TECHNICAL
DOCUMENTATION

Endpoint User Guide

This guide provides procedures and references for installing, deploying, and administering Endpoint VENs. It includes information about the Endpoint Dashboard, ruleset and labeling guidelines, and a typical deployment workflow.

Table of Contents

Legal Notice 4
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

Using Endpoint 10
- About Endpoint 10
- Endpoint Dashboard 10
  - Working with the Endpoint Dashboard 10
  - Endpoint Statistics 11
- Install, Deploy, and Adminster Endpoints 11
  - VEN guide references 11
  - Typical Workflow 12
  - macOS Endpoint-specific Procedures 13
  - Add Public IP addresses to the Corporate Public IPs list 14
- Ruleset and Labeling Guidelines for Endpoints 14
  - Label Endpoints 14
  - About Rulesets That Use Workload Subnets for Endpoints 15
  - Create Rulesets that Use Workload Subnets for Endpoints 15

Legal Notice

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

Resources

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

Contact Information

- Contact Illumio
- Contact Illumio Legal
- Contact Illumio Documentation

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.

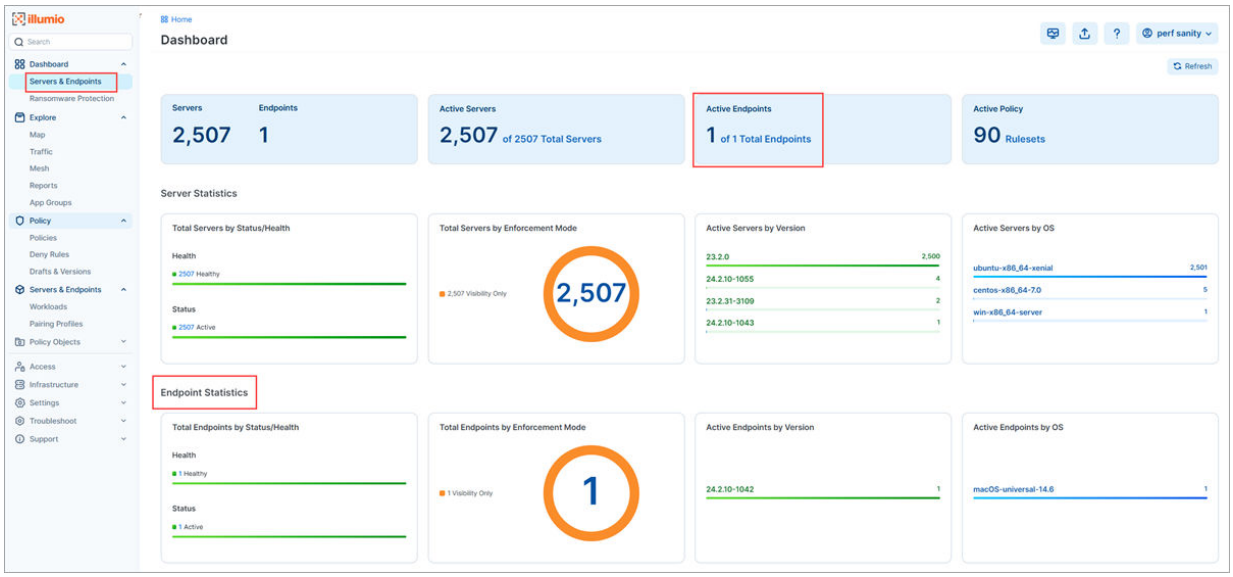
Using Endpoint

About Endpoint

This guide provides procedures and references for installing, deploying, and administering Endpoint VENs. It includes information about the Endpoint Dashboard, ruleset and labeling guidelines, and a typical deployment workflow.

Endpoint Dashboard

Endpoint widgets on the Servers & Endpoints dashboard provide broad information to help you focus on the data you are interested in.



Working with the Endpoint Dashboard

To access Dashboards, click **Dashboard > Servers & Endpoints** in the left menu.

The Endpoint Dashboard uses an API to aggregate various data from the system. For more information about the API support, see Endpoint Dashboard APIs in the REST API Developer Guide.

NOTE
Only the following two user roles are allowed to use the Endpoint Dashboard:

- Global Org Owners
- Global Administrators

Endpoint Statistics

The Endpoint Statistics section of the Dashboard contains several widgets to display summary statistics or status. To get fresh data, click Refresh at the upper right corner of the page. To see more details, click the widget and the list page appears.

- Total active Endpoints (located at the top of the page)
- Total Endpoints by Status/Health
  - Status (stopped, suspended, uninstalling, and active statuses)
  - Health (error, warning, and healthy)
- Total Endpoints by Enforcement Mode
  - Idle
  - Visibility only
  - Selective Enforcement
  - Full
- Active Endpoints by Version
- Active Endpoints by operating system (OS)

Install, Deploy, and Adminster Endpoints

For most installation and activation tasks, you can refer to topics in the VEN Installation and Upgrade Guide and VEN Administration Guide. The procedures and concepts in those guides apply almost equally to Endpoint VENs and Server VENs.

NOTE
Before installing and configuring Illumio Endpoints, see "Endpoint Specification and Requirements" in the Endpoint Concepts Guide.

VEN guide references

Endpoint VEN Installation and Upgrade information

See these topics in the VEN Installation and Upgrade Guide:

- Ways to Install the VEN
- Prepare for VEN Installation

- Set up PCE for VEN Installation
- VEN Installation & Upgrade Using VEN Library
- VEN Installation & Upgrade with VEN CTL
  - With VEN releases 24.2 and later, you can Deploy an Illumio Endpoint VEN as a private app using Intune.
- Reference

Endpoint VEN Administration

See these topics in the VEN Administration Guide:

- Overview of VEN Administration
- VEN State
- VEN Deactivation and Unpairing
- Monitor and Diagnose VEN Status

Typical Workflow

Illumio suggests this typical workflow for deploying Endpoint VENs:

Task 1: Create Labels for Endpoints

To help you distinguish endpoints from other workloads on the PCE, Illumio recommends that you assign them a common **Application** label such as "Endpoints" and use the **Role** label type for endpoint sub-groups. Use these conventions consistently throughout your implementation.

IMPORTANT

See Label Endpoints [14] for guidance on labeling endpoints. For general information about labeling, see also "Labels and Label Groups" in the Security Policy Guide.

Task 2: Add Corporate Public IPs if Using Azure AD

See Add Public IP addresses to the Corporate Public IPs list [14].

Task 3: Create or Modify a Ruleset for Endpoints

Create or modify a ruleset to define the allowed communication between endpoints and servers. See Create Rulesets that Use Workload Subnets for Endpoints [15].

Task 4: Install and Activate VENs in Endpoint Mode

For most installation and activation tasks, you can refer to topics in the VEN Installation and Upgrade Guide and the VEN Administration Guide. The procedures and concepts in those guides apply almost equally to Endpoint VENs and Server VENs.

IMPORTANT

When creating a Pairing Profile for an Endpoint VEN, you must select **Endpoint VEN** in the **Servers & Workloads > Pairing Profiles > Enforcement Node Type** setting. (Conversely, the Enforcement Mode Type for for Server VENs requires the Server VEN setting.) Endpoint mode is required for visualizing and segmenting endpoints from the Core PCE.

TIP

You can also install VENs remotely on multiple endpoints using a network provisioning tool. See Install and Deploy Multiple macOS Endpoint VENs [13].

macOS Endpoint-specific Procedures

This topic includes procedures that apply specifically to macOS Endpoints.

Install a single macOS Endpoint VEN

Perform these steps through the macOS UI.

1. Double-click the package:
   `illumio-ven-<version>-<build#>.mac.universal.pkg`
2. Follow the instructions in the installation dialogs.

The VEN binaries are installed in the following directory: `/opt/illumo_ven`

The VEN data binaries are installed in the following directory: `/opt/illumo_ven_data`

Uninstall a macOS Endpoint VEN

To uninstall a macOS Endpoint VEN from a command line, issue the following command:

```
sudo /opt/illumio_ven/illumio-ven-ctl unpair saved
```

To uninstall the macOS VEN software through the PCE web console:

1. **Workload** > **VENs** > (*select the VEN*) > **Unpair**
2. Activate the VEN. See "VEN Activate Command Reference" in the VEN Installation and Upgrade Guide.

Install and Deploy Multiple macOS Endpoint VENs

This procedure describes how to use Jamf to install and deploy VENs remotely on multiple endpoints. You can also use other macOS-supported network provisioning tools.

1. Download the installation package through the PCE web console.

2. Go to the Jamf Pro console, and locate and upload the package and the registration script.
3. Through the registration script, register the VEN to the PCE. For example:

   ```
   /opt/illumio_ven/illumio-ven-ctl activate -m <PCE_host>.ilabs.io:8443 -a <PCE_ID>
   ```
4. Create a policy to use the package and script.
5. Set the trigger and scope.

Add Public IP addresses to the Corporate Public IPs list

Illumio supports Network Location Awareness for endpoints. To enable your Endpoint VENs to detect interfaces connected to your corporate network, you must specify in the PCE (**Servers > Workloads > Corporate Public IPs**) the public IP addresses that your corporate network uses for endpoints. Once you've specified these IP addresses in the PCE, Endpoint VENs send network profile detection requests to the PCE. These requests (as seen by the PCE) appear to originate from your organization's public IP addresses.

For details, see "NLA Support for Endpoints" in the Endpoint Concepts Guide.

1. Go to **Servers > Endpoints**.
2. Obtain workload interface information:
   a. Click the workload you're interested in to open its details page.
   b. On the **Summary** tab, scroll to **Interfaces**.
   c. Make note of the IP addresses labeled (External) (Public) that you want the PCE to classify as Corporate.
3. Go to **Settings > Corporate Public IPs**.
4. Click **Edit** and enter the desired public IP addresses in the **Addresses** field as single addresses or as CIDR blocks (click the tooltip for formatting help).
5. Click **Save**.

Ruleset and Labeling Guidelines for Endpoints

CAUTION

Illumio strongly recommends that you follow these guidelines creating rulesets and labels for endpoints. When you enforce policy on servers for clients that change their IP addresses frequently, the policy enforcement points (PEPs) continuously need to update security rules for IP address changes. These frequent changes can cause performance and scale challenges and the ipsets of protected workloads to churn.

Label Endpoints

Because endpoints paired to a Core PCE appear like any other workload, label them in a way that makes them easily distinguishable from other workloads. Illumio recommends that you

label endpoints with a single Application label such as "Endpoints" and use the Role label type for endpoint sub-groups. Use these conventions consistently throughout your implementation.

About Rulesets That Use Workload Subnets for Endpoints

When you create policies that allow endpoints to communicate with destination servers, Illumio recommends that you use the endpoints' subnets for enforcement on the servers rather than the individual IP addresses. You can do this using the "Use Workload Subnets" option when writing rules that apply to endpoints. In general, take this approach:

1. Write your endpoint to server policies using labels, as you would write any other policy.
2. If the provider or consumer of a rule includes endpoints (either by using the endpoint label directly, or by using "All Workloads), select "Use Workload Subnets" on that side of the rule. You can do this by enabling "Advanced Options" in the provider/consumer drop down, and then clicking on "Use Workload Subnets".
3. Be careful with broad, label-based rulesets that do not use endpoint subnets, such as **All** | **All** | **All** that specify broad environments or locations, or rulesets that involve large sets of server workloads. Providers in these situations are particularly susceptible to frequent policy changes caused by changes to endpoint network connectivity. As an example for scenarios to avoid, suppose your endpoints are consuming services provided by Active Directory (AD) servers and your endpoint policies specify the AD server's labels without specifying **Use Workload Subnets** on the consumer. In this label-to-label policy scenario involving endpoints, any change in endpoint connectivity triggers policy updates on the AD servers. Because the network connections on endpoints tend to change frequently, firewall policy on the AD servers also change frequently. Depending on the size of your implementation, churn could be significant. However, if **Use Workload Subnets** is enabled, the firewall policy on the AD servers only needs to be updated when the list of subnets change, not when individual IPs change. This leads to significantly fewer firewall updates, faster policy convergence, and potentially a better experience for end users who are connecting to applications from Illumio-managed endpoints.

   Use Workload Subnets

   When **Use Workload Subnets** is selected, the PCE auto-detects the subnets based on the IP addresses and netmasks reported by all VENs with those labels. For example, if **Use Workload Subnets** is used with the `A:Endpoint` application label, the peer servers are programmed with the subnets from all workloads with the `A:Endpoint` label.
   - If **Use Workload Subnets** is used with the `A:Endpoint` application label and the `L:US` location label, the peer servers are programmed with the subnets from all workloads with both the `A:Endpoint` and `L:US` labels.
   - If workloads with the labels `A:Endpoint` and `L:EU` are in a disjoint subnet from the `A:Endpoint` and `L:US` workloads, the EU subnets are not programmed on the peer servers.

Create Rulesets that Use Workload Subnets for Endpoints

Add or edit a rule:

1. Go to **Rulesets and Rules** > **Rulesets**.
2. Click on a ruleset > **Rules**.
3. Locate a consumer and click the edit (pencil) icon > under **Consumers**.

4. Click the down arrow and choose **Use Workload Subnets**.