enforcement which is not correct. This issue is resolved.
- **Draft view between Virtual Service labels and IP lists returned an incorrect result** (E-86999, E-86830)
  In Illumination and Explorer, the draft view policy decision for a flow between labels for Virtual Services and an IP list could have been incorrect. This issue is resolved.
- **Label truncation in Illumination** (E-86960)
  Captions were truncated on the Illumination and App Group map pages. This issue is resolved.
- **Intermittent database backup failure on MNC and Supercluster** (E-86880)
  Backup failure was caused by temporary tables. Reporting database temporary tables, which have not been ignored. This issue is resolved.
- **Missing Reorder Rules option** (E-86755)
  The **Reorder Rules** option was missing from **Rules and Rulesets > Segmentation Rulesets > Scopes and Rules**. This issue is resolved. The Reorder Rules option now appears as expected.

- **Explorer queries fail when filtered on labels** (E-86565)
  Explorer queries were failing when they were filtered on labels involving deletion pending Virtual Servers after the NEN has reported that the virtual server is removed on the SLB device. This issue is resolved.

PCE Platform

- **Too many matching results on the Access Wizard page** (E-85603)
  In the Add Principals dropdown list of the Access Wizard page, invalid items could appear. This was caused by the inclusion of service accounts. This issue is resolved. Only valid users and groups now appear in Matching Results.
- **Make pairing profile last_pairing_at work in Supercluster** (E-44526)
  There was a request to make the pairing profile `last_pairing_at` work in a Supercluster. This issue is resolved.

VEN

- **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 has been resolved. The workaround is to manually create the file, C:\ProgramData\Illumio\etc\platform_handler_config.yml, and restart 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.
- **Pairing line failed with 21.2.4 VEN on Debian 11.2** (E-87023)
  VEN package installation failed on a workload failed. The pairing script reported an error when pairing the PCE with 21.2.4 VEN on Debian 11.2. This issue is resolved.
- **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.
- **Windows 2016 VEN needed a reboot every couple of months 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.

Resolved Issues in 21.5.12-PCE

⚠ Illumio Core 21.5.12-PCE was available for Illumio Core On-Premises customers only.

- **Intermittent database backup failure on PCE MNC and Supercluster** (E-87610)
  PCE backup would sometimes fail when the reporting feature was turned on due to temporary tables not being ignored in the backup. This issue is resolved.
- **LDAP authentication failed with the error "403 Forbidden"** (E-87472)
  User authentication would sometimes fail when the user was a member of a large number of external groups. This issue is resolved.

Resolved Issue in 21.5.11-VEN

⚠ Illumio Core 21.5.11-VEN was available for both Illumio Core On-Premises customers and Illumio Core Cloud customers. Illumio Operations has upgraded Illumio Core Cloud customers to later releases.

- **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.

Resolved Issues in 21.5.10

⚠ Illumio Core 21.5.10-PCE and 21.5.10-VEN are available for Illumio Core On-Premises customers only.

Policy and Workloads

- **Clone re-activation triggers an error in the policy sync** (E-86005)
  For endpoints in Core, clone re-activation could result in an error in the policy sync. This issue is now resolved. Cloned VENs already in an error state should be unpaired and reaired.
- **NEN IP sets are de-duplicated** (E-84837)
  Previously, the NEN might have received IP sets in the policy from the PCE containing duplicate IPs.
  This has been optimized at the PCE. In all cases, the NEN will program the correct policy on the managed device.
- **Can't edit an unmanaged Kerberos workload after it's been activated & deactivated** (E-84570)
  If the VEN reported multiple of the same process running (e.g. svchost.exe), the workload could not be edited after it was deactivated. This issue is resolved.
- **Improved Performance for Container Workloads** (E-84180)
  In this release, Illumio provides improved performance by programming container host CIDRs instead of container host IP addresses. For traffic initiated by a container workload and destined for outside the container cluster, the PCE replaces the container host's IP address in the external workload's inbound policy with the subnet(s) for all container hosts in the container cluster. The subnets are constructed using the IP addresses and subnet masks of IPv4 host network interfaces, with a default gateway, as reported by the VEN on container hosts. This enhancement avoids a policy recalculation on workloads outside the cluster when the following events occur:
    - Scaling up of a Kubernetes service
    - Deleting and recreating of a Kubernetes pod on a different node in the cluster
    - Replacing of a Kubernetes node for upgrade or patch reasons

  By eliminating policy updates for workloads outside the cluster, this enhancement helps reduce the amount of time required to establish communication between the pod in the cluster and a workload outside the cluster.
  NOTE: This enhancement must be enabled in the PCE `runtime_env.yml` file using the following configuration:
  ```
  agent_service:
  use_container_host_cidrs_in_container_policy: true
  ```
- **Improved performance for Kubelink service updates** (E-84179)
  In this release, Illumio provides improved performance by batch processing Kubelink service updates. Previously, when Kubelink cluster service updates occurred, the PCE immediately provisioned the changes to virtual services. Now, with this enhancement, the PCE aggregates the Kubelink-reported changes across all clusters and provisions the changes as batch updates. In environments with many container clusters and/or high rates of change to cluster services, this enhancement helps reduce PCE load and decreases policy distribution times.

If enabling this enhancement in a Supercluster, do so only in an environment where the container clusters are paired to the leader PCE.
This enhancement must be enabled in the PCE `runtime_env.yml` file. The value you specify in the `runtime_env.yml` setting determines the provisioning interval. Illumio has only certified a value of 180 seconds for this setting. Use the following configuration:

```
agent_service:
container_cluster_service_provision_interval_seconds: 180
```

- **Improved convergence times** (E-84172)
  In this release, Illumio provides improved convergence times by preventing unnecessary IP address list updates. Previously, inbound policies on Virtual Servers were updated with all workload IP addresses, including the IP addresses of container workloads that are routable only within the Container Cluster. This occurred even though Virtual Servers outside a Container Cluster never see inbound traffic directly from a Container Workload IP. Now, with this enhancement, Container Workload IP addresses local to a Container Cluster are no longer delivered to Virtual Servers. This prevents unnecessary updates to the list of Container Workload IP addresses maintained on the SLB device that were caused by updates to Container workloads.
  This optimization, combined with the Improved performance by programming Container Host CIDRs instead of Container Host IP addresses enhancement, significantly decreases or eliminates the time required before a Virtual Server outside the Container Cluster allows inbound traffic from a Container Workload.
  This enhancement must be enabled in the PCE `runtime_env.yml` file using the following configuration:

  ```
  agent_service:
  exclude_container_ips_in_virtual_server_policy: true
  ```

- **AUS rules could fail to allow outbound traffic to virtual services** (E-83508)
  When an AUS rule included a virtual service in the provider field or a label in the provider field applied to the virtual service, the rule could fail to allow outbound traffic to that virtual service when it should be allowed. This issue is resolved. In this release, rules with virtual services in the provider field correctly allow traffic for AUS users.
- **Mislabeled link appeared in error on Enforcement Boundaries page** (E-83149)
  If you logged in to Illumio Core as a Supercluster member, navigated to **Rulesets and Rules > Enforcement Boundaries** and there were no enforcement boundary rules to display, the link **Add a new Pairing Profile** appeared in error. There were two problems with this:
    - The link was mislabeled. The label should've specified creating an enforcement boundary.
    - Users logged in as Supercluster members should not have seen a link in this case.
- **PCE Listen Only mode did not yet apply to NENs** (E-80376)
  Listen Only mode allows you to temporarily stop the PCE from sending policy updates to your VENs. Policy updates resume only after you disable "Listen Only" mode. This behavior

wasn't available for NEN/F5 policy updates, which meant that there's a chance that an F5 SLB could receive a stale policy when the PCE was in Listen Only mode. This issue is resolved.

- **Rule search incorrectly calculated label-groups in Scopes** (E-72318)
  When a rule had label groups in the scope, multiple scopes were created and traffic wasn't allowed between scopes unless specified with extra-scope rules. For example, Workload 1 and Workload 2 couldn't talk to each other based on the policy because they were in different scopes. However, rule search for Workload 1 to Workload 2 allowed access by this rule. This issue is resolved.
- **The timestamp "updated_at" was not changed when a workload label was edited** (E-68720)
  When workload labels are updated through the API or the PCE web console, the timestamp "updated_at" in the workload API response was not updated.
  This issue is resolved and the field "updated_at" is now updated with the correct timestamp information.

PCE Web Console

- **Loopback interfaces in use not showing up on the Label Groups list page** (E-85509)
  This issue is resolved. This feature now works as expected.
- **All Services search option not available in Rule Search UI** (E-84582)
  When performing either a Basic or an Advanced search for rules in Illumio Core (**Rulesets and Rules > Rule Search**), the **All Services** option was not available. This issue is resolved. The **All Services** option shows as expected.
- **Events page missing information for workload.offline_after_ven_goodbye event** (E-84391)
  When the PCE encountered the workload.offline_after_ven_goodbye event, it didn't display the name, hostname, HREF, and labels for the affected workload in the PCE web console **Events** page. This issue is resolved. The **Events** page now displays this information for affected workloads.
- **The Events filter "Generated By" allows only System and Users** (E-81277)
  This issue is resolved. The filter shows "Generated by Agent" unless the Agent was unpaired, deleted, or removed.
- **User with Limited Ruleset management permissions could not edit extra-scope rules** (E-60189, E-67698)
  When both the Provider and Consumer were within the scope, a user with Limited Ruleset Management permissions could not edit extra-scope rules. This issue only happened in some scenarios when a user has multiple scopes assigned. The issue is resolved. The issue was due to a bug in our write enforcement for edits. When a user attempts to edit a provisioned rule (which does not exist in draft), we create a copy of the object and perform a save. Then, we perform the edits on top of that newly created object and perform a second save. When the saved draft was invalid, write enforcement stopped edits that would have made it valid. This issue is resolved. We now skip the RBAC write enforcement checks when fetching the draft object.

Data Visualization

- **Qualys vulnerability reports failing to import when using the CLI Tool** (E-85068)
  Qualys vulnerability reports could fail to upload into the PCE when using the CLI (ILO) Tool. This issue occurred when the scan reports in the XML file had overly long names. This issue is resolved. In this release, the CLI Tool successfully uploads Qualys vulnerability reports even when scan reports in the XML file have long names.
- **Deleted labels from proposed ruleset page showing in rules** (E-85046)
  While working with enforcement boundaries, users observed that the deleted labels from the proposed ruleset page are showing in rules along with new labels. This issue is resolved and the deleted labels do not show together with new labels anymore.
- **Explorer queries could return zero results when searching by FQDNs that had wildcard characters** (E-85032)
  This issue occurred because of the way that the PCE supported FQDNs with wildcard characters. It didn't support FQDNs with wildcard characters in IP lists at all. In user-specified FQDNs, the PCE supported wildcards in domain names but only when the wildcards appeared at the beginnings or ends of the domain names; for example, `*.wns.windows.com` was supported but `foo.*.bar` wasn't supported. This issue is resolved for both cases. Explore queries that search by FQDNs that have wildcard characters correctly return results. **High**
- **latency could impact Illumination map display in PCE web console** (E-84816)
  When a user viewed the Illumination map, the PCE web console always refreshed map data regardless of currentness. This behavior could impact performance. This issue is resolved. In this release, the PCE web console will display cached data in the Illumination map when the map has less than 200 workloads (controlled by the user's workload RBAC permissions).
- **Database backup could fail with an error message that illumio/tmp subdirectory already exists** (E-84731)
  When the `ephemeral_data` directory was universally writable, backing up traffic and reporting databases could fail and return a confusing error message. This issue is resolved. In this release, the PCE checks whether the `ephemeral_data` directory is universally writable before the backup runs and, if it is writable, returns an informative error message.
- **Top Detected Processes of a Core Service shows empty results** (E-84618)
  IP is detected as a core service but Explorer returns no results. This issue is resolved and the feature works as expected.
- **Legend wasn't clear in Executive Summary Reports** (E-84343)
  In Executive Summary reports, you view data over a time range. These sections include a legend on the left that displays data for the report time range only. The right side displays the data in stacked bar graphs each time the recurring report is run. When the report was run daily, the legend didn't include a date so it appeared that data was aggregated across all recurring reports, which isn't correct. This issue is resolved. In this release, the legend includes the date for the data. Additionally, the following fields in the feature have clearer values:

Add Report > Time Range: "Last 24 Hours" changed to "Last Day"
Report PDF > Top Summary > Time Range: "1 day" changed to "Last 1 day"

- **Sorting for Unknown IP Detected Core Services not working** (E-84070)
  Sorting on the Server column for Unknown IP Detected Core Services is not working properly and both the ascending and descending sorting show the same values. However, sorting for Workloads works properly. This issue is resolved and the feature works as expected.
- **A deleted unmanaged workload of an accepted core service is still listed in the Accepted tab** (E-84067)
  The deleted unmanaged workload is showing under the Accepted Tab with the Server IP. This issue is resolved and the feature works as expected.
- **Global Explorer queries could fail at least half the time** (E-83921)
  When the Supercluster leader was deployed in a split data center, Global Explorer queries could fail 50% of the time. This issue is resolved.
- **Unexpected and Incorrect 'Permission Denied' alert in the GUI** (E-83445)
  A user who doesn't have Global Org Owner permissions gets the 'Permission Denied' error when he/she tries to use to Explorer page. However, the user was able to perform the required action despite the error. This issue is resolved and the incorrect error was removed.
- **Killed/timeout query doesn't show in Explorer result** (E-83338)
  After an Explorer query was killed or timed out, this query would disappear on the results page, making it impossible to track a failed query. This issue is resolved.

PCE Platform

- **Error occurred when trying to change telegraf_port** (E-85899)
  If a user had a service using port :8125, starting the PCE generated the following error: `[telegraf] Error running agent: starting input inputs.statsd: listen udp :8125: bind: address already in use`
  This issue happened because, prior to this fix, the `telegraf.conf.erb` port value for `statsd` was hard-coded to service_address = ":8125"
  This issue is resolved. Port 8125 is no longer hard-coded and the PCE now allows users to change the `telegraf_port` by updating the `runtime_env` and then restarting the PCE.
- **Rare mismatch prevented PCE data node from coming online** (E-85733)
  When setting up a PCE for the first time, in rare cases a mismatch occurred between the database user `pwd` command in the database and the Illumio key-value store. This prevented PCE data nodes from coming online (runlevel 1-5) and generated the error `Failed to create/alter application DB user`. This issue is resolved.
- **Access denied when editing API Key Settings** (E-85673)
  When trying to edit API Key Settings, SaaS customers without root permissions received the message `Unable to Edit Service. Access denied`. This issue is resolved and now global org owners can edit API Key Settings.

- **PCE in a partial state following an upgrade** (E-85414)
  In rare cases, following an upgrade the PCE remained in a 'PARTIAL' state. Issuing the command `sudo -u ilo-pce illumio-pce-ctl cluster-status` showed that the `set_server_redis_server` service wasn't RUNNING. The `set_server_0_master.log` could have shown entries similar to the following:
  `Warning: Could not create server TCP listening socket 127.0.0.1:6000: listen: Address already in use`
  This issue is resolved.
- **Support bundle wasn't generated when fileserver failed over** (E-85198)
  When using **Troubleshooting** > **PCE Support Bundles** in the PCE web console, an error sometimes occurred if the fileserver failed over. The support bundle functionality couldn't detect the correct fileserver and the support bundle couldn't be created.
  This issue is resolved.
- **Couldn't log into the PCE** (E-84777)
  If the web server was under heavy load, occasional failures could occur when attempting to log in to the PCE. This issue is resolved.
- **Unnecessary number of PCE events generated for SA API key expiration and deletion jobs** (E-84693)
  A PCE event was generated whenever a Service Account (SA) API key expiration and deletion job ran, regardless of whether any SA API keys were expired or deleted at the time. As a result, an unnecessary number of events were generated. This issue is resolved. Now, SA API key expiration and deletion jobs generate an event only when there are such keys that have expired or have been deleted.
- **API returned incorrect values for service account API key management** (E-84459) Querying with the `api_key` API returned incorrect values for X-Total-Count and X-Matched-Count. This issue is resolved. Correct values are now returned when querying with the `api_key` API.
  Updated query parameters for API keys (E-84388)
- Some parameters have been renamed or deprecated to allow differentiation between the type "user" and "service_account:"
  - Query parameter "name" is retained for the type "service_account"
  - Query parameter "name" is changed to "username" for the type "user"
  - Query parameter "service_account_name" was deprecated and consolidated to "name"
  - Query parameter "api_key_name" was deprecated and removed as not needed
- **LDAP user unable to log into PCE when directory search returned more than one result** (E-83974)
  User authentication could fail for user DNs that had LDAP entries below them. This configuration is common for user devices, such as `ExchangeActiveSyncDevices`. This issue is

resolved. In this release, the PCE only queries the LDAP directory for username attributes that are an exact match.

- **Error occurred when editing labels or unpairing workloads** (E-83924)
  When you added a scoped role to a user with an unrestricted role, then tried to edit the labels on a paired workload or manually unpair a workload, a "500 Internal Server Error" occurred. This issue is resolved.
- **Virtual server events API could return missing or incorrect data** (E-81611)
  When using the Events API to update a virtual service, the API did not expose label deletion information in the resource changes section. This issue is resolved. In this scenario, the Events API now exposes label deletion information.
- **UI Service Accounts: Cannot remove Access Restriction** (E-80826)
  When a user removes an access restriction from a service account, the UI does not send the access restriction property along with the updated data.
  Workaround 1: Create another service account instead of removing the access restriction.
  Workaround 2: Remove the access restriction key associated with the service account by using the service account API directly.

VEN

- **VEN Compatibility Report Returns a row with an empty Type** (E-86148)
  This issue is resolved and the UI works as expected.
- **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.
- **Policy that includes wrong PCE IP address fails while in Illumination mode** (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 could 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 retry 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: 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.

- **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, both seemed to be using port 3389. This issue is resolved.

Resolved Issues in 21.5.3-PCE

> ⚠ Illumio Core 21.5.3-PCE was available for Illumio Cloud customers only. This release was not available for Illumio Core On-premises customers. Illumio Operations has upgraded Illumio Core Cloud customers to later releases.

- **Problem when filtering workloads by IP address** (E-86674)
  When filtering workloads by IP address in **Workloads and VENs**, the filter type changed to **Name** when the last digit of the IP address was entered in the filter view field, resulting in a filtered view that found no matches. This issue is resolved. Once selected, the **IP Address** filter type no longer changes to **Name** when filtering by IP address.
- **Missing Reorder Rules option** (E-86755)
  The **Reorder Rules** option was missing from **Rules and Rulesets > Segmentation Rulesets > Scopes and Rules**. This issue is resolved. The Reorder Rules option now appears as expected.

Resolved Issues in 21.5.2-PCE

> ⚠ Illumio Core 21.5.2-PCE was available for Illumio Cloud customers only. This release is not available for Illumio Core On-premises customers. Illumio Operations has upgraded Illumio Core Cloud customers to later releases.

- **High latency could impact Illumination map display in PCE web console** (E-85938, E-84816)
  When a user viewed the Illumination map, the PCE web console always refreshed map data regardless of currentness. This behavior could impact performance. This issue is resolved. In

this release, the PCE web console will display cached data in the Illumination map when the map has less than 200 workloads (controlled by the user's workload RBAC permissions).

- **Explorer queries could take longer to return results** (E-85853)
  When an Explorer query returned a high number of traffic flows (for example, 100,000 or more), the results could take a long time to appear in the PCE web console and when using the Illumio REST API. This issue is resolved. In this release, the performance for Explorer queries that return a high number of traffic flows has improved.

Resolved Issues in 21.5.1-PCE

- **Database restore could fail in an MNC or Supercluster** (E-84681)

  > ⚠ This issue applies to Illumio Core On-Premises customers only.

  Running the `supercluster-data-restore command` failed and displayed an error because the database was being used by another process while restoring the backup data. Consequently, table conversion for the database was incomplete. This issue could affect both an MNC or a Supercluster member. A workaround was available. This issue is resolved. In this release, running the `supercluster-data-restore` command succeeds as expected.
- **Incorrect number of IP addresses reported for traffic flow in App Group Map** (E-85418)
  When viewing details about an application in the App Group Map and setting the time filter option to **Anytime,** too few IP addresses were reported to be contributing to the traffic flow. Narrowing the time period by moving the slider to the right allowed all IP addresses contributing to the flow to be displayed. This behavior was unexpected; the number of IP addresses reported when Anytime is selected shouldn't be less than when the Time filter is set to a narrower time frame. When traffic from different IP addresses used the same port to run different Windows services, selecting **Anytime** allowed IP addresses from the oldest Windows service to be displayed, which was a subset of the actual number of IP addresses contributing to the flow. Narrowing the time period allowed the other IP Addresses from newer Windows services to be displayed. This issue is resolved. The number of IP addresses reported is now correct when the **Filter by Time** setting is set to Anytime.

Resolved Issues in 21.5.0

PCE Web Console

- **The clickable user link in the Provision dialog box didn't open a user page** (E-83641)
  This issue is resolved and the user link opens a user page in a new tab.

- **Initial VEN version reverted to the current default when editing a profile** (E-82523)
  When editing a pairing profile (**Workloads and VENS > Pairing Profiles**), the VEN version specified in the **Initial VEN Version** field reverted to the **Current Default** VEN version automatically. This meant that, unless the user re-entered the previously-specified VEN version, the current default version of the VEN was installed on the workload instead, which was unexpected. This issue is resolved; the Initial VEN Version field retains it's configured version unless it's changed by the user.
- **Problem forwarding syslogs to an external server** (E-82503)

  ⚠ This issue applies to Illumio Core On-Premises customers only.

  When configuring the PCE to forward syslogs to an external server (**Settings > Event Settings**), addresses that include letters followed by any number were disallowed and the message " Invalid address" appeared below the Address field. This issue is resolved. The Address field now accepts addresses with numbers that follow letters.
  Unable to create a rule when providing a service as "stateless" (E-82444)
  The stateless option is not available after saving an Intra Scope rule; however, when first creating a new service and then selecting the stateless option, both options are retained. This issue is resolved.
- **Deleting stale records in the PCE** (E-82435)
  When users viewed a deleted label in the Web Console by entering the ID from the label href directly into the browser's address bar, the Remove button was not disabled for the already deleted label. When using the Remove button to delete the label again, a "404 Not Found" error occurred. This issue is resolved. The UI now shows as grayed-out both the deleted label and the Delete button, making sure that users know this action is not available.

Policy and Workloads

- **Label-based policy for virtual service could be overly broad** (E-84702)
  In rare cases, label-based policy for virtual services could be overly broad. This issue could occur when you specify a label in a rule but the label wasn't applied to any virtual services. This issue is resolved.
- **VEN pairing profile marked as updated at the time of pairing** (E-83967)
  This issue is resolved. The PCE does not change the "last modified" information when the pairing profile is simply used to pair a VEN.
- **Not all container workloads present on PCE** (E-81376)
  In rare cases, during a scale-up event, not all container workloads would be reported to the PCE. This issue is resolved.
- `workload.offline_after_ven_goodbye` **not including affected workloads** (E-78148)
  The event message reported only an event but there was no information about which

workload(s) went offline after the goodbye message. This issue is resolved partially for consuming events via API and syslog.

Data Visualization

- **PCE Health could report a high failure percentage for the flow rate** (E-82901)
  The **PCE Health Application** tab could report a high failure percentage (possibly as high as 100%) in the **Collector Summary** section. The collector log indicated the failures occurred because the database cache wasn't ready and wasn't processing collector requests. The issue occurred after services restarted on the PCE data node. This issue is resolved. In this release, restarting services on the data node no longer causes the PCE Health page to report a high failure percentage for the flow rate.
- **Archived flow data caused high Backlog Disk Utilization** (E-84587)

  ⚠ This issue applies to Illumio Core On-Premises customers only.

  Unexpected archiving of flow data caused an increase in the archive folder size. The problem stemmed from a special character in the username which caused routine uploading of reference data to fail, which in turn caused flow data to be archived, resulting in an abnormal increase in the size of the flow data archive file. Affected customers would have seen an indication of this in **PCE Health > Application > Traffic Summary > Backlog Disk Utilization**. This issue is resolved. The PCE now handles invalid characters in a way that no longer causes this problem.
- **IPv6 address filtering didn't work in Explorer** (E-84481)
  In Explorer, trying to filter Consumers by IPv6 address returned no matching results. This issue is resolved.
- **Workload count incorrect in Executive Summary Report** (E-84300)
  In some environments with workloads that have been paired and unpaired, the Total Workloads count was incorrect in the generated Executive Summary Report (**PCE > Reports**). This issue is resolved.
- **Location view in Illumination couldn't reload and display the map** (E-84091)
  When either end of a connection contained workloads without the Role label in the discovered groups, the Illumination map sometimes failed to reload and display the map. This issue occurred when you clicked the discovered groups on either end of the connection to view the workloads in the group. This issue is resolved. In this release, discovered groups display even when they contain workloads missing the Role label.
- **Global Explorer async query sometimes failed when Supercluster member experienced Health issues** (E-83287)
  The PCE Health monitoring feature provides warnings and errors when Supercluster members experience issues. Under these circumstances, Global Explorer asynchronous queries

sometimes failed for all members instead of returning data for the healthy members. This occurred only in situations where the PCE consul service was unavailable in a Supercluster region and didn't occur for other PCE Health warnings or errors in a region. This issue is resolved.

- **Input validation error using Policy Generator** (E-82828)
  When using Policy Generator, if the ruleset included a rule containing a label_group and Vulnerabilities were enabled, the message "Unexpected input validation error" appeared. This issue is resolved. Policy Generator now works as expected under these circumstances.
- **Illumination Map became stuck in "loading" state** (E-82577)
  In rare circumstances, when attempting to visualize an environment with more than 50 unlabeled workloads, the Illumination Map got stuck in the "loading map data" state and didn't display. This issue is resolved.
- **In Draft View, Illumination map was slow to display in some circumstances** (E-82562)
  In environments with many IP lists, it sometimes took more than a minute for the Illumination map to display while in Draft View. This issue is resolved. While in Draft View, the Illumination map now renders much faster overall.
- **Pagination error after switching filtered views in Explorer** (E-82534)
  In Explorer, a pagination error occurred when switching between two different filtered views. For example, if you filtered by **Draft View > Blocked**, scrolled through five pages of filtered results, and then filtered by **Draft View > Allowed** , the Allowed filtered results began on page 5 instead of page 1, which was unexpected. To show filtered results from page 1, users had to refresh the browser. This issue is resolved. Filtered views now always start on page 1.
- **Roles didn't display in Discovered Group list page** (E-82526)
  When viewing details of a Discovered Group by drilling into the group from the Illumination Map, the Role column in the group's Workloads tab was empty. This issue is resolved.
- **Filters selected in Global Explorer and App Group Explorer appeared in both places** (E-82479)
  When selecting filters in Global Explorer, the same filters were also selected by default in **App Group > Explorer** tab. Likewise, filters selected in **App Group > Explorer** tab were also selected by default in Global Explorer. This behavior was unexpected. The expected behavior is that filter selections apply only in the area of the product from which they are selected. This issue is resolved and filters now apply only where they are selected.
- **Explorer Results page displayed a message that query results exceed limit** (E-82743)
  When querying in Explorer, the result pages sometimes indicated that the number of returned results exceeded the configured maximum number in the PCE. The issue occurred because the PCE incorrectly validated the count based on total matches in the traffic database instead of the actual results the user could view consistent with RBAC permissions or the actual number of results after filtering query exclusions. This issue is resolved.
- **The API parameter max_explorer_query_timespan_days was not honored** (E-82233)
  After setting an org's `max_explorer_query_timespan_days` parameter to fewer than 30 days, the option to filter by **Last Month** still appeared in the API and in the Explore UI, which was

unexpected. The **Last Month** filter option shouldn't be available when the parameter is set to fewer than 30 days. This issue is resolved. The `max_explorer_query_timespan_days` parameter is now honored.

- **X-axis labels were incorrect in the Executive Summary Report** (E-82226)
  When viewing any of the bar charts, the labels on the x-axis did not appear in chronological order or increment one day per bar. This issue is resolved.
- **"Visibility Only" Workload Filter didn't work properly** (E-74231)
  Applying the "Visibility Only" workload filter didn't reduce the Connected App Groups count reliably and could be changed again after a refresh. This issue is resolved.

PCE Platform

- **Potentially blocked syslog traffic was not present in log** (E-84710, E-84789)
  With the PCE set up to forward potentially blocked traffic to the syslog server, other logs appeared, but not potentially blocked traffic. The cause was an error in the syslog configuration code. This issue is resolved. Potentially blocked traffic is now logged.
- **(Supercluster) Migration failed and slony services did not start on upgrade** (E-84281)

  ⚠ This issue applies to Illumio Core On-Premises customers only.

  In some environments and after certain previous upgrades, Supercluster upgrade to 21.2.x or later PCE versions failed during migration on member PCEs with an error like "An error has occurred, this and all later migrations canceled". Or, if migration succeeded, slony services would not start, with an error like "[agent_slony_service] Configuration appears to have failed." Also, on member PCEs, one or more tables might have missing replication triggers, causing replication issues. This issue is resolved. These upgrade issues no longer occur. This issue was described in more detail in Supercluster Upgrade Failure When Upgrading to 21.2.x or Later (login required).
- **Name of removed service account could not be reused** (E-83917)
  After a service account was deleted, its name could not be used again within the same org. This issue is resolved. The name of a deleted service account can be used for a new service account.
- **Isolated node caused error** (E-83819)

  ⚠ This issue applies to Illumio Core On-Premises customers only.

  A 500 Internal Server error occurred some time after a PCE node became isolated, and in server log messages, a long time interval was reported between `isolated_time` and `now`. This

occurred because the "node isolated" flag was not cleared when the node came back online. This issue is resolved. The "node isolated" flag is now cleared.

- **(Supercluster) Tab missing from PCE Health, and information missing** (E-83516)

  > ⚠ This issue applies to Illumio Core On-Premises customers only.

  The Supercluster tab was sometimes missing from the PCE Health page of the PCE web console, and the replication lag was not being calculated. This was caused by a cached connection to a data node that was no longer valid. This issue is resolved.
- **Service discovery log contains debug messages in production** (E-83455)
  In the `service_discovery` log, DEBUG level messages sometimes appeared. These messages could be identified by containing the text "level=debug." This issue is resolved. Only messages of type INFO are now logged, as expected.
- **(Supercluster) During rolling upgrade of PCE, service repeatedly restarted on another PCE** (E-83332)

  > ⚠ This issue applies to Illumio Core On-Premises customers only.

  In a Supercluster, when one PCE is in the midst of a rolling upgrade, the replication monitoring service restarted multiple times on a PCE in another region. This occurred because a PCE in the process of upgrading can be unreachable. This issue is resolved. If a remote PCE becomes unreachable, the connection is retried without restarting the replication monitoring service.
- **PCE upgrade failed** (E-83200)

  > ⚠ This issue applies to Illumio Core On-Premises customers only.

  Upgrading a PCE to release 21.5.0 failed. The failure was reported on data nodes with a NEN installed via the error "PGPASSWORD cannot be included in the command. Please use env_hash to pass is as env variable." This issue is now fixed. Upgrading to PCE release 21.5.0 now succeeds.
- **Access restriction could not be deleted after deleting service account** (E-82752)
  When attempting to delete an access restriction, the message "Access Restriction is associated with one or more users" was displayed. This occurred when using a service account with access restriction in place. If you deleted the service account, you could not later delete the access restriction which had been associated with it. The association between the access restriction and the service account persisted after the service account was deleted. This issue is resolved. When a service account is deleted, the association with the access restriction is explicitly removed.

- **Login denied message changed** (E-82583)
  When the Read Only User feature is turned off, and a local user has no permissions, any login attempts are blocked, which is the expected behavior. However, the message generated had changed from the expected "You are not authorized to access this Organization." to "Access denied." This issue is resolved. The message has been changed back to "You are not authorized to access this Organization."
- **Service accounts: JSON report error** (E-82377)
  When generating an export report, if you selected JSON format and selected Service Accounts in the Containing All dropdown list, the report was not exported. In the Export Reports page, the Status column showed "Error". This issue is resolved. The report is now exported without error.
- **Vacuum backlog warning at almost 50%** (E-80929)
  On systems with very light database activity, the vacuum backlog metric of the policy database sometimes showed a high percentage (>= 40%) and the metric could be in a warning state. This issue is resolved. The vacuum backlog metric no longer promotes a needless warning.
- **Asynchronous GET requests returned 403 errors when using Service Account** (E-84292)
  When using a service account-based API key with the Illumio REST API, performing an async GET request returned an HTTP 403 error. This issue is resolved. This release now supports performing async GET requests while using a service account.
- **Time Drift warning for PCE nodes was misleading** (E-81610)

  > ⚠ This issue applies to Illumio Core On-Premises customers only.

  The Time Drift health warning is displayed in the PCE Health page when time drift is detected between two PCE nodes. Time drift is the difference between the time when PCE cluster health was generated and the time when node health was generated. If NTP was not set up correctly, the PCE might use stale information to generate the Time Drift warning, so the Time Drift warning message could be misleading. This issue is resolved. The Time Drift warning message is now accurate.
- **Details for removed node no longer visible in PCE Health** (E-81353)

  > ⚠ This issue applies to Illumio Core On-Premises customers only.

  The command `illumio-pce-ctl cluster-leave` removes a node from the PCE, but it did not remove details about the removed node from the PCE internal registry. As a result, the PCE Health page showed nodes that were no longer participating in PCE operations. This issue is resolved. The removed nodes do not appear on the PCE Health page.

REST API

- **User RBAC permissions not properly enforced for /system_health API endpoint** (E-82750)

  > ⚠ This issue applies to Illumio Core On-Premises customers only.

  Local PCE users with no role assigned have been able to use the API to obtain potentially sensitive information.
  This issue is resolved. A user who has no role assigned and is sending requests via API now receives the forbidden access error 403.
- **Events API firewall_settings returns wrong values** (E-81959)
  The Events API was exposing only creation and not the deletion information for policy scope sub-properties on `firewall_settings` resource changes. This issue is resolved.
- **Events API returning insufficient information** (E-81867)
  The Events API did not expose changes to the service process `name` or process `path` for Windows-based service updates. This issue is resolved.
- **500 error returned when sending an email address as the query parameter** (E-81798)
  The 500 error was returned when users sent their email address to the Events API, while the error was not returned when they send their user ID.
  This issue is resolved. Users must use only their user ID for a query and not the email address.
- **Events API returns improper information** (E-81615)
  The Events API did not correctly provide all resource changes in the resource changes section of the event for ruleset changes. This issue is resolved.
- **Virtual Services events incorrectly reported** (E-81609)
  The Events API did not expose address pool changes or label deletion information when performing virtual service updates. This issue is resolved.
- **21.2 async API calls response time doubled** (E-80282)
  This issue is resolved so that the Exit Strategy is now memory-usage based, rather than job-count based, which also helps customers with large databases.

VEN

- **Policy error thrown after changing the enforcement state from Full Enforcement to Visibility Only mode** (E-83721)
  Given the following factors:
  - VENs installed on Linux nodes on which IPv6 support was disabled
  - In a domain with a DNS server that could return IPv6 address records
  - An Illumio security policy that included FQDN rules that allowed the DNS server to send IPv6 DNS responses

Issue: A policy error showed up in the **Workloads and VENs > Workloads** page after the user changed the enforcement state from **Full Enforcement** back to **Visibility Only** mode. This issue is resolved.

- **Unsupported Pairing Script option was available through the CLI** (E-83264)
  A deprecated visibility option in the Pairing Script, `flow_full_detail`, appeared for Core 21.2.x-VEN customers who used a command line to pair a VEN. If the deprecated option was chosen, the VEN didn't pair successfully and an error message appeared advising customers to check their activation code. This issue is resolved; the deprecated option has been removed from the Pairing Script.
- **VEN service on RHEL 8.x workloads crashed following upgrade** (E-82319)
  Following an upgrade to Core 19.3.6+H3-VEN, a policy sync error occurred and the VEN service `venPlatformHandler` crashed on workloads running RHEL 8.x with consecutive IP addresses specified in `etc/resolv.conf`. This issue is now resolved and `PlatformHandler` no longer crashes in these circumstances.
- **Unexpected tampering events could occur** (E-79445)
  You could occasionally detect firewall tampering events when the Firewall Coexistence feature was enabled in the PCE for the container and host workloads in the container cluster. This issue occurred when Illumio Kubelink couldn't connect to the PCE and, as a result, the container cluster wasn't “In Sync” with the PCE. This issue is resolved.

Known Issues in 21.5.30

Limitations in 21.5.30

- **Can not perform Supercluster rolling upgrade to 21.5.30 from versions earlier than 21.5.20** (E-91847)
  Due to a software change in 21.5.20, you can only do a rolling upgrade when the installed and upgrade versions are both either before 21.5.20 or after it. For example, you can do a rolling upgrade from 21.5.20 or 21.5.21 to 21.5.30, but not from 21.5.10 to 21.5.30.

PCE Web Console

- **Warning message about discarding pending changes doesn't always appear** (E-82420)
  If you click your browser's Back button when creating or editing a ruleset, the warning message "Are you sure? Leaving this page will discard pending changes" doesn't appear. However, the message does appear if you attempt to navigate away from the page by clicking options in the PCE Web Console.
- **Filtered searches for workloads on Virtual Servers page returns 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 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 and will be fixed 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 presses 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)
  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; see Use a Wildcard to Filter Workloads. 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.

There is no workaround, but this is a rare situation because the % symbol is not used much in values.

- **Clicking deleted ruleset in Policy Versions shows "Resource Not Found"** (E-62929)
  In the PCE web console Policy Versions page, when you click the name of a deleted ruleset, the message "Resource Not Found" is displayed. This is because the deleted ruleset does not exist in that version. The message is correct, but not as informative as it could be.
- **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.
- **Cannot create a rule with a label type defined in the Scope** (E-59100)
  In the UI, you cannot create a Rule with a label type that has also been used in the Scope. Workaround: You can create such a Rule using the API.
- **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 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 could appear in the "Deletion Pending" state on the PCE. You can safely revert these Virtual Servers if they still exist on the F5. The policy is not affected by this issue.

- **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 existing 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.
- **Incorrect Group Label count is displayed while editing a group for a workload** (E-68691)
  Workaround: This issue can be resolved by backend providing a subset of results with the total filtered count.
- **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

- **Last Month time filters incorrectly show for a set timeframe** < 30 days (E-84022)
  Last Month's time filters shouldn't appear when the option `max_explorer_query_timespan_days` is set to < 30 days in the enforcement boundaries Blocked Connections page.
  Workaround: None.
- **Can't filter Enforcement Boundary blocked connections by "Potentially Blocked"** (E-81968)
  When viewing the blocked connections for an Enforcement Boundary (**Rulesets and Rules** > **Enforcement Boundaries** > **Blocked Connections** tab), the drop-down list of filters doesn't include the "Potentially Blocked" option under **Draft View**.
  Workaround: None, however, you can sort the table by connection status to group to potentially blocked connections.
- **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 are not correctly aligned with the columns in the results table.
  Workaround: None; however this issue is cosmetic only and does not impact the query results.
- **Refresh icon in Illumination doesn't update the map** (E-81744)
  Clicking the refresh icon (class="confluence-embedded-file-wrapper confluence-embedded-manual-size"> ) in Illumination to recalculate map data doesn't update the map with new workload details. However, clicking the **Refresh** button in the **Workloads and VENs** > **Workloads** page updates the list with new information.
- **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.
- **Labels added unnecessarily in rules** (E-81286)
  For extra-scope rules, Illumination unnecessarily adds labels that are already in the scope of the ruleset into the rules.
- **Switching categories in an Explorer filter adds extraneous text to the filter** (E-80938)
  When switching between categories in the Explorer query filters without selecting an option from the category, the PCE web console adds the text "or" to the filter.
  Workaround: None; however, this issue is cosmetic only and does not impact the Explorer query.
- **App group name showing in error** (E-76638)
  App group name should not be shown in the consumer or provider filter for the workload

manager role.
The return from database flows the Explorer display is showing as “0” flows.
This is specific to users with workload manager roles. The app groups should not show in the Consumer or Provider filter.

- **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 a 69.8 the Total is showing as 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.
  Workaround: Not available
- **Add Rule panel not displaying for selected traffic with right-click actions** (E-68548)
  On 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.

PCE Platform

⚠ These known issues apply to Illumio Core On-Premises customers only.

- **Support Bundle download gives 502 error** (E-91480)
  Workaround not available. This issue will be resolved in the next release.
- **Backport 2nd fix to 21.5.x: PCE Support bundle failure with 21.5.21** (E-91929)
  Workaround not available. This issue will be resolved in the next release.
- **PCE Support bundle failure with 21.5.21** (E-91132)
  Workaround not available. This issue will be resolved in the next release.
- **PCE node stop command fails** (E-84227, E-84719)
  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`.

- **PCE Health can report unnecessary critical status** (E-71044, E-68442)
  The PCE Health feature uses a 1-hour sliding window to collect and report PCE Node Health status. Initially, the feature can report the state as critical after only a few failures. The critical status clears after more data is posted to the log.
  Workaround: Wait until the PCE collects more Node Health data to verify the actual PCE Node Health.
- **The agent.log in a Supercluster deployment can include an undefined method** (E-66998)
  When a Supercluster configuration fails to load, the `agent.log` for that Supercluster deployment can include an undefined method `external_fqdn` exception.
- **PCE uptime value can be wrong in the PCE Health page** (E-45143)
  Temporary, expected PCE service restarts can reset the PCE uptime values displayed in the PCE web console's PCE Health page so that it is not consistent with the uptime values displayed by "illumio-pce-ctl start".

REST API

- **Events API: Missing information for Access Restriction** (E-82044)
  Auditable events generated during create/update of access restriction do not project the changes correctly.
- **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

- **Windows Services with invalid process paths trigger Policy Sync errors for affected VENs** (E-77105)
  Creating a Windows service with an invalid process path can trigger a Policy sync error on affected Edge endpoints and Core VENs. For example, the path `*\spoolsv.exe` is invalid because Illumio doesn't support wildcards in paths. To avoid this issue when specifying a process path, make sure to provide the full path beginning with the drive letter.
- **platform.log shows "No such file or directory" and "Could not set connect ion policy to loose error" errors** (E-71943)
  Error messages similar to these show up in platform.log:
  ```
  2020-09-29T10:41:36.126-07:00 INFO:: TCP loose connection grace period set to zero. Disabling strict tcp connections.
  2020-09-29T10:41:36.186-07:00 ERROR:: Could not set connection policy to loose error
  ```
  Cause: VEN transitions between managed and unmanaged (Idle) state before conntrack

check timer expires. No workaround is required. The VEN will recover itself once it is in a managed state (out of Idle) and the conntrack loose timer expires.

- **VEN generates event with severity Err instead of Info when unsuspend command is run twice** (E-69196)
  Unsuspend a VEN by using the PCE web console or REST API so that the VEN is active. Then, unsuspend the VEN using the command `/opt/illumio-ven/illumio-vent-ctl unsuspend`. The VEN generates an event with severity Err when it should be severity Info.
  Workaround: None.
- **Repeated logs observed in vtap.log after restarting VEN on Solaris** (E-63072)
  The message `INFO: Waiting for first reconcile file` is logged repeatedly after restarting a VEN. The contents of the Conntrack table are not removed at restart, so long-lived connections established while the VEN was stopped stay active until the next policy change, instead of being marked as "potentially blocked" or removed from the Conntrack table.
- **Healthy VEN can show an error status in the PCE web console** (E-51115)
  When viewed through the PCE web console (by clicking the name of a VEN in Workloads and VENs), a healthy VEN might falsely be shown to have an error status. This can happen if the VEN is installed on a mounted directory. To double-check the status of a VEN in this case, run the VEN status command:
  `illumio-ven-ctl status`
  If the command returns `Agent state: illuminated`, the error status shown in the PCE Web Console is incorrect. For more information, see Monitor and Diagnose VEN Status.
- **Upgrading VEN on workload can cause API to generate 406 error** (E-40132)
  This API error occurs when the API version is incompatible with the VEN. Every 24 hours the VEN retrieves a new master configuration file, which will correct the API version incompatibility. In most cases, this issue corrects itself within a few minutes. If it does not, wait for the VEN to retrieve a new master configuration file or restart the VEN to force it to update the file.

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.

- **Core VEN Installs Weak File Permissions on Debian**
  On Debian, the VEN installation script incorrectly set the owner of `/etc/illumio_ven` to UID 1000. This is resolved by setting the owner UID to 0 (root).
- **Firewall Rules Didn't Properly Require IPsec**
  In certain cases, plaintext connections would not be blocked despite being configured to require IPsec using SecureConnect. This issue is resolved.

- **Postgres Password Included in Command Line**
  In certain scenarios, such as a PCE upgrade, the Postgres password was passed as an argument on the command-line, and could be viewed during a brief window of time by other users logged-in locally to the host. This issue is resolved.
- **Security Headers for nginx**
  Additional security headers were enabled for the nginx endpoint. Under normal circumstances, nginx is inaccessible outside the PCE cluster.
- **Local PCE User with No Role Could Access system_events**
  A local user with all roles removed could still obtain events from `system_events`. This issue is resolved.
- **Resque gem Updated to Address CVE-2015-9251**
  The `resque` gem was updated from 2.0.0. to 2.1.0 to address CVE-2015-9251, which impacts jquery, a dependency for `resque`.

Legal Notices