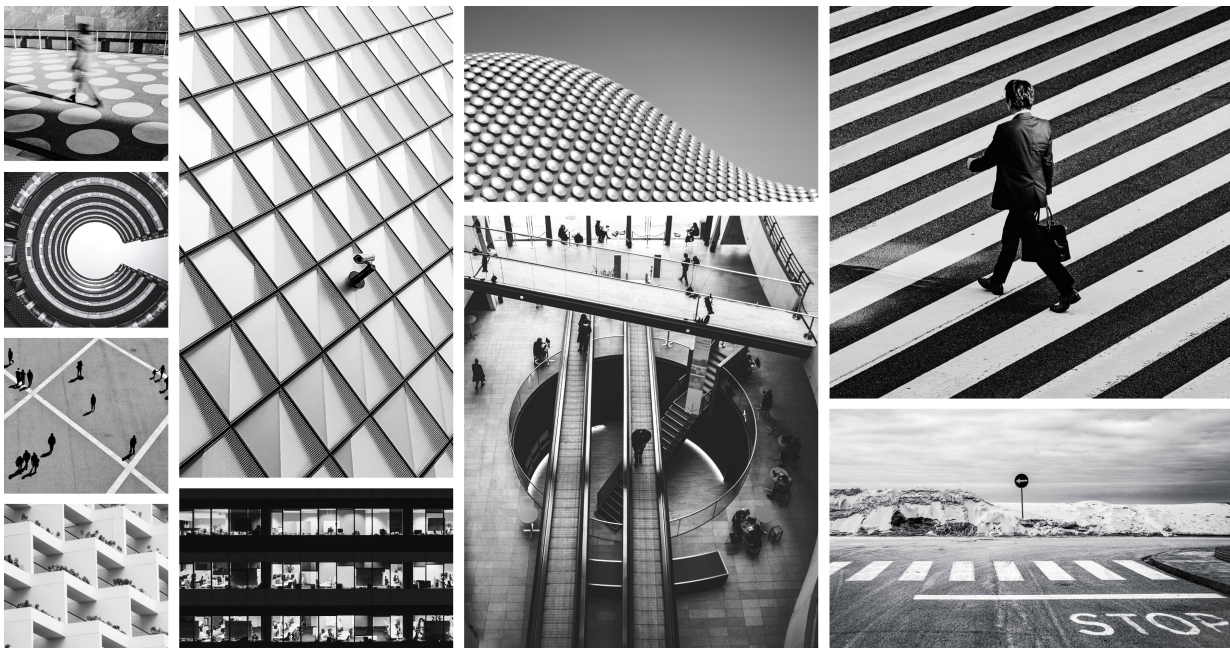




Illumio What's New and Release Notes in 25.4



- [What's New and Changed in 25.4 \[6\]](#)
- [Known Issues in 25.4 \[11\]](#)
- [Resolved Issues in 25.4 \[11\]](#)

Table of Contents

What's New in 25.4	6
Support for safeguarding VENs from accidental unpairing	6
Support for removing inactive VENs	7
Support for more than eight labels for rule search	7
Golden Image Flag	7
New and Changed APIs in 25.4	9
Runtime Parameter to Support More than 8 Labels for Rule Search	9
kubernetes_workload	9
golden_image	10
Release Notes 25.4	11
Known Issues in 25.4	11
Known Issues	11
Resolved Issues in 25.4	11
Resolved Issues	12
LW-VEN Release Notes	14
Resolved Issue in 1.1.20 LW-VEN	14
Resolved Issues in 1.1.10 LW-VEN	14
Resolved Issues in 1.1.0 LW-VEN	15
NEN Release Notes	16
Illumio NEN Release Notes 2.7	16
Product Version	16
What's New in NEN 2.7.x Releases	16
Resolved Issues in NEN 2.7.0	17
Known Issues in NEN 2.7.0	17
Illumio NEN Release Notes 2.6	18
Product Version	18
What's New in NEN 2.6.x Releases	18
Resolved Issues in NEN 2.6.40	22
Known Issues in NEN 2.6.40	22
Resolved Issues in NEN 2.6.30	22
Known Issues in NEN 2.6.30	23
Resolved Issue in NEN 2.6.20	23
Known Issues in NEN 2.6.20	23
Resolved Issues in NEN 2.6.10	23
Known Issues in NEN 2.6.10	23
2.6.10 Security Information	23
Resolved Issues in NEN 2.6.1	24
Known Issues in NEN 2.6.1	24
Resolved Issues in NEN 2.6.0	24
Known Issues in NEN 2.6.0	25
Illumio NEN Release Notes 2.5	25
Product Version	25
Resolved Issue in NEN 2.5.2.A1	25
Known Issues in NEN 2.5.2.A1	26
Resolved Issues in NEN 2.5.2	26
Known Issues in NEN 2.5.2	26
Resolved Issue in NEN 2.5.1	26
Known Issues in NEN 2.5.1	27
Resolved Issues in NEN 2.5.0	27
Known Issues in NEN 2.5.0	28
Illumio NEN Release Notes 2.4	28
Product Version	28
Resolved Issue in NEN 2.4.10	28

Known Issues in NEN 2.4.10	28
Resolved Issues in NEN 2.4.0	29
Known Issues in NEN 2.4.0	29
Limitation in NEN 2.4.0	29
Illumio NEN Release Notes 2.3	30
Legal Notice	30
About This Document	30
Resolved Issues in NEN 2.3.10	31
Known Issues in NEN 2.3.10	32
Resolved Issues in NEN 2.3.0	32
Illumio NEN Release Notes 2.2.0	33
Legal Notice	33
About This Document	33
Resolved Issues in NEN 2.2.0	34
Known Issues in NEN 2.2.0	34
Illumio NEN Release Notes 2.1.1	35
Legal Notice	35
About This Document	35
NEN 2.1.1	36
NEN 2.1.0	36
NEN 2.0.0	41
Illumio NEN Release Notes 2.0.0	41
Legal Notice	41
About This Document	42
New Features in NEN 2.0.0	42
Resolved Issues in NEN 2.0.0	42
Known Issue in NEN 2.0.0	43
Flowlink Release Notes	44
Illumio Flowlink Release Notes for Release 1.4.0	44
Product Version	44
New Features in Illumio Flowlink 1.4.0	44
Resolved and Known Issues in Flowlink 1.4.0	44
Illumio Flowlink Release Notes 1.3.0	45
Product Version	45
New Feature in Flowlink 1.3.0	45
Resolved Issue in Flowlink 1.3.0	46
Illumio Flowlink Release Notes 1.2	46
Welcome	46
Product Version	46
What's New in Flowlink Release 1.2.3	47
What's New in Flowlink Release 1.2.2	47
What's New in Flowlink Release 1.2.1	47
What's New in Flowlink Release 1.2.0	48
Illumio Flowlink Release Notes 1.1.2	48
Welcome	48
Product Version	48
Resolved Issue in Flowlink 1.1.2+H2	49
Resolved Issues in Flowlink 1.1.2+H1	49
Enhancement in Flowlink 1.1.2	49
Resolved Issue in Flowlink 1.1.2	49
Resolved Issue in Flowlink 1.1.1+H2	50
Resolved Issues in Flowlink 1.1.1+H1	50
Resolved Issue in Flowlink 1.1.1	50
Resolved Issue in Flowlink 1.1.0+H1	50
CLI Tool Release Notes	51

Illumio CLI Release Notes 1.4.4	51
What's New in CLI Tool 1.4.4	51
Illumio Core PCE CLI Tool Guide 1.4.3	52
What's New and Changed in Release 1.4.3	52
Support for Proxy	52
Illumio Core PCE CLI Tool Guide 1.4.2	55
Overview of the CLI Tool	55
Installation and Authentication	59
CLI Tool Commands for Resources	65
CLI Tool Tutorials	87

What's New in 25.4

Here's a summary of the new and enhanced features in 25.4.

Support for safeguarding VENs from accidental unpairing

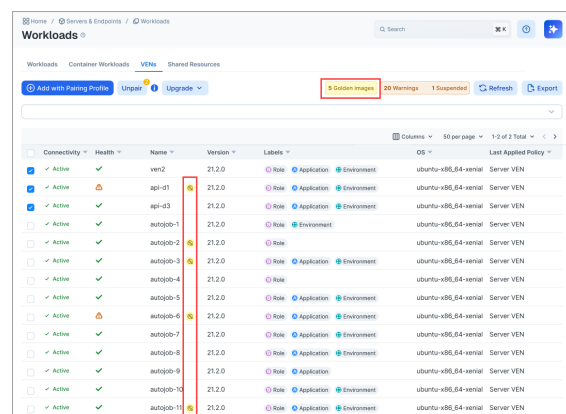
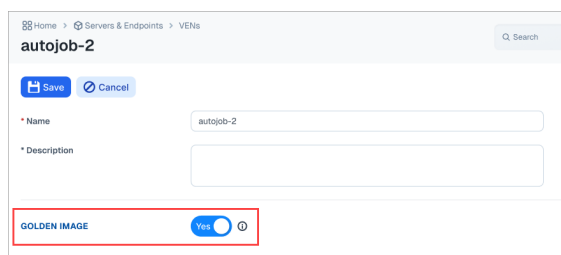
To prevent a VEN from being unpaired or deactivated, designate it as a Golden Image through the VEN Details page in the PCE.

This feature primarily focuses on protecting Golden Image VENs from accidental unpairing or deactivation. In an Illumio context, a Golden Image is a standardized template for cloning multiple pre-configured workloads with a specific operating system, VEN version, labels, enforcement state, security patches, applications, settings, and/or hardware specifications.

After a Golden Image is cloned, it's typically inactive for extended periods, and the associated VEN doesn't send heartbeats to the PCE. This inactivity may make the VEN seem unnecessary and lead some users to unpair or deactivate it mistakenly. This feature is designed to prevent that.

This feature:

- Protects **Golden Image-designated VENs (GIDVs)** from accidental unpairing or deactivation. A GIDV must first be undesignated before it can be unpaired or deactivated.
- Applies a unique icon to GIDVs so they're easily identifiable in the PCE.
- Suppresses events that are generated when a GIDV is cloned. This prevents clogging up the PCE's event stream with events unnecessarily. (However, an event is generated when a VEN is designated as a Golden Image.)
- Allows you to filter the VEN List page for GIDVs.

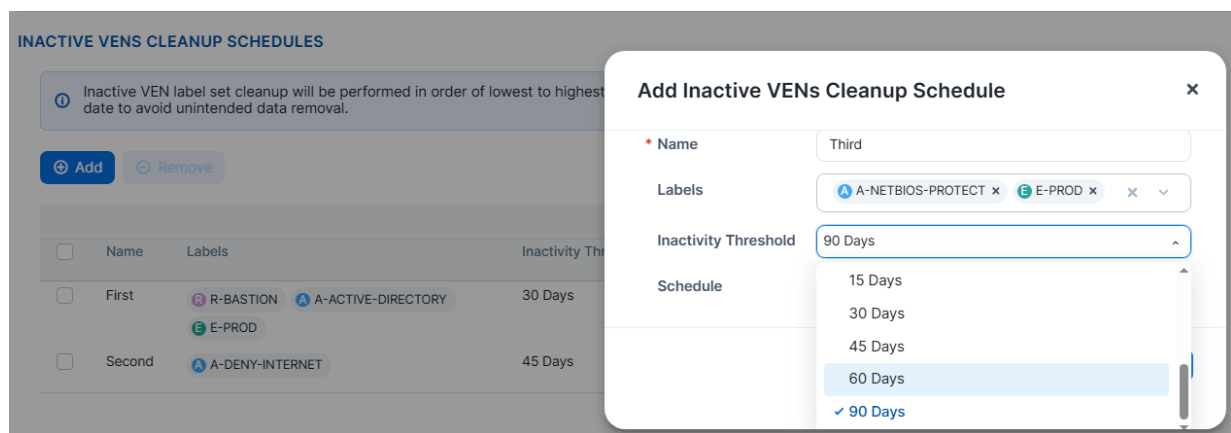


Golden Image toggle on the VEN Details page; Golden Image-designated VENs and quick filter on the VEN List page

Support for removing inactive VENs

Some PCE Segmentation environments may have several inactive VENs that have stopped sending heartbeats to the PCE. This commonly occurs in organizations that deliver Illumio VEN-protected Virtual Desktop Infrastructure (VDI) to end-users who may only use the VDI for a short time. Eventually, the VDI is turned off, abandoned, or destroyed. This can also occur when an organization decommissions a server or when a user's VEN-protected laptop is retired. Although the PCE in these cases can't receive heartbeats from the installed VEN (assuming it still exists), a VEN object representing the actual VEN still resides in the PCE database, unnecessarily consuming VEN licenses and possibly leading to unnecessary costs to the customer.

The Inactive VEN Removal feature removes VEN objects from the PCE that match criteria you define in easily configurable rules.



Support for more than eight labels for rule search

A new parameter has been provided for the runtime environment, as explained in [New and Changed APIs in Release 25.4 \[9\]](#)

Golden Image Flag

The `golden_image` flag is added to prevent accidental deletion of images that are kept offline and used for cloning.

Administrators can create a flag that can be toggled in the PCE to indicate VENs as golden images.

The features of the new flag are:

Toggleable Flag Creation: Administrators can create a toggleable flag in the PCE to mark VENs as golden images.

Filtering Option: Administrators can filter VENs based on whether they have been marked as golden images.

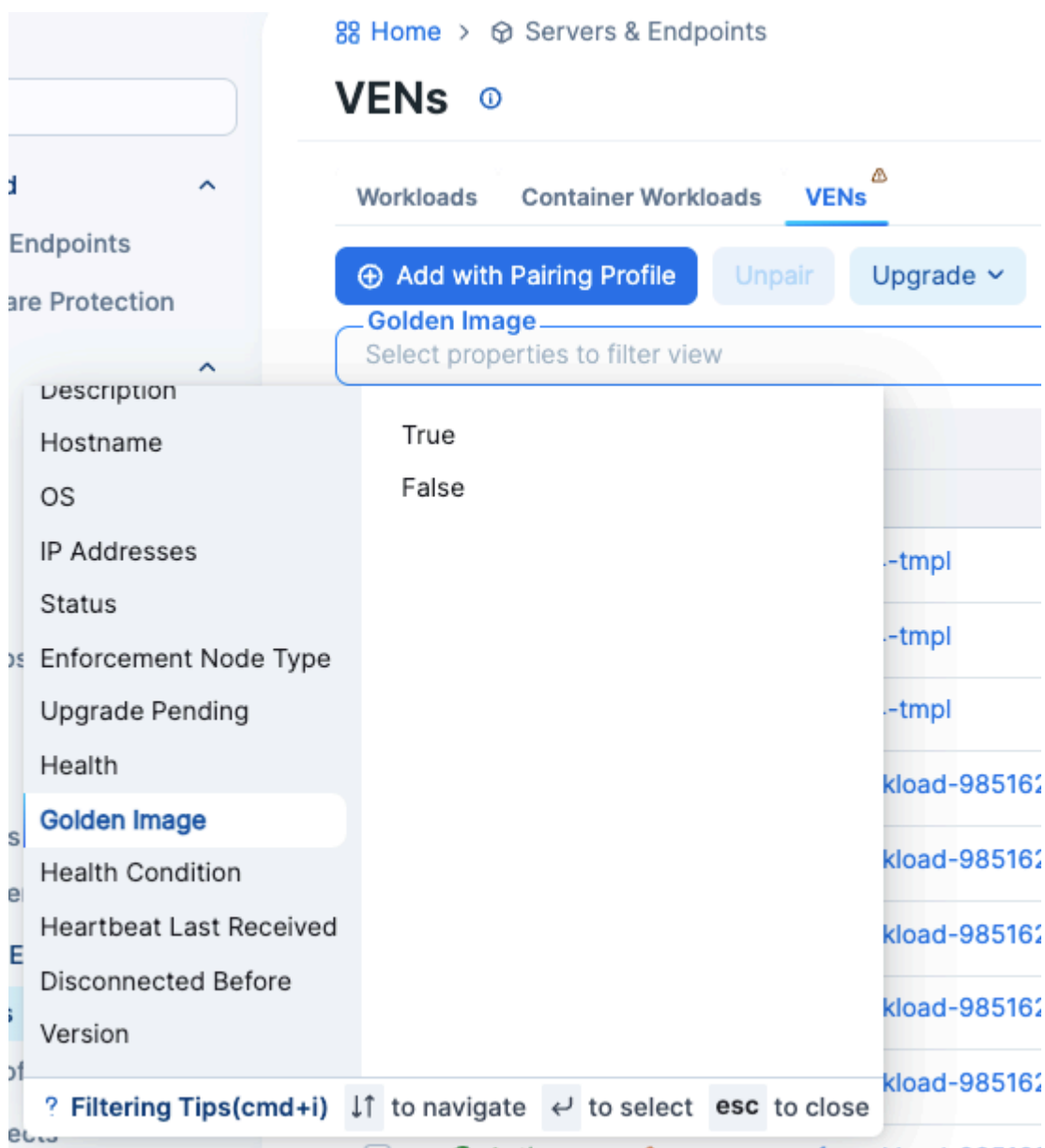
Visibility: Clear visibility of golden image flags in the PCE interface for easy identification.

CSV Export Capability: CSV export that indicates whether the golden image flag is turned on for VENs.

To implement the flag Golden Image in the UI:

1. Go to **Servers & Endpoints > Workloads > VENs**
2. Open the dropdown list "Select properties to filter view" and scroll down to the category "Golden Image". This flag can be set to **True** or **False**.

Figure 1. Golden Image for VENs



3. To see VENs that are golden images, set the flag to **True**. If you select **False**, the VENs that are not golden images will be listed.

New and Changed APIs in 25.4

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

Runtime Parameter to Support More than 8 Labels for Rule Search

A new parameter has been added to the runtime environment:

`max_rule_search_provider_consumer_entities`

By default, the maximum number of rule search provider consumer entities is eight. However, this restriction is not rigid and can be tailored to specific needs.

This parameter constrains the overall count of labels (sum) spanning all dimensions.

```
{
  "properties": {
    "max_rule_search_provider_consumer_entities": {
      "description": "Maximum number of rule search provider consumer
entities",
      "type": "integer",
      "default": 8
    }
  }
}
```

kubernetes_workload

A new property named `kubernetes_workload` was added to the API `sec_policy_rule_coverage_post`

It allows observing coverage of security policy rules for individual Kubernetes Workloads. This change allows the PCE to make a correct policy decision for traffic in draft view.

```
{,
  "kubernetes_workload": {
    "description": "Source kubernetes workload",
    "type": "object",
    "additionalProperties": false,
    "properties": {
      "href": {
        "description": "URI of kubernetes workload",
        "type": "string"
      }
    }
  },
```

golden_image

The property `golden_image` has been added to two APIs:

GET `/api/v2/orgs/:xorg_id/vens/:uuid`

PUT `/api/v2/orgs/:xorg_id/vens/:uuid`

```
{
  "properties": {
    "golden_image": {
      "description": "Indicates whether this VEN is a golden image",
      "type": "boolean",
      "default": false
    }
  }
}
```

The `golden_image` flag is added to prevent accidental deletion of images that are kept offline and used for cloning.

Administrators now have the option to create a toggleable flag in the PCE interface to mark VEN as golden images.

To see the details about using this flag, see [Golden Image Flag \[7\]](#)

Release Notes 25.4

- [Known Issues in 25.4 \[11\]](#)
- [Resolved Issues in 25.4 \[11\]](#)

Known Issues in 25.4

These release notes describe known issues in this release.

Known Issues

Issue	Description	Status
E-130118	<p>Switch model is missing when editing the switch configuration in PCE UI</p> <p>If you 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"). You cannot save the configuration with an field empty. You must enter 9000 manually or cancel the Edit operation.</p>	Unresolved

Resolved Issues in 25.4

These release notes describe the resolved issues in this release.

Resolved Issues

Issue	Fix Description
E-129758	<p>Corrected Mapping Issue between Corporate Network and Internet</p> <p>The issue is resolved. The logic for selecting the initial network with a matching brn and ip_version overlooked introducing the 'Internet' network. This led to the erroneous display of 'Internet' in the traffic user interface even though 'Corporate' was intended.</p>
E-129554	<p>MSP Users Regain Full Access to Policy Generator</p> <p>MSP users encountered an issue accessing the policy generator due to missing configurations for <code>working_org_id</code>, caused by recent updates in cross-org access.</p> <p>This is resolved. MSP users can use the policy generator without any interruptions.</p>
E-128999	<p>Correct Timestamps Reported by VEN</p> <p>An issue arose from incorrect timestamps reported by VEN, leading to inaccurate tables in the PCE database.</p> <p>This problem affected data integrity and consistency, necessitating a review and update of the timestamp handling mechanism to ensure accurate table generation and reliable data reporting.</p>
E-128872	<p>Improved Policy Selection with Autocomplete Feature</p> <p>Previously restricted to selecting from 500 initial policies, users can now choose any policy with the added autocomplete functionality.</p> <p>This update allows dynamic fetching from the full list, enhancing the user experience and streamlining the policy selection process.</p>
E-128723	<p>UI Slowness Issue Resolved in Latest Upgrade</p> <p>The UI slowness issue reported after the 25.2.12 upgrade has been fixed by no longer waiting for the <code>ruleset_overlapping_rule_search</code> API response on the RuleSet detail page.</p> <p>This change improved page load times.</p>
E-128375	<p>Rule Coverage for Traffic in Draft Mode with Kubernetes Workloads</p> <p>Rule Coverage for Traffic in Draft mode was malfunctioning, specifically for Kubernetes Workloads, causing inconsistencies in rule application.</p> <p>This issue is resolved. It ensures that Rule Coverage operates correctly for Traffic in Draft mode within Kubernetes Workloads.</p>
EYE-128267	<p>Traffic Processing and Cluster Naming Fixes</p> <p>Two issues were identified and resolved in this update.</p> <ul style="list-style-type: none"> Reported traffic using the cluster network was mistakenly processed on the PCE with a network belonging to a foreign cluster. The updated container cluster names did not align with the cluster network names. <p>The fixed version ensures correct network matching and an accurate reflection of container cluster names for improved system behavior.</p>

Issue	Fix Description
E-127081	<p>Extended Delay with RuleListEntity Retrieval in /rulesets Endpoint</p> <p>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 delays despite the usual static or org-scoped outcomes.</p> <p>To address this, per-org caching for Exclusion label query results and caching for Service account lookup results were implemented.</p> <p>This optimization decreased redundant database round-trips, enhancing overall latency, throughput, and policy computation during rule list loading.</p>
E-126363	<p>Approximate Scheduled Times for Label Assignment</p> <p>Scheduled times are approximate.</p> <p>Due to system processes, labels may not be assigned to matching workloads precisely when scheduled.</p>
E-114626	<p>Policy Subnet Issue Impairs Endpoint Efficiency</p> <p>The issue with "use workload subnets" causing provider churn and reducing Workload Endpoint efficiency is resolved.</p> <p>The policy now operates optimally, enhancing Endpoint efficiency.</p>

LW-VEN Release Notes

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

Resolved Issue in 1.1.20 LW-VEN

Issue	Description
E-126457	<p>Policy application failure due to unrecognized Local Area Connection header</p> <p>LW-VEN release 1.1.10 failed to apply policy to the customer's firewall because the LW-VEN did not recognize the firewall's Local Area Connection header. The issue occurred because the parsing criteria was too strict. This issue is resolved.</p>

Resolved Issues in 1.1.10 LW-VEN

Issue	Description	Status
E-120840	<p>ICMP rule generation created empty command</p> <p>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.</p>	Resolved
E-120184	<p>Excessive time needed for Windows firewall to apply Illumio rules</p> <p>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.</p>	Resolved
E-120119	<p>Policy conflict lead to policy sync failure and LW-VEN crash</p> <p>A conflict occurred 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.</p>	Resolved

Resolved Issues in 1.1.0 LW-VEN

Issue	Description	Status
E-119190	<p>LW-VEN activation failed on non-UTF-8 legacy Windows workloads</p> <p>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.</p>	Resolved
E-118952	<p>Activate option appeared during "non-fresh" LW-VEN installation</p> <p>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.</p>	Resolved
(E-118764	<p>Users weren't prompted during LW-VEN activation if activation command was run without options</p> <p>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.</p>	Resolved
E-118600	<p>LW-VEN 1.0.1 failed to apply 2008 firewall policy that contained very large port range</p> <p>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.</p>	Resolved

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	<p>NEN-discovered load balancer not added to the PCE is now added</p> <p>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.</p>
E-129077	<p>Incorrect ACL generation now corrected</p> <p>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.</p>

Known Issues in NEN 2.7.0

Issue	Description
E-130713	<p>Extra ACL entry may appear in generated inbound and outbound rules</p> <p>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.</p>
E-130118	<p>Switch model missing when editing the switch configuration in PCE UI</p> <p>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.</p>

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.

```

1 [
2   {
3     "$schema": "http://json-schema.org/draft-04/schema#",
4     "definitions": {
5       "rules": {
6         "description": "Array of rule objects",
7         "type": "array",
8         "items": {
9           "description": "A single rule",
10          "type": "object",
11          "required": ["action", "port", "protocol", "ips"],
12          "properties": {
13            "action": {
14              "description": "Action for the rule either permit or deny",
15              "type": "string",
16              "enum": ["permit", "deny"]
17            },
18            "port": {
19              "description": "Inbound or Outbound port(s) bound to rule. Either a port, port range or *",
20              "type": "string"
21            },
22            "protocol": {
23              "description": "Protocol for rule. Either a protocol number or *",
24              "type": "string"
25            },
26            "ips": {
27              "description": "An array of inbound or outbound IP addresses bound to rule",
28              "type": "array",
29              "items": {
30                "description": "IP address associated to rule. Either IP address, CIDR block, IP address range or *",
31                "type": "string"
32              }
33            }
34          }
35        }
36      },
37      "description": "An array of objects, one per workload",
38      "type": "array",
39      "items": {
40        "type": "object",
41        "required": ["name", "href", "rules"],
42        "properties": {
43          "name": {
44            "description": "Name of workload",
45            "type": "string"
46          },
47          "href": {
48            "description": "href of workload",
49            "type": "string"
50          },
51          "rules": {
52            "description": "Object containing Inbound and Outbound rules",
53            "type": "object",
54            "properties": {
55              "Inbound": {
56                "description": "Array of Inbound rule objects",
57                "$ref": "#/definitions/rules"
58              },
59              "Outbound": {
60                "description": "Array of Outbound rule objects",
61                "$ref": "#/definitions/rules"
62              }
63            }
64          }
65        }
66      }
67    }
68  ]
69 ]
70

```

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-lib** is **3.1 or earlier**.

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

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

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 time-outs.

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 occurred 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 NEN Release Notes 2.3

Legal Notice

Copyright © 2025 Illumio 920 De Guigne Drive, Sunnyvale, CA 94085. All rights reserved.

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](#)

About This Document

These release notes describe the resolved and known issues for the Network Enforcement Node (NEN) 2.3.x releases.

The NEN is the Illumio Core switch and Server Load Balancer (SLB) interface that provides visibility and enforcement on switches and SLBs.

See the NEN Installation and Usage Guide for information.

Product Version

NEN Version: 2.3.10

Compatible PCE Versions: 21.5.10 (LTS Candidate), 21.5.2 (Standard), 21.5.1 (Standard), 21.4.1 (Standard)

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).

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”
- “+e”: Hot Fix release descriptor, for example “+H1”, “+H2”, “+H3”.

What's New In This Release

To learn what's new and changed in this and earlier NEN releases, see *What's New in The Releases* in the latest NEN Installation and Usage Guide.

Resolved Issues in NEN 2.3.10

- **Network enforcement log showed exception when switching from node 2 to the primary node** (E-85609)

On the NEN server, in the `network_enforcement.log`, an error was shown with an exception message when switching from Node 2 to the primary node. This issue is resolved.

- **Deleting VS policy from the F5 might leave AS3 declare in an unstable state** (E-85489)

When deleting a VS policy from the F5, the code ignored the response from the AS3 PATCH command and deleted the policy. However, if the AS3 declare PATCH failed, this left the system in a state where subsequent AS3 PATCH commands failed due to an inconsistency with the AS3 declare and the state of the F5. This caused the policy to not be applied. This issue is resolved.

- **Failed to apply policy to a virtual server after NEN upgrade** (E-85412)

A policy change could generate a 409 error. Policy for the virtual server would then fail to update. This happened because during policy changes, the PCE failed to detect and correct out-of-sync F5 AS3 declarations and virtual server configuration. The NEN would therefore try to create a policy that already existed. This issue is resolved. A subsequent tamper check fixes the policy for the virtual server.

- **NEN logs DEBUG info in prod level** (E-85363)

The NEN was not setting the default log level for the production environment correctly, causing DEBUG information to be logged into the `network_enforcement` log.

This issue is resolved and the NEN now works as expected.

- **Some NEN logs should be at debug level** (E-85341)

Some logs were growing very large (over 5GB) in a very short time because policy information was mistakenly added to the logs.

This issue is resolved so that some parts of that information are added at DEBUG log level instead of INFO log level, while some parts (such as PNports info) are not added to the log.

- **Discovery loop not working on NEN 2.2.0 in production environment** (E-85307)

The discovery job was sometimes not working properly. It did discovery, but for only one SLB. The symptom was increased Ruby gems errors in logs. The issue was caused by an insufficient number of database connections in the pool. The issue is resolved. The default number of connections in the database pool is increased from 4 to 50.

- **NEN health status could display incorrect cluster status** (E-85301)

Running the `illumio-nen-ctl health` command could provide incorrect information for the NEN HA cluster in the Cluster Mode field. For example, the command output could incorrectly display “Standalone (split brain)” when the NEN service on one of the nodes was stopped. The field should have displayed “Standalone (failover).” This issue is resolved and the Cluster Mode field now displays the correct information.

- **NEN - Failover not working if NEN primary freezes** (E-85256)

The NEN primary node could stop logging unexpectedly because of an unforeseen event such as a full disk. The lack of logs made the node appear frozen, but the NEN was still running, so the NEN secondary node did not take over. However, if the disk on the primary node got full and caused the database and node to fail, the primary node would fail, and then failover to the secondary node would occur. This issue is resolved. To address the disk full issue and the lack of logging, if a disk gets 95% or more full, the node will now be stopped, and the NEN fails over to the other node.

- **NEN didn't delete empty iRule and create a new non-empty rule** (E-85211, E-84872)

iRules are a feature within the F5 BIG-IP local traffic management (LTM) system. An iRule can become empty due to tampering. If the NEN detects that an iRule is empty, it's supposed to delete it and then create a new non-empty rule. In this case, the NEN failed to delete the empty iRule and create a new non-empty rule. This issue is resolved.

- **Policy updates and tampering check weren't working** (E-85197)

When the NEN service on the primary node of a NEN HA cluster was stopped, the secondary NEN node did not apply policy updates that the primary node was processing when the primary node failed. This issue is resolved. The secondary NEN node now correctly applies the policy updates from the primary node when it failed over.

Known Issues in NEN 2.3.10

There are no known issues in this release.

Resolved Issues in NEN 2.3.0

NEN 2.3.0 was a Limited Availability (LA) release. However, these issues are also resolved in NEN 2.3.10.

- **PCE and NEN became stuck in a provisioning loop** (E-84712)

Implementing an actor-only policy change caused a provisioning loop in which the PCE continually sent the same policy to the NEN which in turn applied it continually to the F5 SLB. The loop was reported in the `network_enforcement` log and F5 logs. This problem occurred because actor-only policy changes lack a rule version and NENs don't store or acknowledge policy changes that lack a rule version. This issue is fixed. Now, NENs that receive actor-only policy changes use the last-stored rule version from their database, allowing these NENs to acknowledge such policy changes to the PCE.

- **Full policy update not performed on tampered DVSs** (E-84614)

When a NEN was triggered to perform a tampering check on Discovered Virtual Servers (DVS), a full policy update didn't occur and only the address list was updated. This issue is fixed: tampered DVSs now receive a full policy update.

- **Maximum number of auth tokens exceeded** (E-84573) The error *maximum active login tokens* occurred when too many F5 authentication tokens were generated in a 20 minute period. Prior to this fix, a new F5 authentication token was generated whenever a Discovered Virtual Server (DVS) was unprogrammed (for example, when its status changed to unmanaged) or was reprogrammed (for example, when it was identified as tampered). This issue is fixed. NENs now use a single token for these actions.

- **Primary NEN node would hang in some cases** (E-84111)

A logging problem that occurred in the `network_enforcement` service caused the primary NEN node in an HA cluster to hang, which was subsequently not recognized by the secondary NEN node. This issue is fixed. The primary NEN node can now tolerate logging issues

that occur during the `network_enforcement` service and the Secondary NEN node now recognizes when the Primary node hasn't sent its status to the PCE for 3 minutes.

Illumio NEN Release Notes 2.2.0

Legal Notice

Copyright © 2025 Illumio 920 De Guigne Drive, Sunnyvale, CA 94085. All rights reserved.

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](#)

About This Document

These release notes describe the resolved and known issues for the Network Enforcement Node (NEN) 2.2.x releases.

The NEN is the Illumio Core switch and Server Load Balancer (SLB) interface that provides visibility and enforcement on switches and SLBs.

See the NEN Installation and Usage Guide for information.

Product Version

NEN Version: 2.2.0

Compatible PCE Versions: 21.3.0

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).

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”
- “+e”: Hot Fix release descriptor, for example “+H1”, “+H2”, “+H3”.

What's New In This Release

To learn what's new and changed in this and earlier NEN releases, see *What's New in The Releases* in the latest NEN Installation and Usage Guide.

Resolved Issues in NEN 2.2.0

- **Incorrect Cluster Mode shown in NEN Health Report** (E-80063)
In a cluster configured with only one NEN node, the Cluster Mode field in the generated health report showed HA Failover instead of Standalone, as expected. This issue is resolved and the Cluster Mode is now reported as Standalone in this case.
- **NEN didn't specify the VS protocol in rules it programmed on SLBs** (E-79568)
When the NEN programed an SLB Virtual Server with a rule that included an Accept action, the rule specified Any for the protocol instead of the actual protocol of the virtual server. This issue is resolved. Now such rules specify the configured protocol of the virtual server.
- **Some NEN logs were written to the wrong directory** (E-79408)
In standalone NEN implementations, some log files were written to `/var/log/` instead of to `log/illumio-nen`. This issue is resolved. NEN logs are now written to the `log/illumio-nen` directory.
- **NEN logs are now archived** (E-79328)
To prevent the disk on standalone NEN nodes from filling up with unarchived log files, log files older than 1 day are now rotated and archived to the `logs/archive` directory. Log files older than 7 days are deleted.
- **Time-based SLB/VS discovery and tamper checking frequency** (E-78352)
To better secure environments with a large number of load balancers and virtual servers, SLB VS discovery now occurs approximately every 5 minutes instead of according to a loop count. Tamper checking now occurs after policy programming has been completed and then approximately every 5 minutes when policy is not running.
- **AVI load balancer integration in pending state** (E-72540)
After integrating an AVI Vantage load balancer with the Illumio Core NEN, the load balancer remained in the Pending connection state. From the PCE web console menu (**Infrastructure > Load Balancers**) the hourglass icon in the Status column indicated that the load balancer was stuck in the Pending connection state. This issue is resolved. Beginning in this release, AVI Vantage load balancers are supported.

Known Issues in NEN 2.2.0

- **Not possible to apply policy to network switches** (E-81421)
In this release, generating ACLs for a switch policy fails. The file generated by clicking **Generate ACLs (Infrastructure > Switches)** contains an error message instead of ACLs.
- **PCE Listen Only mode does not yet apply to NENs** (E-80376)

Listen Only mode allows you to temporarily stop the PCE from sending policy updates to your VENs. Policy updates resume only after you disable Listen Only mode. This behavior is not yet available for NEN/F5 policy updates, which means that there's a chance that an F5 SLB could receive a stale policy when the PCE is in Listen Only mode.

- **Only TCP and UDP protocols are discoverable by NENs** NENs will only discover SLB Virtual Servers that are programmed with the TCP or UDP protocol.

Illumio NEN Release Notes 2.1.1

Legal Notice

Copyright © 2025 Illumio 920 De Guigne Drive, Sunnyvale, CA 94085. All rights reserved.

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](#)

About This Document

These release notes describe the new features, enhancements, resolved issues, and known issues for the Network Enforcement Node (NEN) 2.x.y releases.

The NEN is the Illumio Core's switch interface, which allows you to get visibility and enforcement on switches. The NEN has both switch and server load balancer capabilities.

See the NEN Installation and Usage Guide for information.

Product Version

NEN Version: 2.1.1

Compatible PCE Versions: 21.2.3, 21.2.4

Illumio NEN 2.1.1 is only compatible with Illumio Core PCE 21.2.3 and 21.2.4. Earlier versions of NEN 2.1.0 are compatible with PCE 21.2.2, 21.2.1, 21.2.0, 21.1.0, 20.2.0.

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).

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 “20.2”
- “.c”: Maintenance release number, for example “.1”
- “-d”: Optional descriptor for pre-release versions, for example “preview2”
- “+e”: Hot Fix release descriptor, for example “+H1”, “+H2”, “+H3”.

What's New In This Release

To learn what's new and changed in this and earlier NEN releases, see *What's New in The Releases* in the latest NEN Installation and Usage Guide.

NEN 2.1.1

Resolved Issues

- **Error occurs after installing the NEN on CentOS 8 or RHEL 8** (E-85689)
Attempting to install a NEN on a CentOS Linux 8 or RHEL 8 node generates the following error after restarting the PCE:

```
failed to create symbolic link 'runtime_environment_extensions.rb': File exists You must now restart the PCE.
```


Workaround: The NEN is not supported on CentOS 8 nor RHEL 8. Don't attempt to install the NEN on a node running those operating systems.
- **NEN didn't delete empty iRule and create a new non-empty rule** (E-84872)
iRules are a feature within the F5 BIG-IP local traffic management (LTM) system. An iRule can become empty due to tampering. If the NEN detects that an iRule is empty, it's supposed to delete it and then create a new non-empty rule. In this case, the NEN failed to delete the empty iRule and create a new non-empty rule. This issue is resolved.
- **NEN didn't discover all tenants and VIPs from AVI load balancer** (E-84047)
When attempting to import Virtual IPs (VIPs) into the PCE from an AVI load balancer, the NEN didn't discover all tenants and VIPs. The issue occurred because the previous NEN version didn't support API paging. This issue is resolved with this release.

NEN 2.1.0

Resolved Issue in NEN 2.1.0+H7

- **PCE upgrade failed** (E-82713)
Upgrading a PCE to release 21.2.3 failed. The failure was reported on data nodes with a NEN installed via the error " PGPASSWORD cannot be included in the command. Please

use `env_hash` to pass it as env variable." This issue is resolved and upgrading to PCE release 21.2.3 now succeeds.

Resolved Issues in NEN 2.1.0+H6

- **Discovering a load balancer's virtual servers could take 30 minutes or longer** (E-80718)
In the previous release, the NEN completed the following operations serially: load balancer policy programming, tamper checking, and virtual server discovery. Programming policy can take up to 30 minutes; therefore, the NEN could take 30 minutes or longer to discover the load balancer's virtual servers (especially, when the NEN performed tamper checking too). This issue is resolved. In this release, the NEN discovers virtual servers in parallel with programming policy and tamper checking. Discovering new virtual servers occurs much faster because the NEN no longer waits for policy programming and tamper checking to finish first.



NOTE

Because Illumio added separate concurrent threads to the NEN for virtual server discovery in this release, the PCE data nodes can experience increased CPU utilization. Please ensure that your PCE has enough capacity to run the NEN in this release.

- **PCE could mark discovered virtual servers as pending deletion** (E-80662, SFDC Issue 15594)
The PCE could mark a discovered virtual server as pending deletion when it wasn't unpaired via the PCE web console or REST API, or removed from the F5. This issue could occur due to the F5 returning unexpected errors during virtual server discovery. When the NEN rediscovered the virtual server in the "Deletion Pending" state, the PCE did not revert that state automatically. This issue is resolved. The PCE no longer marks discovered virtual servers as pending deletion when the NEN encounters unexpected errors from the F5.

Resolved Issues in NEN 2.1.0+H5

- **Badly formed JSON when reprogramming DVS** (E-79438)
JSON was sometimes badly formed due to tampering when DVS was reprogrammed. This issue is resolved.
- **NEN needs to ignore VS when filtering is disabled** (E-78454)
NEN needs to ignore VS when filtering is disabled and when protocol is neither TCP nor UDP.
This issue is resolved and the system is able to discover all VIP's configured on F5.
- **Increase timeouts on NEN requests** (E-78109)
When handling large number of SLBs and VSs it was needed to increase timeouts for NEN requests to PCE for the SLB configuration and policy.
This issue is resolved.
- **Change in policy order or policy action state on AFM does not trigger tampering** (E-77888)
The NEN was not always detecting minor modifications in VS rule values or the change in order of rules within a policy, when programming a policy.
This issue is resolved.

Resolved Issues in NEN 2.1.0+H4

- **SLB reject rules now support logging** (E-77278)

In the previous release, traffic flows for server load balancer (SLB) reject rules ("action": "reject") were not logged by the NEN. In this release, the log option is set ("log": "yes") for SLB reject rules.

- **NEN didn't propagate rule with updated IP list** (E-77038)

When customers provisioned a rule with a new IP list, the virtual server(s) impacted by the rule received the update but it wasn't propagated through the F5 interface to the Advanced Firewall Manager (AFM) cluster. This issue is resolved. Provisioned rules with updates to their IP lists are propagated to the AFM cluster.

- **Script to back up or duplicate the NEN database can now run when the NEN is part of a Supercluster** (E-76952)

In the previous release, you could not run the `illumio-nen-db-management` script on a NEN that was part of a Supercluster deployment because it required running at runlevel 1. In this release, you can run the `illumio-nen-db-management` script on a NEN that is part of a Supercluster deployment, because it no longer requires running at runlevel 1 in a Supercluster deployment.

When the NEN is deployed as a standalone NEN primary node, you still must run the `illumio-nen-db-management` script at runlevel 1.

- **The Policy Manager process stopped responding and closed** (E-76934)

When programming an F5 Application Services 3 (AS3) virtual server that didn't exist, the NEN `PolicyMgr` process stopped responding and closed. This issue could happen when a virtual server was renamed or deleted on a server load balancer (SLB) before the NEN discovered it by polling the SLB. This issue is resolved. When attempting to program a virtual server that doesn't exist, the NEN no longer stops responding or closes and instead writes a message to the log that it cannot program the missing virtual server.

Resolved Issues in NEN 2.1.0+H3

- **NEN failed to detect a policy rule change** (E-75343)

The NEN did not detect when the F5 UI was used to remove and replace the policy for an AS3 managed VIP. It should have detected that the original policy had been modified. This issue is resolved.

- **NEN failed to detect enforcement that had been tampered with** (E-75342)

The NEN did not detect when the F5 UI was used to tamper with the enforcement state of the policy for an F5 AS3 managed VIP, despite a change that should have been detected. This issue is resolved.

- **PCE did not display a list of discovered virtual servers** (E-75088) An API version mismatch between the PCE and the NEN caused the NEN to discover the presence of virtual servers, but the PCE could not display the list of these virtual servers. This issue is resolved.

- **PCE was setting 0.0.0.0/32 even when policy existed** (E-75028)

When the PCE encountered a rule set with both empty and non-empty IP sets, the PCE replaced the empty sets with the 0.0.0.0/32 entry to make sure nothing matched. The non-empty IP sets were still set to the correct IPs, so no traffic was incorrectly blocked; this was only a display issue. The empty IP sets could be caused when there were not currently any workloads with those labels. This issue is resolved. The PCE now only adds the 0.0.0.0/32 entry if the entire combined IP list for the rule is empty.

- **NEN updated AFM Policies even when no changes were triggered from PCE** (E-74952)

This issue arose only for AS3 managed BIG-IP Advanced Firewall Manager (AFM)s. The NEN would repeatedly create and delete AFM policies, even when no changes were triggered from the PCE. This issue happened because the NEN code used the wrong address list name when comparing policy information during AS3 managed VIP tamper checking. This caused tamper checking to fail and the NEN to reprogram the VIP. This issue is resolved. The NEN now uses the correct format of the address list name for AS3 VIPs.

- **AFM policy provisioning failure on the NEN-managed VIPs** (E-74876)

If VIPs were removed from the NEN DB but not from the PCE DB, when a policy for the unknown VIPs was sent to a NEN it stopped programming policy instead of ignoring the VIP.

This issue is resolved. The code was updated to ignore the VIPs it doesn't know about.

- **NEN 2.1.0+HF2 was unable to provision policy to both active/standby devices in an AFM pair** (E-74515)

When the NEN sent a PATCH command to update the F5 AS3 declare, the F5 returned a 202 response code which was not expected by the NEN. This issue was resolved.

- **Incomplete removal of VIPs from SLB** (E-66278)

When you used the server load balancer (SLB) UI to remove all virtual IP addresses (VIPs) from the SLB, the VIPs were still displayed in the PCE UI. This issue is resolved and the VIPs are not displayed in the PCE web console after being removed.

Known Issue in NEN 2.1.0+H3

- **F5 16.x not supported** (E-75470)

Due to a known F5 issue, NEN 2.1.0+H3 does not support F5 16. x.

Resolved Issues in NEN 2.1.0+H2

- **NEN was unable to provision policy to AFM HA pair** (E-73673)

NEN was unable to provision policy written on the PCE to the AFM HA pair even though it could communicate with that pair. This issue was caused due the way in which credential/connectivity information was stored for an HA pair. This issue is resolved and the NEN can successfully provision policies.

- **NEN was not overriding Illumio policies on AFM when tampered manually** (E-72468)

After logging in to AFM, if you selected an AFM policy that was written by Illumio and edited that policy by adding a 'dummy IP', the Illumio ACL did not remove the 'dummy IP'. This issue is resolved and NEN overrides the manually tampered Illumio ACL back to its original state.

Resolved Issues in NEN 2.1.0+H1

- **NEN was not able to program rules to the AVI controller when IPv6 was present** (E-72952)

After setting up AVI integration with the PCE, when you wrote a policy rule that contained virtual servers and managed workloads, the NEN could not program that rule. This issue is resolved and the NEN programs the AVI controller with the correct ACLs.

- **SLB Tampering checks did not detect errors if the address-list generation number contained a zero** (E-72923)

If anything in a rule was changed other than the data group information, then the tampering was not detected if the address list generation value contained a zero. This issue is resolved.

- **AVI load balancer integration would be in a pending state** (E-72704, E-72540)

After integrating an AVI Vantage load balancer with the Illumio Core NEN, the load balancer would remain in the Pending connection state. This issue is resolved.

Resolved Issue in NEN 2.1.0

- **NEN stopped updating the IPset addresses** (E-71650)

A bad heartbeat or config response from the PCE would cause the NEN to clear its config and it never requested the config, because as per the PCE the configured policy had not changed. This issue is resolved and the NEN gets the config as soon as it gets a valid heartbeat response.

New Features and Enhancements in NEN 2.1.0

The NEN 2.1.0 release includes the following features and enhancements:

Policy on Both Members of SLB cluster

The policy can be applied to both the configured members of an SLB cluster:

- You can create and update rules on both members of an AFM/LTM cluster, with up to two load balancers.
- Both members must be in sync before informing the PCE that the policy has been applied.
- If only one SLB is available, the operation will fail. You can retry to apply the policy only after both are in sync.
- If one member fails to program the rules, you should not retry.

Remove Filtering of F5 VIPs

You can view all types of Virtual Services configured on F5 load balancers, by running a specific command during the NEN installation. To disable (enabled, by default) the built-in filter running on the NEN on the leader PCE cluster, run the following command:

```
illumio-nen-ctl slb-enable --virtual-server-filtering disabled
```

Single NEN RPM

From the NEN 2.1.0 release onwards, a single NEN RPM is available, which you can install either on a PCE/NEN system or a standalone system.

If you are upgrading from Illumio Core 19.3.0 or below to Illumio Core 20.2.0 or from Illumio Core 20.1.0 to Illumio Core 20.2.0 and you have the NEN installed on a PCE, run the following command before installing the PCE RPMs and NEN RPM:

```
rpm -e illumio-pce-nen --noscript
```

Manage NEN on Supercluster Leader

For Supercluster deployment, you can install the NEN only on the 2 database nodes of the Supercluster leader. You cannot install on a standalone system or on non-Supercluster leader nodes.

Scale

The NEN 2.1.0 release supports up to 500 VIPs and up to 15 SLBs.

Known Issue in NEN 2.1.0

- **AVI load balancer integration in pending state** (E-72540)

After integrating an AVI Vantage load balancer with the Illumio Core NEN, the load balancer remains in the Pending connection state. From the PCE web console menu, choose **Infrastructure > Load Balancers**. The Server Load Balancer page appears. The hourglass icon in the Status column indicates that the load balancer is in the Pending connection state. AVI Vantage load balancers are not supported in this release.

NEN 2.0.0

Resolved Issues in NEN 2.0.0

- **SLB HA didn't work as expected** (E-66731)

If the first configured Server Load Balancer (SLB) device of high availability (HA) pair became unavailable or unreachable, the second SLB device was not used and the NEN was unable to program rules for the managed DVS. This issue is resolved.

- **Unable to pair AFMs in HA mode with the PCE** (E-66640)

Pairing F5 Advanced Firewall Managers (AFM) individually with the PCE would work. However, pairing them in the HA mode would fail due to the request to the PCE getting timed out. This issue is resolved and you can pair AFMs with the PCE in the HA mode.

- **NEN able to re-pair with the existing PCE** (E-61765)

If a standalone NEN was lost due to machine failure, you could not re-pair a new NEN with the same hostname to the existing PCE. This issue is resolved and you can re-pair a new NEN.

New Feature in NEN 2.0.0

The NEN 2.0.0 release includes support for AVI Vantage load balancers.

Known Issue in NEN 2.0.0

- **Incomplete removal of VIPs from SLB** (E-66278)

If the SLB UI is used to remove all virtual IP addresses (VIPs) from a PCE-monitored SLB, the VIPs are still displayed in the PCE UI and policy change requests may be generated for those VIPs.

Illumio NEN Release Notes 2.0.0

Legal Notice

Copyright © 2025 Illumio 920 De Guigne Drive, Sunnyvale, CA 94085. All rights reserved.

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](#)

About This Document

These release notes describe the new features, enhancements, resolved issues, and known issues for the Network Enforcement Node (NEN) 2.x.y releases.

The NEN is the Illumio Core's switch interface, which allows you to get visibility and enforcement on switches. The NEN has both switch and server load balancer capabilities.

See the NEN Installation and Usage Guide for information.

Product Version

Current PCE Version: 20.1.0+H4 (Standard Release)

Current VEN Version: 20.1.0 (Standard Release)

Current NEN Version: 2.0.0

Standard versus LTS Releases

20.1.0-PCE is a standard release. Illumio will designate a version of 20.x.y as a Long Term Support (LTS) release. Do not upgrade to 20.1.0 if your environment requires an LTS release.

For information on Illumio software support for Standard and LTS releases, see [Illumio Versions and Compatibility](#).

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 "20.1"
- ".c": Maintenance release number, for example ".1"
- "-d": Optional descriptor for pre-release versions, for example "preview2"
- "+e": Hot Fix release descriptor, for example "+H1", "+H2", "+H3".

New Features in NEN 2.0.0

The NEN 2.0.0 release includes support for AVI Vantage load balancers.

Resolved Issues in NEN 2.0.0

- **SLB HA did not work as expected** (E-66731)

If the first configured Server Load Balancer (SLB) device of an high availability (HA) pair became unavailable or unreachable, the second SLB device was not used and the NEN was unable to program rules for the managed DVS. This issue is resolved.

- **Unable to pair AFMs in HA mode with the PCE** (E-66640)

Pairing F5 Advanced Firewall Managers (AFM) individually with the PCE would work. However, pairing them in the HA mode would fail due to request to the PCE getting timed-out. This issue is resolved and you can pair AFMs with the PCE in the HA mode.

- **NEN unable to re-pair with the existing PCE** (E-61765)

If a standalone NEN was lost due to machine failure, you could not re-pair a new NEN with the same hostname to the existing PCE. This issue is resolved and you can re-pair a new NEN.

Known Issue in NEN 2.0.0

- **Incomplete removal of VIPs from SLB** (E-66278)

If the SLB UI is used to remove all virtual IP addresses (VIPs) from a PCE-monitored SLB, the VIPs are still displayed in the PCE UI and policy change requests may be generated for those VIPs.

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.

CLI Tool Release Notes

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

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
<code>-v, --verbose</code>	Verbose logging mode
<code>--trace</code>	Enable API Trace Mode
<code>--server SERVER_NAME</code>	Illumio API Access gateway server name
<code>--login-server LOGIN_SERVER</code>	Illumio login server name
<code>--kerberos-spn KERBEROS_SPN</code>	Illumio Kerberos SPN Kerberos authentication is only applicable to --login-server option
<code>--proxy-server PROXY_SERVER</code>	proxy server
<code>--proxy-port PROXY_PORT</code>	proxy port
<code>--proxy-server-username PROXY_SERVER_USERNAME</code>	proxy server username
<code>--proxy-server-password PROXY_SERVER_PASSWORD</code>	proxy server password
<code>--logout</code>	Logout
<code>--username USER</code>	User Name
<code>--username USER</code>	User Name
<code>--auth-token AUTH_TOKEN</code>	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
<code>--key-id</code>	API Key ID
<code>--key-secret</code>	API Key Secret
<code>--org-id</code>	Illumio Org ID
<code>--user-id Illumio</code>	User ID
<code>-v, --verbose</code>	Verbose logging mode
<code>--trace</code>	Enable API Trace Mode
<code>--server SERVER_NAME</code>	Illumio API Access gateway server name
<code>--login-server LOGIN_SERVER</code>	Illumio login server name
<code>--kerberos-spn KERBEROS_SPN</code>	proxy server
<code>--proxy-port PROXY_PORT</code>	proxy port
<code>--proxy-server-username PROXY_SERVER_USERNAME</code>	proxy server username
<code>--proxy-server-password PROXY_SERVER_PASSWORD</code>	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 Segmentation for Data Centers CLI Tool version 1.4.2 is compatible with Illumio Segmentation for Data Centers 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.

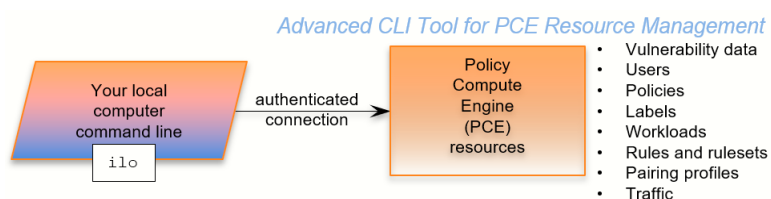
Notational Conventions in This Guide

- 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.



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 Segmentation for Data Centers 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 Segmentation for Data Centers 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 \[75\]](#).

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 \[77\]](#) 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 envvar for alternative trusted certificate store z

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

Set the Illumio Segmentation for Data Centers REST API Version

The CLI Tool uses v2 of the Illumio Segmentation for Data Centers 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 \[62\]](#).

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=elfa1262461ca2859fcf9d91a0546478d10a1bcc4c579d888a4e1cace71f9787
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 \[64\]](#) 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 \[70\]](#) 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
+-----+
| Name | Href |
+-----+
+-----+
| [[-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 \[70\]](#).

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 \[70\]](#). 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 \[70\]](#) 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"} | fool | | 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 \[68\]](#) 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 \[73\]](#) 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 \[72\]](#) 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 \[73\]](#) 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 Segmentation for Data Centers 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 <code>license.json</code> file from Illumio Example: <code>"~/secretDir/license.json"</code>
"feature_name"	Yes	The quoted string <code>"vulnerability_maps"</code> , 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`).

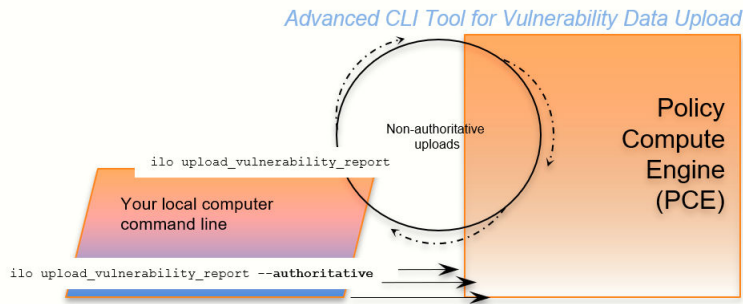
The ILO-CLI tool was updated to add a switch for `--api-user`.

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.



- **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 \[85\]](#) 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 \[75\]](#) 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
<p>--enable-proxy</p> <div>  <div> NOTE This is available in CLI Tool 1.4.4. </div> </div>	N O	<p>Use this to enable the proxy between tenable and CLI.</p> <p>Use this command to enable the proxy:</p> <pre>ilo upload_vulnerability_report --source-scanner tenable-sc --format api --severities=3 --enable-proxy -v --debug</pre> <p>Use this command if you do not want to enable the proxy:</p> <pre>ilo upload_vulnerability_report --source-scanner tenable-sc --format api --severities=3 -v --debug</pre>
<p>--input-file path_to_data-file.xml [path_to_data-file.xml]...</p>	Y e s	<p>Location of one or more data files to upload.</p> <p>The path to the data file can be either an absolute path or a relative path.</p> <p>If more than one data file is listed (bulk upload), separate the file names with space characters.</p>
--debug	N O	Enable debugging
--authoritative	N O	For uploading authoritative vulnerability data. The default command is without the --authoritative option. See Kinds of Vulnerability Data Uploads [76] for information.
--workload-cache FILE	N O	DEBUGGING ONLY: Workload Cache file - use this if available

What	Required	Description
<code>--source-scanner [nessus-pro qualys tenable-sc]</code>	Yes	Indicates the source of the scan. Note for rapid data: <ul style="list-style-type: none">• Vulnerability data from Rapid must have been exported from Rapid in Qualys XML format.• To load the Rapid data, use the 'qualys' argument
<code>--format</code> <code>REPORT_FORMAT</code>	Yes	Report format. Allowed values are: xml <ul style="list-style-type: none">• <code>--source-scanner nessus-pro</code>• <code>--source-scanner qualys</code> csv <ul style="list-style-type: none">• <code>--source-scanner tenable-sc</code>• <code>--source-scanner tenable-io</code> api <ul style="list-style-type: none">• <code>--source-scanner tenable-sc</code>• <code>--source-scanner qualys</code>• <code>--source-scanner nessus-pro</code> See also <code>--api-server</code> and <code>--api-user</code> .
<code>--api-server SourceApiServer:port</code> <code>SERVER_FQDN</code>	Yes for Tenable bl ew it h - - f o r m a t a p i	API server FQDN. Allowed formats are HOST or HOST:PORT
<code>--api-user ApiServerUserName</code>	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 Quality and Tenable	Appropriate page size if API supports pagination. The default page is 1000.
--skip-cert-verification	Yes for Quality and Tenable	Disable certificate verification for API.

What	Required	Description
	ble	
<code>--on-premise</code>	Yes only for Tenable IO	Tenable IO deployment is on-premise.
<code>--mitigated</code>	Yes only for Tenable SC	Tenable SC input is exported from the mitigated vulnerabilities analysis view.
<code>--scanned-after</code> <code>SCANNED_AFTER</code>	Yes for Qualys	<p>Qualys users can select scan data to process after a specific date, in ISO 8601 format.</p> <p>When the optional <code>scanned-after</code> 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 <code>scanned-after</code> 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.</p>
<code>--severities</code> <code>SEVERITIES</code>	No	<p>Qualys API users can select vulnerabilities with defined severity levels to include in their reports.</p> <p>Users can filter based on severity and avoid severity levels 1 and 2, which are often very informational and noisy.</p> <p>Example: <code>--only-include-severity=3,4,5</code></p> <p>For Windows, be sure to include quotes around the severity levels:</p> <p>Example: <code>--only-include-severity="3,4,5"</code></p>

What	R e q u i r e d	Description
NOTE: This option was added in Release 1.4.1		
<code>-v, --verbose</code>	N o	Verbose logging mode
<code>--trace</code>	N o	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 overwrites 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 \[78\]](#) 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 \(CVE\) \[78\]](#) and [Vulnerability Identifier \[78\]](#) 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 \(CVE\) \[78\]](#) and [Vulnerability Identifier \[78\]](#) 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 \[68\]](#).

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-eb56c4ffale3
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-eb56c4ffale
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 \[75\]](#). 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 \[78\]](#) 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.