TECHNICAL
DOCUMENTATION

What's New and Release Notes 25.3

IMPORTANT

Review the updated license information for PCE UI visualization components.

Review the resolved and known issues in Illumio and other components.

- What's New in 25.3
- Resolved Issues in 25.3
- Known Issues in 25.3

Table of Contents

Licenses for PCE UI Visualization Components

A license used by PCE UI components expires on May 30, 2025. This impacts all on-premise PCE versions from 22.5 and later.

License Expired Watermark Message

Beginning May 31, 2025, you may see a "License Expired" watermark message for any on-premises PCE version from 22.5 and later in these PCE UI visualization components:

- Explore > Map
- App Groups > App Group Name > Map
- Workloads > Blocked Traffic
- Deny Rules > Blocked Connections

Download and Apply the Patch

You must download and apply the patch available on the Support Portal **before May 31st, 2025** to make sure that you have uninterrupted access to PCE UI visualization components and functionality.

NOTE
If you don't apply the patch by May 31st, 2025, you will see a "License Expired" watermark message on the affected UI pages. However, the maps will continue to work.

IMPORTANT
If you don't apply the patch by July 11th, 2025, the affected PCE UI visualization components will no longer display content and your pages will be blank.

Review the Knowledge Base article or contact Illumio Support if you need help.

What's New in 25.3

What's New and Changed in Release 25.3

Before upgrading to Illumio Core 25.3, familiarize yourself with the new and modified features in this release for PCE, REST API, and the PCE web console.

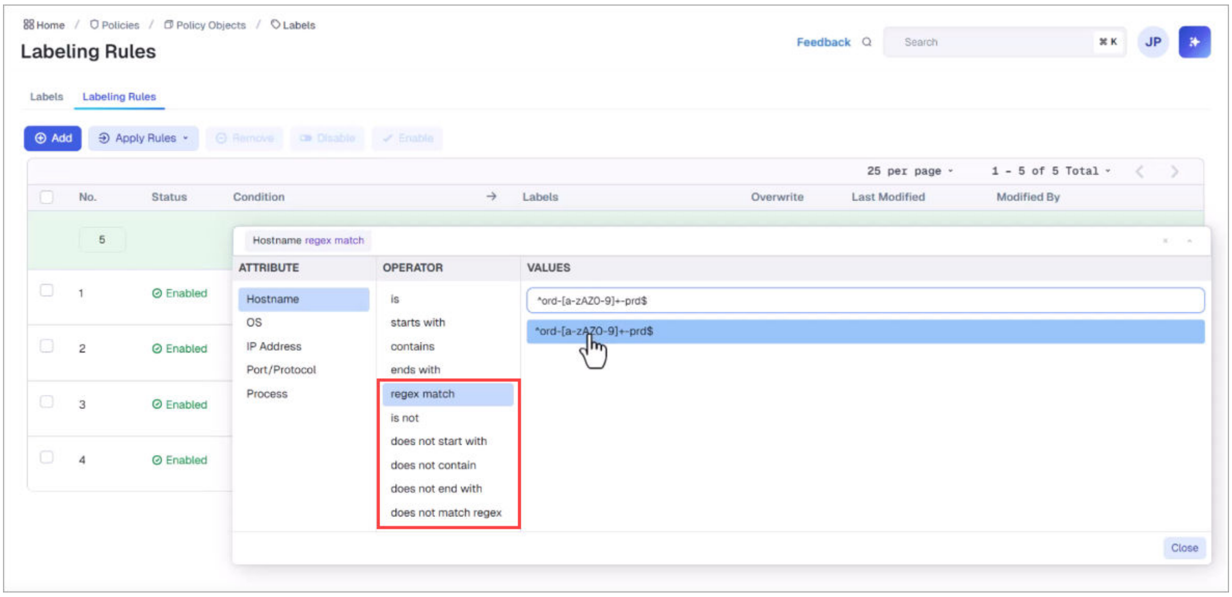
Rule-Based Labeling Enhancements

For details about Rule-Based Labeling, see Rule-Based Labeling.

This release introduces the following enhancements to the Rule-Based Labeling feature:

Support for Regular Expressions and NOT operators

- **Regular Expressions**
  Regular Expressions (regex) allow you to define complex patterns to precisely match workloads in your environment. This precision is particularly useful when you're trying to find and label workloads that have multiple attributes. www
- **NOT Operators**
  NOT operators allow you to refine search queries by excluding certain values. You can combine NOT operators with other search operators (like AND, OR) to create complex queries that precisely target the desired information while excluding irrelevant data.



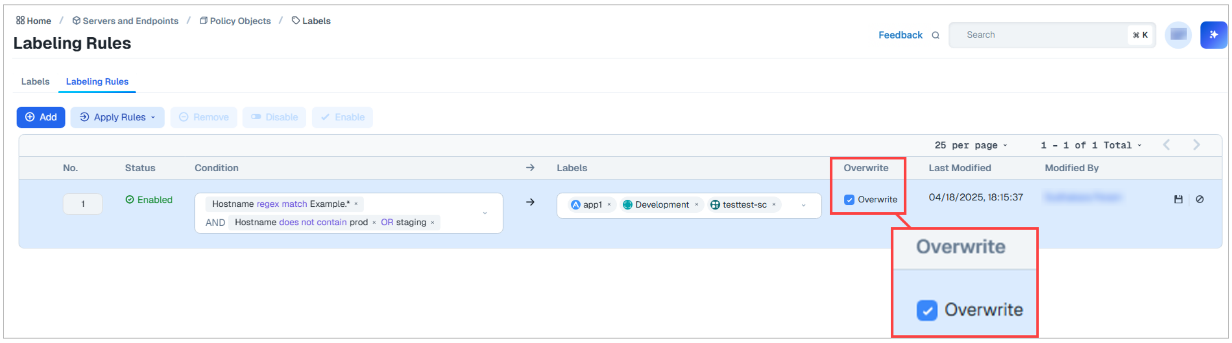
☐	No.	Status	Condition	→	Labels	Overwrite	Last Modified	Modified By
	5		Hostname regex match					
☐	1	Enabled						
☐	2	Enabled						
☐	3	Enabled						
☐	4	Enabled						

VALUES: ^ord-[a-zAZ0-9]+-prd$

^ord-[a-zAZ0-9]+-prd$

Support for Overwriting Existing Labels

The Overwrite option allows you to replace labels already assigned to workloads with new labels of the same type. For example, if your labeling rule is set to assign an Application label to matching workloads, selecting this option ensures that any Application label already assigned to these workloads is overwritten by the new Application label when you click Assign.



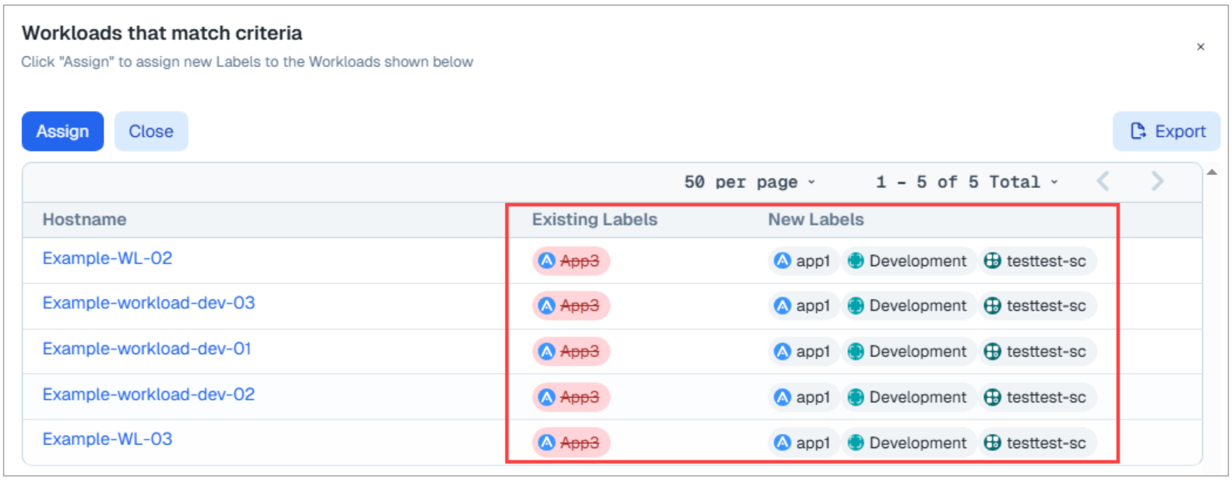
Home / Servers and Endpoints / Policy Objects / Labels

Labeling Rules

No.	Status	Condition	→	Labels	Overwrite	Last Modified	Modified By
1	Enabled	Hostname regex match Example.* AND Hostname does not contain prod OR staging	→	app1 Development testtest-sc	☑ Overwrite	04/18/2025, 18:15:37	[redacted]

Overwrite

☑ Overwrite



Workloads that match criteria

Click "Assign" to assign new Labels to the Workloads shown below

Hostname	Existing Labels	New Labels
Example-WL-02	~~App3~~	app1 Development testtest-sc
Example-workload-dev-03	~~App3~~	app1 Development testtest-sc
Example-workload-dev-01	~~App3~~	app1 Development testtest-sc
Example-workload-dev-02	~~App3~~	app1 Development testtest-sc
Example-WL-03	~~App3~~	app1 Development testtest-sc

New and Changed APIs in Illumio 25.3

Here's a summary of the new and enhanced features in this release.

New APIs

Release 25.3 introduces these new APIs:

- ip_list_attributes_get [9]
- ip_list_attributes_post [9]
- sec_policy_ip_lists_bulk_upload_put [9]
- vens_remote_action_put [9]

ip_list_attributes_get

This new endpoint extends IP Lists to add support for attributes.

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "required": [
    "name"
  ],
  "properties": {
    "id": {
      "description": "ID of the ip list attribute",
      "type": "string"
    },
    "href": {
      "description": "URI of the ip list attribute",
      "type": "string"
    },
    "name": {
      "description": "Name (must be unique)",
      "type": "string"
    },
    "external_data_set": {
      "description": "External data set identifier",
      "type": [
        "string",
        "null"
      ]
    },
    "external_data_reference": {
      "description": "External data reference identifier",
      "type": [
        "string",
        "null"
      ]
    }
  }
}
```

ip_list_attributes_post

This API creates an IP List attribute. It has a name, an External data set identifier, and an External data reference identifier.

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "additionalProperties": false,
  "required": [
    "name"
  ],
  "properties": {
    "name": {
      "description": "Name (must be unique)",
      "type": "string"
    },
    "external_data_set": {
      "description": "External data set identifier",
      "type": [
        "string",
        "null"
      ]
    },
    "external_data_reference": {
      "description": "External data reference identifier",
      "type": [
        "string",
        "null"
      ]
    }
  }
}
```

sec_policy_ip_lists_bulk_upload_put

This API allows customers to upsert IP lists in bulk via CSVs.

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "description": "IpList bulk_update",
  "type": "array",
  "maxItems": 1000
}
```

vens_remote_action_put

This API was designed to control the VEN from the PCE and restart it without access to the server.

Using vens_remote_action_put, you can refresh the VEN's internal states and resolve cases where the VEN may not be fully operational. Currently, this API allows for the remote VEN service to restart.

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "additionalProperties": false,
  "required": [
    "action",
    "vens"
  ],
  "properties": {
    "action": {
      "description": "Remote action type",
      "type": "string",
      "enum": [
        "restart"
      ]
    },
    "vens": {
      "description": "An array of VENs to restart",
      "type": "array",
      "minItems": 1,
      "maxItems": 1,
      "items": {
        "type": "object",
        "additionalProperties": false,
        "required": [
          "href"
        ],
        "properties": {
          "href": {
            "description": "VEN URI",
            "type": "string"
          }
        }
      }
    }
  }
}
```

Users can implement this API as follows:

1. Initiate a 'restart' action for a particular VEN to the PCE, which archives this remote action request for the VEN in a database.
2. The heartbeat response includes the 'restart' command upon receiving the VEN heartbeats.
3. The VEN processes the command and undergoes a restart operation.
4. During the subsequent heartbeat, the VEN transmits the timestamp of the last restart performed, which the PCE logs.

   At this point, the PCE designates this action request as fulfilled.

Changed APIs

The following APIs have been changed in release 25.3:

- `common-aggregated_detected_vulnerability`

  Type NULL added for port, proto, and cve_ids
- `common-vulnerability_summary` , `common-workloads_detected_vulnerabilities`

  Type NULL added for num_vulnerabilities, vulnerability_score, max_vulnerability_score, and last_updated_at
- `container_clusters_get`

  Added new properties: **`machine_id`** and **`name`** .
- `destination_get`

  Type NULL added for the **`tls_ca_bundle`**.
- `label_mapping_rule_expression`l

  A new property was added: **`regex`** . It involves writing regular expressions for labeling.
- `label_mapping_rules_getlabel_mapping_rules_post`, `label_mapping_rules_put`

  A new property **`overwrite`** was added. If set to true, an existing label of the same dimension will be overwritten.
- `network_device_get`

  The property **`endpoints`** was deleted and replaced with the property **`network_endpoints`**.
- `network_enforcement_node_get`

  This schema was expanded with new properties: **`first_reported_timestamp`** and **`latest_event`**.
- `optional_features_put`

  Two new properties have been added: **`hybrid_policy`** and **`container_cluster_label_set_based_kubernetes_workload_instructions`**

  `hybrid_policy`: For more details about **`hybrid_policy`** see Hybrid Policy in the document What's New in release 25.2.10.

  `container_cluster_label_set_based_kubernetes_workload_instructions`: This property is enabled by default for each organization. The PCE uses policy deduplication for Kubernetes workloads within the CLAS Container Clusters.

  This means you must calculate only one instruction for every Kubernetes workload with the same set of labels. This reduces the number of calculated instructions in production by 70-95%.
- **`orgs_auth_security_principal`** and **`orgs_auth_security_principals`**: Two properties, **`name`** and **`display_name`**, were removed, while the new property **`uuid`**, was added to supply the UUID for the authentication security principal.
- `reports_post`

  Minor change for reports_post: in addition to mxLengt:255, the additional type NULL was added.
- `sec_policy_ip_lists_get`

  The added query parameter **`ip_list_attribute`** allows filtering IP Lists with an attribute assigned.
- `sec_policy_ip_lists_post`

  The added query parameter **`ip_list_attribute`** specifies which attribute should be linked to an IP List.
- `sec_policy_ip_lists_put`

  The added query parameter **`ip_list_attribute`** specifies which attribute should be linked to an IP List.
- `service_accounts_post`

  The property **`uuid`** was added for the service account.
- `settings_put`

  In 25.3, the flag **`use_census_permissions`** was deleted.

  This flag indicates whether the PCE org will obtain permissions from the census or from the local database.

- `users_get`

  For the new object `user_full` ,new properties have been added: `display_name` -user's display name), and `permissions` - list of permissions for this user.

  For the new object `user_org_permissions` additional properties have been added: `href` - URI of the user, `display_name` - user's display name, and `permissions` - list of permissions for this user.
- `vulnerability`

  This API in 25.3 has a change for the property _ids: in addition to the type array,
  type NULL was added

Illumio Core Release Notes 25.3

These release notes describe resolved and known issues in these releases:

- 25.3

Updated: July 2025

Product Version 25.3

These release notes provide a list of resolved issues for Illumio Core 25.3.*x* releases.

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

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

Resolved Issues in Release 25.31.0-PCE

These release notes describe the new features, enhancements, resolved issues, and known issues for this release.

Resolved Issues

Issue	Fix Description
E-128815	**Unable to Login to Dev Console** Users were experiencing issues logging into the dev console with the devtest235 PCE. The PCE was not functioning correctly, leading to a failure in fetching PCE organization information. This issue is resolved.
E-128193	**Enhanced Rule Search Accuracy in ruleset_overlapping_rule_search** An omission was revealed in the ruleset_overlapping_rule_search call, lacking the addition of exclude_rules_not_resolving_to_ruleset_scope_actors=true in the URL. This exclusion led to conflicting rules not being filtered out, resulting in the retrieval of two conflicting rules instead of none. By rectifying this URL parameter oversight, scopes are now properly verified, ensuring the elimination of conflicting rules within the search results for improved accuracy.
E-128086	**Refined Labeling Process for Cloud Resources** An update has been implemented to ensure that cloud resources are no longer included in the resources picked up for labeling by default when label rules are applied. This refinement streamlines the labeling process, offering more precise control over resource identification within the cloud environment.
E-128073	**API sometimes omits byteIn and byteOut fields** In UC, the API omits byteIn and byteOut fields when there is no data, whereas in regular SaaS Core, the API returns these fields with a value of 0. This inconsistency leads to UI errors in UC during byte aggregation. Resolution: A UI fix has been added to default missing byteIn and byteOut values to 0. This will resolve the issue and ensure correct behavior when aggregating connections. In UC, the API omits byteIn and byteOut fields when there is no data, whereas in regular SAAS core, the API returns these fields with a value of 0. This inconsistency causes UI errors in UC when it tries to aggregate the bytes. The added UI fix will resolve the issue and ensure the byteIn and byteOut functions work correctly with aggregating connections.
E-128016	**Mitigated Rate Limiting with Consolidated Endpoint Calls** The issue was resolved by replacing multiple endpoint calls with a single new endpoint call. The system anticipates reducing rate-limiting concerns, enhancing overall performance, and operational efficiency.

Resolved Issues in Release 25.3-PCE

These release notes describe this release's new features, enhancements, resolved issues, and known issues.

Resolved Issues

Issue	Fix Description
E-128999	**Incorrect Timestamps from VEN Leading to Database Inconsistencies** The incorrect timestamps reported by the VEN were causing the PCE to generate inaccurate tables within the database. This discrepancy has resulted in system issues. This was resolved to ensure the accuracy and reliability of the database operations.
E-128877	**Enhanced Deny Rule Scope Accuracy** Previously, deny rules and override deny rules failed to consider label groups or exclusions in the scope, leading to misapplied rules. These rules are now accurately applied based on specified label groups and exclusions, ensuring correct enforcement on targeted workloads.
E-128872	**Enhanced Policy Selection with Autocomplete Feature** Users could not select a policy if it were not initially part of the list of 500 policies. To resolve this limitation, autocomplete functionality has been added, enabling dynamic fetching of policies from the full list. This enhancement empowers users to conveniently search and select any valid policy beyond the initial set of 500 options, thereby improving the overall user experience and flexibility within the system.
E-128375	**Rule Coverage Issue for Traffic in Draft Mode with Kubernetes Workloads** Rule Coverage for Traffic in Draft mode was malfunctioning, specifically for Kubernetes Workloads, causing inconsistencies in rule application. This issue has been successfully resolved, ensuring that Rule Coverage now operates correctly for Traffic in Draft mode within Kubernetes Workloads.
E-128235	**Policy Rules for NodePorts and LoadBalancers in CLAS Clusters** This update addresses an issue with policy rules specifically designed for managing Node Ports and Load Balancers within CLAS (Cluster-Level Application Set) clusters. The fix ensures that these rules now function as intended, providing accurate and consistent governance over networking configurations associated with Node Ports and Load Balancers within the CLAS environment.
E-128193	**Improved Conflict Resolution in ruleset_overlapping_rule_search API** This update addresses an issue where the parameter **exclude_rules_not_resolving_to_ruleset_scope_actors=true** was missing in the URL when calling **ruleset_overlapping_rule_search**. By adding this parameter, scopes will be thoroughly checked to ensure no conflicting rules are displayed. This enhancement leads to a more accurate identification of conflicts, providing a more straightforward overview of rules without duplicates in the specified scenarios.
E-128016	**Optimization for Performance and Rate Limiting Avoidance through Consolidated Endpoint Call** Addressed the rate-limiting problem by substituting multiple endpoint calls with a single, consolidated one. Thanks to the optimization, users can now operate without concerns about rate limiting, resulting in enhanced performance and smoother API functionality.

Issue	Fix Description
E-127789	**Improved Subnet Caching Behavior to Prevent Empty Sets During Server Reload**
E-127354	Fixed an issue where subnet caching occurring concurrently with a set_server reload could lead to empty sets being cached.
	Addressing this scenario ensures that sets related to workloads are not cached as empty during server reload, thereby preventing inaccurate caching results.
E-127763	**Reversal of Hostname Case Sensitivity in 25.21.0 Update**
	A change occurred in version 25.21.0, causing the hostname to become case-sensitive, deviating from prior releases. The behavior has been reverted to its original state of being case-insensitive, aligning with users' familiarity with previous versions.
	This adjustment ensures consistency across releases and minimizes potential disruptions for users accustomed to the former configuration.
E-127740	**Log message missing from the agent log**
	The log message `sec_policy commit: Computing affected workloads` was missing from the agent log. The issue is resolved, and the timing log has been added to the non-lazy-impact calculation.
E-127644	**Enhanced Flow Separation for Different IP Address Decorations in Draft Policies**
	Previously, when some flows were adorned with a Workload while others were associated with an IP List for the same IP address, they were erroneously merged as one flow in the draft policy. This caused the draft policy to display only for the combined flow.
	The solution maintains these flows as distinct entities, ensuring accurate representation and visibility within the policy structure.
E-127435	**Enhanced Policy Commit Stability via Batching Strategy for Arguments in Lua Script**
	Previously, policy commits encountered a Redis Lua script error due to attempting to unpack an excessive number of arguments.
	The Lua script has implemented a fix introduced through a pull request mentioned in the comments. This resolves the issue by batching arguments efficiently rather than unpacking them all at once, ensuring smoother processing of policy commits without encountering script errors.
E-127354	**Optimizing Subnet Caching and Server Reload Interaction to Prevent Empty Set Caching**
	Subnet caching overlapped with a set_server reload operation, which could lead to the caching of empty sets. This occurs because workloads could be empty during a reload, resulting in incomplete or erroneous data being cached.
	Optimizations were implemented to ensure that subnet caching and server reload processes are synchronized effectively.
E-127344	**Policy Check Failure Caused by Outdated Deny Rules**
	Fixed policy check failures that occurred due to the presence of outdated (legacy) deny rules included in the results.
	This update ensures that outdated deny rules no longer cause policy check failures, improving the accuracy and reliability of policy validation processes.

Issue	Fix Description
E-127276	**Query in Draft View not triggering rule calculations correctly** When a user ran a query in Draft View with both Blocked and Potentially Blocked quick filters enabled, the query did not trigger rule calculations correctly for the returned flows. However, the rule calculations were sent properly when the user manually toggled the quick filters (i.e., unchecks and rechecks them). This inconsistency leads to misleading flow counts and inaccurate data representation. The fix ensures that rule calculations are triggered consistently when the query is run with Blocked and Potentially Blocked quick filters without requiring the user to toggle filters manually. This will correct the flow count discrepancies and improve the reliability of Draft View query results.
E-127081	**Extended Delay with RuleListEntity Retrieval in /rulesets Endpoint** Previously, the RuleListEntity loading was slow due to repetitive queries to the database for exclusion labels and service accounts. These queries, executed redundantly per rule or rule list, resulted in unnecessary delays despite the usual static or org-scoped outcomes. This optimization notably decreased redundant database round-trips, enhancing overall latency, throughput, and policy computation during rule list loading. To address this, per-org caching for Exclusion label query results and caching for Service account lookup results were implemented.
E-126207	**Custom Time Range Query** A bug was addressed where filtering the Blocked Traffic list by a custom date range on a Workload's details page proved ineffective. The issue arose as the query was always initiated 24 hours before the current time, disregarding the specified start date from the date selector.
E-126162	**Troubleshooting VEN Activation Failure with "Ephemeral" Parameter** The VEN activation issue previously encountered with the "ephemeral" parameter was successfully resolved. Users can now activate VEN without any hindrance, as the fix implemented has ensured a smooth activation process.
E-126121	**Configurable Runtime Thresholds and Logging Added for Event Bus Bulk Operations** The runtime thresholds were configured for total_event_bus_bulk_threshold and workload_in_out_event_bus_bulk_threshold, enhancing flexibility in managing event bus bulk operations. Logging features have been incorporated to assist users in fine-tuning these thresholds effectively. The update gives users increased control over event bus operations while facilitating optimization through detailed logging mechanisms.
E-126022	**Improved Policy Consistency for Workload Assignments to Virtual Services** Resolved an issue where, when multiple Virtual Services (VS) were assigned to a single Workload (WL), some policies contained only one VS ID in the source_rule_ids instead of all assigned VS IDs. This inconsistency resulted in certain Virtual Service rules not recording any hits. The issue has been rectified, ensuring all associated Virtual Service IDs are correctly reflected within policies for accurate rule evaluation and traceability of hits.
E-125150	**Boosted PCE Performance with Optimized C-VEN and Kubelink API Queries**

Issue	Fix Description
	Resolved issue by optimizing C-VEN and Kubelink API queries, enhancing PCE (Policy Computing Engine) performance. The optimization efforts have significantly improved PCE efficiency, benefiting large clusters by streamlining operations and boosting overall system performance.
E-124916	**Resolved lock contention to reduce a 500 error** Resolved an issue where some containers could not fetch and apply the policy, which caused a 500 error in logs.
E-124289	**container_clusters Policies Breaking Perspective Cache** The endpoint container_clusters/<uuid>/policies caused disruptions to the non-blocking policy perspective cache, affecting its ability to maintain accurate and current policy perspectives. This issue is resolved to ensure the seamless operation of policies within container clusters.
E-124261	**Convergence in Container Clusters** Due to convergence issues in specific Container Clusters, clusters are falling out of synchronization, impacting operations. VENs experienced difficulties obtaining the VPC IPs allocated by their policies. This issue is resolved.
E-124060	**Formatting Issues Due to Incorrect Service Addition in the Query Field** The incorrect procedure of adding a defined service to the service query field resulted in improper formatting issues, particularly affecting the UI (User Interface). This incongruity results in complications with how data is displayed or processed, causing confusion and hindering the user experience. Resolution of this issue is crucial to ensure accurate data representation and smooth functionality of the service query field within the system.
E-121656	**Container Service Backends View Loading Failure in PCE** Resolved the customer-reported issue where the Container Service Backends view failed to load in the PCE for all non-Dev clusters. The problem was traced to the service_backends API call stalling and timing out specifically for this view. This affected only the specified API response and view without affecting the functionality of other container cluster-related APIs.
E-121094	**Improved Draft View Calculation Reliability for Large Queries** Addressed an issue where draft view calculations were timing out for large queries, leading to missing draft policy decisions in the downloaded file. The resolution ensures that draft view calculations are more robust, even for extensive queries, guaranteeing that all draft policy decisions are accurately included in downloaded files.
E-120909	**Updates in API Authentication Code Path Exposes Gap in User Session Verification** An update in the API authentication process has introduced a different code path, inadvertently affecting user session verification in the system. While aiming to bolster security measures, this change resulted in user session checks being omitted for this particular case, potentially impacting user access and system security.

Issue	Fix Description
	The recent update addresses this issue, ensuring robust authentication practices and consistent user session verification across all scenarios
E-117295	**Enhanced Rule Search Filter Logic for Multiple Ports** Resolved an issue where the Rule Search filter incorrectly applied the AND logic instead of the expected OR logic when multiple ports were supplied. The filter correctly interprets multiple ports as an OR condition, ensuring accurate and efficient rule search results based on the specified port inputs.
E-108511	**PCE "Upgrading" Status not Cleared** This issue addresses the persistent problem of the PCE (Policy Computing Engine) status remaining stuck in an "Upgrading" state even after successful upgrades of VENs. Despite completing VEN upgrades, the PCE fails to clear the "Upgrading" status, causing confusion and potential delays in system operations.

Known Issues in Release 25.3-PCE

These release notes describe this release's new features, enhancements, resolved issues, and known issues.

Known Issues

Issue	Description	Status
E-126354	**Weekly Table Flows Missing Due to Start of Week Calculation Issue** Identified an issue where weekly table flows were missing due to the incorrect calculation of the week's start. The issue has been brought to light, and efforts are underway to rectify the discrepancy in determining the start of each week to ensure comprehensive data representation.	Unresolved
E-124202	**VEN Image Download Unavailable for Global Viewer Role** The ability to download VEN images from the UI remains inaccessible for users assigned the global viewer role. The issue is recognized, and efforts are ongoing to address this limitation, ensuring that users with the global viewer role can download VEN images as intended.	Unresolved

What's New and Release Notes for LW-VEN 1.1

What's New in LW-VEN Release 1.1.0

The following new feature is added in this release:

Support for flow reporting for legacy Windows servers

Beginning with release 1.1.0, the LW-VEN can enable the native Windows Firewall log on your legacy Windows server, which allows the LW-VEN to generate and log traffic flow information for ingestion by the PCE. After ingesting the log information, the PCE displays it in its Map and Traffic views to help you gain insights about and create policy for your business applications. See Enable Flow Reporting.

Release Notes in LW-VEN 1.1

Review these release notes for a list of resolved and known issues.

Resolved Issues in 1.1.10 LW-VEN

Issue	Description	Status
E-120840	**ICMP rule generation created empty command** When the LW-VEN generated a rule to add/modify/delete an ICMP rule, it also generated an empty command which caused the LW-VEN to fail when it tried to apply policy to that empty command.	Resolved
E-120184	**Excessive time needed for Windows firewall to apply Illumio rules** Policy application failed when the Windows firewall took longer than expected to apply PCE-generated rules. This issue is fixed. Policy is now applied in the background. Note that applying firewall commands on a low-powered server can take longer than expected.	Resolved
E-120119	**Policy conflict lead to policy sync failure and LW-VEN crash** A conflict occured when merging the default Illumio policy with the customer's Illumio-generated policy. This caused an Illumio policy sync failure and crashed the LW-VEN service.	Resolved

Resolved Issues in 1.1.0 LW-VEN

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

Illumio Core for Kubernetes

Illumio Core for Kubernetes What's New and Release Notes for 5.4

These release notes describe the resolved issues, known issues, and related information for the 5.4.x releases of Illumio Core for Kubernetes, formerly known as Illumio Containerized VEN, or C-VEN. Illumio Core for Kubernetes also includes the related required component, Kubelink. Because of this heritage, many references to this product as "C-VEN" are still used throughout the documentation.

Published: May 20, 2025

Core for Kubernetes 5.4.x

Compatible PCE Versions: 23.5.32 and most later releases

Current Illumio Core for Kubernetes Version: 5.4.1, which includes:

- C-VEN version: 23.4.5
- Kubelink version: 5.4.1
- Helm Chart version: 5.4.1

Compatible PCE Versions: 23.5.32 and most later releases

Current Illumio Core for Kubernetes Version: 5.4.0, which includes:

- C-VEN version: 23.4.5
- Kubelink version: 5.4.0
- Helm Chart version: 5.4.0

Before deploying any Illumio Core for Kubernetes 5.4.x version, confirm your PCE version supports it. For example, currently Illumio Core for Kubernetes versions 5.1.0 and 5.1.2 are supported **only** with PCE versions 23.5.10 (for On Premises customers) or 24.1.x (for SaaS customers), but NOT on PCE versions 23.5.1 or 23.6.0, or any lower versions. For complete compatibility details, see the Kubernetes Operator OS Support and Dependencies page on the Illumio Support Portal.

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

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

Resolved Issues in Kubernetes 5.4.1

This section provides a list of resolved issues in Release 5.4.1

Issue	Fix Description
E-127741	**Kubelink can now send policies to clusters with approximately 50 nodes** In clusters with approximately 50 nodes, Kubelink became non-responsive and stopped sending policies because the channel for managing C-VEN updates was too small. This issue is resolved.
E-127610	**Kubelink is now able to update workloads** Kubelink was unable to update Kubernetes workloads because the timeout period available for fetching data from the PCE was too short. This is resolved.

What's New in Release 5.4.0

Here's a summary of the new and enhanced features in this release.

Add support for Helm Chart with Argo CD

Starting in release 5.4.0, Illumio Core for Kubernetes can be deployed with the Argo CD tool, a convenient way of managing Helm Chart deployments. Valuable features of using Argo CD with Illumio Core for Kubernetes include:

- Repeated resources are identified using a new `argoCD` variable (default value is `false`).
- Supports unpairing with a new `unpair` option to `clusterMode` parameter.
- Triggers a new rollout by using checksum annotations whenever a `Secret` or `ConfigMap` value changes in the repository.
- Adds a new `verbosity` parameter as a value in `values.yaml` so it can be managed.

Add proxy support to C-VEN

A new Helm chart variable `httpProxy` was added, which sets the HTTP proxy URL to be used for Kubelink and C-VEN PCE requests, much like existing VEN proxy support.

Exclude or include host-networked workloads from PCE total workload count

Starting with 5.4.0, Kubelink does not create Kubernetes Workloads on PCE if the workload is in the host network. Pods running these workloads don't have a separate network namespace. Policy for these workloads must be part of the policy for Nodes. Added a new `reportHostNetworkKubernetesWorkloads: true` option to `values.yaml` to exclude host-networked Kubernetes Workloads from being counted in the PCE total workload calculation.

To count these workloads, turn on the reporting of workloads in the host network with the setting `` `includeHostNetworkWorkloads: true` ``. Workloads will be counted into Workload limits, and policy instructions for Pods in the host network will be ignored like in previous versions.

Report operating system of nodes for Azure, GKE, and OpenShift

C-VEN now accurately reports the OS of the node running on the cluster of underlying source to PCE, such as Azure, GKE, OpenShift, and the like.

Release Notes for Kubernetes 5.4.0

These release notes describe the new features, enhancements, resolved issues, and known issues for this release.

Resolved Issues in Release 5.4.0

Issue	Fix Description
E-127347, E-126604	**Updated Universal Base Image to UBI 9.6 micro** The Universal Base Image for Kubelink and C-VEN was updated to UBI 9.6 micro to fix several golang vulnerabilities, including CVE-2025-30204, CVE-2025-30204, and CVE-2025-22869.
E-126290	**Fixed RHSA-2025:1330** This vulnerability in OpenSSL was fixed in the Kubelink included in release 5.4.0.
E-124299	**When running in degraded mode, Kubelink might send the wrong policy to CoreDNS pods** Policy delivery for new Kubernetes Workloads in degraded mode can be disabled by setting the Helm chart variable `disableDegradedMode: true`. For more information about degraded mode, see the section on "CLAS Degraded Mode: disableDegradedMode and degradedModePolicyFail" in the "Deployment with Helm Chart" chapter on the Containers Guide.
E-123377	**Fixed inaccuracies in the output of the metrics service** Two inaccuracies in the output of the metrics service have been fixed (host_policy_status running on port 8080 when in CLAS mode).

Illumio Core for Kubernetes What's New and Release Notes for 5.3

This document describes the new features, enhancements, resolved issues, and known issues for the 5.3.*x* releases of Illumio Core for Kubernetes, also known as Illumio Kubernetes Operator. This product was formerly known as Illumio Containerized VEN, or C-VEN. Illumio Core for Kubernetes also includes the related required component Kubelink. Because of this heritage, some references to this product as "C-VEN" occur throughout the documentation.

What's New in Illumio Core for Kubernetes 5.3.2

Learn what's new in the 5.3.2 release of Illumio Core for Kubernetes, also known as Illumio Kubernetes Operator.

Product Version

Compatible PCE Versions: 23.5.31 and later

Current Illumio Core for Kubernetes Version: 5.3.2, which includes:

- **C-VEN version:** 23.4.4
- **Kubelink version:** 5.3.2
- **Helm Chart version:** 5.3.2

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

What's New in Release 5.3.2

Illumio Core for Kubernetes release 5.3.2 consists of several resolved issues and bug fixes described here:Release Notes for 5.3.2 [29].

What's New in Illumio Core for Kubernetes 5.3.1

The following describes what is new in the 5.3.1 release of Illumio Core for Kubernetes, also known as Illumio Kubernetes Operator.

Product Version

Compatible PCE Versions: 23.5.31 and later

Current Illumio Core for Kubernetes Version: 5.3.1, which includes:

- **C-VEN version:** 23.4.3
- **Kubelink version:** 5.3.1
- **Helm Chart version:** 5.3.1

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

What's New in Release 5.3.1

Here's a summary of the new features in this release:

- **Support installation of Illumio Core for Kubernetes into a custom namespace**

  You can now install Illumio Core for Kubernetes into a custom namespace instead of into the default namespace of `illumio-system`. The default namespace is overridden for backward compatibility by using the variable `namespaceOverride: illumio-system`.

  For example, to install into the `ilo` namespace, specify the namespace with the `--namespace` option and the `--set` option specifying `namespaceOverride` to `null`:

  ```
  helm install illumio -f illumio-values.yaml oci://quay.io/illumio/
  illumio --version 5.3.1 --namespace ilo --create-namespace --set
  namespaceOverride=null
  ```

Alternatively, specify the namespace with the `--namespace` option but also use `--set` to explicitly set `namespaceOverride` to `ilo`:

```
helm install illumio -f illumio-values.yaml oci://quay.io/illumio/
illumio --version 5.3.1 --namespace ilo --create-namespace --set
namespaceOverride=ilo
```

- "**Enforce NAT Mode 1:1" option creates public workload interface**

  Workloads now have a new optional feature "Enforced NAT mode 1:1" that, when enabled, ensures that pseudo-public IP addresses are detected and are then saved as workload interfaces even when the C-VEN (or VEN) cannot identify the datacenter or service source. If this option remains disabled, the PCE either relies on the C-VEN to report the public IP address or derives it based on a datacenter match. When this option is enabled on a Container Cluster, the feature applies to all host workloads on all of its cluster nodes.
- **Map Kubernetes Workload labels to Illumio labels**

  You can now map labels on Kubernetes Workloads to corresponding Illumio labels by using a `workloadLabelMap` section in a label mapping Custom Resource Definition (CRD) within a YAML, in a `kind: LabelMap` declaration. This Kubernetes Workload label mapping is otherwise defined like the existing feature for mapping Kubernetes node (or host workloads) labels to Illumio labels. See Map Kubernetes Node or Workload Labels to Illumio Labels.

  > **CAUTION**
  >
  > Mapping labels for Kubernetes Workloads only works in CLAS-enabled deployments, and requires PCE release 24.5.0.

- **Added Support for hostPort**

  Traffic enforcement of Kubernetes Workloads, which have Pods exposed via hostPort, is now available.

  > **CAUTION**
  >
  > The support for hostPort is available only on deployments running PCE 24.5.0.

- **Added support for Google Kubernetes Engine (GKE)**

  The Google Kubernetes Engine (GKE) is now a supported orchestration platform on Illumio Core for Kubernetes CLAS-enabled deployments that use PCE release 24.5.0 or later. For complete requirements for GKE support. see the Illumio Support Portal page on "Kubernetes Operator OS Support and Dependencies."
- **Kubernetes Workloads Show Label Source**

  A new a `com.ilo.result.*` annotation on a PCE label for a Kubernetes Workload now shows the source of that label with a code appended to the annotation: where the code `cwp` means from a Container Workload Profile, `map` means from a LabelMap, and `annotations` means from a Kubernetes annotation. These values are shown in the PCE UI on the workload details page (under the Kubernetes Attributes section), and at the command-line as part of the `kubectl get deploy` command output.

Limitations

- You cannot change an existing deployment in the illumio-system namespace to a custom namespace through an upgrade.
- Mapping labels for Kubernetes Workloads is available only in CLAS-enabled deployments, and currently requires PCE release 24.5.0.

Base Image Upgraded

The C-VEN base OS image has been upgraded to address several vulnerabilities, including CVE-2024-45337 and 2024-45338. Customers are advised to upgrade to Core for Kubernetes 5.3.1 for these security fixes.

Release Notes for 5.3.2

These release notes describe the resolved issues for this release.

Resolved Issues in Release 5.3.2

Issue	Description
E-125731, E-125362	**C-VEN - Improve performance by adjusting retry handling** Retry logic has been adjusted to reduce latency times, and improve performance.
E-125661	**Kubelink: Improved PCE load handling** Several PCE timeout values have been adjusted to improve PCE performance and resilience when under load, and to more appropriately enter degraded mode when appropriate.

Resolved Issues in 5.3.1

This section provides a list of resolved issues in Release 5.3.1.

Resolved Issues

Issue	Description
E-123084	**Kubelink: wrong LabelMap feature flag for older 24.x PCE versions** Kubelink incorrectly interpreted some older PCE versions as higher (more recent) than 24.5, which enabled the LabelMap feature for PCE versions that do not support it. This caused Kubelink 5.3.0 to be incompatible with many older 24.x PCE versions.
E-123080	**Kubelink: labels defined by Container Workload Profile are ignored when Kubelink restarts** Kubelink was not receiving accurate data for workloads using managed Container Workload Profiles. So when Kubelink restarted, it might use out-of-date Container Workload Profile data and improperly remove or mislabel some workloads, causing incorrect policies.
E-122830	**Kubelink: skip of ACK of unknown workload causes repeated policy calculations and sets ACK** Part of the policy Kubelink received from the PCE for disconnected C-VENs was not being acknowledged back to the PCE, which caused unnecessary policy calculations and high PCE load.
E-122553	**C-VEN 23.4.x fw_tampering_revert_failure after upgrade** False-positive firewall tamper alerts ("VEN firewall tampered") appeared after upgrading to C-VEN 23.x, because of the old and unused Illumio iptables chain.
E-122422	**C-VEN activation failing** In some cases, attempts to bring onboard and pair a second Kubernetes AWS EKS cluster were failing to activate the C-VENs.
E-122306	**Kubelink: One service appears multiple times in service update** Kubelink was sending one service multiple times in an update request to PCE, which caused multiple duplicates of Service Backends, and slowed PCE responsiveness. Older Kubelink 3.1.x and 4.x also have this issue and should be upgraded to Kubelink 5.3.0, either using Helm chart 5.3.0, or by using YAML files generated from this Helm chart version. Kubelink 5.3.0 in non-CLAS mode is backward compatible with all currently supported PCE versions.
E-121122	**C-VEN: False positive vulnerability detection on Quay** The Quay vulnerability scanner falsely detected C-VEN as having high severity vulnerabilities.
E-120773	**Increasing memory use and "out of memory errors" occur on 22.5.14 C-VEN nodes** Resolved intermittent "out of memory" occurrences in C-VEN 22.5.14.

Illumio Core for Kubernetes Release Notes 5.2

January 2025

About Illumio Core for Kubernetes 5.2

These release notes describe the resolved issues, known issues, and related information for the 5.2.*x* releases of Illumio Core for Kubernetes, formerly known as Illumio Containerized VEN, or C-VEN. Illumio Core for Kubernetes also includes the related required component, Kubelink. Because of this heritage, many references to this product as "C-VEN" are still used throughout the documentation.

Document Last Revised: January 2025

Product Version

Compatible PCE Versions: 23.5.10 and later releases

Current Illumio Core for Kubernetes Version: 5.2.3, which includes:

- C-VEN version: 23.4.2
- Kubelink version: 5.2.1
- Helm Chart version: 5.2.3

Updates for Core for Kubernetes 5.2.3

Kubelink

Resolved Issue

- **One service appears multiple times in service update** (E-122306)
  Kubelink was sending one service multiple times in an update request to PCE, which caused multiple duplicates of Service Backends, and slowed PCE responsiveness. Older Kubelink 3.1.x and 4.x also have this issue and should be upgraded to Kubelink 5.2.1, either using Helm chart 5.2.3, or by using yaml files generated from this Helm chart version. Kubelink 5.2.1 in non-CLAS mode is backward compatible with all currently supported PCE versions.

Updates for Core for Kubernetes 5.2.2

C-VEN

Resolved Issues

- **Multiple C-VENs not syncing policy** (E-122102)
  In larger CLAS-enabled clusters with very big policies, even though C-VENs initially appeared to to be properly synced, the policy was not updated.
- **C-VEN on PCE UI has "-dev" in version but image pulled from helm does not** (E-120423)
  After upgrading to release 5.2.0, the C-VEN version was reported with a "-dev" string appended (for example, "23.4.0-8-dev") in the PCE UI (at the VEN details page) and other locations like in `/etc/agent_version`, but the image specified in the C-VEN daemonset resource did not.
- **C-VEN: unable to send flows if there is a lot of data** (E-119110)

When C-VEN attempted to send a large amount of flow data at once, the transmission would fail, and after a few retries the AgentMgr process would crash, causing C-VEN to stop sending flow records.

What's New in Release 5.2.1

- **Helm Chart option to Disable NodePort Forwarding**

  A new option was added to Helm Chart for C-VEN that disables NodePort forwarding on host workloads. After setting `enforceNodePortTraffic: never` in the Helm values file, C-VEN behaves like before in its 22.5 version-- that is, the forward chain on Node is open, and custom iptables rules must be used to enforce traffic in this chain.

Updates for Core for Kubernetes 5.2.1

Kubelink

Resolved Issues

- **Kubelink can't start on OpenShift because of fsGroup 1001** (E-120425)

  When using Helm Chart 5.2.0 on OpenShift, Kubelink would not start because of fsGroup 1001.

C-VEN

Resolved Issues

In an early version of these Release Notes issues E-119682 and E-119110 were incorrectly listed as being resolved.

- **NodePort access is working when it should be blocked** (E-120655)

  NodePort traffic was being always allowed, with or without a rule allowing the traffic from an external resource to the NodePort service. This issue was fixed by adding missing legacy iptables command line utilities to the UBI9-based C-VEN.
- **Move C-VEN base image to a smaller image** (E-118492)

  C-VEN now uses a UBI9-micro image as its base image, using the current latest version 9.4-15.

What's New in Release 5.2.0

- **"Wait for Policy" Feature**

  With a new Wait For Policy feature, CLAS-enabled Kubelink can be configured to automatically and transparently delay the start of an application container in a pod until a policy is properly applied to the pod. This feature replaces the local policy convergence controller, the Illumio readiness gate. A readiness gate required adding the `readinessGates.conditionType` into the spec YAML file of the Kubernetes Workload. Instead, Wait For Policy uses an automatically injected init container, with no change of the user application needed. When enabled, Wait For Policy synchronizes the benefit of Kubernetes automatic container creation with the protection of proper policy convergence into the new container.

  For more information, see "Wait For Policy" Feature [36].
- **CLAS Flat Network Support**

Starting in version 5.2.0, the Kubelink Operator supports flat network CNIs in CLAS mode, a feature that was previously only available in non-CLAS mode. This update includes compatibility with flat network types such as Azure CNI Pod Subnet and Amazon VPC CNI. To enable a flat network CNI, set the `networkType` parameter to `flat` in the Helm Chart's `illumio-values.yaml` file during installation.

Also note that in CLAS-enabled flat networks, if a pod communicates with a virtual machine outside the cluster using private IP addresses, you must enable the annotation `meta.illumio.podIPObservability`. This is a scenario in which the virtual machine is in a private network and has an IP address from the same range as cluster nodes and pods. In this case, the PCE needs to know the private IP address of the pod to be able to open a connection on the virtual machine. The main benefit of CLAS is that the PCE no longer directly manages individual pods, so the implementation expects a specific annotation on such pods. Traffic between such private IPs will be blocked without this annotation, and will appear in the UI as blocked.

In this case, when the application communicates through private IPs, add the following annotation so that Kubelink can then report the private IPs of Kubernetes Workloads to the PCE:

```
metadata:
    annotations:
        meta.illumio.podIPObservability: "true"
```

- **Kubelink Support Bundle**

  To assist the Illumio Support team with more details for troubleshooting, Kubelink now provides a support bundle that collects up to 2 GB of logs, metrics, and other data inside its pod. Future versions will add the option to upload these support bundles to the PCE. Currently, you must copy this support bundle by running the script `/support_bundle.sh` inside the Kubelink pod. The script generates debug data, creates a gzipped tar archive using stdout as output, and encodes this data using Base64.

  Use the following command to generate and transfer the Kubelink support bundle from its pod:

  ```
  kubectl --namespace illumio-system exec deploy/illumio-kubelink
  -- /support_bundle.sh | base64 --decode > /tmp/kubelink_support.tgz
  ```

  Send the resulting compressed archive file to Illumio Support when requested.

- **Base OS Upgraded to UBI9**

  The base OS has been upgraded to Red Hat Universal Base Image 9 (micro UBI9 for Kubelink, mini UBI9 for C-VEN).

  IMPORTANT

  Important Notice: With the base image upgrade for both Kubelink and C-VEN, you must adjust resource allocations according to the guidance described below in the Resource Allocation Guidelines [34] section. You must ensure that resources are updated prior to the upgrade to achieve optimal performance and avoid any potential degradation in product performance.

- **Enhanced Pod Stability for Kubelink and C-VEN**

  To address the challenge of pod eviction during Kubernetes cluster issues or space shortages, Kubelink was previously the first pod to be evicted, which led to failures in policy enforcement. Recognizing the critical need for stability, Helm Chart version 5.2.0 introduces default priority classes for both Kubelink and C-VEN. Kubelink is now assigned the priority class of `system-cluster-critical`, while C-VENs receive `system-node-critical`. This implementation significantly enhances the resilience of your deployments, ensuring that key components remain operational even under resource constraints.

- **Changes to Supported Orchestration Platforms and Components in 5.2.0**
  The 5.2.0 release contains several changes to supported platforms and components. For full details, see Kubernetes Operator OS Support and Dependencies on the Illumio Support portal (log in required).

Resource Allocation Guidelines

New resource allocation guidelines have been developed to help configure deployments to achieve optimal performance and cost-efficiency.

These guidelines are grouped into the following general deployment sizes:

- **Small-scale:** Customers with limited Kubernetes deployments and moderate workloads.
- **Medium-scale:** Customers with moderate-sized Kubernetes environments and growing workloads.
- **Large-scale:** Customers with extensive Kubernetes deployments and high-performance requirements.

The following variables determine the deployment sizes listed above:

- Number of nodes per cluster
- Total number of workloads per cluster
- Total policy size per cluster

Set the `resources` values in the appropriate pod spec (Kubelink or C-VEN) `yaml` file under the `storage` section, as shown in the following example:

```
storage:
  sizeGi: 1
  resources:
    limits:
      memory: 600Mi
    requests:
      memory: 500Mi
      cpu: 500m
```

If you have two parameters that match one category, and a third parameter that matches another, it's important to select the category based on the highest value among them.

For instance, if the number of nodes per cluster is 8, and the total number of Kubernetes workloads is 500, but the average size of the policy is 1 Gi, the resource allocation should align with the large-scale resource allocation. This ensures that your resources are appropriately scaled to meet the demands of your workloads, optimizing performance and stability.

In practice, monitor these resources, and if usage is at 80% of these limits, then consider increasing.

NOTE that amounts are expressed in mebibytes (Mi) and gibibytes (Gi) and not in megabytes (MB) or gigabytes (GB).

Small-scale resource allocation

Customer Category	Nodes per Cluster	Total K8s Workloads	Total Policy Size	
Small-scale	1 - 10	0 - 1000	0 - 1.5 Mi	
Resources		**C-VEN**	**Kubelink**	**Storage**
Requests	CPU	0.5	0.5	0.5
Requests	memory	600 Mi	500 Mi	500 Mi
Limits	CPU	1	1	1
Limits	memory	700 Mi	600 Mi	600 Mi
Volumes	size limits	n/a	n/a	1 Gi

Medium-scale resource allocation

Customer Category	Nodes per Cluster	Total K8s Workloads	Total Policy Size	
Medium-scale	10 - 20	1000 - 5000	1.5 Mi - 500 Mi	
Resources		**C-VEN**	**Kubelink**	**Storage**
Requests	CPU	2	2	1
Requests	memory	3 Gi	5 Gi	5 Gi
Limits	CPU	3	2	2
Limits	memory	5 Gi	7 Gi	7 Gi
Volumes	size limits	n/a	n/a	5 Gi

Large-scale resource allocation

Customer Category	Nodes per Cluster	Total K8s Workloads	Total Policy Size	
Large-scale	20+	5000 - 8000	500 Mi - 1.5 Gi	
Resources		**C-VEN**	**Kubelink**	**Storage**
Requests	CPU	2	3	1
Requests	memory	6 Gi	10 Gi	10 Gi
Limits	CPU	3	4	2
Limits	memory	8 Gi	12 Gi	12 Gi
Volumes	size limits	n/a	n/a	10 Gi

"Wait For Policy" Feature

With a new *Wait For Policy* feature, CLAS-enabled Kubelink can be configured to automatically and transparently delay the start of an application container in a pod until a policy is properly applied to that container. This synchronizes the benefit of automatic container creation with the protection of proper policy convergence into the new container.

This Wait For Policy feature replaces the existing local policy convergence controller, also known as a readiness gate. A readiness gate required manually adding the `readinessGate` condition into the spec of the Kubernetes Workload. Instead, Wait For Policy uses an automatically injected init container, which requires no change to the user application.

Behavior

When Wait For Policy is enabled, Kubelink creates a new `MutatingWebhookConfiguration`. This webhook injects an Illumio init container into every new pod. Now, a new pod lifecycle consists of the following sequence of actions:

1. Kubernetes creates a pod.
2. The pod creation request is intercepted by a mutating webhook.
3. Kubernetes requests MutatingAdmissionWebhook Controller running in Kubelink.
4. Controller returns with a new pod patched with an Illumio init container.
5. Init container starts in the pod, and periodically checks the policy status of the pod using the Kubelink status server.
6. At the same time, Kubelink is preparing a policy for the new pod, and is sending the policy to the pod's C-VEN.
7. The C-VEN applies policy to the pod and sends an acknowledgment to Kubelink.
8. Kubelink reports that the policy is now applied to the init container.
9. The Init container exits and allows the original container to start.
10. If a policy is not applied within the configured time (see Configuration [37] section for Helm Chart `waitForPolicy.timeout` parameter), the init container exits anyway, and allows the original container to start.

The Illumio init container must be accessible from all namespaces that use Wait for Policy. An easy way to ensure this accessibility is to make the init available from a public repository.

However, a private repository can be used if you manage the secret deployment properly, such as by deploying init from the same repository as all other containers or using a secret management tool.

Configuration

The Wait For Policy feature is disabled by default. To enable it, change the `waitForPolicy: enabled` value to `true` in the Helm Chart `illumio-values.yaml` file. The following is the default Helm Chart configuration for Wait For Policy:

```
## Wait for Policy - Illumio delays the start of Pods until policy is
applied
waitForPolicy:
  ## @param waitForPolicy.enabled Enable Wait for Policy feature
  enabled: false
  ## @param waitForPolicy.ignoredNamespaces List of namespaces where
Illumio
  ## doesn't delay start of Pods. kube-system and
  ## illumio-system name are ignored by Kubelink for this feature by
default,
  ## even if not specified in this list.
  ignoredNamespaces:
    - kube-system
    - illumio-system
  ## @param waitForPolicy.timeout How long will pods wait for policy, in
seconds
  timeout: 130
```

Pods starting in namespaces listed in `ignoredNamespaces` start immediately, without an Illumio init container injected into them. The namespaces `kube-system` and `illumio-system` are always ignored by the MutatingAdmissionWebhook Controller running in Kubelink, even if those are not specified in the configuration. The default value of `ignoredNamespaces` contains `kube-system` and `illumio-system` for reference, and can be extended with custom namespaces.

The `timeout` value is the total allowed run time of the init container. After this time elapses, the init container exits even if the policy is not applied, and allows the original container to start.

Updates for Core for Kubernetes 5.2.0

Kubelink

Resolved Issues

- **Helm: pull secret to quay gets created even if no credentials are set** (E-119659)
  Helm chart now creates Illumio pull secret only if credentials are specified and also externally passed secret names are included.
- **Kubelink: error concurrent map read and map write** (E-119626)
  Kubelink was restarted because previous container exited with the message "`fatal error concurrent map read and map write`."
- **Kubelink: Update base image to address vulnerabilities** (E-119429)
  The Unified Base Image was upgraded to address CVE-2023-45288.

- **Kubelink needs to have higher priority assigned to avoid going to evicted state** (E-113920)

  If the Kubernetes cluster encounters problems or runs out of space, Kubelink was the first pod to be put into the evicted state, which caused policy enforcement to fail. To prevent permanent eviction, in Helm chart version 5.2.0 the Kubelink Deployment and C-VEN DaemonSets are assigned priority classes by default -- `system-cluster-critical` for Kubelink and `system-node-critical` for C-VENs.

C-VEN

Resolved Issues

- **CVEN: Update base image to address vulnerabilities** (E-119428)

  The 23.4 C-VEN Unified Base Image was upgraded to the latest UBI9 to address vulnerabilities described in CVE-2014-3566, CVE-2014-3566, CVE-2014-3566, CVE-2022-3358, and CVE-2023-27533.
- **Cannot deploy C-VEN to GKE when using default OS** (E-116506)

  For GKE clusters, when using the default cluster OS (Container-Optimized OS from Google), the node filesystems are read-only. This prevented C-VEN from mounting `/opt/illumio_ven_data` and writing into it for persistent storage.

  To resolve this issue, a new variable `` `cven.hostBasePath `` was added to the 5.2.0 Helm Chart to specify where the C-VEN DaemonSet mounts its data directory. The default value is `/opt`. Use this variable to specify where the C-VEN DaemonSet mounts its data directory. If using a Container-Optimized OS, you can set the directory to `/var`.
- **[CVEN]: Failed to load policy** (E-115231)

  The log message "`Error: Failed to load policy`" was appearing during scenarios that were obvious or expected. The log level for this message has been changed from Error to Info.
- **Re-adding node does not re-pair it** (E-98120)

  When deleting and then re-adding the same node, the node would not reappear, and its policy disappeared.

Illumio Core for Kubernetes Release Notes 5.1

Published: September 4, 2024

Core for Kubernetes 5.1.10

Compatible PCE Versions: 23.5.10 and most later releases

Current Illumio Core for Kubernetes Version: 5.1.10, which includes:

- C-VEN version: 23.3.1
- Kubelink version: 5.1.10
- Helm Chart version: 5.1.10

Before deploying any Illumio Core for Kubernetes 5.1.x version, confirm your PCE version supports it. For example, currently Illumio Core for Kubernetes versions 5.1.0 and 5.1.2 are supported **only** with PCE versions 23.5.10 (for On Premises customers) or 24.1.x (for SaaS customers), but NOT on PCE versions 23.5.1 or 23.6.0, or any lower versions. For complete compatibility details, see the Kubernetes Operator OS Support and Dependencies page on the Illumio Support Portal.

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

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

Limitations

- **NodePort**
  The following limitations exist regarding NodePort policy enforcement and flows:
  - Only NodePort Services with `externalTrafficPolicy` set to "`cluster`" are supported. (This is the default and most frequently used value for this setting.)
  - When writing rules to allow traffic to flow from external (to the cluster) entities and NodePort Service, the source side of the rule must contain all nodes in the cluster.

    For example, given the following setup:

    - Worker nodes in the cluster are labeled as Role: Worker Node

    - Clients accessing the Service running in the Kubernetes cluster are labeled Role: Client

    - The NodePort Service is labeled Role: Ingress

    Normally, the rule would be written as Role: Client -> Role: Ingress. However, for thisrelease the rule must also include all nodes in the cluster to work correctly: Role: Client + Role: Worker Node -> Role: Ingress.
- **Flat Network support in CLAS mode**
  Using EKS or AKS in a flat network topology, such as EKS with AWS VPC CNI or AKS with Azure CNI, is not supported in CLAS-enabled clusters.

Updates for Core for Kubernetes 5.1.10

Kubelink

Resolved Issues

- **Last updated policy timestamp for C-VENs reflects Kubernetes Workload policy changes** (E-118372)
  The last updated policy timestamp on C-VENs now updates after a C-VEN successfully updates the policy for its pods.
- **Unexpected Potentially Blocked traffic in Explorer (CLAS mode)** (E-116105)
  In CLAS environments, some allowed traffic flows were wrongly reported as Potentially Blocked because of missing IP sets in the firewall test database.

Updates for Core for Kubernetes 5.1.7

Kubelink

Resolved Issues

- **Kubelink: policy service blocked when agent disconnects while receiving policy message** (E-117099)

  In some situations, policies stopped being sent due to a policy channel lock after C-VEN disconnected while receiving a policy update.
- **Kubelink: policy service blocked if one agent is not reading policy message** (E-116967)

  In some situations, policies stopped being sent after a C-VEN became unresponsive.
- **Kubelink can't save sets because of message size limit** (E-116825)

  Policy updates were being interrupted when large policy sets were being sent. The message size has been increased to permit larger policy transmissions .
- **Kubelink: workload events processing is slowed down by policy updates** (E-116706)

  The processing of workload events from Kubernetes sometimes became slow when handling thousands of Kubernetes Workloads, or the policy PCE requests were taking too long, or if there was no previous policy version in storage.
- **Kubelink sends wrong workload href in policy ACK request** (E-116640)

  In some CLAS-enabled clusters that host large numbers of workloads, the Kubernetes Workloads page showed an old policy apply date. Kubelink incorrectly sent a policy ACK for some Kubernetes Workloads with the host workload URI. The PCE responded with a 406 error, and a "no policy" ACK was stored.

Updates for Core for Kubernetes 5.1.3

Kubelink

Resolved Issues

- **Kubelink can't save policy to storage** (E-116539)

  Kubelink could not store cluster policy due to storage size limitations. To permit increased storage sizes, the Helm chart now includes new `resources` values under the `storage` component, as well as under `cven` and `kubelink` (note that amounts are in MiB not MB, and GiB not GB):

```
kubelink:
  resources:
    limits:
      memory: 500Mi
    requests:
      memory: 200Mi
      cpu: 200m

cven:
  resources:
    limits:
      memory: 300Mi
    requests:
      memory: 100Mi
      cpu: 250m

storage:
  resources:
    limits:
      memory: 500Mi
    requests:
      memory: 200Mi
      cpu: 100m
```

- **Pod to pod flows and pod labels are missing from Explorer search results** (E-116271, E-116272)

  In CLAS-enabled clusters, Explorer was not showing pod labels, only workload labels. In addition, Explorer did not return some traffic flows, even when trying with label-based search, or port-based search, or even searching using workload labels + pod labels. Also, pod traffic was being mapped to workloads.

Updates for Core for Kubernetes 5.1.2

Kubelink

Resolved Issues

- **Helm Chart: etcd storage size limit** (E-115417)

  Kubelink in CLAS mode uses etcd as a local cache for policy and runtime data. The Helm Chart now accepts a new variable called `storage.sizeGi` to set the size (in GiB not GB) of ephemeral storage. The default value is 1.
- **Kubelink - Unable to process policy with custom iptables rules** (E-115250)

  Kubelink in CLAS mode failed to process policy received from the PCE when custom iptables rules were present, producing the error message "json: cannot unmarshal object into Go struct field."
- **Kubelink to PCE connectivity issues - connection reset by peer** (E-115049)

  CLAS-enabled Kubelink was entering degraded mode too soon because of PCE connectivity problems. Now Kubelink also retries requests after network and OS errors, which avoids premature degraded mode entry.
- **C-VEN reporting potentially blocked traffic between worker nodes** (E-114691)

  CLAS processing of outbound rules to a ClusterIP Service replaced the "All Services" destination in the rule with actual ports from the Kubernetes Service. If a destination label included a Kubernetes Service, this caused a missing iptables rule between nodes.
- **Max policy message size between Kubelink and C-VEN is too small** (E-113714)

The default gRPC message size was set to too small of a value, which caused C-VENs to reject policy messages that were larger than this value. The default gRPC message size is now larger, to avoid this problem.

Updates for Core for Kubernetes 5.1.0

What's New in the 5.1.0 Release

The following are new and changed items in the 5.1.0 release from the previous releases of C-VEN and Kubelink:

- **New CLAS architecture option**

  Kubelink now can be deployed with a Cluster Local Actor Store (CLAS) module, which manages flows from C-VENs to PCE, and policies from PCE to C-VENs. The CLAS-enabled Kubelink tracks individual pods, and when they are created or destroyed, instead of this being communicated directly to the PCE. To migrate from an existing (non-CLAS) environment to a CLAS-enabled one, set the `clusterMode` parameter to `migrateLegacyToClas` in your deployment YAML file (typically named `illumio-values.yaml`). See the `README.md` file accompanying the Helm Chart for full details on this and other Helm Chart parameters.
- **Workloads more closely match Kubernetes architecture**

  In CLAS-enabled environments, workloads are now conceptually tied to their containers, instead of being referred to in context of their pods, which more closely matches Kubernetes practice. To reflect this change, such workloads in CLAS environments are called *Kubernetes Workloads*, regardless of what containers have been spun up or destroyed to run the applications. In non-CLAS environments, the existing term *Container Workloads* is still used as in prior releases, corresponding to Pods. In mixed environments (with both non-CLAS and CLAS-enabled clusters), the PCE UI shows both Container Workloads and Kubernetes Workloads, as appropriate.
- **Degraded mode for CLAS-enabled Kubelink**

  If a CLAS-enabled Kubelink detects that its connection with the PCE becomes unavailable (for example, due to connectivity problems or an upgrade), Kubelink by default enters a *degraded mode*. In this degraded mode, new Pods of existing Kubernetes Workloads get the latest policy version cached in CLAS storage. When Kubelink detects a new Kubernetes Workload with exactly the same label sets and in the same namespace as an existing Kubernetes Workload, Kubelink delivers the existing, cached policy to Pods to this new Workload. If Kubelink cannot find a cached policy (that is, when labels of a new Workload do not match those of any existing Workload in the same namespace), Kubelink delivers a “fail open” or “fail closed” policy based on the Helm Chart parameter `degradedModePolicyFail`. The degraded mode can also be turned on or off by the Helm Chart parameter `disableDegradedMode`.
- **Illumio annotations in CLAS mode specified on the workload and not on Pod's template**

  Illumio annotations when in CLAS mode are now specified on the Kubernetes Workload and not on the pod's template.
- **Docker support dropped**

  The Docker CRI is no longer supported as of the 5.0.0 release of Illumio Core for Kubernetes.

C-VEN

Resolved Issue

- **Permanently delete Kubernetes Workloads after certain period when they are unpaired** (E-112362)

Kubernetes Workloads (from a CLAS environment) are pruned from the PCE one day (by default) after they are unpaired. The length of time that elapses (in seconds) before this pruning occurs is configurable with the `vacuum_entities_wait_before_vacuum_seconds` parameter, which is set in the PCE `agent.yml` file. The default value for this parameter is 86400 (24 hours).

Known Issues

- **When C-VEN starts first, a 404 from PCE when getting CLAS token** (E-109259)

  When C-VEN is started first, it tries to contact the PCE in order to obtain CLAS token, but receives a 404 error. This is expected behavior for this scenario, which is only momentary. Kubelink eventually starts normally, and C-VEN obtains the CLAS tokens as expected.
- **Helm install fails with Helm version 3.12.2 but works with 3.10** (E-108128)

  When installing with Helm version 3.12.2, the installation fails with a YAML parse error.

  Workaround: Use Helm version 3.10, or version 3.12.3 or later.
- **Re-adding node does not re-pair it** (E-98120)

  After deleting a node and re-adding the same node, the node does not reappear, and previously established policy disappears from the node.

  Workaround: Uninstall and re-install Illumio Core for Kubernetes from scratch with the node present.

Kubelink

Resolved Issues

- **CLAS: NodePort - pod rules are not removed after disabling rule** (E-111689)

  After disabling a NodePort rule that opens it to outside VMs, iptable entries for pods with a virtual service's targetPort were not being removed as expected. Now the pod no longer remains opened. Host iptables are removed, so traffic does not go through, and the pod ports are properly closed.
- **CLAS - The etcd pod crashes when node reboots** (E-106236)

  The etcd pod would crash if one of the nodes in the cluster was rebooted.

Known Issues

- **CLAS-mode Kubelink pod gets restarted once when deploying Illumio Core for Kubernetes** (E-109284)

  The Kubelink pod is restarted after deploying Illumio Core for Kubernetes in CLAS mode.

  There is no workaround. Kubelink runs properly after this single restart.
- **CLAS: Container Workload Profile label change is not applied to Kubernetes Workloads, only to Virtual Services** (E-109168)

  When removing labels in a Container Workload Profile, existing Kubernetes Workloads that are managed by that profile do not have their labels changed automatically to labels based on annotations. These existing Kubernetes Workloads must be updated with the `kubectl apply` command for the labels change to take effect. New Kubernetes Workloads created after the profile label change will have the new labels.

  This works as designed.

Security Information for Core for Kubernetes 5.1

For information about security issues, security advisories, and other security guidance pertaining to this release, see Illumio’s Knowledge Base in Illumio's Support portal.

Illumio Core for Kubernetes Release Notes 5.0.0

About Illumio Core for Kubernetes 5.0

These release notes describe the resolved issues, known issues, and related information for the 5.0.0 release of Illumio Core for Kubernetes, formerly known as Illumio Containerized VEN, or C-VEN. Illumio Core for Kubernetes also includes the related required component, Kubelink. Because of this heritage, many references to this product as "C-VEN" are still used throughout the documentation.

Document Last Revised: January 2024

Product Version

Compatible PCE Versions: 23.5.10 and later releases

Current Illumio Core for Kubernetes Version: 5.2.3, which includes:

- C-VEN version: 23.4.2
- Kubelink version: 5.2.1
- Helm Chart version: 5.0.0

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

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

What's New in C-VEN and Kubelink

The following are new and changed items in this release from the previous releases of C-VEN and Kubelink:

- **New CLAS architecture option**
  Kubelink now can be deployed with a Cluster Local Actor Store (CLAS) module, which manages flows from C-VENs to PCE, and policies from PCE to C-VENs. The CLAS-enabled Kubelink tracks individual pods, and when they are created or destroyed, instead of this being communicated directly to the PCE. To migrate from an existing (non-CLAS) environment to a CLAS-enabled one, set the `clusterMode` parameter to `migrateLegacyToClas` i n your deployment YAML file (typically named `illumio-values.yaml`). See the `README.md` file accompanying the Helm Chart for full details on this and other Helm Chart parameters.
- **Workloads more closely match Kubernetes architecture**
  In CLAS-enabled environments, workloads are now conceptually tied to their containers, instead of being referred to in context of their pods, which more closely matches Kubernetes practice. To reflect this change, such workloads in CLAS environments are called *Kubernetes Workloads*, regardless of what containers have been spun up or destroyed to run the applications. In non-CLAS environments, the existing term *Container Workloads* is

still used as in prior releases, corresponding to Pods. In mixed environments (with both non-CLAS and CLAS-enabled clusters), the PCE UI shows both Container Workloads and Kubernetes Workloads, as appropriate.

- **Illumio annotations in CLAS mode specified on the workload and not on Pod's template**

  Illumio annotations when in CLAS mode are now specified on the Kubernetes Workload and not on the pod's template.
- **Docker support dropped**

  The Docker CRI is no longer supported as of this 5.0.0 release of Illumio Core for Kubernetes.

NodePort Limitations

- **NodePort**

  Here are some limitations around NodePort policy enforcement and flows:
  - Only NodePort Services with `externalTrafficPolicy` set to "`cluster`" are supported. (This is the default and most frequently used value for this setting.)
  - When writing rules to allow traffic to flow from external (to the cluster) entities and NodePort Service, the source side of the rule must contain all nodes in the cluster.

    For example, given the following setup:

    - Worker nodes in the cluster are labeled as Role: Worker Node

    - Clients accessing the Service running in the Kubernetes cluster are labeled Role: Client

    - The NodePort Service is labeled Role: Ingress
  - Normally, the rule would be written as Role: Client -> Role: Ingress. However, for this beta1 release the rule must also include all nodes in the cluster to work correctly: Role: Client + Role: Worker Node -> Role: Ingress.

Updates for Core for Kubernetes 5.0.0-LA

C-VEN

Resolved Issues

- **Scaling a Deployment with changed labels was not being updated on PCE** (E-107274)

  After deploying a workload with a non-existing label, create labels on the PCE and wait a few minutes before updating and applying the YAML to change the number of replicas. The deployment was not properly updated on the PCE. This issue is resolved.

Known Issues

- **When C-VEN starts first, a 404 from PCE when getting CLAS token** (E-109259)

  When C-VEN is started first, it tries to contact the PCE in order to obtain CLAS token, but receives a 404 error. This is expected behavior for this scenario, which is only momentary. Kubelink eventually starts normally, and C-VEN obtains the CLAS tokens as expected.
- **Helm install fails with Helm version 3.12.2 but works with 3.10** (E-108128)

  When installing with Helm version 3.12.2, the installation fails with a YAML parse error.

  Workaround: Use Helm version 3.10, or version 3.12.3 or later.

- **Re-adding node does not re-pair it** (E-98120)

  After deleting a node and re-adding the same node, the node does not reappear, and previously established policy disappears from the node.

  Workaround: Uninstall and re-install Illumio Core for Kubernetes from scratch with the node present.

Kubelink

Resolved Issues

- **CLAS on IKS with Calico, the flow of ClusterIP is not displayed correctly** (E-109238)

  In a CLAS environment on IKS with Calico, when running traffic to a clusterIP service from a pod, flows were being displayed incorrectly. Sometimes flows were incorrectly shown as Allowed. Other times, flows that should not be present were being shown as Blocked. This issue is resolved.
- **Kubernetes cluster falsely detected as an OpenShift cluster** (E-107910)

  After deployment, Kubelink falsely detected a Kubernetes cluster as an OpenShift cluster based on misinterpretations of installed VolumeReplicationClass and VolumeReplications APIs on the cluster. This issue is resolved.
- **Problem when label from PCE was deleted after Kubelink starts** (E-107779)

  When creating a new workload on PCE, Kubelink uses cached or preloaded labels to label a workload. However, if the label was deleted before the workload was actually created, the PCE responded with a 406 status error. This issue is resolved.
- **Kubelink did not properly apply label mappings with PCE using two-sided management ports** (E-105391)

  Label mappings were not properly applied when using the LabelMap CRD if the PCE used two-sided management ports. This issue is resolved.

Known Issues

- **CLAS: NodePort - pod rules are not removed after disabling rule** (E-111689)

  After disabling a NodePort rule that opens it to outside VMs, iptables entries for pods with a virtual service's targetPort are not removed as expected. The pod is still opened. Host iptables are removed, so traffic does not go through, but the pod ports stay opened towards original IPs.

  There is no workaround available.
- **Non-CLAS mode: Failed to clean up the pods** (E-109687)

  After deleting a non-CLAS container cluster, the cluster gets deleted but Container Workloads are not deleted, and remain present.
- **CLAS-mode Kubelink pod gets restarted once when deploying Illumio Core for Kubernetes** (E-109284)

  The Kubelink pod is restarted after deploying Illumio Core for Kubernetes in CLAS mode.

  There is no workaround. Kubelink runs properly after this single restart.
- **CLAS: Container Workload Profile label change is not applied to Kubernetes Workloads, only to Virtual Services** (E-109168)

  In CLAS environments, after changing a label in a Container Workload Profile, the Kubernetes Workloads that are managed by that Profile do not have their labels changed as expected. No changes to these Kubernetes Workloads occur even when the Profile is changed to "No Label Allowed;" the original labels remain in the Kubernetes Workloads. However, Virtual Services managed by that profile do successfully have their labels changed properly.

  No workaround is available.
- **CLAS - The etcd pod crashes when node reboots** (E-106236)

  The etcd pod crashes if one of the nodes in the cluster is rebooted.

There is no workaround available.

Security Information for Core for Kubernetes 5.0.0-LA

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

Illumio Core for Kubernetes Release Notes 4.3.0

What's New in Kubernetes 4.3.0

These release notes describe the resolved issues and related information for the 4.3.0 release of Illumio Core for Kubernetes, formerly known as Illumio Containerized VEN, or C-VEN.

Illumio Core for Kubernetes also includes the related required component, Kubelink. Because of this heritage, many references to this product as "C-VEN" are still used throughout the documentation.

Here are the new and changed items in this release:

- **New Kubelink 3.3.1**
  This Kubernetes 4.3.0 release includes an upgraded Kubelink component, version 3.3.1 .
- **New C-VEN 22.5.14**
  This Kubernetes 4.3.0 release includes an upgraded C-VEN component, version 22.5.14.

> **NOTE**
> C-VEN 22.5.14 requires PCE version 22.5.0 or later, and supports PCE 23.3.0 or later.

Security Information

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

Base Image Upgraded

The C-VEN base OS image is upgraded to minimal UBI for Red Hat Linux 7.9-979.1679306063, which is available at https://catalog.redhat.com/software/containers/ubi7/ubi-minimal/5c3594f7dd19c775cddfa777.

Customers are advised to upgrade to Core for Kubernetes 4.1.0 or higher for these security fixes.

Product Version

Compatible PCE Versions: 22.5.0 and later releases

Current Illumio Core for Kubernetes Version: 4.3.0, which includes:

- C-VEN version: 22.5.14
- Kubelink version: 3.3.1
- Helm Chart version: 4.3.0

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

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

Updates for Core for Kubernetes 4.3.0

C-VEN

Resolved Issues

- **C-VEN support report does not contain container workload firewalls** (E-106932)

  VEN support reports for C-VENs were missing the active firewall information for all container workloads. This issue is resolved. Support reports now include full firewalls from each network namespace, as gathered by `iptables-save` and `ipset list` output.
- **Conntrack tear-down for containers with policy updates** (E-44832)

  Although policy was changed to block a container workload from talking to another, traffic was still passing between the workloads, due to a conntrack connection remaining incorrectly active. This issue is resolved. Conntrack connections on sessions affected by a policy change are now properly torn down.

Known Issue

- **C-VENs not automatically cleaned up after AKS upgrade** (E-103895)

  After upgrading an AKS cluster, sometimes a few duplicate C-VENs might not be automatically removed as part of the normal upgrade process, and remain in the PCE as "non-active." Note there is no compromise to the security or other functionality of the product.

  Workaround: Manually prune the extra unmigrated C-VENs from the PCE by clicking the **Unpair** button for each of them.

Kubelink

Resolved Issue

- **Kubelink does not pair with PCE when a separate management port is used** (E-107001)

  Kubelink would crash after start when the PCE had `front_end_management_https_port` set to 9443 instead of 8443, because of a missing label_map URL. This issue is resolved.

Known Issue

- **Kubelink does not properly apply label mappings with PCE using two-sided management ports** (E-105391)

  Label mappings are not properly applied when using the LabelMap CRD if the PCE uses two-sided management ports.

Workaround: Use the label map feature only with a PCE that uses only one management port.

Illumio Flowlink Release Notes

Illumio Flowlink Release Notes for Release 1.4.0

December 2024

Product Version

Flowlink Version: 1.4.0

Compatible PCE Version: PCE 19.3.0 and later releases

Standard versus LTS Releases

For information about Standard versus Long Term Support (LTS) releases, see Versions and Compatibility in the Illumio Support portal (log in required).

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

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

New Features in Illumio Flowlink 1.4.0

The following new features were added in Illumio Flowlink 1.4.0.

- **Support for FIPS compliance on RHEL 9**
  Beginning with this release, Flowlink now supports FIPS compliance on RHEL 9. For more information, see FIPS Compliance for Flowlink.
- **Increased buffer size**
  Flowlink buffer size is increased to 65kb. This was done to address an issue where Flowlink failed to process large `UDP` packets.
- **Support for ingesting multiple flow types**
  Beginning with this release, the Flowlink text flow collector supports flows with any `IP` protocol number, not just `UDP`, `TCP` and `ICMP`.

Resolved and Known Issues in Flowlink 1.4.0

Resolved Issue

Flowlink became non-responsive (E-114431)

A parsing issue with the IPFIX packet caused Flowlink 1.3.0 to become non-responsive, requiring a manual restart. This issue is fixed with this release.

Known Issue

No Automatic Restart Following Reboot (E-15146)

Flowlink is not installed as a service, nor does it support a High Availability (HA) configuration. As such, it doesn't restart automatically if the host fails or is rebooted. In those cases, you need to restart Flowlink manually.

Illumio Flowlink Release Notes 1.3.0

Product Version

Flowlink Version: 1.3.0

Compatible PCE Version: PCE 19.3.0 and later releases

Standard versus LTS Releases

For information about Standard versus Long Term Support (LTS) releases, see Versions and Compatibility in the Illumio Support portal (log in required).

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

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

New Feature in Flowlink 1.3.0

Support for HTTP/HTTPS Proxy

Beginning with this release, Flowlink now supports HTTP/HTTPS proxy. When Flowlink is running behind a proxy or in a corporate network and the PCE is in the cloud, Flowlink can now access the PCE via HTTP/HTTPS proxy configurations.

The following configuration parameter is available to define an HTTP/HTTPS proxy:

```
proxy_config:
  https_proxy: <HTTPS_PROXY>
  http_proxy: {} <HTTPS_PROXY>{}
```

See the following example of Flowlink YAML configuration file:

```
proxy_config:
  https_proxy: http://proxy.corporate.com:3128
  http_proxy: http://proxy.corporate.com:3128
```

In the above example, the HTTP/HTTPS proxy is running on FQDN `proxy.corporate.com{{ port: 3128}}`.

Resolved Issue in Flowlink 1.3.0

The following security issue was resolved in this release:

go-lang upgraded to 1.19.11 (E-107998)

The go-lang package was upgraded to 1.19.11 to address CVE-2023-29406.

Illumio Flowlink Release Notes 1.2

Welcome

These release notes describe the enhancements, resolved, and known issues for Illumio Flowlink 1.2.x releases.

Document Last Revised: August 2023

Document ID: 28000-100-1.2.3

Product Version

Flowlink Version: 1.2.3

Compatible PCE Version: 23.3.0 (Standard) and earlier.

Standard versus LTS Releases

For information about Standard versus Long Term Support (LTS) releases, see Versions and Compatibility in the Illumio Support portal (log in required).

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

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

What's New in Flowlink Release 1.2.3

This release provides no new features. Illumio made some changes for security purposes (see Security Information below).

Security Information

go-lang upgraded to 1.19.11 (E-107998)

The go-lang package was upgraded to 1.19.11 to address:

- CVE-2023-29406

What's New in Flowlink Release 1.2.2

This release provides no new features. Illumio made some changes for security purposes (see Security Information below).

Security Information

go-lang upgraded to 1.19.0 (E-106453)

The go-lang package was upgraded to 1.19.10 to address:

- CVE-2023-29405
- CVE-2023-29404
- CVE-2023-29403
- CVE-2023-29402
- CVE-2023-29400
- CVE-2023-24540
- CVE-2023-24539

What's New in Flowlink Release 1.2.1

This release provides no new features. Illumio made some changes for security purposes (see Security Information below).

Security Information

go-lang upgraded to 1.19.8 (E-104330)

go-lang has been upgraded to 1.19.8 to address:

- CVE-2022-41725
- CVE-2022-41724
- CVE-2022-41723
- CVE-2022-41717
- CVE-2023-24538

- CVE-2023-24537
- CVE-2023-24536
- CVE-2023-24534
- CVE-2023-24532

What's New in Flowlink Release 1.2.0

FIPS Compliance

Support for Federal Information Processing Standard Publication (FIPS). FIPS (FIPS PUB) 140-2 is a U.S. government computer security standard used to approve cryptographic modules.

Resolved Issue in Flowlink 1.2.0

Flowlink crashed when pushing NetFlow v9-formatted traffic flow data from Fortinet devices (E-95072)

When attempting to push NetFlow v9-formatted traffic flow data from Fortinet devices, Flowlink stopped processing data and the error message "unexpected EOF" appeared. The issue was caused by incorrect handling of padding bytes in the NetFlow v9 template record. This issue is resolved.

Illumio Flowlink Release Notes 1.1.2

Welcome

These release notes describe the enhancements, resolved, and known issues for the Illumio Flowlink 1.1.x release.

Document Last Revised: April 2021

Document ID: 28000-100-1.1.2

Product Version

Flowlink Version: 1.1.2+H2

Compatible PCE Version: 21.1.0 (Standard), 20.2.0 (Standard), 20.1.0 (Standard), 19.3.*x* (LTS)

Standard versus LTS Releases

For information about Standard versus Long Term Support (LTS) releases, see Versions and Compatibility in the Illumio Support portal (log in required).

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

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

Resolved Issue in Flowlink 1.1.2+H2

- **Flowlink encountered a fatal error** (E-77177)

  Further investigation of this issue uncovered that Flowlink could still encounter the fatal error. While processing reported IPs in sFlow data, Flowlink could experience a race condition due to simultaneous update and read operations of the `reportedIps` table. This issue is resolved. The race condition no longer occurs which caused Flowlink to stop responding and close.

Resolved Issues in Flowlink 1.1.2+H1

- **Flowlink printed error messages when parsing sFlow data** (E-77019)

  When parsing sFlow data, Flowlink continuously wrote the following errors to the flowlink.log, causing the log to fill:

  ```
  2021-03-16T22:21:10.038051-07:00 Error: unexpected EOF
  2021-03-16T22:21:10.038120-07:00 Line: /usr/local/bin/flowlink/sflow_collector.go:742
  2021-03-16T22:21:10.052053-07:00 Error: unexpected EOF
  2021-03-16T22:21:10.052102-07:00 Line: /usr/local/bin/flowlink/sflow_collector.go:750
  2021-03-16T22:21:10.052053-07:00 Error: unexpected EOF
  2021-03-16T22:21:10.052102-07:00 Line: /usr/local/bin/illumio/flowlink/sflow_collector.go:758
  ```

  This issue is resolved. Flowlink no longer continuously writes these errors to the flowlink.log.
- **Flowlink encountered a fatal error** (E-77177)

  While processing reported IPs in sFlow data, Flowlink encountered the following fatal error:

  ```
  fatal error: concurrent map read and map write
  ```

  The fatal error caused Flowlink to stop responding and close. This issue is resolved. Flowlink is no longer affected by this fatal error, which caused it to stop responding and close.

Enhancement in Flowlink 1.1.2

Newly Discovered IP Addresses Displayed

Previously, you did not know which unmanaged workloads you may need to create because you did not know which IP addresses Flowlink was reporting to the PCE. From the Flowlink 1.1.2 release onwards, every time Flowlink sends flow data to the PCE, it reports the newly discovered IP addresses in its log.

Resolved Issue in Flowlink 1.1.2

- **Flowlink was storing zero byte data file and not sending the data** (E-70217)

Flowlink was storing a zero byte data file. It was not sending the data with a response code 403 from the PCE. This issue is resolved and a zero length traffic flow file is not created in the data directory.

Resolved Issue in Flowlink 1.1.1+H2

- **Flowlink time format incompatibility with IPFix on NetScaler** (E-70139)
  Flowlink was incompatible with the time format used by IPFix on NetScaler, which led to traffic processing errors on the PCE. This issue is resolved.

Resolved Issues in Flowlink 1.1.1+H1

- **Compatibility issues with NetFlow V9 and V10/IPFix formats** (E-69173)
  NetFlow V9 and V10/IPFix formats failed to handle timestamps information in the 150-156 fields types correctly and that caused Flowlink to crash . This issue is resolved.
- **Flowlink data not displayed in Explorer** (E-69016)
  Due to incorrect (future) timestamps being assigned, data flows were not being displayed in Explorer. This issue only affected flows generated by NetFlow V5 and V7 and is resolved.

Resolved Issue in Flowlink 1.1.1

- **Unable to install Flowlink on RHEL 6.10** (E-68015)
  Installing the Flowlink RPM on RHEL 6.10 would fail and display an error. This issue is resolved and Flowlink can be successfully installed.

Resolved Issue in Flowlink 1.1.0+H1

- **sFlow traffic not displayed in Illumination** (E-65899)
  The Flowlink application relies on sFlow to provide network traffic flow data for Illumination. Flowlink received sFlow events that it did not handle correctly and caused the traffic handler to crash. This issue is resolved and sFlow traffic is now visible in Illumination.

Illumio NEN Release Notes

Illumio NEN Release Notes 2.7

Product Version

NEN Version 2.7.0

Compatible PCE Versions: 25.3.0 and later

Standard versus LTS Releases

For information about Standard versus Long Term Support (LTS) releases, see Versions and Compatibility in the Illumio Support portal (log in required).

What's New in NEN 2.7.x Releases

This section describes new features introduced in the following NEN releases.

NEN 2.7.0 New Features

- **Top-of-rack Cisco IOS XR series routers**
  This release supports integrating the NEN with Cisco IOS series routers. (Illumio Core PCE 25.3.0 or later, SaaS only.)
- **Support for CIDR block interfaces**
  Allows you to assign CIDR blocks to unmanaged workloads. Each unmanaged workload can represent a subnet, a Layer 3 interface, or a group of workloads instead of just a single workload. (Illumio Core PCE 25.3.0 or later, SaaS only.) See Enhance network security for Top Of Rack routers using Illumio NEN 2.7.0 and Cisco IOS XR.
- **Support for NVIDIA BlueField DPU (with OVS)**
  OVS is a software-based network technology that enhances virtual machine (VM) communication within internal and external networks. It functions as a virtual switch, allowing VMs to communicate within a host and across different hosts. Typically installed on a NIC (for example NVIDIA's BlueField-3 Data Processing Unit; support for other cards may also be available), OVS' software-based approach for packet switching relieves the strain on CPU resources that can impact system performance and network bandwidth. See Integrate the NEN with the NVIDIA BlueField®-3 DPU featuring OVS.
  - **Illumio NEN + OVS Use Case**
    Integrating the NEN with OVS enables visibility and policy enforcement for traffic within and between IT and OT layers, allowing you to visualize all traffic to and from OT systems. Illumio's flexible labeling architecture helps you understand how your assets communicate. The NEN converts your segmentation policies into ACLs that are then installed on the OVS to secure your OT/IT infrastructure.
  - **Streamlined integration through the Illumio API**
    Integrating the NEN with OVS through the PCE web console is straightforward enough, but integration through the PCE API is even easier: enter the IP address and credentials

for the OVS switch (see note below) and the NEN automatically discovers the switch configuration, programs flow monitoring on the switch, discovers and creates workloads in the PCE, and programs the ACLs on the OVS.

> **IMPORTANT**
>
> The user credentials you provide for the OVS must allow access to the `ovs-vsctl` and `ovs-ofctl` commands either through the user login or password-less `sudo` access.

- **Support for NetFlow and IPFIX flow data monitoring protocols**
  These protocols are added to the NEN's existing support for sFlow.
- **Support for IPv6 Access Control Lists (ACLs)**
  Provided in addition to existing support for IPv4.

Resolved Issues in NEN 2.7.0

Issue	Fix description
E-129909	**NEN-discovered load balancer not added to the PCE is now added** During the NEN's VIP discovery process, a discovered F5 VIP was not added to the PCE due to a duplicate database identifier. This issue is resolved.
E-129077	**Incorrect ACL generation now corrected** In an Illumio NEN + Precisely integration, incorrect ACLs were generated for an **all port** (wildcard) rule because the wrong formatting routine was called. This issue is resolved.

Known Issues in NEN 2.7.0

Issue	Description
E-130713	**Extra ACL entry may appear in generated inbound and outbound rules** In some circumstances, when NEN 2.7.0 generates ACLs for a switch integration, it may generate an extra ACL entry at the end of the generated inbound and outbound rules. As the information in the extra entry is already included in the previous ACL entry in the rules, it's merely redundant and has no effect. Illumio plans to correct this in a future NEN release.
E-130118	**Switch model missing when editing the switch configuration in PCE UI** If you try to edit an existing Cisco 9000 switch configuration in the PCE Web Console (**Infrastructure > Switches**), the Model field will be empty (no longer populated with "9000"). As you cannot save the configuration with that field empty, you must either enter 9000 manually or cancel the Edit operation.

Illumio NEN Release Notes 2.6

Product Version

NEN Version: 2.6.40

Compatible PCE Versions: NEN 2.6.40 is compatible with any PCE release.

NEN Version: 2.6.30

Compatible PCE Versions: 21.5.1 – 24.4

Standard versus LTS Releases

For information about Standard versus Long Term Support (LTS) releases, see Versions and Compatibility in the Illumio Support portal (log in required).

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

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

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

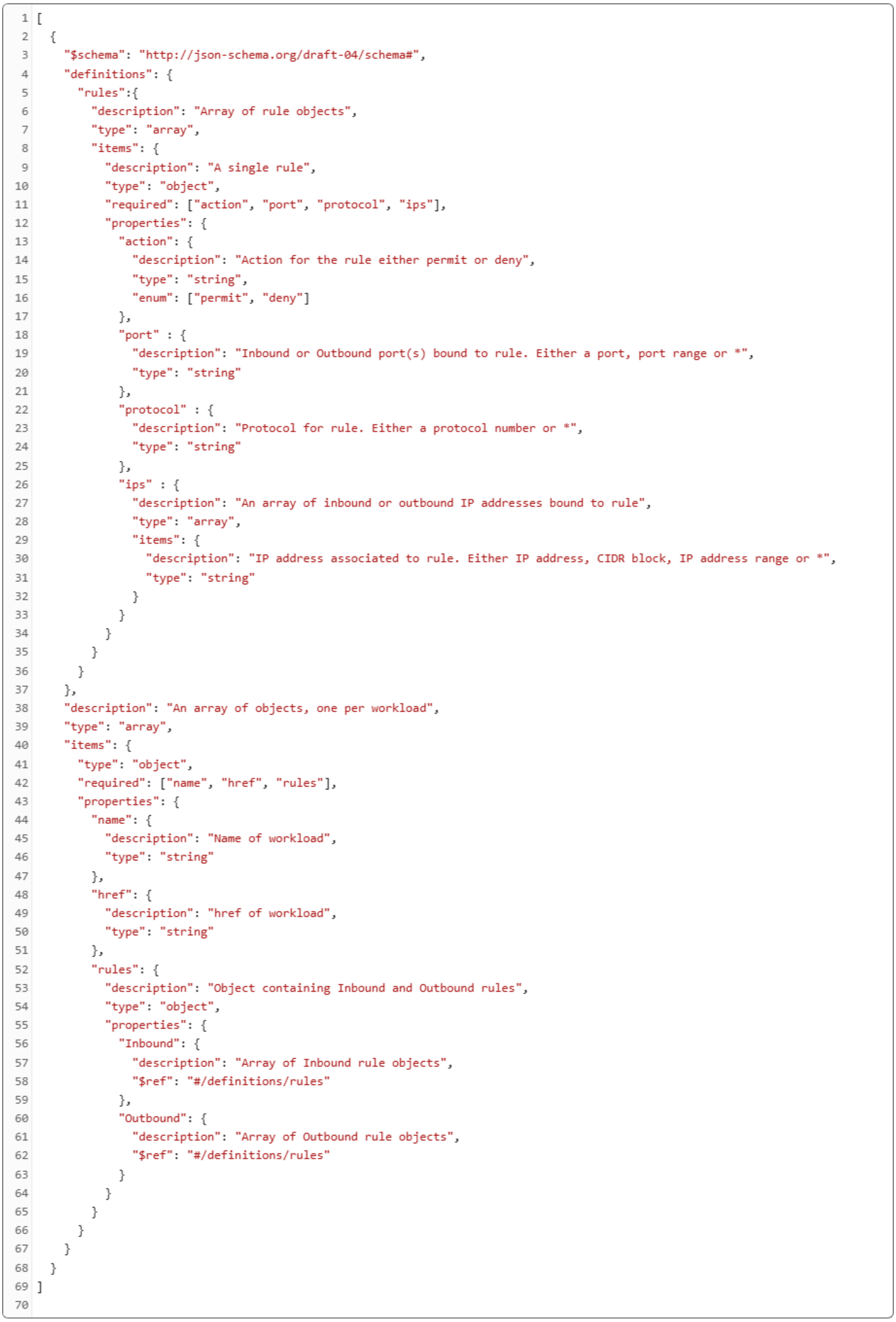
What's New in NEN 2.6.x Releases

This section describes new features introduced in the following NEN releases.

NEN 2.6.40 New Feature

JSON Format Change

Beginning with this release, generic workload JSON files are uploaded as a single, parseable object. This new format allows a program to use the JSON file to apply policy to a device customers want to protect.



```
[
  {
    "$schema": "http://json-schema.org/draft-04/schema#",
    "definitions": {
      "rules":{
        "description": "Array of rule objects",
        "type": "array",
        "items": {
          "description": "A single rule",
          "type": "object",
          "required": ["action", "port", "protocol", "ips"],
          "properties": {
            "action": {
              "description": "Action for the rule either permit or deny",
              "type": "string",
              "enum": ["permit", "deny"]
            },
            "port" : {
              "description": "Inbound or Outbound port(s) bound to rule. Either a port, port range or *",
              "type": "string"
            },
            "protocol" : {
              "description": "Protocol for rule. Either a protocol number or *",
              "type": "string"
            },
            "ips" : {
              "description": "An array of inbound or outbound IP addresses bound to rule",
              "type": "array",
              "items": {
                "description": "IP address associated to rule. Either IP address, CIDR block, IP address range or *",
                "type": "string"
              }
            }
          }
        }
      }
    },
    "description": "An array of objects, one per workload",
    "type": "array",
    "items": {
      "type": "object",
      "required": ["name", "href", "rules"],
      "properties": {
        "name": {
          "description": "Name of workload",
          "type": "string"
        },
        "href": {
          "description": "href of workload",
          "type": "string"
        },
        "rules": {
          "description": "Object containing Inbound and Outbound rules",
          "type": "object",
          "properties": {
            "Inbound": {
              "description": "Array of Inbound rule objects",
              "$ref": "#/definitions/rules"
            },
            "Outbound": {
              "description": "Array of Outbound rule objects",
              "$ref": "#/definitions/rules"
            }
          }
        }
      }
    }
  }
]

```

NEN 2.6.30 New Features

IMPORTANT

Before installing NEN release 2.6.30

Installing this release upgrades the existing database on the NEN to a newer version of the database software. Illumio recommends that you back up the existing NEN database before you install NEN 2.6.30 so that you can revert the installation if necessary.

To back up the existing NEN database, issue the following commands on the NEN primary node:

```
illumio-nen-ctl set-runlevel 1 -svw
```

```
illumio-nen-db-management dump --file <outputfile-name>
```

```
illumio-nen-ctl stop
```

Support for CentOS Stream 9

This release includes support for installing NENs on nodes running CentOS Stream 9.

Switch ACL generation now supports all protocols

With this release, the NEN now recognizes all PCE-supported protocols, ensuring that the NEN can translate switch policy into ACLs when such policy references any PCE-supported protocol.

Support for VMware NSX Advanced Load Balancer AVI 22.1.6

With this release, the NEN now supports VMware NSX Advanced Load Balancer AVI version 22.1.6.

NEN 2.6.20 New Features

Support for RHEL 9

This release includes support for running standalone NENs on Red Hat Enterprise Linux (RHEL) 9 where the version of **openssl-libs** is **3.1 or earlier**.

To determine the openssl-libs version, issue `rpm -qa | grep openssl-libs` .

NEN 2.6.10 New Features

Support for Verifying NEN RPM Signature

Beginning with NEN release 2.6.10, you can verify the signature of the NEN RPM package before installation. This allows you to ensure that the package hasn't been modified since it was signed. For details, see Verify the NEN RPM digital signature.

Support for NEN Proxy Communication

Beginning with NEN release 2.6.10, there is now `runtime_env` support for defining an HTTP/HTTPS proxy for communication between the NEN and the PCE or between the NEN and managed devices (such as Server Load Balancers (SLBs)). You can also specify a list of IP address that are not allowed to communicate via a proxy server. For details, see Configure Proxy Support for NENs.

Ruby updated to version 3.1.2

Ruby was upgraded from version 2.7.1 to 3.1.2.

NEN 2.6.1 New Features

Support for all Citrix ADC (Netscaler) Load Balancer-supported protocols

With this release, the NEN now supports all the protocols that Citrix (NetScaler) 13.1 lists in the **Load Balancing > Virtual Servers > Add > Protocol** menu.

NEN 2.6.0 New Features

Support for Citrix ADC (Netscaler) Load Balancer

With this release, the NEN now supports Citrix ADC (Netscaler) Load Balancers and their associated virtual servers that have only a single IPv4 address.

To add a Citrix Software Load Balancer, see the section *Configure Load Balancers* in the "Load Balancers and Virtual Servers for the NEN" topic.

Support for allowing customers to specify whether disabled VIPs are reported to the PCE

Prior to the release of NEN 2.6.0, if VIP filtering was disabled, all VIPS – including disabled VIPs – were reported to the PCE. You can now disable this reporting using the following new option in the `illumio-nen-ctl slb-enable` command:

```
--disabled-virtual-server-reporting enabled|disabled
```

To ensure backwards compatibility, the default value is `enabled`.

PCE-provided rule IP addresses and ports now combined into CIDR blocks

NENs now combine rule IP addresses and ports provided by the PCE into CIDR blocks and port ranges. This reduces the number of ACLs that NENs need to generate for switches.

Benefits include:

- Fewer ACLs that the NEN generates for switches.
- Fewer ACLs generated for the IBM iSeries integration with Precisely (current limit: 10k ACLs) allows for optimization of IP addresses into ranges larger than can be covered by a single CIDR block.
- Lower demand on switch TCAM where ACLs are stored.

Support for Rocky Linux 8.7

This release includes support for running standalone NENs on Rocky Linux 8.7.

Support for configuring a PCE policy request timeout

Beginning with NEN 2.5.2.A1, you can configure a PCE policy request timeout. This may be needed If your NEN SLB implementation will involve large policy calculations. The timeout ensures that the NEN doesn't wait too long for the PCE to respond to policy requests in scenarios involving large policy calculations.

To configure the timeout, use the following runtime environment variable:

```
pce_policy_request_timeout_minutes
```

- Default value: 10 minutes
- Minimum value: 3 minutes

Resolved Issues in NEN 2.6.40

Issue	Description
E-119690	**NEN setup command failed and 'unknown property' error thrown** After the user configured the `proxy_config` entry in the `runtime_env`, the `illumio-nen-env setup` command failed with an 'unknown property' error.
E-119644	**NEN activation failed and SSL error thrown** When the user activated the NEN using the `proxy_config` settings in the `runtime_env`, the NEN ignored the specified values and failed with an SSL error.
E-122961	**Not all Virtual IPs appeared on the PCE** When using a VMware NSX Advanced Load Balancer greater than version 21.0, the NEN did not honor the "next" field in the vsvip API response and didn't read all entries that define the virtual server IP values. Therefore, it skipped related virtual server entries.

Known Issues in NEN 2.6.40

There are no known issues in this release.

Resolved Issues in NEN 2.6.30

- **ACL Generation Hangs if Switch Policy Includes Multicast Addresses** (E-117247)

If a PCE switch policy includes a multicast address, the NEN became inoperative when trying to generate ACLs for that policy. This issue is fixed.

- **Rules referencing some protocols didn't appear in ACLs** (E-117013)

  PCE policy rules referencing certain protocols didn't appear in NEN-generated switch ACLs. This issue is fixed. With this release, the NEN now supports all PCE-supported protocols.

Known Issues in NEN 2.6.30

There are no known issues in this release.

Resolved Issue in NEN 2.6.20

- **Potential unexpected denial of some traffic flows** (E-114782)

  In NEN releases 2.6.10 and earlier, while in Selective Enforcement the NEN applied ACL deny rules before allow rules, which could inadvertently deny flows that you want to allow. This issue is fixed. Beginning with this release, NENs now apply ACL allow rules before deny rules.

Known Issues in NEN 2.6.20

There are no known issues in this release.

Resolved Issues in NEN 2.6.10

- **In NEN HA pair SLB jobs aborted in some circumstances** (E-112912)

  In a NEN HA pair, after the Secondary Node served temporarily as the Primary Node and then returned to its normal Secondary role, an issue occurred where SLB policy jobs on the Secondary Node were aborted and the database wasn't being reset to allow other SLB policy jobs to run on those SLBs. The issue stems from the timeout behavior being too aggressive. This issue is resolved: the Secondary Node now gracefully returns to its normal role.
- **Unnecessary word prevented some rules from being applied in IBM AS400 integration** (E-111870)

  In an IBM AS400 integration, the ACL files generated by the NEN contained the word `permit` at the end on each rule line, which prevented Precisely from ingesting the rules. This issue is resolved: `permit` is no longer appended at the end of rules.

Known Issues in NEN 2.6.10

There are no known issues in this release.

2.6.10 Security Information

- Upgraded netaddr-1.5.0.gem to 2.0.4 or higher to address CVE-2019-17383
- Upgraded tzinfo-1.2.7.gem to 0.3.61,1.2.10 or higher to address CVE-2022-31163

- Upgraded json-1.8.6.gem to 2.3.0 or higher to address CVE-2020-10663
- Upgraded activesupport-5.2.4.2.gem to 5.2.4.3,6.0.3.1 or higher to address CVE-2020-8165 CVE-2023-22796
- Upgraded addressable-2.7.0.gem to 2.8.0 or higher to address CVE-2021-32740
- Upgraded cURL to v7.87.0 on the Illumio NEN to address CVE-2019-5443 & CVE-2019-3882

Resolved Issues in NEN 2.6.1

- **Timeout issue prevented NEN from updating SLB Policy** (E-107324)

  Due to the shortness of the default connect timeout in the CURL library (5 minutes), the NEN was susceptible to timing out when trying to connect to the PCE. This in turn prevented the NEN from updating policy on the SLB. The issue was resolved by adding the following configurable PCE runtime_env parameter:

  `pce_policy_connect_timeout_minutes`

  - Default value: 10 minutes
  - Minimum value: 3 minutes
- **Handling of SLB empty data response led to erroneous "deletion pending" state** (E-106930)

  An issue caused an F5 SLB to return an empty data response when the NEN queried it for virtual servers, even though managed virtual servers actually existed on the SLB. This occurred at a time when the NEN was programming the SLB. This in turn caused the PCE to put these existing virtual servers in a 'deletion pending' state. After the NEN was restarted, all the virtual servers were discovered and available on the PCE Web Console. This issue is resolved. The NEN will now ignore empty data responses if the SLB has managed virtual servers or is currently being programmed with policy.
- **Route domain length prevented virtual server discovery** (E-106800)

  F5 SLB virtual servers with route domains longer than two digits weren't discovered by the NEN and consequently weren't displayed on the PCE Web Console. This issue is resolved. The NEN now recognizes route domains up to five digits in length.

Known Issues in NEN 2.6.1

There are no known issues in this release.

Resolved Issues in NEN 2.6.0

- **Unable to deactivate the NEN** (E-104053)

  In a certain circumstance (described below), after using the PCE Web Console to remove all the SLBs and associated virtual servers from the NEN, users were unable to deactivate the NEN. Details are as follows:

  1. The user removed SLBs through the PCE Web Console.
  2. As the SLBs no longer existed on the PCE, the NEN couldn't inform the PCE of their state.
  3. This prevented the NEN from removing the SLBs correctly from its database.
  4. This caused the NEN to think it was still managing the SLBs.
  5. This in turn prevented the user from deactivating the NEN.

  Circumstance: At the time the user removed the SLBs through the PCE Web Console, the associated virtual servers were unmanaged.

This issue is resolved. The NEN now recognizes when the SLB is being removed and no longer tries to inform the PCE of changes in SLB state. This allows the NEN to remove SLBs from its database correctly.

- **NEN 2.5.2 Failed to Update SLB Policy** (E-103432)
  An issue caused the NEN policy process to hang while sending an SLB policy request to the PCE. The NEN issue was resolved by adding a configurable PCE policy request timeout to the NEN's code. To configure the optional timeout, use the following runtime environment variable:
  `pce_policy_request_timeout_minutes`
  - Default value: 10 minutes
  - Minimum value: 3 minutes
- **Extraneous API call to the load balancer** (E-96324)
  The NEN made an extraneous GET API call to the AVI Advantage Load Balancer for programming the virtual server. This issue is resolved. The NEN no longer makes this extraneous API call.

Known Issues in NEN 2.6.0

There are no known issues in this release.

Illumio NEN Release Notes 2.5

Product Version

NEN Version: 2.5.2

Compatible PCE Versions: 21.5.1 – 24.4

Standard versus LTS Releases

For information about Standard versus Long Term Support (LTS) releases, see Versions and Compatibility in the Illumio Support portal (log in required).

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

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

Resolved Issue in NEN 2.5.2.A1

NEN 2.5.2 Failed to Update SLB Policy (E-103432)

An issue caused the NEN policy process to hang while sending an SLB policy request to the PCE. The NEN issue was resolved by adding a configurable PCE policy request timeout to the NEN's code. To configure the optional timeout, use the following runtime environment variable:

```
pce_policy_request_timeout_minutes
```

```
pce_policy_request_timeout_minutes
```

- Default value: 10 minutes
- Minimum value: 3 minutes

Known Issues in NEN 2.5.2.A1

There are no known issues in this release.

Resolved Issues in NEN 2.5.2

- **Tamper checking was prevented on the SLB** (E-98697)
  In some circumstances, the PCE may inform the NEN that there is a policy update for an SLB when there isn't actually an update. This may prevent the NEN from running tamper checking on the SLB. To help resolve this condition going forward, if the NEN is told about a non-existent policy update for the SLB and the time for performing a tamper check has lapsed, the NEN will now perform a full policy check for the SLB.
- **Problems caused when deleting a VS before unmanaging it on the PCE** (E-97909)
  Deleting an enforced VS from an SLB without first unmanaging the VS on the PCE interfered with the NEN's attempt to remove policy from the SLB, which prevented the NEN from correctly handling error responses from the SLB. This caused the NEN to:
  - Retry removing policy multiple times, which put a load on the SLB.
  - Run multiple simultaneous SLB programming jobs.

  This issue is resolved. Now, the NEN no longer retries sending APIs requests when 4xx API response codes are returned during the removal of policy from a VS and only runs one programming job per SLB at a time.

Known Issues in NEN 2.5.2

There are no known issues in this release.

Resolved Issue in NEN 2.5.1

Excessive NEN API GET calls to F5 prevented policy programming (E-96989)

When trying to unmanage F5 Virtual Servers, NEN API GET requests to the F5 encountered slower than expected response times, which lead to the following sequence of events:

1. Responses from the F5 timed out.
2. Which in turn caused the NEN to retry its requests repeatedly.
3. Lacking timely F5 responses, the NEN ran multiple simultaneous unmanage jobs for VSs.

4. This caused the NEN to DDOS the F5 with `GET /mgmt/tm/security/firewall/policy?expandSubcollections=true` API calls.
5. **Result:** This overloaded the F5 and caused policy programming to fail due to API timeouts.

This issue is resolved. The NEN now serializes unmanage VS jobs for server load balancers.

Known Issues in NEN 2.5.1

There are no known issues in this release.

Resolved Issues in NEN 2.5.0

- **When processing multi-paged AVI API responses, policy programming failed** (E-95740)
  While processing multiple-paged AVI `networksecuritypolicy` API responses during policy programming, the NEN incorrectly stored the policy ID to associate the policy to its rules. This caused the NEN to point to an invalid memory location, which in turn caused `network_enforcement_policymgr` to crash and policy programming to fail. This issue is resolved.
- **Problem when tamper checking AVI SLBs in multi-page AVI API responses** (E-95546)
  An invalid check of the returned API response occured when the NEN performed tamper checking of multiple-paged AVI `networksecuritypolicy` API responses. This issue could have caused the NEN to miss some Illumio `networksecuritypolicies` . The NEN could then have interpreted the missed policy as policy tampering, triggering a check on the SLB for those missing policies, resulting in no errors found. The issue was resolved by fixing the API response checks to make sure the NEN retrieved all `networksecuritypolicies` from the AVI SLB.
- **Generating switch policy failed in a HA configuration** (E-94344)
  Generating policy by running the `switch policy generate` command on the primary node of an High Availability (HA)-configured NEN (from either the UI or from the CLI) could cause policy generation to fail and return the following error message: *This command can only be run on the node running the primary Network Enforcement Service* . This issue is resolved. The command can now be run on any NEN node – primary or secondary – that is running the `network_enforcement` service.
- **Policy update failed when new Illumio iRules weren't applied correctly** (E-93921)
  An error occurred when trying to create a policy that applied a new Illumio iRule to block an existing non-Illumio iRule. The error prevented policy from being updated. This issue is resolved. New Illumio iRules are now applied before non-Illumio iRules.
- **PCE sent multiple unnecessary policy updates to the NEN** (E-93851)
  Illumio updated the NEN 2.5.0 to address this issue in the PCE. In previous releases, the PCE sent policy updates to the NEN even when the SLB virtual services address list hadn't changed. This issue occurred because pods frequently go down and come back up and that triggered a policy job with "no address list changes" in the PCE. In this release, this issue is resolved for the NEN. The issue will be resolved in the PCE in a future release. In this release, the NEN optimizes the addresses in the address list and stores the SHA of the sorted address list for comparison between policies. The PCE ignores policy updates that don't contain changes in the overall address list by comparing the SHA of new address list with the previous one.
- **F5 AM policy deletion for a deleted VS failed** (E-92008)
  When a NEN tried to delete a policy from an F5 BIG-IP Advanced Firewall Manager (F5 AFM) for a virtual server (VS) that had been deleted, the NEN defaulted to treating the VS

like a non-AS3 managed VS. This resulted in the policy remaining on the F5 AFM. This issue is resolved and the NEN now makes sure (as originally intended) that no artifact of a policy remains on the SLB for the deleted VS.

Known Issues in NEN 2.5.0

There are no known issues in this release.

Illumio NEN Release Notes 2.4

Product Version

NEN Version: 2.4.10

Compatible PCE Versions: 21.5.1 – 24.4

Standard versus LTS Releases

For information about Standard versus Long Term Support (LTS) releases, see Versions and Compatibility in the Illumio Support portal (log in required).

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

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

Resolved Issue in NEN 2.4.10

F5 AFM Policy Deletion for a Deleted VS Failed (E-92008)

When a NEN tried to delete a policy from an F5 BIG-IP Advanced Firewall Manager (F5 AFM) for a virtual server (VS) that had been deleted already, the NEN defaulted to treating the VS like a non-AS3 managed VS. This resulted in the policy remaining on the F5 AFM. This issue is resolved and the NEN now makes sure (as originally intended) that no artifact of a policy remains on the SLB for a deleted VS.

Known Issues in NEN 2.4.10

There are no known issues in this release.

Resolved Issues in NEN 2.4.0

- **VS filtering failed to work correctly on secondary NEN nodes** (E-90850)

  The secondary NEN node didn't perform Virtual Server (VS) filtering even though VS filtering was enabled on the NEN. This meant that VS filtering occurred only on the primary NEN node, which sometimes caused the VS to appear and disappear in the PCE Web Console.
- **For an AVI SLB, NENs reported tenant names incorrectly in the non-admin tenant space** (E-90758)

  When discovering non-admin tenant Virtual Servers on an AVI multi-tenant Server Load Balancer (SLB), the NEN reported Virtual Server names according to their tenant **UUID** instead of their tenant **name** (**Infrastructure > Load Balancers > AVI SLB > Virtual Servers** tab). The NEN also used the tenant UUID in the API header it sent to the AVI SLB when it tried to program the Virtual Server. This prevented policy from being programmed on those Virtual Servers. This issue is resolved; NENs now correctly use the tenant name of discovered Virtual Servers.
- **When adding a switch, the list of supported switches was incomplete for the attached NENs** (E-85844)

  Given two active NENs attached to a PCE, each a different version supporting different switches:

  When adding a new switch through the PCE Web Console, the **Manufacturer** drop down list showed only switches that are supported by the first NEN in the **NEN host name** drop down list. This occurred regardless of which NEN host the user selected. The incomplete list of switches could've prevented users from selecting the precise switch type they were trying to integrate or might have lead them to select a switch type that's not supported by the selected NEN host. This issue is resolved. The **Manufacturer** list now shows the switch(es) supported by whichever host is selected in the **NEN host name** drop down list.
- **Memory leak in NEN process** (E-85114)

  When programming a large number of virtual servers, excessive memory consumption in the `network_enforcement_ndconfig` process could've resulted in an out-of-memory exception in rare circumstances. This issue is resolved.

Known Issues in NEN 2.4.0

There are no known issues in this release.

Limitation in NEN 2.4.0

Enforcement Boundaries not supported for NENs

The PCE doesn't support Enforcement Boundary policies for devices attached to the NEN.

Enforcement Boundaries are a security policy model available in the Core PCE for broadly managing communication across a set of workloads, ports, and/or IP addresses. They allow you to define the end state and then the PCE implements an Enforcement Boundary to create the appropriate native firewall rules. For more, see Enforcement Boundaries .

Illumio CLI Release Notes 1.4.4

What's New in CLI Tool 1.4.4

Here's a summary of the new and enhanced features in this release.

The CLI Tool 1.4.4 is compatible with these versions of the PCE:

- 25.2.10 and earlier versions
-

> **NOTE**
>
> See the Compatibility Matrix for the complete list of compatible versions.
>
> You must log into Illumio Support.

Support for Proxy Communication

The new CLI version includes support for enabling or disabling the proxy for communication between Tenable or Qualis and the PCE CLI tool.

Table 1. New in CLI 1.4.4

Command	Description

`--enable-proxy`	Use this to enable the proxy between tenable and CLI.
	Use this command to enable the proxy:
	`ilo upload_vulnerability_report --source-scanner tenable-sc --format api --severities=3  --enable-proxy -v --debug`
	Use this command if you do not want to enable the proxy:
	`ilo upload_vulnerability_report --source-scanner tenable-sc --format api --severities=3  -v --debug`

Illumio Core PCE CLI Tool Guide 1.4.3

What's New and Changed in Release 1.4.3

Illumio CLI Tool 1.4.3

Illumio CLI Tool 1.4.3 includes an updated version of the CLI Tool software which now includes proxy support.

Illumio provides regular maintenance updates for reported bugs and security issues and adds support for new operating system versions.

For the new commands for authenticated and unauthenticated proxies, `ilo login` and `ilo_use_api_key` , see PCE CLI Tool Guide , "Support for Proxy".

This release of the CLI Tool has no Release Notes issues.

Support for Proxy

Release CLI 1.4.3 includes support for authenticated and unauthenticated proxies.

Type the `ilo login --help` command to see proxy-related options.

Table 2. ilo login --help

Command Options	Description
`-v, --verbose`	Verbose logging mode
`--trace`	Enable API Trace Mode
`--server SERVER_NAME`	Illumio API Access gateway server name
`--login-server LOGIN_SERVER`	Illumio login server name
`--kerberos-spn KERBEROS_SPN`	Illumio Kerberos SPN Kerberos authentication is only applicable to --login-server option
`--proxy-server PROXY_SERVER`	proxy server
`--proxy-port PROXY_PORT`	proxy port
`--proxy-server-username PROXY_SERVER_USERNAME`	proxy server username
`--proxy-server-password PROXY_SERVER_PASSWORD`	proxy server password
`--logout`	Logout
`--username USER`	User Name
`--username USER`	User Name
`--auth-token AUTH_TOKEN`	authorization token

Connecting via a Proxy

The command for connecting via an unauthenticated proxy:

```
 ilo login --server <fqdn:port> --proxy-server <proxy_ip> --proxy-port
<proxy_port> --user-name selfserve@illumio.com
```

An example of connecting via an unauthenticated proxy:

```
 ilo login --server 2x2testvc308.ilabs.io:8443 --proxy-server 10.2.184.62 --
proxy-port 3128 --user-name selfserve@illumio.com
```

An example of connecting via an authenticated proxy:

```
 ilo login --server 2x2testvc308.ilabs.io:8443 --proxy-server
devtest30.ilabs.io --proxy-port 3128 --user-name selfserve@illumio.com --
proxy-server-username proxy_user --proxy-server-password proxy_124
```

After the command is executed, users are prompted to enter the PCE user's password, and then a session will be created in the context of the proxy server.

From this point on, all connections/traffic will use the proxy to send traffic.

Using API Keys and Secrets with a Proxy Server

With the command `ilo use_api_key` , you can use an API Key and a secret with a proxy server:

Table 3. ilo use_api_key --help

Command options	Description
`--key-id`	API Key ID
`--key-secret`	API Key Secret
`--org-id`	Illumio Org ID
`--user-id Illumio`	User ID
`-v, --verbose`	Verbose logging mode
`--trace`	Enable API Trace Mode
`--server SERVER_NAME`	Illumio API Access gateway server name
`--login-server LOGIN_SERVER`	Illumio login server name
`--kerberos-spn KERBEROS_SPN`	proxy server
`--proxy-port PROXY_PORT`	proxy port
`--proxy-server-username PROXY_SERVER_USERNAME`	proxy server username
`--proxy-server-password PROXY_SERVER_PASSWORD`	proxy server password

The command for using an API Key with an unauthenticated proxy:

```
 ilo use_api_key --key-id <key_id> --key-secret <secret> --server
<pce_fqdn> --org-id <orgid> --proxy-server <proxy_server> --proxy-port
<proxy_port>
```

The command for using an API Key with an authenticated proxy:

```
 ilo use_api_key --key-id <key_id> --key-secret <secret> --server
<pce_fqdn> --org-id <orgid> --proxy-server <proxy_server> --proxy-port
<proxy_port>  --proxy-server-username <proxy_username> --proxy-server-
password <proxy_password>
```

After a command is executed, all connections/traffic from this point on will use the proxy.

Illumio Core PCE CLI Tool Guide 1.4.2

Overview of the CLI Tool

This topic provides an overview of the CLI Tool, describes the general syntax of the CLI Tool command, and lists the environment variables you can use to customize the CLI Tool.

IMPORTANT
See the *Illumio Core CLI Tool 1.4.0 Release Notes* and *Illumio Core CLI Tool 1.4.2 Release Notes* and *Illumio CORE CLI Tool 1.4.2* Release Notes in your respective Illumio Core Technical Documentation portal for the updates to the CLI Tool for these releases.

About This Guide

The following sections provide useful information to help you get the most out of this guide.

CLI Tool Versioning

Illumio Core CLI Tool version 1.4.2 is compatible with Illumio Core PCE versions:

PCE 19.3.6-H2 (LTS)

PCE 21.2.4 (LTS)

PCE 21.5.20 (LTS)

PCE 22.1.1 (Standard)

PCE 22.2.0 (Standard)

The CLI Tool version numbering is independent of PCE and VEN's release and version numbering. The CLI Tool works with multiple versions of the PCE and the VEN and does not necessarily need software changes in parallel with releases of the PCE or the VEN.

IMPORTANT
See the *Illumio Core CLI Tool 1.4.0 Release Notes*, *Illumio Core CLI Tool 1.4.1 Release Notes* and *Illumio Core CLI Tool 1.4.2 Release Notes* in your respective Illumio Core Technical Documentation portal for the updates to the CLI Tool for these releases.

How to Use This Guide

This guide includes several major sections:

- Overview of the CLI Tool
- Installation
- The formal syntax of the `ilo` command
- Tutorials for various operations
- Uploading vulnerability data
- Security policy import and export

Before Reading This Guide

Before performing the procedures in this guide, be familiar with the following information:

- The CLI Tool interacts with the PCE; therefore, be familiar with PCE concepts such as core and data nodes, workloads, and traffic. See the PCE Administration Guide.
- The CLI Tool is often used to upload vulnerability data; therefore, understand how vulnerability data is used in the PCE web console. See the "Vulnerability Maps" topic in Visualization Guide.
- The CLI Tool can be used with workload data; therefore, you must understand what workloads are. See the "VEN Architecture and Components" topic in VEN Administration Guide.
- The CLI Tool can be used with security policy rules, rulesets, labels, and similar resources; therefore, be familiar with these concepts. See "The Illumio Policy Model" in Security Policy Guide.

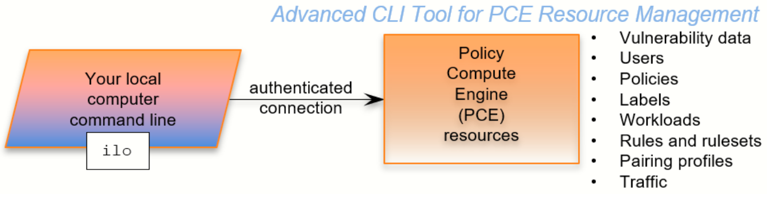
Notational Conventions in This Guide

- Newly introduced terminology is italicized. Example: *activation code* (also known as pairing key)
- Command-line examples are monospace. Example: `illumio-ven-ctl --activate`
- Arguments on command lines are monospace italics. Example: `illumio-ven-ctl --activate activation_code`
- In some examples, the output might be shown across several lines but is actually on one single line.
- Command input or output lines not essential to an example are sometimes omitted, as indicated by three periods in a row. Example:

```
...
some command or command output
...
```

CLI Tool and PCE Resource Management

The Illumio CLI Tool allows you to manage many of your PCE resources directly from your local computer.


Advanced CLI Tool for PCE Resource Management
Your local computer command line
ilo
authenticated connection
Policy Compute Engine (PCE) resources
Vulnerability data
Users
Policies
Labels
Workloads
Rules and rulesets
Pairing profiles
Traffic

Use the CLI Tool to:

- Import vulnerability data for analysis with Illumination.
- Help with tasks such as directly importing workload information to create workloads in bulk.
- Create, view, and manage your organization's security policy rules, rulesets, labels, and other resources.

> ⚠ **CAUTION**
>
> The CLI Tool is a tool that you can use to work with your PCE resources. Test your CLI Tool commands against a non-production system before using them on your production PCEs.

The CLI Tool is named `ilo`. It is a wrapper around the Illumio Core REST API. No knowledge of the REST API is required.

The `ilo` Command

Learn about the general syntax of the CLI Tool command, `ilo`, and how to use the command-line help to get more specific syntax information.

CLI Tool Formal Syntax

The formal syntax for the `ilo` command is:

```
ilo resource_or_specialCommand argument options
```

Where:

- `resource_or_specialCommand` represents either a resource managed by the PCE or a command unrelated to a particular resource.

  A resource is an object that the PCE manages, such as a workload, label, or pairing profile.

  Example resource command on Linux (create a workload):

  ```
  ilo workload create --name FriendlyWorkloadName --hostname
  myWorkload.BigCo.com
  ```

  A special command is a command that is not related to a specific resource. Special commands include `user`, `login`, `use_api_key`, and `node_available`.

  Example special command on Windows (log out of PCE):

  ```
  ilo user logout --id 6
  ```
- The `argument` represents an operation on the resource or special command.
- The `options` are allowed options for the `resource_or_specialCommand`. The specific option depends on the type of resource or special command.

CLI Tool Help

To get a complete list of all the available CLI Tool commands, use the `ilo` command without options. This command displays the high-level syntax of special commands, resources, and their allowable options.

For details about a resource's or special command's arguments, specify the resource's name followed by the argument followed by the `--help` option. For example:

```
ilo workload create --help
```

HTTP Response Codes and Error Messages

Learn about the response codes and error messages that are returned using CLI Tool commands.

REST API HTTP Response Codes

At the end of its output, the `ilo` command displays the REST API HTTP response code from the command. For example, a successful operation shows the following output:

```
...
200, OK
```

Error Messages

For many syntactical or other types of errors, the CLI Tool displays a general message encouraging you to verify your syntax with the CLI Tool help:

```
The ilo command has encountered an error. Check your syntax with either of
the
following commands:

- ilo
- ilo <command> --help
```

In some circumstances, the CLI Tool writes a detailed log of errors:

```
For detailed error messages, see the file:
location-of-local-temp-directory/illumio-cli-error.log
```

Where `location-of-local-temp-directory` is:

- Linux: `/tmp`
- Windows: `C:\Windows\Temp`

Environment Variables

Illumio provides Linux environment variables to allow you to customize the operation of the CLI tool.

Environment Variable	Purpose
`ILO_API_KEY_ID`	API key for non-password-based authentication and cookie-less session with PCE. See "Authenticate with an API Key".
`ILO_API_KEY_SECRET`	API key secret for non-password-based authentication and cookie-less session with PCE. See "Authenticate with an API Key".
`ILO_API_VERSION`	API version to be used to execute CLI commands. Set this to override the default API version. See "Set the Illumio ASP REST API Version." Default: v2. Example: $ export ILO_API_VERSION=v1
`ILO_CA_DIR`	Directory that contains certificates. See "TLS/SSL Certificate for Access to the PCE".
`ILO_CA_FILE`	Absolute path to the certificate file. See "TLS/SSL Certificate for Access to the PCE".
`ILO_DISPLAY_CONFIG`	An absolute path to the display configuration file is to be used with the list command. See "Linux Save Specific Fields to File For Reuse".
`ILO_INSECURE_PASSWORD`	Provide a password for login. If this variable is set, the login password prompt does not appear, and this password is used instead. Do not use in a production system when authentication security is desired.
	Example: `$ export ILO_INSECURE_PASSWORD=myInsecurePassword`
`ILO_KERBEROS_SPN`	Kerberos service principal name (SPN). Specify this variable when using Kerberos authentication.
`ILO_LOGIN_SERVER`	PCE login server FQDN. Use this variable when the login server FQDN is not the same as the PCE FQDN. See "Explicit Log into the PCE".
`ILO_ORG_ID`	Organization identifier for certificate-authenticated session with PCE. Value is always 1. Does not need to be explicitly set The environment variable is set by the system and should not be explicitly set. See "Authentication to PCE with API Key or Explicit Login".
`ILO_PCE_VERSION`	PCE version for the CLI to use. Default: 19.1.0
	Example: `$ export ILO_PCE_VERSION=18.2.5`
`ILO_PREVIEW`	Enable any preview features that are included in this release. To disable preview features, remove this variable from the environment.
`ILO_SERVER`	FQDN of PCE for login and authentication with PCE. See "Authentication to PCE with API Key or Explicit Login".
`TSC_ACCESS_KEY`	These two ENV variables have been added in the release 1.4.2 to set up the Tenable SC API keys, which are used for authentication.
`TSC_SECRET_KEY`	
`TSC_HOST`	The variable that specifies the target host for Tenable
`QAP_HOST`	The variable that specifies the target host for Qualys

Installation and Authentication

Learn how to install the CLI Tool, set up authentication, upgrade the tool, and uninstall it.

Review the prerequisites before you install the PCE CLI Tool.

Prerequisite Checklist

- □ License for vulnerability data upload
- □ Vulnerability data for upload
- □ Functional PCE
- □ Supported operating systems
- □ TLS/SSL certificate for authenticating to the PCE
- □ API version set in configuration
- □ The CLI Tool installation program

Installation Prerequisites

This section details the prerequisites for installing the CLI Tool. Be sure you meet the prerequisites in the checklist.

Prerequisite Checklist

- □ License for vulnerability data upload
- □ Vulnerability data for upload
- □ Functional PCE
- □ Supported operating systems
- □ TLS/SSL certificate for authenticating to the PCE
- □ API version set in configuration
- □ The CLI Tool installation program

License for Vulnerability Data

The Illumio Core Vulnerability Maps license is required to import vulnerability data into the Illumio PCE. For information about obtaining a license, contact Illumio Customer Support. For information on activating the license, see Add the License for Vulnerability Data Upload [95].

Upload Vulnerability Data

When you plan on using the CLI Tool to upload vulnerability data, make sure you have the data to upload in advance. See Supported Vulnerability Data Sources [97] for information.

Install Functional PCE

Because the CLI Tool is for managing resources on your PCE, you must already have installed a fully functional PCE.

Supported Computer Operating Systems

The CLI Tool is supported by the following operating systems:

Linux

- Ubuntu 18.04
- Ubuntu 20.04
- Centos/RHEL 7.9
- Centos/RHEL 8.4

Microsoft Windows

> **NOTE**
> The CLI Tool is not supported on Windows 32-bit CPU architecture. Ensure that you run it on Windows 64-bit CPU architecture.

- Windows 2012 64 bit
- Windows 2016 64 bit
- Windows 10 64 bit

TLS/SSL Certificate for Access to the PCE

You need a TLS/SSL certificate to connect to the PCE securely. Requirements for this certificate are provided in the PCE Installation and Upgrade Guide.

Alternative Trusted Certificate Store

To secure the connection to the PCE, by default, the CLI Tool relies on your computer's trusted certificate store to verify the PCE's TLS certificate. You can specify a different trusted store. When you have installed a self-signed certificate on the PCE, an alternative trusted store might be necessary.

Example: Set envar for alternative trusted certificate store z

```
export ILO_CA_FILE=~/self-signed-cert.pem
```

Set the Illumio Core REST API Version

The CLI Tool uses v2 of the Illumio Core REST API by default.

Install, Upgrade, and Uninstall the CLI Tool

This section explains how to install, upgrade, or uninstall the CLI Tool on Linux or Windows.

Download the Installation Package

Download the CLI Tool installation package from the Tools Catalog page (login required) to a convenient location on your local computer.

Install Linux CLI Tool

The CLI Tool installer for Linux is delivered as an RPM for RedHat/CentOS and DEB for Debian/Ubuntu.

The CLI Tool is installed in the local binaries directory `/usr/local/bin`.

Log into your local Linux computer as a normal user and then use `sudo` to run one of the following commands.

RedHat/CentOS:

```
sudo rpm -ivh /path_to/nameOfCliRpmFile.rpm
```

Debian/Ubuntu:

```
sudo dpkg -i / path_to / nameOfCliDebFile .deb
```

Upgrade Linux CLI Tool

Log into your local Linux computer as a normal user and then use `sudo` to run one of the following commands.

RedHat/CentOS:

```
sudo rpm -Uvh /path_to/nameOfCliRpmFile.rpm
```

Debian/Ubuntu:

```
sudo dpkg -i / path_to / nameOfCliDebFile .deb
```

The same option, `-i`, is used for installation or upgrade.

Uninstall the Linux CLI Tool

Log into your local Linux computer as a normal user and then use `sudo` to run one of the following commands.

RedHat/CentOS:

```
sudo rpm -e nameOfCliRpmFile
```

Debian/Ubuntu:

```
sudo dpkg -r nameOfCliDebFile
```

Install Windows CLI Tool

The CLI Tool installer for Windows is delivered as an **.exe** file.

Log into your local Windows computer as an administrator and start the installation program in the following ways.

- In the Windows GUI, double-click the .exe file.
- In a cmd window, run the .exe.

- In a PowerShell window, run the .exe.

After starting the installation program, follow the leading prompts.

A successful installation ends with the "Installation Successfully Completed" message, and the help text for the CLI Tool is displayed.

Upgrade Windows CLI Tool

The CLI Tool cannot be directly upgraded from an existing CLI Tool installation.

If you have already installed a previous version of the CLI Tool, manually uninstall it using the Windows Control Panel's Add/Remove Programs.

After uninstalling the previous version of the CLI Tool, install the new version of the CLI Tool as described in Install Windows CLI Tool [82].

Uninstall the Windows CLI Tool

Log into your local Windows computer as an administrator, and from the Windows Control Panel, launch Add/Remove Programs.

Select Illumio CLI from the list and click the **Uninstall** button.

Authenticate with the PCE

When using the CLI Tool, you can authenticate to your PCE in the following ways:

- **With an API key and key secret:**
  This is the easiest way. Before you create the API key and secret, you need to log in to authenticate to the PCE. After creating and using the key, you do not have to specify your username and password again.
- **With the explicit command to log in:**
  This always requires a username and password.
  This method also requires you to log out with a user ID displayed at login. The explicit login times out after ten minutes of inactivity, after which you must log in again.

For both authentication mechanisms, on the command line, you always need to specify the FQDN and port of your PCE. The default port for the PCE is 8443. However, your system administrator can change this default. Check with your system administrator to verify the port you need.

Authenticate with an API Key

To authenticate to the PCE with an API key, you must first explicitly log into the PCE, create the API key, and then use the key to authenticate.

1. Authenticate via explicit login:

   ```
   ilo login --server yourPCEfqdn:itsPort
   ```

2. Create the API key:

   ```
   ilo api_key create --name someLabel
   ```

   `someLabel` is an identifier for the key.
3. Use the API key to authenticate:

   ```
   ilo use_api_key --server yourOwnPCEandPort --key-id yourOwnKeyId --org-
   id --key-secret yourOwnKeySecret
   ```

Create an API Key

On Linux, for later ease of use, with the `api_key --create-env-output` option, you can store the API key, API secret, and the PCE server name and port as environment variables in a file that you source in future Linux sessions.

Linux Example

This example creates the API key and secret and stores them as environment variables in a file named `ilo_key_MY_SESSION_KEY`.

```
# ilo api_key create --name MY_SESSION_KEY --create-env-output
# Created file ilo_key_MY_SESSION_KEY with the following contents:

export ILO_API_KEY_ID=14ea453b6f8b4d509
export ILO_API_KEY_SECRET=e1fa1262461ca2859fcf9d91a0546478d10a1bcc4c579d888
a4e1cace71f9787
export ILO_SERVER=myPCE.BigCo.com:8443
export ILO_ORG_ID=1

# To export these variables:
# $ source ilo_key_MY_SESSION_KEY
```

Log Into the PCE

Without an API key, you must explicitly log into the PCE.

For on-premises PCE deployments, the login syntax is the FQDN and port of the PCE:

```
ilo login --server yourPCEfqdn:itsPort
```

For `yourPCEfqdn:itsPort`, do not specify a URL instead of the PCE's FQDN and port. If you do, an error message is displayed.

For the Illumio Secure Cloud customers, the login syntax is:

```
ilo login --server URL_or_bare_PCEfqdn:itsPort --login-server
login.illum.io:443
```

See the explanation above about the argument to the `--server` option.

- After login, the output of the command shows a user ID value. Make a note of this value. You need it when you log out.

- The session with the PCE remains in effect as long as you keep using the CLI Tool. After 10 minutes of inactivity, the session times out, and you must log in again.

Example

In this example, the user ID is 6.

```
C:\Users\marie.curie> ilo login --server myPCE.BigCo.com:8443
Enter User Name: albert.einstein@BigCo.com
Enter Password: Welcome Albert!
User ID = 6
Last Login Time 2018-08-10T-09:58:07.000Z from someIPaddress
Access to Orgs:
Albert: (2)
Roles: [3]
Capabilities: {"basic"=>["read", "write"], "org_user_roles"=>["read",
"write"]}
User Time Zone: America/Los_Angeles
Server Time: 2018-08-12T17:58:07.522Z
Product Version: 16.09.0-1635
Internal Version: 48.0.0-255d6983962db54dc7ca627534b9f24b94429bd5
Fri Aug 6 16:11:50 2018 -0800
Done
```

Log Out of the PCE

To end a session with the PCE, use the following command:

```
ilo user logout --id valueOfUserIdFromLogin
```

Where:

- `valueOfUserIdFromLogin` is the user ID associated with your login. See Log Into the PCE [84] for information.

Example

In this example, the user ID is 6.

```
ilo user logout --id 6
```

CLI Tool Commands for Resources

This section describes how to use the CLI Tool with various PCE resources.

View Workload Rules

You can view a specific workload's rules with the following command:

```
ilo workload rule_view --workload-id UUID
```

Where:

- UUID is the workload's UUID. See About the Workload UUID [90] for information.

In the example below, the workload's UUID is as follows:

```
2ca0715a-b7e3-40e3-ade0-79f2c7adced0
```

Example View Workload Rules

```
ilo workload rule_view --workload-id 2ca0715a-b7e3-40e3-ade0-79f2c7adced0
+------------+-------+
| Attribute  | Value |
+------------+-------+
|  providing |  []   |
+------------+-------+
Using
+---------------------
+---------------------------------------------------------------------------
-------------
| Ports And Protocols |
Rulesets


                            | Href                                        |
Name         |
+---------------------
+---------------------------------------------------------------------------
-------------
| [[-1, -1, nil]]     | [{"href"=>"/api/v2/orgs/28/sec_policy/8/rule_sets/
1909", "name"=>"Default", "secure_connect"=>false,
"peers"=>[{"type"=>"ip_list", "href"=>"/api/v2/orgs/28/sec_policy/8/
ip_lists/188", "name"=>"Any (0.0.0.0/0)",
"ip_ranges"=>[{"from_ip"=>"0.0.0.0/0"}]}]}] | /api/v2/orgs/28/sec_policy/8/
services/1153 | All Services |
+---------------------
+---------------------------------------------------------------------------
-------------
200, OK
```

View Report of Workload Services or Processes

The following command lists all running services or processes on a workload:

```
ilo workload service_reports_latest --workload-id UUID
```

Where:

- UUID is the workload's UUID. See About the Workload UUID [90].

In the example, the workload's UUID is as follows:

```
2ca0715a-b7e3-40e3-ade0-79f2c7adced0
```

Example Workload Service Report

```
ilo workload service_reports_latest --workload-id 2ca0715a-b7e3-40e3-
ade0-79f2c7adced0
+-----------------+---------------------------+
| Attribute       | Value                     |
+-----------------+---------------------------+
|  uptime_seconds |  1491                     |
|  created_at     |  2015-10-20T15:13:00.681Z |
+-----------------+---------------------------+
Open Service Ports
+----------+---------+-------+--------------+-----------------+---------
+------------------+
| Protocol | Address | Port  | Process Name | User
| Package | Win Service Name |
+----------+---------+-------+--------------+-----------------+---------
+------------------+
| udp      | 0.0.0.0 | 5355  | svchost.exe  | NETWORK
SERVICE |         | Dnscache         |
...
| tcp      | 0.0.0.0 | 135   | svchost.exe  | NETWORK
SERVICE |         | RpcSs            |
+----------+---------+-------+--------------+-----------------+---------
+------------------+
200, OK
```

View Host and System Inventory

You can use the following commands to get a quick source of information for troubleshooting or when working with Illumio Customer Support. Using these commands is a quicker and less detailed alternative to running a PCE support report.

To show host inventory for the "local" node:

```
$ illumio-pce-env show host-inventory
```

To show system inventory for the PCE:

```
$ illumio-pce-env show system-inventory
```

To show host inventory for all PCE nodes and also the PCE system inventory:

```
$ illumio-pce-env show inventory
```

Use the `list` Option for Resources

Many resources take the `list` option. This section details some of its uses.

Default List of All Fields

The default `list` command displays all fields associated with the resource:

```
ilo resource list
```

List Only Specific Fields

With the `--field` option, specify the fields to display:

```
ilo resource list --field CSV_list_of_fieldnames
```

For example, to display a list of labels with only the href, key, and value fields, use the `--field` option with those fields as comma-separated arguments.

Example List with Selected Fields

```
ilo label list --fields href,key,value
+---------------------+------+-----------------+
| Href                | Key  | Value           |
+---------------------+------+-----------------+
| /api/v2/2/labels/1  | role | Web             |
| /api/v2/2/labels/2  | role | Database        |
...
| /api/v2/2/labels/48 | loc  | Asia            |
+---------------------+------+-----------------+
```

Nested Resource Fields and Wildcards

Some resources have hierarchical, nested fields. For example, the workload resource includes the following hierarchy for the agent field:

```
agent/config/log_traffic
```

- A field named agent
  - That has a field named `config`
    - That has a field named `log_traffic`

To list nested fields, separate the hierarchy of the field names with a slash to the depth of the desired field.

To see all nested fields of one of a resource's fields, use the asterisk (`*`) wildcard.

Examples

The following example displays all fields under the agent/config field.

Example of All Nested Fields with Wildcard (*)

```
ilo workload list --field agent/config/*
+-------------+------------------+-------------+
| Log Traffic | Visibility Level | Mode        |
+-------------+------------------+-------------+
| false       | flow_summary     | illuminated |
| false       | flow_summary     | idle        |
+-------------+------------------+-------------+
```

You can combine individual field names, nested field names, and the * wildcard.

Example: Combination of Individual fields, Nested fields, and Wildcard

```
ilo workload list --fields href,hostname,agent/config/*,agent/status/
uid,agent/status/status
+----------------------------------------------------------
+-----------------------------+-------------+-------
| Href
| Hostname                    | Log Traffic | Visibility
Level | Mode        | Uid                                  | Status |
+----------------------------------------------------------
+-----------------------------+-------------+-------
| /api/v2/1/workloads/527b8aca-97aa-43b9-82e1-29b17a947cdd
| hrm-web.webscaleone.info    | false       | flow_summary
| illuminated | 0ffd2290-e26a-4ec6-b241-9e2205c0b730 | active |
| /api/v2/1/workloads/4a8743a4-14ee-40d0-9ed2-990fe3f0ffb1
| hrm-db.webscaleone.info     | false       | flow_summary
| illuminated | 145a3cc8-01a8-4a52-97b8-74264ad690e4 | active |
+----------------------------------------------------------
+-----------------------------+-------------+----
...
```

Linux: Save Fields for Reuse

On Linux, to easily reuse specific fields, create a display configuration file in YAML format and set the environment variable `ILO_DISPLAY_CONFIG` to point to that file. You no longer need to specify specific fields on the list command line.

Examples

Configure the workloads list command to display only the href, hostname, all agent configuration fields, and agent version:

Example Command to Save to List Configuration File

```
ilo workload list --fields href,hostname,agent/config/*,agent/status/
agent_version
```

Add the field names to a display configuration file in the following YAML format:

Example YAML Layout of Display Configuration File

```
workload:
  fields:
    - href
    - hostname
  agent:
    config:
      fields:
        - '*'
    status:
      fields:
        - agent_version
```

Set the Linux environment variable `ILO_DISPLAY_CONFIG` to the path to the YAML file:

Example ILO_DISPLAY_CONFIG environment variable

```
$ export ILO_DISPLAY_CONFIG=~/ilo_display/display_config.yaml
```

List of All Workloads

To view all details for all workloads, use the following command:

```
ilo workload list
```

About the Workload UUID

To view an individual workload, you need the workload's identifier, called the UUID, or Universal Unique Identifier.

The UUID is shown in the list of all workloads described in List of All Workloads [90]. The UUID is the last word of the value of the workload's href field, as shown in bold in the following example:

```
/api/v2/orgs/28/workloads/2ca0715a-b7e3-40e3-ade0-79f2c7adced0
```

View Individual Workload

To see the details about an individual workload, use the following command:

```
ilo workload read -workload-id UUID
```

Where:

- UUID is the workload's UUID. See About the Workload UUID [90] for information.

The details of an individual workload are grouped under major headings:

- Workload > Interfaces
- Workload > Labels
- Workload > Services
- Services > Open Service Ports
- Agent > Status

Example List of Individual Workload

```
ilo workload read --workload-id 2ca0715a-b7e3-40e3-ade0-79f2c7adced0
+--------------------------
+----------------------------------------------------------------------------
--------
| Attribute                |
Value

+--------------------------
+----------------------------------------------------------------------------
--------
|  href                    |  /orgs/1/workloads/2ca0715a-b7e3-40e3-
ade0-79f2c7adced0
|  deleted                 |
false

...
Workload -> Interfaces
+------+------------------+------------+-------------------------
+------------+------------+------------------
| Name | Address          | Cidr Block | Default Gateway Address | Link
State | Network Id | Network Detection Mode
+------+------------------+------------+-------------------------
+------------+------------+------------------
| eth0 | 10.0.0.16        | 8          | 10.0.0.1                |
up         | 1           | single_private_brn
...
Workload -> Labels
+-------------------+
| Href              |
+-------------------+
| /orgs/1/labels/37 |
...
Workload -> Services
+-----------------+---------------------------+
| Attribute       | Value                     |
+-----------------+---------------------------+
|  uptime_seconds |  69016553                 |
...
Services -> Open Service Ports
+----------+---------+------+--------------+------+---------
+------------------+
| Protocol | Address | Port | Process Name | User | Package | Win Service
Name |
+----------+---------+------+--------------+------+---------
+------------------+
| 17       | 0.0.0.0 | 123  | ntpd         | root |
|                  |
...
Workload -> Agent
+-----------
+----------------------------------------------------------------------------
-----+
| Attribute |
Value
   |
+-----------
+---------------------------------------------------------------------------
-----+
|  config   |  {"log_traffic"=>true, "visibility_level"=>"flow_summary",
"mode"=>"enforced"} |
|  href     |  /orgs/1/
agents/16                                                                 |
...
Agent -> Status
+------------------------------+----------------------------------------+
| Attribute                    | Value                                  |
+------------------------------+----------------------------------------+
|  uid                         |  db482b06-41c6-4297-a60c-396de13576ad |
|  last_heartbeat_on           |  2016-12-07T04:07:03.756Z              |
...
200, OK
```

List Draft or Active Version of Rulesets

A security policy includes a ruleset, IP lists, label groups, services, and security settings. Before changes to these items take effect, the policy must be provisioned on the managed workload by setting its state to active with the CLI Tool or provisioning it with the PCE web console.

To view a ruleset and provisioning state, use the following command:

```
ilo rule_set list --pversion state
```

Where `state` is one of the following values:

- Draft: Any policy item that has not yet been provisioned.
- Active: All policy items that have been provisioned and are enabled on workloads.

The provisioning states are listed in the Enabled column:

- True: The policy is provisioned.
- Empty: The policy is a draft.

Example Draft Versions of Rulesets

```
ilo rule_set list --pversion draft
+--------------------------------------------------
+-------------------------------+---------+-------------+-----
| Href
| Created By                    | Name    | Description | Enabled |
+--------------------------------------------------
+-------------------------------+---------+-------------+-----
| /api/v2/orgs/28/sec_policy/draft/rule_sets/2387
| {"href"=>"/api/v2/users/74"} | foo1    |             | true
| /api/v2/orgs/28/sec_policy/draft/rule_sets/1909
| {"href"=>"/api/v2/users/0"}  | Default |             | true    ...
200, OK
```

The state of the policy is stored in the agent/status/status field. See Nested Resource Fields and Wildcards [88] for information.

Import and Export Security Policy

You can export and import security policy to and from the PCE using the CLI Tool. Importing and exporting security policy is particularly useful for moving policy from one PCE to another to avoid recreating policy from scratch on the target PCE. For example:

- You can test the policy on a staging PCE and then move it to your production PCE.
- You can move the policy from a proof-of-concept PCE deployment to your production PCE.

Export and Import Policy Objects

You can use the CLI Tool to export or import the following objects in the PCE:

- Labels: `labels`
- Label groups: `label_groups`
- Pairing profiles: `pairing_profiles`
- IP lists: `ip_lists`
- Services: `services`
- Rulesets and rules: `rule_sets`

About Exporting Rules

You can export rules for workloads, virtual services, or virtual servers.

Illumio recommends that you base your security policy rules on labels for flexibility. Do not tie the rules to specific individual workloads, virtual services, or virtual servers.

Virtual servers and virtual services are not exported.

The CLI Tool policy export does not include such references. A warning is displayed on export when you have rules tied to individual workloads, virtual services, or virtual servers. Attempts to import such rules fail, and the reason for the failure is displayed.

Example: Failed Attempt to Export Rules for Workload

```
WARNING: rule /orgs/1/sec_policy/active/rule_sets/3/sec_rules/39
contains non-transferrable providers: workload /orgs/1/workloads/
a51ae67d-472a-44c3-984e-d518a8e95aee
Unable to proceed, please verify input
```

Workflow for Security Policy Export/Import

- Authenticate to the source PCE.
- Export the policy to a file. Syntax summary:

  ```
  ilo sec_policy export --file someExportFilename
  ```
- Authenticate to the target PCE.

- Import the saved policy. Syntax summary:

```
ilo sec_policy import --file someImportFilename
```

Output Options, Format, and Contents

All exported policy is written to standard output. To write to a file, use the `--file` option.

The exported policy is in JSON format.

By default, all supported policy objects are exported. You can export a subset of policy by specifying one or more resource types with the `–resource` option (`labels`, `label_groups`, `pairing_profiles`, `ip_lists`, `services`, or `rule_sets`).

When a subset of policy items is exported (such as only labels), all referenced resources are also exported.

See also About Exporting Rules [93] for information.

Exported Rulesets

With the `-- rule_set` option, you can export multiple rulesets.

By default, only the most recently provisioned, active policy is exported. To export the current draft policy or a previous policy, use the `-–pversion` state option. See List Draft or Active Version of Rulesets [92]for information.

For a single ruleset, make sure the `--pversion` state you specify matches the provisioned state of the ruleset. In the following example, the state is draft:

```
ilo sec_policy export --pversion draft --rule_set /orgs/1/sec_policy/draft/
rule_sets/1
```

Effects of Policy Import

All imported policies are read from standard input unless you import from a file with the `--file` option.

You can import policy files multiple times. Each import affects only a single copy of a resource.

All imported policies are set in the draft provisioned state. After the import, you must explicitly provision the active state.

Non-transferrable policy rules (that is, rules tied to specific workloads, virtual servers, and bound services), the import aborts with a warning. See About Exporting Rules [93] for information.

Policy items already on the target PCE are updated by imported resources whose names match existing resources' names. Services do not have to have the same names. Services match if they have the same set of ports and protocols.

An import does not delete resources. For example, if you export policy from PCE-1 to PCE-2, delete a resource “R” from PCE 1, and then export and import again, resource “R” is still present on PCE 2. You must explicitly delete resource “R” from PCE2.

Upload Vulnerability Data

This section describes how to use the `ilo` commands to upload vulnerability data to the PCE for analysis in Illumination.

After uploading the data, you can use Vulnerability Maps in the PCE web console to gain insights into the exposure of vulnerabilities and attack paths across your applications running in data centers and clouds. See the "Vulnerability Maps" topic in the Visualization Guide for information.

Add the License for Vulnerability Data Upload

An Illumio Core Vulnerability Maps license is required to upload vulnerability data into the Illumio PCE. For information about obtaining the license, contact Illumio Customer Support.

You are provided with a license file named `license.json`. After you have obtained your license key, store it in a secure location.

NOTE

Before adding the license, you must first authenticate to the PCE.

To add the license, you must be the organization owner or a be a user who has owner privileges.

Use the following command to inform the PCE of your valid license:

```
ilo license create --license-file "path_to_license_file/license.json" --
feature "feature_name" [debug [v | verbose] trace]
```

Where:

What	Required?	Description
`"path_to_license_file/license.json"`	Yes	The quoted path to the `license.json` file from Illumio Example: `"~/secretDir/license.json"`
`"feature_name"`	Yes	The quoted string `"vulnerability_maps"`, which specifies the feature name the license enables
`debug`	No	Enable debugging
`v | verbose`	No	For verbose logging
`trace`	No	Enable API trace

Vulnerability Data Upload Process

On upload, the CLI Tool associates a workload's IP addresses with corresponding vulnerabilities identified for that workload.

Using API to Download Vulnerability Data

Starting from the release of CLI 1.4.0, Qualys supports API downloads with some minor differences in options.

For the release CLI 1.4.1, it is suggested that users use an API key instead of a login session while using Qualys API download.

For the release CLI 1.4.2 for Tenable, the most reliable way to provide authentication is through API keys instead of username/password. If customers observe any authentication issues while using Tenable SC API upload, they are advised to use API keys.

There are 2 ENV variables to set up the Tenable SC API keys which are used for authentication:

```
TSC_ACCESS_KEY
```

```
TSC_SECRET_KEY
```

The API connects directly to the cloud instance of Tenable or Qualys and the vulnerability tool then scans new vulnerabilities and downloads them into the PCE.

Users can also set up cron jobs that run in the desired intervals and check the state of the vulnerability scanner.

Qualys and Tenable scanners work in a similar way, using the username and password and similar options.

Automating Vulnerability Imports from Tenable-SC

Users of Illumio vulnerability maps can automate the import of vulnerabilities from tenable-sc using a script.

Illumio CLI supports the API username and password as environment variables or a cmd line switch (such as `--api-password`).

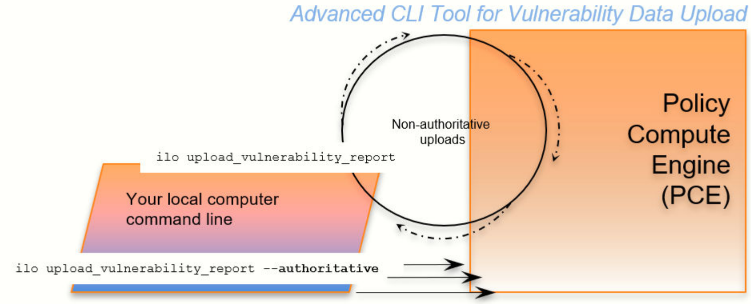
The ILO-CLI tool was updated to add a switch for `--api-user`.

Kinds of Vulnerability Data Uploads

There are two kinds of upload: non-authoritative and authoritative.

- **Non-authoritative:** This is the default. A non-authoritative upload:
  - Appends incoming data to any previously loaded records
  - Accumulates records for the same workloads without regard to duplicates.

  You can repeat the non-authoritative upload as many times as you like until you are satisfied with the results.


Advanced CLI Tool for Vulnerability Data Upload
Non-authoritative uploads
ilo upload_vulnerability_report
Your local computer command line
ilo upload_vulnerability_report --authoritative
Policy Compute Engine (PCE)

- **Authoritative:** You indicate authoritative data with the -authoritative option. An authoritative upload:
  - Overwrites any previously uploaded records for workloads matched to the incoming records.
  - Eliminates duplicate records.
  - Adds new records not previously written by other uploads.

  You can repeat the authoritative upload as many times as you like until you are satisfied with the results.

After either kind of upload, you can examine the uploaded data with the CLI Tool or the PCE web console. See “Vulnerability Maps” in the Visualization Guide for information.

Supported Vulnerability Data Sources

The CLI Tool works with vulnerability data from the following sources.

- Nessus Professional™
- Qualys®
- Tenable Security Center
- Tenable.io
- Rapid7©

NOTE

Before uploading Rapid7 data to the PCE, export the data from Rapid7 to Qualys format with Qualys XML Export.

Vulnerability Data Formats

In the CLI 1.4.0, 1.4.1 and 1.4.2 releases, Illumio supports the following report formats:

- For tenable-io: API, CSV
- For tenable-sc: API, CSV
- For nessus-pro: XML
- For qualys: API, XML

Common Vulnerabilities and Exposures (CVE)

Vulnerabilities are defined by Common Vulnerabilities and Exposures (CVE), with identifiers and descriptive names from the U.S. Department of Homeland Security National Cybersecurity Center.

Vulnerability Scores

Illumio computes a vulnerability score, which measures the vulnerability of your entire organization. The score is displayed by the ilo vulnerability list command for all vulnerabilities or individual vulnerabilities via the vulnerability identifier.

Vulnerability Identifier

An uploaded vulnerability has an identifier, as shown in the example below. The vulnerability identifier is tied to a specific CVE. You use this identifier with `--reference-id` option to examine specific uploaded vulnerabilities. See Example – List Single Uploaded Vulnerability [106] for information.

The following are examples of vulnerability identifiers.

- Nessus Professional: nessus-65432
- Qualys: qualys-23456
- Rapid7: qualys-98765. Because Rapid7 data is first exported from Rapid7 in Qualys format, it is given a Qualys identifier when uploaded to the PCE.

Vulnerabilities for Unmanaged Workloads

You can upload vulnerabilities for unmanaged workloads. However, unmanaged workloads do not have any vulnerability score or associated CVE. This information becomes available if the unmanaged workload is later changed to managed.

Prerequisites for Vulnerability Data Upload

Before uploading vulnerability data, ensure you are ready with the following requirements.

- An Illumio Vulnerability Maps license is required to upload vulnerability data to the PCE. See Add the License for Vulnerability Data Upload [95] for information.
- XML-formatted vulnerability data files from one of the supported sources.
- Authenticated CLI-tool access to the target PCE.
- Authenticated access and necessary permissions in the PCE web console for working with vulnerability maps.

Vulnerability Data Upload CLI Tool Syntax

The key argument and options for uploading vulnerability data are as follows. For readability, this syntax is broken across several lines.

```
ilo upload_vulnerability_report
--input-file path_to_datafile.xml [path_to_datafile.xml]...
--source-scanner [nessus-pro|qualys|tenable-sc|tenable-io]
--format xml
[--authoritative]
[ --api-user ApiServerUserName --api-server SourceApiServer:port ]
```

Where:

What	Required	Description

`--enable-proxy`
NOTE This is available in CLI Tool 1.4.4.
	No	Use this to enable the proxy between tenable and CLI.
		Use this command to enable the proxy:
		`ilo upload_vulnerability_report --source-scanner tenable-sc --format api --severities=3  --enable-proxy -v --debug`
		Use this command if you do not want to enable the proxy:
		`ilo upload_vulnerability_report --source-scanner tenable-sc --format api --severities=3  -v --debug`

`--input-file path_to_data-file.xml [path_to_data-file.xml]...`	Yes	Location of one or more data files to upload. The path to the data file can be either an absolute path or a relative path. If more than one data file is listed (bulk upload), separate the file names with space characters.
`--debug`	No	Enable debugging
`--authoritative`	No	For uploading authoritative vulnerability data. The default command is without the `--authoritative` option. See Kinds of Vulnerability Data Uploads [97] for information.
`--workload-cache FILE`	No	DEBUGGING ONLY: Workload Cache file - use this if available

What	Required	Description
`--source-scanner [nessus-pro| qualys| tenable-sc]`	Yes	Indicates the source of the scan. Note for rapid data: • Vulnerability data from Rapid must have been exported from Rapid in Qualys XML format. • To load the Rapid data, use the 'qualys' argument

`--format`
`REPORT_FORMAT`
	Yes	Report format. Allowed values are:
		`xml`
		• `--source-scanner nessus-pro`
		• `--source-scanner qualys`
		`csv`
		• `--source-scanner tenable-sc`
		• `--source-scanner tenable-io`
		`api`
		• `--source-scanner tenable-sc`
		• `--source-scanner qualys`
		• `--source-scanner nessus-pro`
		See also `--api-server` and `--api-user`.

`--api-server SourceApiServer:port`
`SERVER_FQDN`
	Yes for
	Tenable with `--format api`
		API server FQDN. Allowed formats are `HOST` or `HOST:PORT`

`--api-user ApiServerUserName`	Yes	The user name for authenticating to the SourceApiServer.

What	Required	Description
`USERNAME`	for source API server authentication	You are always prompted to enter your password.
`--api-page-size` `PAGE_SIZE`	Yes for Qualys and Tenable	Appropriate page size if API supports pagination. The default page is 1000.
`--skip-cert-verification`	Yes for Qualys and Tena	Disable certificate verification for API.

What	Required	Description
	ble	
`--on-premise`	Yes only for Tenable io	Tenable IO deployment is on-premise.
`--mitigated`	Yes only for Tenable sc	Tenable SC input is exported from the mitigated vulnerabilities analysis view.
`--scanned-after` `SCANNED_AFTER`	Yes for Qualys	Qualys users can select scan data to process after a specific date, in ISO 8601 format. When the optional **`scanned-after`** option is not provided, the system will pull all the historical vulnerability records from your Qualys account. If your account has historical records, it may take a very long time for the first time. With the **`scanned-after`** option, vulnerability data scanned after a specific date will be extracted and uploaded. Including a particular scanned-after time is recommended if you use Qualys API upload option for the first time.
`--severities` `SEVERITIES`	No	Qualys API users can select vulnerabilities with defined severity levels to include in their reports. Users can filter based on severity and avoid severity levels 1 and 2, which are often very informational and noisy. Example: **`--only-include-severity=3,4,5`** For Windows, be sure to include quotes around the severity levels: Example: **`--only-include-severity="3,4,5"`**

What	Required	Description
		NOTE: This option was added in Release 1.4.1
`-v, --verbose`	No	Verbose logging mode
`--trace`	No	Enable API trace mode.

Using the ILO Command with Windows Systems

Windows systems take up to four options with the ILO command for the vulnerability data upload. Users who choose to use more optional parameters must set `api-server`, `username`, and `password` as the environmental variables to use other options in the command.

Work with Vulnerability Maps in Illumination

See "Vulnerability Maps" in Visualization Guide for information.

Vulnerability Data Examples

Example – Upload Non-Authoritative Vulnerability Data

In this example, the `--source-scanner nessus-pro` option indicates that the data comes from Nessus Professional. On Windows, provide the absolute path to the data file. This Windows example is broken across several lines with the PowerShell line continuation character (`` ` ``).

```
C:\Users\donald.knuth> ilo upload_vulnerability_report `
--input-file C:\Users\donald.knuth\Desktop\vuln_reports\nessus3.xml `
--source-scanner nessus-pro --format xml

Elapsed Time [0.05 (total : 0.05)] - Data parsing is done.
Elapsed Time [1.08 (total : 1.13)] - Got workloads. Workload count: 5.
Elapsed Time [0.0 (total : 1.13)] - Built workload interface mapping. Total
interfaces : 11.
Elapsed Time [4.57 (total : 5.7)] - Imported Vulnerabilities..
Elapsed Time [0.0 (total : 5.7)] - Detected Vulnerabilities are associated
with vulnerability and workload data..
Elapsed Time [0.83 (total : 6.53)] - Report Imported.

Summary:
Processed the report with the following details :
Report meta data =>
Name          : Generic
Report Type   : nessus
Authoritative : false
Scanned IPs   : ["10.1.0.74", "10.1.0.223", "10.1.0.232", "10.1.0.221",
"10.1.0.11", "10.1.0.82", "10.1.0.43", "10.1.0.91", "10.1.0.8",
"10.1.1.250"]

Stats :
   Number of vulnerabilities           => 19
   Number of detected vulnerabilities  => 31

Done.
```

Example – Upload of Rapid7 Vulnerability Data

The syntax for uploading vulnerability data from Rapid7 is identical to the syntax for uploading vulnerability data from Qualys. On Windows, you use the `--format qualys` option and the absolute path to the data file. This Windows example is broken across several lines with the PowerShell line continuation character (`).

Rapid7 data exported in Qualys format.

Before uploading to the PCE, Rapid7 vulnerability data must have been exported in Qualys format from Rapid7 with Qualys XML Export.

```
C:\Users\edward.teller> ilo upload_vulnerability_report `
--input-file C:\Users\edward.teller\Desktop\vuln_reports\rapid7.xml `
--source-scanner qualys --format xml
...
Done.
```

Example – Upload Authoritative Vulnerability Data

In this example, the prompt shows this is an authoritative upload.

To proceed, you must enter the word YES in all capital letters.

```
C:\Users\jrobert.oppenheimer> ilo upload_vulnerability_report --input-file
dataDir/authoritativedata.xml --authoritative --source-scanner qualys --
format xml

Using /home/centos/.rvm/gems/ruby-2.4.1
Authoritative scan overwites the previous entries for all the ips within
this scan. There is no ROLLBACK
Are you sure this is an authoritative scan? (YES | NO)
YES
Elapsed Time [11.86 (total : 11.86] - Data parsing is done.
Elapsed Time [0.27 (total : 12.13] - Got workloads. Workload count: 3.
Elapsed Time [0.0 (total : 12.13] - Built workload interface mapping. Total
interfaces : 6.
Elapsed Time [3.02 (total : 15.15] - Imported Vulnerabilities..
Elapsed Time [0.0 (total : 15.15] - Detected Vulnerabilities are associated
with vulnerability and workload data..
Elapsed Time [0.84 (total : 16.0] - Report Imported.
Summary:
Processed the report with the following stats -
    Number of vulnerabilities           => 14
    Number of detected vulnerabilities  => 48
Done.
```

Example – List Single Uploaded Vulnerability

This example uses a single Qualys vulnerability identifier to show the associated vulnerability. The value passed to the `--reference-id` option is shown as qualys-38173. See Vulnerability Identifier [98] for information.

```
$ ilo vulnerability read --xorg-id=1 --reference-id=qualys-38173
...

| Attribute | Value |
+-------------
+----------------------------------------------------------------+
| href | /orgs/1/vulnerabilities/qualys-38173 |
| name | SSL Certificate - Signature Verification Failed Vulnerability
| score | 39 |
| cve_ids | [] |
| created_at | 2018-11-05T18:16:56.846Z |
...
```

Example – List All Uploaded Vulnerabilities

This example highlights the vulnerability identifier, the CVE identifiers, and the description of the CVE. See Common Vulnerabilities and Exposures (CVE) [98] and Vulnerability Identifier [98] for information. The layout of the output is the same for all supported vulnerability data sources.

Nessus Professional

```
C:\Users\werner.heisenberg> ilo vulnerability list --xorg-id=1
...
| Href | Name | Score | Description | Cve Ids | Created At | Updated At |
Created By | Updated By |
---------------------+--------------------------+-----------------------
+-----------------------+
| /orgs/1/vulnerabilities/nessus-18405 | Microsoft Windows Remote
Desktop Protocol Server Man-in-the-Middle Weakness | 51    |
| ["CVE-2005-1794"]                  | 2018-11-07T03:15:39.410Z |
2018-11-07T03:15:39.410Z | {"href"=>"/users/1"} | {"href"=>"/users/1"} |
...
```

Qualys

```
C:\Users\isaac.newton> ilo vulnerability list --xorg-id=1
...
| Href | Name | Score | Description | Cve Ids | Created At | Updated At |
Created By | Updated By |
---------------------+--------------------------+-----------------------
+-----------------------+
| /orgs/1/vulnerabilities/qualys-38657 | Birthday attacks against
TLS ciphers with 64bit block size vulnerability (Sweet32)
| 69 | | ["CVE-2016-2183"] | 2018-07-27T18:16:57.166Z |
2018-08-08T22:30:32.421Z | {"href"=>"/users/1"} | {"href"=>"/users/16"} |
...
```

Rapid7

Because Rapid7 vulnerability data must be in Qualys format before upload, the output is the same as for Qualys data, including the vulnerability identifier (qualys-38657 in the example above) and CVE. See Common Vulnerabilities and Exposures (CVE) [98] and Vulnerability Identifier [98] for information.

Example – View Vulnerability Report

The Report Type column identifies the source of the scan; in this example, Qualys.

```
C:\Users\gracemurry.hopper> ilo vulnerability_report list --xorg-id=1
...
| Href | Report Type | Name | Created At | Updated At | Num Vulnerabilities
| Created By | Updated By |
+-----------------------------------------------------+-------------
+----------------------+--------------------------+-----------------------
| /orgs/1/vulnerability_reports/scan_1502310096_09344 | qualys  |
NewAuthoritativeScan | 2018-08-08T22:30:34.877Z | 2018-08-08T22:30:34.877Z
| 62 | {"href"=>"/users/16"} | {"href"=>"/users/16"} |
...
```

Example - Upload a Qualys Report Using API

```
upload_vulnerability_report --source-scanner  qualys --format api
--api-server qualysguard.qg3.apps.qualys.com  --api-user um3sg
--scanned-after 2021-09-20
```

CLI Tool Tutorials

This section provides several hands-on exercises that demonstrate step-by-step how to perform common tasks using the CLI Tool.

How to Import Traffic Flow Summaries

Static Illumination provides "moment-in-time" visibility of inter-workload traffic. This visibility is useful to model policies, to look for specious traffic flows, and to ensure that metadata for labels is accurate.

Goal

Load workload and traffic data needed for analysis with static Illumination.

Setup

This tutorial relies on the following data to import.

- 1,000 workloads defined in the file `bulkworkloads-1000.csv`, which has the following columns:

  ```
  hostname,ips,os_type
  10.14.59.8.netstat,10.14.59.8,linux
  10.4.78.178.netstat,10.4.78.178,linux
  10.37.134.179.netstat,10.37.134.179,linux
  ...
  ```
- 1,000,000 traffic flows defined in the CSV file `traffic.clean-1m.csv`, which has the following columns:

  ```
  src_ip,dst_ip,dst_port,proto
  10.40.113.86,10.14.59.8,10050,6
  10.14.59.8,10.8.251.138,8080,6
  10.40.113.124,10.14.59.8,22,6
  ...
  ```

Steps

The workflow is authenticated to the PCE and run two `ilo bulk_upload_csv` commands.

1. Authenticate to the PCE via API key or explicit login.
2. Load the workload data:

   ```
   ilo workload bulk_upload_csv --file bulkworkloads-1000.csv
   ```
3. Load the traffic flow data:

   ```
   ilo traffic bulk_upload_csv --file traffic.clean-1m.csv
   ```

Results

The data from the CSV files are uploaded.

How to Create Kerberos-Authenticated Workloads

This tutorial describes how to create workloads that use Kerberos for authentication. The tutorial makes the following assumptions:

- This tutorial assumes that you already have your Kerberos implementation in place.
- As Kerberos requires, the Kerberos realm name is shown in all capital letters as `MYREALM`.
- VEN environment variables must be set *before* VEN installation. Environment variables for Linux are detailed in the VEN Installation and Upgrade Guide.

Goals

- Create two workloads on Linux that are authenticated by Kerberos.
- Set the workloads' modes to idle and illuminated.

Setup

The key data for using the **`ilo`** command to create these workloads are the name of the Kerberos realm and the Service Principle Name (SPN).

Steps

The workflow is authenticate, run two **`workload create`** commands that set the workloads' modes, set the VEN environment variables, install the VEN, and run two Kerberos **`kinit`** commands to get Kerberos tickets for the workloads.

1. Authenticate to the PCE via API key or explicit login.
2. Create Kerberos-authenticated `myWorkload1` and set its `mode` to `idle`:

   ```
   ilo workload create --hostname myPCE.BigCo.com --name myWorkload1
   --service-principal-name host/myKerberosTicketGrantingServer@MYREALM --
   agent/config/mode idle
   ```

   For information about how the mode is a nested field, see Nested Resource Fields and Wildcards [88].
3. Create Kerberos-authenticated `myWorkload2` and set its `mode` to `illuminated`:

   ```
   ilo workload create --hostname myPCE.BigCo.com --name myWorkload2
   --service-principal-name host/myKerberosTicketGrantingServer@MYREALM --
   agent/config/mode illuminated
   ```
4. Before installation, set VEN environment variables:

   ```
   # Activate on installation
   VEN_INSTALL_ACTION=activate
   # FQDN and port PCE to pair with
   VEN_MANAGEMENT_SERVER=myPCE.BigCo.com:8443
   # Kerberos Service Principal Name
   VEN_KERBEROS_MANAGEMENT_SERVER_SPN=host/myKerberosTicketGrantingServer
   # Path to Kerberos shared object library
   VEN_KERBEROS_LIBRARY_PATH=/usr/lib/libgssapi_krb5.so
   ```
5. Install the Linux VEN:

   ```
   rpm -ivh illumio-ven*.rpm
   ```
6. Run **`kinit`** to get a Kerberos ticket for `myWorkload1`:

   ```
   kinit -k -t /etc/krb5.keytab host/myWorkload1.BigCo.com@MYREALM
   ```

7. Run `kinit` to get a Kerberos ticket for `myWorkload2`:

   ```
   kinit -k -t /etc/krb5.keytab host/myWorkload2.BigCo.com@MYREALM
   ```

Results

The Kerberos-authenticated workloads are created, set in the desired modes, and given a Kerberos ticket.

How to Work with Large Datasets

The `--async` option is for working with large data sets without waiting for the results. The option works like "batch job."

The option can be used with any resource. The workflow is as follows:

1. You issue the desired `ilo` command with the `--async` option, which displays a job ID.
2. You take note of the job ID.
3. Your session is freed up while the job runs.
4. The job creates a data file, which you view with `datafile --read --job-id jobID`.

Goal

Get a report of a large workload data set.

Steps

1. Issue the `--async` request for a workload list. Take note of job ID, which is the final word of the href displayed on the Location line.

   ```
   [kurt.goedel~]$ ilo workload list --async
   Using /home/kurt.goedel/.rvm/gems/ruby-2.2.1
   Location: /orgs/1/jobs/fe8a1c2b-1674-4b83-8967-eb56c4ffa1e3
   202, Accepted
   ```
2. Check to see if the job completed. Use the job ID from the `Location` output in previous command:

   ```
   [sigmund.freud~]$ ilo job read --job-id fe8a1c2b-1674-4b83-8967-
   eb56c4ffa1e
   Using /home/sigmund.freud/.rvm/gems/ruby-2.2.1
   ```
3. Download the resulting data file, specifying the job ID with `-uuid jobID`:

```
[bill.gates ~]$ ilo datafile read --uuid 1e1c1540-8a01-0136-
ec14-02f4d6c1190c
Using /home/ bill.gates /.rvm/gems/ruby-2.2.1
+---------------------------------------------------------+---------
+------+--
... Many lines not shown
+----------------------------+---------------------
+----------------------------+---------------------+
| Href
| Deleted | Name | Description | Hostname
| Service Principal Name | Public Ip
| Distinguished Name | External Data Set | External Data Reference
| Interfaces | Ignored Interface Names | Service Provider | Data Center
| Data Center Zone | Os
Id | Os Detail | Online | Labels  | Services | Agent
 | Created At                  |
Created By           | Updated At                 | Updated By
+---------------------------------------------------------+---------
+------+------------+---------------
... More lines not shown
----------------------------------------------------------+
| /orgs/1/workloads/50ce441e-75ac-4be8-9201-96169545019c
| false   |      |             | 10.14.59.8.netstat
...
... Many lines not shown
...
```

How to Upload Vulnerability Data

This example tutorial shows how to upload vulnerability data to the PCE. For more information, see Upload Vulnerability Data [95]. The source of the vulnerability data in this example comes from Qualys®.

Goal

Upload authoritative vulnerability data for analysis in Illumination.

Steps

1. Do a non-authoritative upload of vulnerability data for examination:

   ```
   ilo upload_vulnerability_report --input-file C:\Users\albert-
   einstein0.xml --source-scanner qualys --format xml
   ```
2. Examine a single uploaded vulnerability record identified by its vulnerability identifier, `qualys-38173`. See Vulnerability Identifier [98] for information.

   ```
   ilo vulnerability read --xorg-id=1 --reference-id=qualys-38173
   ```
3. Do another non-authoritative upload of vulnerability data.

   ```
   ilo upload_vulnerability_report --input-file C:\Users\albert-
   einstein99.xml --source-scanner qualys --format xml
   ```
4. Do an authoritative upload of vulnerability data, overwriting any previously uploaded records and adding any new vulnerability records.

```
ilo upload_vulnerability_report --input-file
C:\Users\albert.einstein_FINAL.xml --authoritative --source-scanner
qualys --format xml
```

Results

The authoritative vulnerability data has been uploaded and is ready for use in Illumination.

Legal Notice

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

Resources

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

Contact Information

- Contact Illumio
- Contact Illumio Legal
- Contact Illumio Documentation