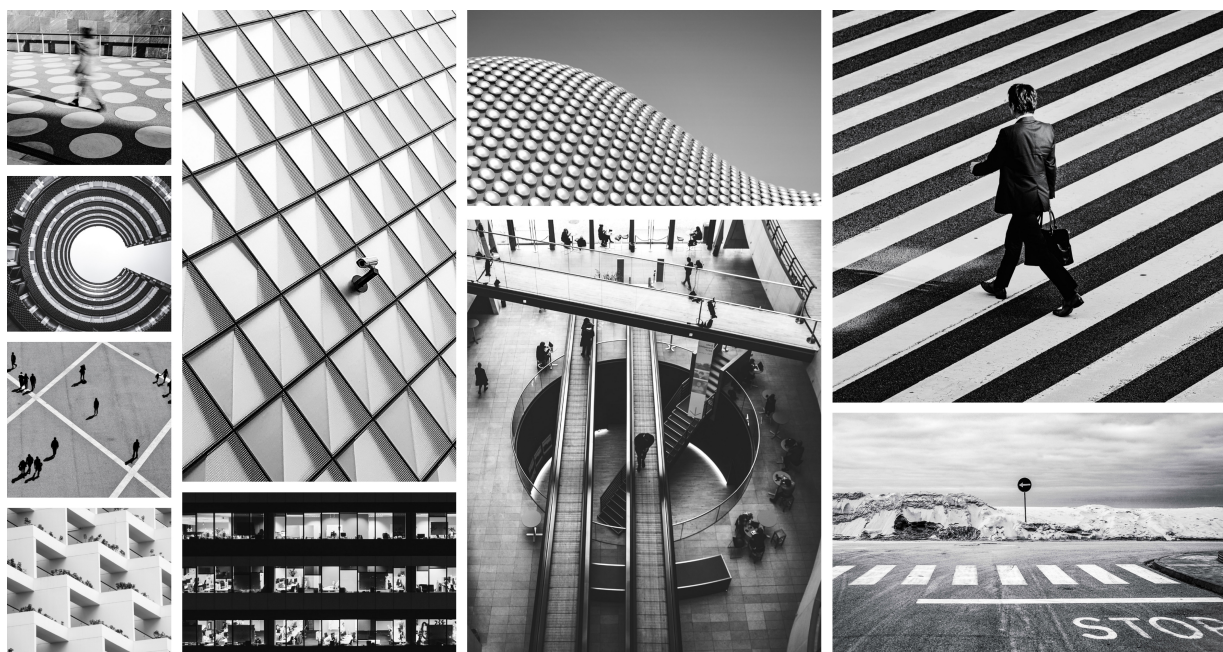




# Illumio Core What's New and Release Notes for 24.4

Published: December 2024



Learn about new features, and review the resolved and known issues for Illumio Core, Illumio LW-VEN, and Illumio Core for Kubernetes.

## Table of Contents

Security Advisories .....	5
September 2024 Security Advisories .....	5
Ruby SAML gem component authentication bypass vulnerability .....	5
Severity .....	5
Affected Products and Patch Information .....	5
Resolution .....	5
References .....	6
Skipped Critical Patch Updates .....	6
Discovered By .....	6
Frequently Asked Questions .....	6
Modification History .....	7
September 2023 Security Advisories .....	7
Authenticated RCE due to unsafe JSON deserialization .....	7
Severity .....	7
Affected Products and Patch Information .....	7
Resolution .....	8
References .....	8
Skipped Critical Patch Updates .....	8
Discovered By .....	8
Frequently Asked Questions .....	8
What's New in 24.4 .....	10
What's New and Changed in Release 24.4 .....	10
Compare V-E scores by Enforcement Type .....	10
Vulnerability API Changes in the UI .....	11
No license required for Enhanced Data Collection .....	12
New and Changed APIs in Release 24.4 .....	12
New Vulnerability APIs .....	12
common vulnerability_summary_exposure .....	12
common workloads_detected_vulnerabilities_exposure .....	13
Vulnerability API Changes .....	13
Ransomware API Changes .....	16
Workload API Changes .....	16
Illumio Core Release Notes 24.4 .....	18
Product Version .....	18
Resolved Issues in Release 24.4 .....	18
Security Information .....	19
Changes in Release 24.4.0 .....	19
Illumio LW-VEN Release 1.1 .....	20
What's New in LW-VEN Release 1.1.0 .....	20
Support for flow reporting for legacy Windows servers .....	20
Resolved Issues in 1.1.10 LW-VEN .....	20
Resolved Issues in 1.1.0 LW-VEN .....	20
Illumio Core for Kubernetes Release Notes .....	22
Illumio Core for Kubernetes Release Notes 5.2 .....	22
About Illumio Core for Kubernetes 5.2 .....	22
What's New in Release 5.2.1 .....	22
Updates for Core for Kubernetes 5.2.1 .....	23
What's New in Release 5.2.0 .....	23
Updates for Core for Kubernetes 5.2.0 .....	28
Illumio Core for Kubernetes Release Notes 5.1 .....	29
Core for Kubernetes 5.1.10 .....	29
Limitations .....	29
Updates for Core for Kubernetes 5.1.10 .....	30

Updates for Core for Kubernetes 5.1.7 .....	30
Updates for Core for Kubernetes 5.1.3 .....	30
Updates for Core for Kubernetes 5.1.2 .....	31
Updates for Core for Kubernetes 5.1.0 .....	32
Security Information for Core for Kubernetes 5.1 .....	34
Illumio Core for Kubernetes Release Notes 5.0.0 .....	34
About Illumio Core for Kubernetes 5.0 .....	34
Product Version .....	34
What's New in C-VEN and Kubelink .....	34
NodePort Limitations .....	35
Updates for Core for Kubernetes 5.0.0-LA .....	35
Illumio Core for Kubernetes Release Notes 4.3.0 .....	37
What's New in Kubernetes 4.3.0 .....	37
Product Version .....	37
Updates for Core for Kubernetes 4.3.0 .....	38
New Document Locations .....	40
Core .....	41
Cloud .....	43
Other Products: Edge, Xpress, MSP .....	44
Integrations .....	44
PDF Library .....	46
Legal Notice .....	50

# Security Advisories

This category includes announcements of security fixes and updates made in critical patch update advisories, security alerts and bulletins.

## September 2024 Security Advisories

Here's a list of the security advisories for 2024.

### Ruby SAML gem component authentication bypass vulnerability

The Ruby SAML gem is affected by an authentication bypass vulnerability, which impacts the Illumio PCE in both SaaS and on-premises deployments. An authenticated attacker could potentially leverage this vulnerability to authenticate as another SAML user. For SaaS customers, the target user can be in a different org and on a different cluster.

#### Severity

Critical: CVSS score is 9.9

CVSS: AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

### Affected Products and Patch Information

Security vulnerabilities addressed by this Security Alert affect the products listed below.

**Table 1. Products Affected by the Security Vulnerability**

Affected Products	Affected Versions	Fixed Version
Illumio Core PCE	<= 21.5.36	>= 21.5.37
	<= 22.2.42	>= 22.2.43
	<= 22.5.32	>= 22.5.34
	<= 23.2.30	>= 23.2.31
	<= 23.5.21	>= 23.5.22
	<= 24.2.0	>= 24.2.10

#### Resolution

Upgrade to the latest release for a given major version.

## References

- <https://nvd.nist.gov/vuln/detail/CVE-2024-45409>
- <https://github.com/advisories/GHSA-jw9c-mfg7-9rx2>

## Skipped Critical Patch Updates

Illumio strongly recommends that customers apply security patches as soon as possible. For customers that have skipped one or more Critical Patch Updates and are concerned about products that do not have security patches announced in this Critical Patch Update, please review previous Critical Patch Update advisories to determine appropriate actions.

## Discovered By

External Security Firm

## Frequently Asked Questions

- What software components are affected?  
Only the Illumio PCE is impacted by this vulnerability.
- What products did this affect?  
This vulnerability impacts the PCE, including Core on-premises deployments, Core SaaS, Endpoint, MSP, and Edge.
- Is Core SaaS affected?  
SaaS PCE clusters were impacted. Those environments have been patched.
- I'm using Cloud. Am I impacted?  
The Cloud platform is not affected.
- Will the patch affect performance?  
The update is not expected to affect performance.
- How can I tell if this vulnerability was used against my on-premises PCE?  
Illumio is creating queries that can be used by customers to detect known vectors for exploitation of this vulnerability. Please contact Illumio Support or your account team for assistance. If you suspect this vulnerability was used within your environment, please reach out to Illumio Support.
- Has Illumio investigated if this vulnerability was used on any SaaS PCEs?  
Illumio is currently investigating all available data from the production SaaS environment and has so far found no indications that the issue has been exploited.
- I can't apply the patch immediately. How can I mitigate the issue in the meantime?  
This vulnerability requires SAML to be enabled on the customer's PCE in order to be exploited. Customers who cannot patch their PCEs immediately, and who wish to mitigate this issue, can choose to disable SAML authentication on the PCE. For details, see the "Authentication" topic in the PCE Administration Guide. Additionally, customers can enable IP restrictions to limit access to only trusted source IPs (for example, for privileged accounts). For details, see the "Configure Access Restrictions and Trusted Proxy IPs" topic in the PCE Administration Guide.
- How long will the upgrade take?  
The fix will be provided in a normal code release so this will take the same amount of time as any PCE upgrade.
- Were any Illumio customers impacted by this vulnerability?

Illumio is not aware of any exploitation of this vulnerability within any customer environments.

**Modification History**

- September, 2024: Initial Publication of CVE

**September 2023 Security Advisories**

Here's a list of the security advisories for 2023.

**Authenticated RCE due to unsafe JSON deserialization**

Unsafe deserialization of untrusted JSON allows execution of arbitrary code on affected releases of the Illumio PCE. Authentication to the API is required to exploit this vulnerability. The flaw exists within the network\_traffic API endpoint. An attacker can leverage this vulnerability to execute code in the context of the PCE's operating system user.

**Severity**

Critical: CVSS score is 9.9

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

**Affected Products and Patch Information**

Security vulnerabilities addressed by this Security Alert affect the products listed below.

**Table 2. Products Affected by the Security Vulnerability**

Affected Products	Affected Versions	Fixed Version
Illumio Core PCE	<= 19.3.6	>= 19.3.7
	<= 21.2.7	>= 21.2.8
	<= 21.5.35	>= 21.5.36
	<= 22.2.41	>= 22.2.42
	<= 22.5.30	>= 22.5.31
	<= 23.2.10	>= 23.2.11

## Resolution

Upgrade to the latest release for a given major version.

## References

<https://www.cve.org/CVERecord?id=CVE-2023-5183>

## Skipped Critical Patch Updates

Illumio strongly recommends that customers apply security patches as soon as possible. For customers that have skipped one or more Critical Patch Updates and are concerned about products that do not have security patches announced in this Critical Patch Update, please review previous Critical Patch Update advisories to determine appropriate actions.

## Discovered By

External Security Firm

## Frequently Asked Questions

- What software components are affected?  
Only the Illumio PCE is impacted by this vulnerability.
- What products did this affect?  
This vulnerability impacts the PCE, including Core on-premises deployments, Core SaaS, Endpoint, MSP, and Edge.
- Is Core SaaS affected?  
SaaS PCE clusters were impacted. Those environments have been patched.
- I'm using Cloud. Am I impacted?  
The Cloud platform is not affected.
- How can I tell if this vulnerability was used against my on-premises PCE?  
Illumio is creating queries that can be used by customers to detect known vectors for exploitation of this vulnerability. Please contact Illumio Support or your account team for assistance. If you suspect this vulnerability was used within your environment, please reach out to Illumio Support.
- Has Illumio investigated if this vulnerability was used on any SaaS PCEs?  
Illumio is currently investigating all available data from the production SaaS environment and has so far found no indications that the issue has been exploited.
- I can't apply the patch immediately. How can I mitigate the issue in the meantime?  
This vulnerability requires SAML to be enabled on the customer's PCE in order to be exploited. Customers who cannot patch their PCEs immediately, and who wish to mitigate this issue, can choose to disable SAML authentication on the PCE.
- Reference  
For details, see the topic Authentication in the PCE Administration Guide.  
Additionally, customers can: Enable IP restrictions to limit access to only trusted source IPs (for example, for privileged accounts). For details, see the topic Configure Access Restrictions and Trusted Proxy IPs in the PCE Administration Guide.



- How long will the upgrade take?  
The fix will be provided in a normal code release so this will take the same amount of time as any PCE upgrade.
- Were any Illumio customers impacted by this vulnerability?  
Illumio is not aware of any exploitation of this vulnerability on any customer environments.

## What's New in 24.4

Learn about new features released in this version.

### What's New and Changed in Release 24.4

The **Compare V-E scores by Enforcement Type** feature, already available in the Illumio Core PCE 24.2.10 On-Premises release, is now available in Illumio Core PCE 24.4 SaaS.

#### Compare V-E scores by Enforcement Type

The Show Vulnerability Exposure (V-E) Score tool makes it easy to see how the security of your workloads and app groups would change if you were to change their current enforcement mode. New columns in the Workload and App Group list and details pages provide a side-by-side comparison of the effect different enforcement modes would have on Vulnerability Exposure (V-E) scores. A toggle allows you to simulate the switch between Full Enforcement and Visibility Only enforcement modes.



#### NOTE

This option allows you to simulate the switch between Full Enforcement and Visibility Only modes. It doesn't change the actual enforcement mode of your workloads or app groups.

Home > Servers & Endpoints

### Workloads

Workloads Container Workloads VENs

+ Add - Remove Edit Labels Enforcement Visibility

Select properties to filter view

Show Vulnerability Exposure Score (V-E) Score in: Full Enforcement Visibility Only

	Connectivity	Full Enforcement V-E Score	Current V-E Score	Enforcement	Visibility	Policy Sync	Ransomware Exposure	Protection Coverage Score	Name
<input type="checkbox"/>	Online	0	3.1	Visibility Only	Blocked + Allowed	Active	Critical	0%	409_vm4.local
<input type="checkbox"/>	Online	0	3	Selective	Blocked + Allowed	Active	Critical	0%	409_vm1.local
<input type="checkbox"/>	Online	0	0	Full	Blocked + Allowed	Active	Protected	82%	409_vm2.local
<input type="checkbox"/>	Online			Full	Blocked + Allowed	Active	Protected	82%	409_vm3.local



For more information, see:

- [Compare V-E Scores in App Groups](#)
- [Compare V-E Scores in Workloads](#)

## Vulnerability API Changes in the UI

The changes in vulnerability APIs have the following effect on the UI:

**Table 3. Vulnerability API Changes**

API	UI Changes
GET /orgs/:xorg_id/workloads/<id>/detected_vulnerabilities	Four new columns are added to the workload details page in the UI to allow you to compare exposure and VE scores based on different enforcement types.
GET /orgs/:xorg_id/workloads?representation=workload_labels_vulnerabilities	Two new columns are added to the workload list page in the UI to allow you to compare exposure and VE scores for different enforcement types.
GET /orgs/:xorg_id/workloads/:workload_id?representation=workload_labels_vulnerabilities	
GET /orgs/:xorg_id/aggregated_detected_vulnerabilities	The vulnerability and summary scores are now in additional tables, and their scores have been added to the response.
GET /orgs/:xorg_id/app_groups	
GET /orgs/:xorg_id/workloads/detailed_vulnerabilities	The vulnerability data in response is not computed at runtime. Instead, it is taken from the database generated by the proper stats processor.

## No license required for Enhanced Data Collection

Beginning with release 24.4, the Enhanced Data Collection feature is available to all users and does not require a separate license.

For more information, see the "Enhanced Data Collection" section of the [Workloads and VENS](#) topic.

## New and Changed APIs in Release 24.4

This release includes major changes for the vulnerability APIs and minor changes for the Ransomware and Workload APIs.

### New Vulnerability APIs

Before release 24.4, the vulnerability APIs allowed users to calculate vulnerability exposure for full enforcement mode only.

The UI now allows users to see exposure scores for different enforcement modes without changing the workload's enforcement mode.

Two new schemas and other updated schemas support the "Vulnerability Exposure per Enforcement Mode" functionality.

### common\_vulnerability\_summary\_exposure

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "description": "Vulnerability exposure details",
  "properties": {
    "vulnerable_port_exposure": {
      "description": "The aggregated vulnerability port exposure score of the workload in the specified mode across all the vulnerable ports",
      "type": ["integer", "null"]
    },
    "vulnerability_exposure_score": {
      "description": "The aggregated vulnerability exposure score of the workload in the specified mode across all vulnerable ports",
      "type": ["integer", "null"]
    }
  }
}
```

This new common schema provides vulnerability exposure details, such as the aggregated vulnerability exposure score with specified mode across all vulnerable ports.

## common workloads\_detected\_vulnerabilities\_exposure

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "description": "Vulnerability exposure details for workloads",
  "properties": {
    "vulnerable_port_exposure": {
      "description": "The exposure of the port based on the current
policy for the specified enforcement mode",
      "type": ["integer", "null"]
    },
    "port_vulnerability_exposure_score": {
      "description": "The vulnerability exposure score calculated for
the port, based on the port exposure and vulnerability for the specified
enforcement mode",
      "type": ["integer", "null"]
    }
  }
}
```

This new common schema provides the port's exposure based on the current policy and the vulnerability exposure score calculated for it.

## Vulnerability API Changes

Changes in the existing schemas are described below.

### common aggregated\_detected\_vulnerability

```
{
  "properties": {
    "aggregated_detected_vulnerabilities": {
      "items": {
        "properties": {
          "full_enforcement_vulnerability_exposure__added": {
            "$ref":
"workloads_detected_vulnerabilities_exposure.schema.json",
            "description": "vulnerability exposure details for full
enforcement mode"
          },
          "selective_enforcement_vulnerability_exposure__added": {
            "$ref":
"workloads_detected_vulnerabilities_exposure.schema.json",
            "description": "vulnerability exposure details for selective
enforcement mode"
          },
          "visibility_enforcement_vulnerability_exposure__added": {
            "$ref":
"workloads_detected_vulnerabilities_exposure.schema.json",
            "description": "vulnerability exposure details for visibility-
only enforcement mode"
          }
        }
      }
    }
  }
```

```

        "current_enforcement_vulnerability_exposure__added": {
            "$ref":
"workloads_detected_vulnerabilities_exposure.schema.json",
            "description": "vulnerability exposure details for the current
enforcement mode"
        }
    }
}

```

New properties are added to this schema:

- full\_enforcement\_vulnerability\_exposure
- selective\_enforcement\_vulnerability\_exposure
- visibility\_enforcement\_vulnerability\_exposure
- current\_enforcement\_vulnerability\_exposure

### **common vulnerability\_summary**

```

{
  "properties": {
    "full_enforcement_vulnerability_exposure__added": {
      "$ref": "vulnerability_summary_exposure.schema.json",
      "description": "vulnerability exposure details for full enforcement
mode"
    },
    "selective_enforcement_vulnerability_exposure__added": {
      "$ref": "vulnerability_summary_exposure.schema.json",
      "description": "vulnerability exposure details for selective
enforcement mode"
    },
    "visibility_enforcement_vulnerability_exposure__added": {
      "$ref": "vulnerability_summary_exposure.schema.json",
      "description": "vulnerability exposure details for visibility-only
enforcement mode"
    },
    "current_enforcement_vulnerability_exposure__added": {
      "$ref": "vulnerability_summary_exposure.schema.json",
      "description": "vulnerability exposure details for the current
enforcement mode"
    },
    "max_vulnerability_exposure_score__added": {
      "description": "The maximum vulnerability exposure score of the
workload in its current enforcement state across all vulnerable ports",
      "type": [
        "integer",
        "null"
      ]
    },
    "last_updated_at__added": {
      "description": "Indicates when the vulnerability data was last
updated",
      "type": "string",

```

```

    "format": "date-time"
  },
  "vulnerable_port_exposure": {
    "description": {
      "__old": "The aggregated vulnerability port exposure score of the workload across all the vulnerable ports",
      "__new": "The aggregated vulnerability port exposure score of the workload in full enforcement mode across all the vulnerable ports"
    }
  },
  "vulnerability_exposure_score": {
    "description": {
      "__old": "The aggregated vulnerability exposure score of the workload across all the vulnerable ports.",
      "__new": "The aggregated vulnerability exposure score of the workload in full enforcement mode across all the vulnerable ports."
    }
  }
}

```

In addition to the four properties that have been added for `common aggregated_detected_vulnerability`, this common schema includes other new and changed properties:

- `max_vulnerability_exposure_score`
- `last_updated_at`
- `vulnerable_port_exposure` changed exposure score of the workload across all the vulnerable ports to specify it is done "in full enforcement mode"
- `vulnerability_exposure_score` changed exposure score of the workload across all the vulnerable ports to specify it is done "in full enforcement mode"

### **common workload\_detected\_vulnerabilities**

```

{
  "properties": {
    "last_updated_at__added": {
      "description": "Indicates when the vulnerability data was last updated",
      "type": "string",
      "format": "date-time"
    },
    "workload_detected_vulnerabilities": {
      "items": {
        "properties": {
          "full_enforcement_vulnerability_exposure__added": {
            "$ref": "workloads_detected_vulnerabilities_exposure.schema.json",
            "description": "vulnerability exposure details for full enforcement mode"
          },
          "selective_enforcement_vulnerability_exposure__added": {
            "$ref": "workloads_detected_vulnerabilities_exposure.schema.json",
            "description": "vulnerability exposure details for selective enforcement mode"
          }
        }
      }
    }
  }
}

```

```

    },
    "visibility_enforcement_vulnerability_exposure__added": {
      "$ref":
"workloads_detected_vulnerabilities_exposure.schema.json",
      "description": "vulnerability exposure details for visibility-
only enforcement mode"
    },
    "current_enforcement_vulnerability_exposure__added": {
      "$ref":
"workloads_detected_vulnerabilities_exposure.schema.json",
      "description": "vulnerability exposure details for the current
enforcement mode"
    }
  }
}
}
}
}
}
}

```

The same properties have been added as in common aggregated\_detected\_vulnerability.

## Ransomware API Changes

New properties are added to the APIs used to power the ransomware dashboard:

- settings\_get
- settings\_put

The new property is named cloud\_secure\_tenant\_id.

```

{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "type": "object",
  "properties": {
    =====
  },
  "cloud_secure_tenant_id": {
    "description": "Cloud Secure tenant id corresponding to this
organization",
    "type": "string"
  }
}
}

```

## Workload API Changes

In the API traffic\_flows\_endpoint a new property is added: cloud\_resource.

```

{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "description": "Traffic flow endpoint details",

```



```
"type": "object",
"additionalProperties": false,
"properties": {
=====
},
"cloud_resource": {
  "ref": "traffic_flows_cloud_resource.schema.json"
},
```

# Illumio Core Release Notes 24.4

## Product Version

PCE Version: 24.4 (Illumio Cloud customers)

These release notes provide a list of resolved issues and known issues for Illumio Core 24.4.

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

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

## Resolved Issues in Release 24.4

Issue	Description	Known Issues Resolved in Release
E-120537	Summary: Remove the option <code>aggregate_flows_across_days</code> from traffic filters in the UI  This option is always set to <code>true</code> by default. The ability to change it to <code>false</code> with the UI filters caused an increase in the time required to complete traffic queries, so this ability has been removed from the UI.	Resolved in 24.2.20
E-119969	Summary: Explorer query causing CPU spikes  Explorer query with " <code>aggregate_flows_across_days</code> " = <code>false</code> for longer duration was causing CPU spikes and poor query performance. This issue is resolved by having the flag now set to " <code>true</code> " permanently.	Resolved in 24.3.0
E-119321	Summary: RBL Scheduler throwing a JS error  The scheduler for Rule-based Labeling was throwing a JavaScript error that was breaking the page.	Resolved in 24.2.20, 24.3.10
E-119205	Summary: Incorrect links for the draft and pending policies  An incorrect link was showing after opening the draft policy, and a "View the active version" link was showing for the additional pending Policy.	Resolved in 24.2.10
E-118558	Summary: Flows in Illumination or traffic database summary not visible  In Flow Analytics, an error occurred, and users did not see flows in Illumination or traffic database summary.	Known in 24.3.0  Resolved in 23.5.30, 24.2.20

## Security Information

This section provides important security information for this release. For additional information about security issues, security advisories, and other security guidance about this release, go to the [Illumio Support portal](#). You must have a valid login and password.

### Changes in Release 24.4.0

- **Curl is upgraded to version 8.10.0**  
Curl is upgraded to version 8.10.0 to address CVE-2024-6197 and CVE-2024-7264.
- **Postgres is upgraded to version 15.8**  
Postgres is upgraded to version 15.8 to address CVE-2024-7348.
- **Express is upgraded to version 4.21.1**  
Express is upgraded to version 4.21.1 to address CVE-2024-43796.
- **Path-to-regexp is upgraded to version 0.1.10**  
Path-to-regexp is upgraded to version 0.1.10 to address CVE-2024-45296.
- **Serve-static is upgraded to version 1.16.2**  
Serve-static is upgraded to version 1.16.2 to address CVE-2024-43800.
- **Send is upgraded to version 0.19.0**  
Send is upgraded to version 0.19.0 to address CVE-2024-43799.
- **Body-parser is upgraded to version 1.20.3**  
Body-parser is upgraded to version 1.20.3 to address CVE-2024-45590.
- **Redis is upgraded to version 7.4.1**  
Redis is upgraded to version 7.4.1 to address CVE-2024-31449, CVE-2024-31227, CVE-2024-31228.

## Illumio LW-VEN Release 1.1

### What's New in LW-VEN Release 1.1.0

The following new feature is added in Illumio Legacy Windows VEN:

#### Support for flow reporting for legacy Windows servers

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

### Resolved Issues in 1.1.10 LW-VEN

- **ICMP rule generation created empty command** (E-120840)  
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. This issue is fixed.
- **Excessive time needed for Windows firewall to apply Illumio rules** (E-120184)  
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.
- **Policy conflict lead to policy sync failure and LW-VEN crash** (E-120119)  
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. This issue is fixed.

### Resolved Issues in 1.1.0 LW-VEN

- **LW-VEN activation failed on non-UTF-8 legacy Windows workloads** (E-119190)  
LW-VEN activation failed on workloads configured for non-US languages. This happened because LW-VEN version 1.0.1 doesn't support non-UTF-8 strings. This issue is fixed. Support for non-UTF-8 was added in LW-VEN 1.1.0.
- **Activate option appeared during "non-fresh" LW-VEN installation** (E-118952)  
When installing an LW-VEN on a supported legacy Windows machine on which an LW-VEN is already activated, the option Start + Activate appeared, which was unexpected. As this wasn't a fresh installation, only the Start option should've appeared, not Start+Activate. This issue is resolved. Now, only Start appears during non-fresh installations.
- **Users weren't prompted during LW-VEN activation if activation command was run without options** (E-118764)  
Attempting to activate LW-VEN failed if users issued the `illumio-lwven-ctl activate` command without options. A command prompt appeared but no prompts displayed and the activation hung. This issue is fixed.

- **LW-VEN 1.0.1 failed to apply 2008 firewall policy that contained very large port range** (E-118600)

The Windows Firewall rejected Illumio security policy rules that specified extremely large port ranges, resulting in policy not being applied. This issue is resolved. Rules exceeding 1000 ports are now split into multiple rules, and rules with large port ranges are no longer rejected. 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.

# Illumio Core for Kubernetes Release Notes

This section provides release notes for the following versions of Kubernetes:

- 5.2.x
- 5.1.x
- 5.0.x
- 4.3.x

## Illumio Core for Kubernetes Release Notes 5.2

November 6, 2024

### About Illumio Core for Kubernetes 5.2

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

**Document Last Revised:** November 2024

### Product Version

**Compatible PCE Versions:** 23.5.0+A1 and later releases

**Current Illumio Core for Kubernetes Version:** 5.2.1, which includes:

- C-VEN version: 23.4.0
- Kubelink version: 5.2.1
- Helm Chart version: 5.2.1

### What's New in Release 5.2.1

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

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

## Updates for Core for Kubernetes 5.2.1

### Kubelink

#### Resolved Issues

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

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

### C-VEN

#### Resolved Issues

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

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

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

- **Move C-VEN base image to a smaller image** (E-118492)

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

## What's New in Release 5.2.0

- **"Wait for Policy" Feature**

With a new Wait For Policy feature, CLAS-enabled Kubelink can be configured to automatically and transparently delay the start of an application container in a pod until a policy is properly applied to the pod. This feature replaces the local policy convergence controller, the Illumio readiness gate. A readiness gate required adding the `readinessGates.conditionType` into the spec YAML file of the Kubernetes Workload. Instead, Wait For Policy uses an automatically injected init container, with no change of the user application needed. When enabled, Wait For Policy synchronizes the benefit of Kubernetes automatic container creation with the protection of proper policy convergence into the new container. For more information, see ["Wait For Policy" Feature \[26\]](#).

- **CLAS Flat Network Support**

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

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

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

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

- **Kubelink Support Bundle**

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

Use the following command to generate and transfer the Kubelink support bundle from its pod: (Note that the backslash (\) character is included to indicate the continuation of a long command line that will be truncated by the right margin of this document in PDF form.)

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

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

- **Base OS Upgraded to UBI9**

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



### IMPORTANT

**Important Notice:** With the base image upgrade for both Kubelink and C-VEN, you must adjust resource allocations according to the guidance described below in the "[Resource Allocation Guidelines \[24\]](#)" section. You must ensure that resources are updated prior to the upgrade to achieve optimal performance, and to avoid any potential degradation in product performance.

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

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

- **Changes to Supported Orchestration Platforms and Components in 5.2.0**

The 5.2.0 release contains several changes to supported platforms and components. For full details, see [Kubernetes Operator OS Support and Dependencies](#) on the Illumio Support portal (log in required).

## Resource Allocation Guidelines

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

These guidelines are grouped into the following general deployment sizes:



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

The following variables determine the deployment sizes listed above:

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

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

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

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

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

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

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

### Small-scale resource allocation

Customer Category	Nodes per Cluster	Total K8s Workloads	Total Policy Size	
Small-scale	1 - 10	0 - 1000	0 - 1.5 Mi	
<b>Resources</b>		<b>C-VEN</b>	<b>Kubelink</b>	<b>Storage</b>
Requests	CPU	0.5	0.5	0.5
Requests	memory	600 Mi	500 Mi	500 Mi
Limits	CPU	1	1	1

Customer Category	Nodes per Cluster	Total K8s Workloads	Total Policy Size	
Limits	memory	700 Mi	600 Mi	600 Mi
Volumes	size limits	n/a	n/a	1 Gi

### Medium-scale resource allocation

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

### Large-scale resource allocation

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

### "Wait For Policy" Feature

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

This Wait For Policy feature replaces the existing local policy convergence controller, also known as a readiness gate. A readiness gate required manually adding the `readinessGate`

condition into the spec of the Kubernetes Workload. Instead, Wait For Policy uses an automatically injected init container, which requires no change to the user application.

## Behavior

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

1. Kubernetes creates a pod.
2. The pod creation request is intercepted by a mutating webhook.
3. Kubernetes requests MutatingAdmissionWebhook Controller running in Kubelink.
4. Controller returns with a new pod patched with an Illumio init container.
5. Init container starts in the pod, and periodically checks the policy status of the pod using the Kubelink status server.
6. At the same time, Kubelink is preparing a policy for the new pod, and is sending the policy to the pod's C-VEN.
7. The C-VEN applies policy to the pod, and sends an acknowledgment to Kubelink.
8. Kubelink reports that the policy is now applied to the init container.
9. The Init container exits, and allows the original container to start.
- 10 If a policy is not applied within the configured time (see [Configuration \[27\]](#) section for Helm Chart `waitForPolicy.timeout` parameter), the init container exits anyway, and allows the original container to start.

The Illumio init container must be accessible from all namespaces that use Wait for Policy. An easy way to ensure this accessibility is to make init available from a public repository. However, a private repository can be used if you manage the secret deployment properly, such as by deploying init from the same repository as all other containers, or by using a secret management tool.

## Configuration

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

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

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

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

## Updates for Core for Kubernetes 5.2.0

### Kubelink

#### Resolved Issues

- **Helm: pull secret to quay gets created even if no credentials are set** (E-119659)  
Helm chart now creates Illumio pull secret only if credentials are specified and also externally passed secret names are included.
- **Kubelink: error concurrent map read and map write** (E-119626)  
Kubelink was restarted because previous container exited with the message "fatal error concurrent map read and map write."
- **Kubelink: Update base image to address vulnerabilities** (E-119429)  
The Unified Base Image was upgraded to address CVE-2023-45288.
- **Kubelink needs to have higher priority assigned to avoid going to evicted state** (E-113920)  
If the Kubernetes cluster encounters problems or runs out of space, Kubelink was the first pod to be put into the evicted state, which caused policy enforcement to fail. To prevent permanent eviction, in Helm chart version 5.2.0 the Kubelink Deployment and C-VEN DaemonSets are assigned priority classes by default -- `system-cluster-critical` for Kubelink and `system-node-critical` for C-VEs.

### C-VEN

#### Resolved Issues

- **CVEN: Update base image to address vulnerabilities** (E-119428)  
The 23.4 C-VEN Unified Base Image was upgraded to the latest UBI9 to address vulnerabilities described in CVE-2014-3566, CVE-2014-3566, CVE-2014-3566, CVE-2022-3358, and CVE-2023-27533.
- **Cannot deploy C-VEN to GKE when using default OS** (E-116506)  
For GKE clusters, when using the default cluster OS (Container-Optimized OS from Google), the node filesystems are read-only. This prevented C-VEN from mounting `/opt/illumio_ven_data` and writing into it for persistent storage.  
To resolve this issue, a new variable `cven.hostBasePath` was added to the 5.2.0 Helm Chart to specify where the C-VEN DaemonSet mounts its data directory. The default value is `/opt`. Use this variable to specify where the C-VEN DaemonSet mounts its data directory. If using a Container-Optimized OS, you can set the directory to `/var`.
- **[CVE]: Failed to load policy** (E-115231)  
The log message "Error: Failed to load policy" was appearing during scenarios that were obvious or expected. The log level for this message has been changed from Error to Info.

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

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

## Illumio Core for Kubernetes Release Notes 5.1

Published: September 4, 2024

### Core for Kubernetes 5.1.10

**Compatible PCE Versions:** 23.5.10 and most later releases

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

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

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

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

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

### Limitations

- **NodePort**

The following limitations exist regarding NodePort policy enforcement and flows:

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

For example, given the following setup:

- Worker nodes in the cluster are labeled as Role: Worker Node
- Clients accessing the Service running in the Kubernetes cluster are labeled Role: Client
- The NodePort Service is labeled Role: Ingress

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

- **Flat Network support in CLAS mode**

Using EKS or AKS in a flat network topology, such as EKS with AWS VPC CNI or AKS with Azure CNI, is not supported in CLAS-enabled clusters.

## Updates for Core for Kubernetes 5.1.10

### Kubelink

#### Resolved Issues

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

## Updates for Core for Kubernetes 5.1.7

### Kubelink

#### Resolved Issues

- **Kubelink: policy service blocked when agent disconnects while receiving policy message** (E-117099)  
In some situations, policies stopped being sent due to a policy channel lock after C-VE disconnected while receiving a policy update.
- **Kubelink: policy service blocked if one agent is not reading policy message** (E-116967)  
In some situations, policies stopped being sent after a C-VE became unresponsive.
- **Kubelink can't save sets because of message size limit** (E-116825)  
Policy updates were being interrupted when large policy sets were being sent. The message size has been increased to permit larger policy transmissions .
- **Kubelink: workload events processing is slowed down by policy updates** (E-116706)  
The processing of workload events from Kubernetes sometimes became slow when handling thousands of Kubernetes Workloads, or the policy PCE requests were taking too long, or if there was no previous policy version in storage.
- **Kubelink sends wrong workload href in policy ACK request** (E-116640)  
In some CLAS-enabled clusters that host large numbers of workloads, the Kubernetes Workloads page showed an old policy apply date. Kubelink incorrectly sent a policy ACK for some Kubernetes Workloads with the host workload URI. The PCE responded with a 406 error, and a "no policy" ACK was stored.

## Updates for Core for Kubernetes 5.1.3

### Kubelink

#### Resolved Issues

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

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

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

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

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

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

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

## Updates for Core for Kubernetes 5.1.2

### Kubelink

#### Resolved Issues

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

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

- **Kubelink - Unable to process policy with custom iptables rules** (E-115250)

Kubelink in CLAS mode failed to process policy received from the PCE when custom iptables rules were present, producing the error message "json: cannot unmarshal object into Go struct field."

- **Kubelink to PCE connectivity issues - connection reset by peer** (E-115049)

CLAS-enabled Kubelink was entering degraded mode too soon because of PCE connectivity problems. Now Kubelink also retries requests after network and OS errors, which avoids premature degraded mode entry.

- **C-VEN reporting potentially blocked traffic between worker nodes** (E-114691)  
CLAS processing of outbound rules to a ClusterIP Service replaced the "All Services" destination in the rule with actual ports from the Kubernetes Service. If a destination label included a Kubernetes Service, this caused a missing iptables rule between nodes.
- **Max policy message size between Kubelink and C-VEN is too small** (E-113714)  
The default gRPC message size was set to too small of a value, which caused C-VEs to reject policy messages that were larger than this value. The default gRPC message size is now larger, to avoid this problem.

## Updates for Core for Kubernetes 5.1.0

### What's New in the 5.1.0 Release

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

- **New CLAS architecture option**  
Kubelink now can be deployed with a Cluster Local Actor Store (CLAS) module, which manages flows from C-VEs to PCE, and policies from PCE to C-VEs. The CLAS-enabled Kubelink tracks individual pods, and when they are created or destroyed, instead of this being communicated directly to the PCE. To migrate from an existing (non-CLAS) environment to a CLAS-enabled one, set the `clusterMode` parameter to `migrateLegacyToClas` in your deployment YAML file (typically named `illumio-values.yaml`). See the `README.md` file accompanying the Helm Chart for full details on this and other Helm Chart parameters.
- **Workloads more closely match Kubernetes architecture**  
In CLAS-enabled environments, workloads are now conceptually tied to their containers, instead of being referred to in context of their pods, which more closely matches Kubernetes practice. To reflect this change, such workloads in CLAS environments are called *Kubernetes Workloads*, regardless of what containers have been spun up or destroyed to run the applications. In non-CLAS environments, the existing term *Container Workloads* is still used as in prior releases, corresponding to Pods. In mixed environments (with both non-CLAS and CLAS-enabled clusters), the PCE UI shows both Container Workloads and Kubernetes Workloads, as appropriate.
- **Degraded mode for CLAS-enabled Kubelink**  
If a CLAS-enabled Kubelink detects that its connection with the PCE becomes unavailable (for example, due to connectivity problems or an upgrade), Kubelink by default enters a *degraded mode*. In this degraded mode, new Pods of existing Kubernetes Workloads get the latest policy version cached in CLAS storage. When Kubelink detects a new Kubernetes Workload with exactly the same label sets and in the same namespace as an existing Kubernetes Workload, Kubelink delivers the existing, cached policy to Pods to this new Workload. If Kubelink cannot find a cached policy (that is, when labels of a new Workload do not match those of any existing Workload in the same namespace), Kubelink delivers a "fail open" or "fail closed" policy based on the Helm Chart parameter `degradedModePolicyFail`. The degraded mode can also be turned on or off by the Helm Chart parameter `disableDegradedMode`.
- **Illumio annotations in CLAS mode specified on the workload and not on Pod's template**  
Illumio annotations when in CLAS mode are now specified on the Kubernetes Workload and not on the pod's template.
- **Docker support dropped**  
The Docker CRI is no longer supported as of the 5.0.0 release of Illumio Core for Kubernetes.



## C-VEN

### Resolved Issue

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

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

### Known Issues

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

When C-VEN is started first, it tries to contact the PCE in order to obtain CLAS token, but receives a 404 error. This is expected behavior for this scenario, which is only momentary. Kubelink eventually starts normally, and C-VEN obtains the CLAS tokens as expected.

- **Helm install fails with Helm version 3.12.2 but works with 3.10** (E-108128)

When installing with Helm version 3.12.2, the installation fails with a YAML parse error. Workaround: Use Helm version 3.10, or version 3.12.3 or later.

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

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

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

## Kubelink

### Resolved Issues

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

After disabling a NodePort rule that opens it to outside VMs, iptable entries for pods with a virtual service's targetPort were not being removed as expected. Now the pod no longer remains opened. Host iptables are removed, so traffic does not go through, and the pod ports are properly closed.

- **CLAS - The etcd pod crashes when node reboots** (E-106236)

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

### Known Issues

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

The Kubelink pod is restarted after deploying Illumio Core for Kubernetes in CLAS mode. There is no workaround. Kubelink runs properly after this single restart.

- **CLAS: Container Workload Profile label change is not applied to Kubernetes Workloads, only to Virtual Services** (E-109168)

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

This works as designed.

## Security Information for Core for Kubernetes 5.1

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

## Illumio Core for Kubernetes Release Notes 5.0.0

### About Illumio Core for Kubernetes 5.0

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

**Document Last Revised:** January 2024

### Product Version

**Compatible PCE Versions:** 23.5.0+A1 and later releases

**Current Illumio Core for Kubernetes Version:** 5.2.1, which includes:

- C-VEN version: 23.4.0
- Kubelink version: 5.2.1
- Helm Chart version: 5.0.0

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

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

### What's New in C-VEN and Kubelink

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

- **New CLAS architecture option**

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

- **Workloads more closely match Kubernetes architecture**

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

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

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

- **Docker support dropped**

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

## NodePort Limitations

- **NodePort**

Here are some limitations around NodePort policy enforcement and flows:

- Only NodePort Services with `externalTrafficPolicy` set to "cluster" are supported. (This is the default and most frequently used value for this setting.)

- When writing rules to allow traffic to flow from external (to the cluster) entities and NodePort Service, the source side of the rule must contain all nodes in the cluster.

For example, given the following setup:

- Worker nodes in the cluster are labeled as Role: Worker Node
- Clients accessing the Service running in the Kubernetes cluster are labeled Role: Client
- The NodePort Service is labeled Role: Ingress

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

## Updates for Core for Kubernetes 5.0.0-LA

### C-VEN

#### Resolved Issues

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

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

#### Known Issues

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

When C-VEN is started first, it tries to contact the PCE in order to obtain CLAS token, but receives a 404 error. This is expected behavior for this scenario, which is only momentary. Kubelink eventually starts normally, and C-VEN obtains the CLAS tokens as expected.

- **Helm install fails with Helm version 3.12.2 but works with 3.10** (E-108128)

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

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

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

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

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

## Kubelink

### Resolved Issues

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

In a CLAS environment on IKS with Calico, when running traffic to a clusterIP service from a pod, flows were being displayed incorrectly. Sometimes flows were incorrectly shown as Allowed. Other times, flows that should not be present were being shown as Blocked. This issue is resolved.

- **Kubernetes cluster falsely detected as an OpenShift cluster** (E-107910)

After deployment, Kubelink falsely detected a Kubernetes cluster as an OpenShift cluster based on misinterpretations of installed VolumeReplicationClass and VolumeReplications APIs on the cluster. This issue is resolved.

- **Problem when label from PCE was deleted after Kubelink starts** (E-107779)

When creating a new workload on PCE, Kubelink uses cached or preloaded labels to label a workload. However, if the label was deleted before the workload was actually created, the PCE responded with a 406 status error. This issue is resolved.

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

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

### Known Issues

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

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

There is no workaround available.

- **Non-CLAS mode: Failed to clean up the pods** (E-109687)

After deleting a non-CLAS container cluster, the cluster gets deleted but Container Workloads are not deleted, and remain present.

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

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

There is no workaround. Kubelink runs properly after this single restart.

- **CLAS: Container Workload Profile label change is not applied to Kubernetes Workloads, only to Virtual Services** (E-109168)

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

No workaround is available.

- **CLAS - The etcd pod crashes when node reboots** (E-106236)

The etcd pod crashes if one of the nodes in the cluster is rebooted.  
There is no workaround available.

## Security Information for Core for Kubernetes 5.0.0-LA

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

## Illumio Core for Kubernetes Release Notes 4.3.0

### What's New in Kubernetes 4.3.0

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

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

Here are the new and changed items in this release:

- **New Kubelink 3.3.1**

This Kubernetes 4.3.0 release includes an upgraded Kubelink component, version 3.3.1 .

- **New C-VEN 22.5.14**

This Kubernetes 4.3.0 release includes an upgraded C-VEN component, version 22.5.14.



#### NOTE

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

### Security Information

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

### Base Image Upgraded

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

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

### Product Version

**Compatible PCE Versions:** 22.5.0 and later releases

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

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

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

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

## Updates for Core for Kubernetes 4.3.0

### C-VEN

#### Resolved Issues

- **C-VEN support report does not contain container workload firewalls** (E-106932)  
VEN support reports for C-VEs were missing the active firewall information for all container workloads. This issue is resolved. Support reports now include full firewalls from each network namespace, as gathered by `iptables-save` and `ipset list` output.
- **Conntrack tear-down for containers with policy updates** (E-44832)  
Although policy was changed to block a container workload from talking to another, traffic was still passing between the workloads, due to a conntrack connection remaining incorrectly active. This issue is resolved. Conntrack connections on sessions affected by a policy change are now properly torn down.

#### Known Issue

- **C-VEs not automatically cleaned up after AKS upgrade** (E-103895)  
After upgrading an AKS cluster, sometimes a few duplicate C-VEs might not be automatically removed as part of the normal upgrade process, and remain in the PCE as "non-active." Note there is no compromise to the security or other functionality of the product.  
Workaround: Manually prune the extra unmigrated C-VEs from the PCE by clicking the **Unpair** button for each of them.

### Kubelink

#### Resolved Issue

- **Kubelink does not pair with PCE when a separate management port is used** (E-107001)  
Kubelink would crash after start when the PCE had `front_end_management_https_port` set to 9443 instead of 8443, because of a missing label\_map URL. This issue is resolved.

#### Known Issue

- **Kubelink does not properly apply label mappings with PCE using two-sided management ports** (E-105391)  
Label mappings are not properly applied when using the LabelMap CRD if the PCE uses two-sided management ports.

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

## New Document Locations

Welcome to the new and improved Illumio documentation library. These tables provide links to the new documentation locations. Remember to update your bookmarks.

Use the new search (powered by Coveo) to search for version specific documentation. You can filter search results by product, version, and content type.

- [Core \[41\]](#)
- [Cloud \[43\]](#)
- [Edge, Xpress, MSP \[44\]](#)
- [Integrations \[44\]](#)

The screenshot shows the Illumio Technical Documentation website. At the top, there is a navigation bar with links for Home, Cases, Community, Knowledge Base, and Training. Below the navigation bar is a large section titled "Explore Illumio Documentation" with a search bar. Underneath this is a large orange banner for the "Illumio Zero Trust Segmentation Platform" with a subtext: "Discover Illumio's ZTS Platform, including getting started guides and user documentation." Below the banner are four colored buttons: "ILLUMIO CORE" (purple), "ILLUMIO CLOUDSECURE" (blue), "ILLUMIO ENDPOINT" (orange), and "CONTAINERS" (dark grey). Below these are two buttons: "AI/ML" and "Other Products", both with right-pointing arrows. The "Integrations" section follows, listing various integrations with right-pointing arrows: IBM QRadar, Sentinel, Splunk, Netskope, ServiceNow CMDB, and Terraform. At the bottom, there is a dark grey footer with copyright information: "Copyright © 2024 | About Support | EULA | Privacy Policy".

TECHNICAL DOCUMENTATION

Home Cases Community Knowledge Base Training

## Explore Illumio Documentation

Search...

### Illumio Zero Trust Segmentation Platform

Discover Illumio's ZTS Platform, including getting started guides and user documentation.

ILLUMIO CORE ILLUMIO CLOUDSECURE ILLUMIO ENDPOINT CONTAINERS

AI/ML > Other Products >

### Integrations

- > IBM QRadar
- > Sentinel
- > Splunk
- > Netskope
- > ServiceNow CMDB
- > Terraform

Copyright © 2024 | About Support | EULA | Privacy Policy



## Core

**Table 4. New Locations for the Illumio Documentation: Core**

Top-Level Category/Topics	New Location for Category/Topics	Second Level Topics
Get Started	<a href="#">Application Ringfencing Tutorial</a>	
	<a href="#">Glossary</a>	
Install and Upgrade	<a href="#">Upgrading Illumio Core: Why and How</a>	
	<a href="#">VEN Installation and Upgrade Guide</a>	<a href="#">Prepare for VEN Installation</a> <a href="#">Set Up PCE for VEN Installation</a> <a href="#">VEN Installation and Upgrade</a> <a href="#">VEN Installation and Upgrade with VEN CTL</a> <a href="#">VEN Reference</a>
	<a href="#">Endpoint Concepts Guide</a>	<a href="#">NLA Support for Endpoints</a>
	<a href="#">Endpoint Installation and User Guide</a>	
	<a href="#">LW-VEN Installation and Configuration Guide</a>	<a href="#">LW-VEN Requirements and Limitations</a> <a href="#">Install and Configure the Illumio LW-VEN Service</a> <a href="#">Manage and Troubleshoot the LW-VEN</a>
	<a href="#">Illumio Core for Kubernetes and Openshift</a>	
Release Notes	<a href="#">What's New and Release Notes for 24.3</a> <a href="#">What's New and Release Notes for 24.2.10</a> <a href="#">Kubernetes What's New and Release Notes for 5.2, 5.1, 5.0, 4.3.0</a>	
Use Core	<a href="#">Security Policy Guide</a>	<a href="#">Security Policy Objects</a> <a href="#">Workloads</a> <a href="#">Create Security Policy</a> <a href="#">Policy Enforcement</a> <a href="#">Secure Workload Connections</a>

Top-Level Category/Topics	New Location for Category/Topics	Second Level Topics
	Visualization Guide	<a href="#">Visualization Tools</a>  <a href="#">Dashboards</a>  <a href="#">Vulnerability Map</a>
Administer	PCE Administration Guide	<a href="#">Overview of PCE Administration</a>  <a href="#">Connectivity Configuration for PCE</a>  <a href="#">Access Configuration for PCE</a>  <a href="#">PCE Troubleshooting</a>
	VEN Administration Guide	<a href="#">Overview of VEN Administration</a>  <a href="#">VEN State</a>  <a href="#">VEN Deactivation and Unpairing</a>  <a href="#">Monitor and Diagnose VEN Status</a>
	Events Administration Guide	<a href="#">Overview of Events Administration</a>  <a href="#">Events Described</a>  <a href="#">Events Setup</a>  <a href="#">Traffic Flow Summaries</a>
	PCE CLI Tool Guide	<a href="#">Overview of the CLI Tool</a>  <a href="#">Installation and Authentication</a>  <a href="#">CLI Tool Commands for Resources</a>  <a href="#">CLI Tool Tutorials</a>
Develop	REST API Developer Guide	<a href="#">REST API Reference</a>
	<a href="#">REST API Public Schemas 24.3 (Zipped File),</a>  <a href="#">REST API Public Schemas 24.2.10 (Zipped File)</a>	
	<a href="#">24.3 OpenAPI Specification (JSON)</a>  <a href="#">24.2.10 OpenAPI Specification (JSON)</a>	

Top-Level Category/Topics	New Location for Category/Topics	Second Level Topics
	<a href="#">Illumio Core REST API Getting Started Guide</a>  This content is retired and no longer available.	
Connect	<a href="#">Flowlink Configuration and Usage Guide</a>	<a href="#">Flowlink Configuration</a>  <a href="#">Flowlink Usage</a>
	<a href="#">NEN Installation and Usage Guide</a>	<a href="#">NEN Installation and Configuration</a>  <a href="#">Load Balancers and Virtual Servers for the NEN</a>  <a href="#">NEN Integration with Switches</a>
Support	<a href="#">Knowledge Base</a>	
	<a href="#">Training</a>	
	<a href="#">Community</a>	
	<a href="#">Contact Support</a>	
	<a href="#">Documentation Archives</a>	
	<a href="#">Legal Notices</a>	
	<a href="#">Open Source Licensing Disclosure</a>	
	<a href="#">Illumio 24.2 Documentation Library</a>	
Archived Documentation	<a href="#">Log in to view archived documentation on Support.</a>	

## Cloud

**Table 5. New Locations for the Illumio Documentation: Cloud**

Top-Level Category/Topics	New Location for Category/Topics
Get Started	<a href="#">Getting Started</a>
Release Notes	<a href="#">Current Release Notes</a>
Visualize	<a href="#">Visualize</a>
Define	<a href="#">Define Deployments and Applications</a>
Policy	<a href="#">Policy Model</a>

Top-Level Category/Topics	New Location for Category/Topics
Administer	<a href="#">User Management</a>
Reference	<a href="#">Onboarding AWS</a>
Support	<a href="#">Legal Notices</a>
	<a href="#">Knowledge Base</a>
	<a href="#">Training</a>
	<a href="#">Community</a>
	<a href="#">Contact Support</a>

## Other Products: Edge, Xpress, MSP

**Table 6. New Locations for the Illumio Documentation: Edge, Xpress, MSP**

Top-Level Category/Topics	New Location for Category/Topics
Other Products	<a href="#">Edge 22.31</a>
	<a href="#">Xpress</a>
	<a href="#">MSP</a>

## Integrations

**Table 7. New Locations for the Illumio Documentation: Integrations**

Integration	Description	New Location for Documentation and Link to App	Validated Compatibility
Ansible	Ansible modules for <ul style="list-style-type: none"> <li>• VEN and C-VEN pairing</li> <li>• Label creation/update/removal</li> </ul>	<a href="#">0.2.6</a> <a href="#">Ansible Website</a>	Ansible 2.12+PCE 22.5, 22.2, 21.5, 21.2, SaaS
IBM QRadar (SIEM)	Connector and Dashboards to view Illumio flow and event data	<a href="#">1.4</a> <a href="#">1.4 Integration Guide: PDF</a> <a href="#">1.3</a>	QRadar 7.4.3+ PCE 24.1 (SaaS), 23.5, 23.2, 22.5, and 21.5 QRadar 7.4.1+ PCE 21.2, 19.3, SaaS

Integration	Description	New Location for Documentation and Link to App	Validated Compatibility
IBM QRadar (SOAR)	Provides a selective port-blocking playbook	1.0 <a href="#">User Guide: PDF</a>	PCE 21.2+, SaaS
Netskope Cloud Exchange	Ensures dynamic access controls and security across hybrid and multi-cloud environments	<a href="#">1.0.0 Integration Guide: PDF</a>	
Palo Alto Cortex (SOAR)	Provides a selective port-blocking playbook	1.0.1 <a href="#">Configuration Guide</a> <a href="#">Port Blocking Playbook Guide</a>	Cortex 6.0 (6.2, 6.5, 6.8, and master), PCE 22.2, 21.5, 21.2, SaaS
Python SDK	Python REST client for Illumio PCE APIs	1.1.3 <a href="#">User Guide</a>	PCE 21.2+, SaaS
Sentinel	Azure function Apps for data ingestion, Analytics rules	3.2.2 <a href="#">Integration Guide : PDF</a>	PCE SaaS
ServiceNow (CMDB)	Uses ServiceNow as the source of truth for labeling PCE workloads with R/A/E/L labels	2.1.0 <a href="#">Installation and Configuration Guide: PDF</a>	Vancouver, Washington DC, Xanadu  PCE 22.5, 23.2.30, 23.5.20, 24.2.10, or SaaS
Splunk (SIEM)	Connector and Dashboards to view Illumio flow and event data	<a href="#">TA-Illumio 3.2.3</a> <a href="#">Illumio App for Splunk</a> <a href="#">User Guide v3.2.3 (PDF)</a>  <a href="#">EULA</a> <a href="#">TA-Illumio 4.0.2</a>  <a href="#">Illumio App for Splunk 4.0.1</a> <a href="#">Integration Guide 4.0: PDF</a>	For 3.2.3:  Splunk 9.1, 9.0, 8.2, 8.1 + PCE 21.2, 21.5, 22.2, 22.5, and SaaS  For 4.0.2:  Splunk 9.3, 9.2, 9.1, 9.0, 8.2, 8.1 + PCE 21.5, 22.2, 22.5, 23.2, 23.5, and SaaS
Terraform	Terraform HCL scripts to manage PCE policy and policy objects	1.1.4 <a href="#">User Guide</a>	Terraform 1.4+  PCE 22.5, 22.2, 21.5, 21.2, SaaS

## PDF Library

Download PDFs for version 24.4. If you need a PDF that's not listed in this library, send a request to [Illumio Documentation](#).



### NOTE

Documentation versions 21.2 and earlier are archived and available as PDFs from the [Documentation Archives](#) library. You must log in to get access.

## PDFs for Core 24.4

PDF	Description
What's New and Release Notes	
<a href="#">What's New and Release Notes for 24.4</a>	Provides a list of new and updated features in version 24.4. Describes resolved issues and known issues and applicable workarounds.
<a href="#">What's New and Release Notes in 24.2.x</a>	Provides a list of new and updated features in version 24.2.11, 24.2.10, and 24.2.0. Describes resolved issues and known issues and applicable workarounds.
<a href="#">What's New and Release Notes in 23.5</a>	Provides a list of new and updated features in version 23.5. Describes resolved issues and known issues and their workarounds for the Illumio Core 23.5.x release.
<a href="#">Illumio Core for Kubernetes and OpenShift 5.1.x</a>	Describes the resolved issues and related information for several Illumio Core for Kubernetes releases, formerly known as Illumio Containerized VEN, or C-VEN. Illumio Core for Kubernetes also includes the related required component, Kubelink. Because of this heritage, many references to this product as "C-VEN" are still used throughout the documentation.
NEN Release Notes, versions 2.6.x through 2.0.0	Describes resolved issues and known issues and their workarounds for the Illumio Network Enforcement Node (NEN). <ul style="list-style-type: none"> <li>• <a href="#">2.6.x</a></li> <li>• <a href="#">2.5.x</a>,</li> <li>• <a href="#">2.4.x</a></li> <li>• <a href="#">2.3.x</a></li> <li>• <a href="#">2.1.1</a></li> <li>• <a href="#">2.0.0</a></li> </ul>
Install, Configure, and Upgrade Guides	
<a href="#">24.4 Install, Configure, Upgrade (NEN, VEN, LW-VEN, Kubernetes and Openshift)</a>	A combined installation guide for 24.4 NEN, VEN, Legacy Windows VEN (LW-VEN), Kubernetes and Openshift.
<a href="#">VEN Installation and Upgrade Guide 24.2.10</a>	Provides installation and upgrade information for VENs on the hosts in your environment.

PDF	Description
<a href="#">NEN Installation and Usage Guide 24.2.10</a>	Learn how to install the Illumio Network Enforcement Node (NEN), configure switches to work with it, and use the NEN to secure workloads that are attached to network switches.
<a href="#">LW-VEN Installation and Configuration Guide 24.2.10</a>	Learn how to install and use the Legacy Windows VEN (LW-VEN) with the Illumio Core PCE to enforce security policies on computers running the Windows Server 2003 SP1 and SP2 or Windows Server 2008 SP1 and SP2 operating system.
<a href="#">Administration Guide</a>	
<a href="#">24.4 Administration Guide</a>	A combined administration guide for 24.4 NEN, VEN, Legacy Windows VEN (LW-VEN), and Kubernetes and Openshift.
<a href="#">Events Administration Guide</a>	Learn how to control the behavior of the PCE as it records events and how to change event-related settings in the PCE web console.
<a href="#">PCE Administration Guide</a>	Learn how to maintain and operate the Policy Compute Engine (PCE). This guide also includes other important tasks required to manage your PCE deployment.
<a href="#">VEN Administration Guide</a>	Learn how to manage the VENs that you have installed on the hosts in your environment. This guide provides information about VEN functionality and explains how to troubleshoot issues with the VENs in your environment.
<a href="#">REST API Developer Guide</a>	
<a href="#">REST API Developer Guide 24.4</a>	Learn about the Illumio Core REST APIs.
<a href="#">REST API Developer Guide 24.2.10</a>	Learn about the Illumio Core REST APIs.
<a href="#">User Guides</a>	
<a href="#">Visualization Guide 24.4</a>	Describes the Illumio Core Visualization tools, the problems they solve, some use cases, and examples for 24.4.
<a href="#">Visualization Guide 24.2.10</a>	Describes the Illumio Core Visualization tools, the problems they solve, some use cases, and examples.
<a href="#">Security Policy Guide 24.4</a>	Learn about new and updated features in the 24.4 version of the security policy including the policy objects.
<a href="#">Security Policy Guide 24.2.10</a>	Learn about the Illumio Core security policy including the policy objects. Get guidance about designing a label schema and learn about recommended approaches for Illumio's security policy design including how to create rulesets and rules.
<a href="#">Flowlink Configuration and Usage Guide</a>	Learn about Flowlink, an Illumio-provided standalone application to collect network flow data from different network sources, and its configuration and known limitations.
<a href="#">Application Ringfencing</a>	The Application Ringfencing tutorial is divided into a series of lessons. The lessons correspond to the major phases of creating an application ringfence in your environment and are organized according to the workflow for creating an application ringfence.
<a href="#">Using XPress User Guide</a>	Describes how to use the Xpress features to onboard servers and endpoints.
<a href="#">Edge User Guide 22.31</a>	Describes the new features, enhancements, and platform support for the Illumio Edge 22.31.

PDF	Description
<a href="#">Managed Services Portal User Guide</a>	Describes how to use MSP to onboard your customers in to Illumio Core, Illumio Xpress, and Illumio Edge in the Illumio Cloud and then manage and administer those Illumio products on their behalf.

## PDFs for Older Releases

Guide	Description
CLI Tool Release Notes and Containerized VEN Release Notes	
<a href="#">Illumio Core CLI Tool Release Notes 1.4.2</a>	These release notes describe the new features and enhancements for the Illumio Core Advanced Command-line Interface Tool 1.4.2 release. For more information about the CLI, see the Illumio Core PCE CLI Tool Guide, which describes the installation, setup, usage, and tutorials for the CLI tool.
<a href="#">Illumio Core PCE CLI Tool Guide 1.4.2</a>	This guide provides an overview of the CLI Tool, describes how to install and authenticate it, and provides CLI Tools commands for resources.
<a href="#">Illumio Containerized VEN Release Notes 21.5.15</a>	These release notes describe the resolved issues and known issues for the Illumio Containerized VEN 21.5.15 release.
Kubernetes and OpenShift Release Notes and User Guides	
<a href="#">Illumio Core for Kubernetes Release Notes 3.0.0</a>	This document describes the resolved issues and related information for the 3.0.0 release of Illumio Core for Kubernetes, formerly known as Illumio Containerized VEN, or C-VEN.
<a href="#">Illumio Core for Kubernetes Release Notes 3.1.0</a>	This document describes the resolved issues and related information for the 3.1.0 release of Illumio Core for Kubernetes, formerly known as Illumio Containerized VEN, or C-VEN.
<a href="#">Illumio Core for Kubernetes Release Notes 4.0.0</a>	This document describes the resolved issues and related information for the 4.0.0 release of Illumio Core for Kubernetes, formerly known as Illumio Containerized VEN, or C-VEN.
<a href="#">Illumio Core for Kubernetes Release Notes 4.1.0</a>	This document describes the resolved issues and related information for the 4.1.0 release of Illumio Core for Kubernetes, formerly known as Illumio Containerized VEN, or C-VEN.
<a href="#">Illumio Core for Kubernetes Release Notes 4.2.0</a>	This document describes the resolved issues and related information for the 4.2.0 release of Illumio Core for Kubernetes, formerly known as Illumio Containerized VEN, or C-VEN.
<a href="#">Illumio Core for Kubernetes Release Notes 5.2</a>	These release notes describe the resolved issues, known issues, and related information for the 5.2.x releases of Illumio Core for Kubernetes, formerly known as Illumio Containerized VEN, or C-VEN.
<a href="#">Illumio Core for Kubernetes and OpenShift Guide 4.1</a>	This guide explains how deploy the Illumio Core with Kubernetes or OpenShift on your distributed, on-premises and cloud systems.
<a href="#">Illumio Core for Kubernetes and OpenShift Guide 4.2</a>	This guide explains how deploy the Illumio Core with Kubernetes or OpenShift on your distributed, on-premises and cloud systems.
Kubelink	
<a href="#">Illumio Kubelink Release Notes 2.0.2</a>	These release notes describe the enhancements, resolved, and known issues for the Illumio Kubelink 2.0.2 release.



Guide	Description
<a href="#">Illumio Kubelink Release Notes 2.1.1</a>	These release notes describe the enhancements, resolved, and known issues for the Illumio Kubelink 2.1.1 release and earlier releases.
Flowlink	
<a href="#">Illumio Flowlink Release Notes 1.2.2</a>	These release notes describe the enhancements, resolved, and known issues for the Illumio FlowLink 1.2.2 release.
<a href="#">Illumio FlowLink Release Notes 1.3.0</a>	These release notes describe the enhancements, resolved, and known issues for the Illumio FlowLink 1.3.0 release.
NEN and LW-VEN Installation and Configuration PDFs	
<a href="#">Illumio NEN Installation and Usage Guide 2.3.10</a>	This guide introduces the Illumio Network Enforcement Node and describes how to install and configure it and how to integrate the NEN with load balancers and switches.
<a href="#">Illumio NEN Installation and Usage Guide 2.4.10</a>	This guide introduces the Illumio Network Enforcement Node and describes how to install and configure it and how to integrate the NEN with load balancers and switches.
<a href="#">Illumio NEN Installation and Usage Guide 2.5.2</a>	This guide introduces the Illumio Network Enforcement Node and describes how to install and configure it and how to integrate the NEN with load balancers and switches.
<a href="#">Illumio NEN Installation and Usage Guide 2.6.0</a>	This guide introduces the Illumio Network Enforcement Node and describes how to install and configure it and how to integrate the NEN with load balancers and switches.
<a href="#">Illumio NEN Installation and Usage Guide 2.6.10</a>	This guide introduces the Illumio Network Enforcement Node and describes how to install and configure it and how to integrate the NEN with load balancers and switches.
<a href="#">Illumio NEN Installation and Usage Guide 2.6.30</a>	This guide introduces the Illumio Network Enforcement Node and describes how to install and configure it and how to integrate the NEN with load balancers and switches.
<a href="#">Illumio LW-VEN Installation and Configuration Guide 1.0.10</a>	This guide describes the Illumio LW-VEN requirements and how to install and configure the service.
<a href="#">Illumio LW-VEN Installation and Configuration Guide 1.1.0</a>	This guide describes the Illumio LW-VEN requirements and how to install and configure the service.

## Legal Notice

Copyright © 2024 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](#)