TECHNICAL
DOCUMENTATION

Endpoint Concepts Guide

Published: 2024

Illumio Endpoint is a type of Virtual Enforcement Node (VEN) that allows you to visualize and segment workloads running on both Windows and macOS endpoints accessible by the PCE. Illumio Endpoint lets you manage and secure endpoint workloads efficiently, whether they are domain-joined or not, across wired, wireless, and VPN network interfaces.

Table of Contents

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.

Endpoint Concepts

Overview of Endpoint Concepts

Illumio Endpoint is a Virtual Enforcement Node (VEN) that allows you to visualize and segment workloads running on Windows and macOS endpoints accessible by the PCE. These are typically highly-mobile laptops that your team members use outside of your corporate security perimeter. Illumio Endpoint lets you manage and secure endpoint workloads efficiently, whether they are domain-joined or not, across wired, wireless, and VPN network interfaces.

Illumio Endpoints Benefits

- **Endpoint traffic visibility**. Obtain a comprehensive view of all endpoint workloads, including both wired and wireless connections.
- **Deny by default.** Block all but necessary communication to and from laptops, VDIs and workstations.
- **Limit zero-day risk**. Protect your environment without waiting for an attack to create a signature and be detected by your security tools.
- **Zero touch to the network**. Use endpoint segmentation that is not tied to the network, unlike NAC or SD-WAN.
- **Dynamic policy management**. Create and enforce security policies tailored to endpoints and automatically change those policies when the device is used outside of the corporate environment.

Differences from Server VENs

While Endpoint VENs are nearly identical to Server VENs, they do differ in the following ways:

- When creating a Pairing Profile for an Endpoint VEN, you must select **Endpoint VEN** in the **Servers & Workloads > Pairing Profiles > Enforcement Node Type**. (Conversely, the Enforcement Mode Type for Server VENs requires the Server VEN setting.)
- Endpoint VENs don't support SecureConnect or AdminConnect.
- Endpoint VENs support wireless connections and VPNs.

Endpoint VEN on macOS does not support the following features:

- Process-based policy
- Adaptive User Segmentation (AUS)
- Aggressive tamper detection
- Kerberos authentication
- Installation on server workloads

Illumio Endpoint Specifications and Requirements

Illumio Endpoints support the following configurations:

Illumio Environment

- **Illumio Core SaaS**: Illumio Core PCE 22.2.0 and later releases.
- **Illumio Core On-prem**: 21.5.11 or 21.5.20 VEN and later releases.

Customer Environment

- Computers running these Windows versions:
  - Windows 7
  - Windows 10
- Computers running these macOS versions:
  - 14.0, 14.1, 14.2, and 14.3 (Sonoma)
  - 13.x (Ventura)
  - 12.x (Monterey)
  - 11.0 (formerly 10.16) (Big Sur)
- Supported domain-joined endpoint interfaces:
  - Wired
  - Wireless
  - PPP/VPN

NOTE

Endpoint segmentation is not compatible with hypervisors such as Windows Hyper-V. The connectivity to or from virtual machines might be blocked if the Endpoint VEN is in Full Enforcement mode.

Wireless Connections and VPNs

To activate a VEN installed on endpoints and to support a wireless network connection, the **Enforcement Type** in the Pairing Profile must be set to **Endpoint VEN**.

NOTE

When creating a Pairing Profile with the Endpoint **Enforcement Type**, the Illumio VEN detects two additional interface types on the endpoint: WLAN/802.11 and PPP. To detect these interface types, the endpoint must be domain authenticated with the corporate domain.

The VPN and WiFi interfaces must be domain authenticated for on-prem domain-joined systems, or within the corporate range for Additional Authenticated Data (AAD)-joined systems. The VPN must report an interface type of Ethernet, tunnel, or PPP. (AnyConnect reports the Ethernet interface type.)

NOTE

Wireless network support is only available for Illumio Endpoints. No support is provided for other server types, such as bare-metal servers, virtual machines (VMs), or container hosts.

About macOS Endpoint

Endpoint VENs support macOS versions listed in Illumio Endpoint Specifications and Requirements [11]. The macOS VEN software package is a universal binary that can be installed on Intel and ARM Mac platforms. You can use the macOS VEN to write policies for corporate (BRN network) and external (non-BRN network) interfaces.

Endpoint on macOS reports interfaces of the following types when they are active:

- Ethernet
- USB Ethernet
- IP over Thunderbolt
- Wi-Fi
- Tunnel (utun)

For troubleshooting purposes, use the `ifconfig -v` command and filter out the interface of the before mentioned types with the status of `active`. Use the `scutil --nwi` command and filter out entries with `utun`.

The Endpoint on macOS supports the following third-party products:

- CrowdStrike
- Palo Alto Networks Global Protect
- Cisco AnyConnect VPN

NLA Support for Endpoints

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.

When those IP addresses fall within the range of the corporate public IP addresses entered in the PCE, the PCE recognizes that endpoint interface as a corporate interface. If an endpoint interface's IP address is outside the specified range, the PCE recognizes that interface as an external interface.

Endpoint VENs enforce the corporate firewall policies that are calculated by the PCE but only for the interfaces connected to the corporate network. The existing firewalls on endpoints, such as the Windows Firewall, manage non-corporate or “external” interfaces on endpoints.

In the workload details pages in the PCE (**Servers > Workloads > Workloads**), the word Public is prepended to the IP address (as seen by the PCE) of non-domain-joined Windows workloads and macOS endpoint interfaces reachable by the PCE. When you enter these Public IP addresses in the PCE (**Settings > Corporate Public IP**), the PCE classifies them as Corporate and programs their corresponding endpoint interfaces with the appropriate Illumio security policies.

For the procedure, see "Add a public IP address to the Corporate Public IPs list" in the Endpoint User Guide.

Non-corporate (External) Interface Support

Illumio Core Cloud supports writing policies for both corporate and non-corporate (external) interfaces on endpoints using Illumio Core Cloud version 22.3 and later releases and the endpoint VEN.

Endpoint VENs for Windows recognize both corporate and non-corporate interfaces in on-premises AD, Azure AD, and hybrid AD environments.

The Endpoint VENs for macOS recognize both corporate and non-corporate interfaces.

About Non-corporate Interfaces

In Illumio Core, corporate interfaces are defined as interfaces that are domain authenticated, such as an endpoint’s VPN interface or any interface connected to a Microsoft Active Directory (AD) domain. Non-corporate (external) interfaces are defined as interfaces that connect to all other networks that the endpoint connects to, such as home wireless networks or public networks. These networks are not domain authenticated.

No connectivity is expected between endpoints off the corporate network. Therefore, rules for non-corporate interfaces are only supported between labels (or workloads) and IP lists. Rules between workloads and labels are not supported for the non-corporate network, nor between corporate and non-corporate networks. The endpoint VEN reports the IP addresses of non-corporate interfaces and the traffic flows observed on those interfaces to the PCE.

Backward Compatibility

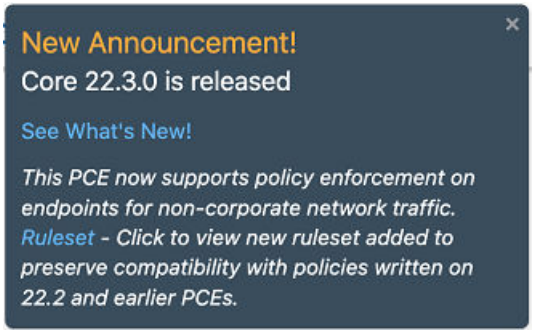
Prior to Illumio Core Cloud version 22.3, the VEN did not manage or report any traffic on non-corporate interfaces. Even in full enforcement, traffic on non-corporate interfaces was ignored by the firewall policy managed by the VEN.

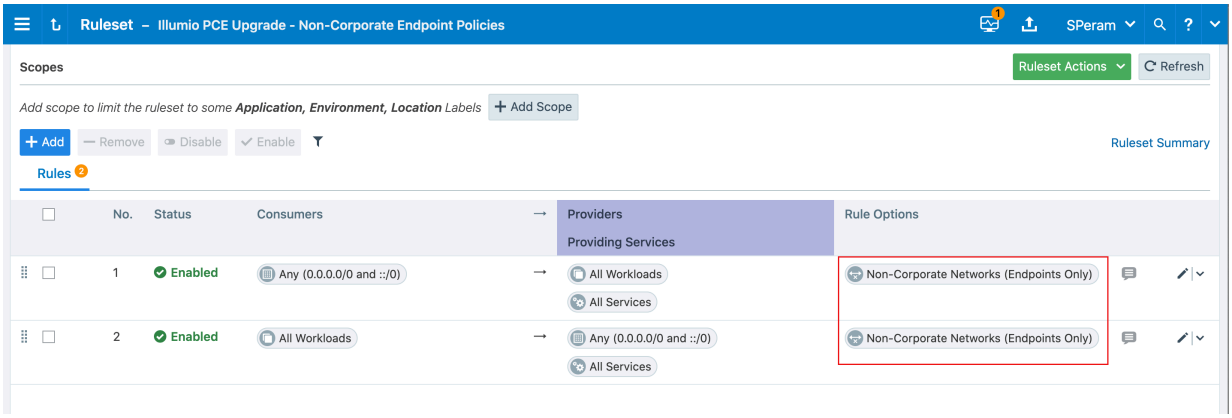
After the upgrade to the 22.3, the Illumio Core will enforce all traffic, including traffic on non-corporate interfaces, by using the Illumio firewall policy.

IMPORTANT

To use this additional enforcement functionality, you must be running the 22.3.0 PCE and later releases and the 22.3.0 endpoint VEN and later releases. Even after the upgrade to 22.3.0, the Illumio Core will not provide visibility or enforcement of traffic on non-corporate networks until the endpoint VEN is upgraded.

To preserve backward compatibility, if any endpoints are paired to Illumio Core Cloud prior to the upgrade to 22.3.0, Illumio will automatically insert a ruleset named "Illumio PCE Upgrade – Non-Corporate Endpoint Policies". This ruleset preserves the enforcement behavior of earlier endpoint VENs on the 22.3.0 endpoint VEN by explicitly allowing all traffic on non-corporate interfaces. After implementing your desired policies for non-corporate interfaces, you may modify or delete this ruleset.

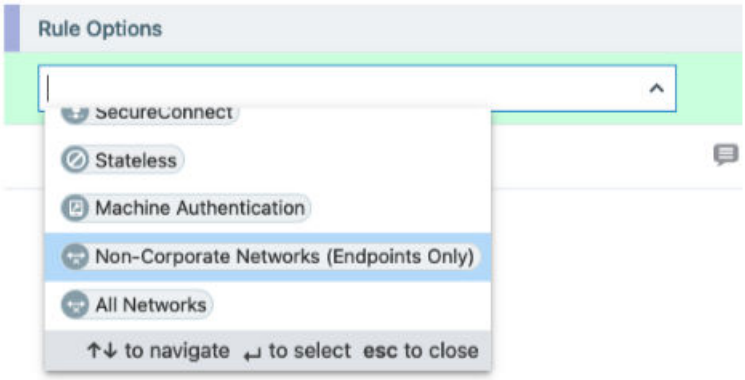




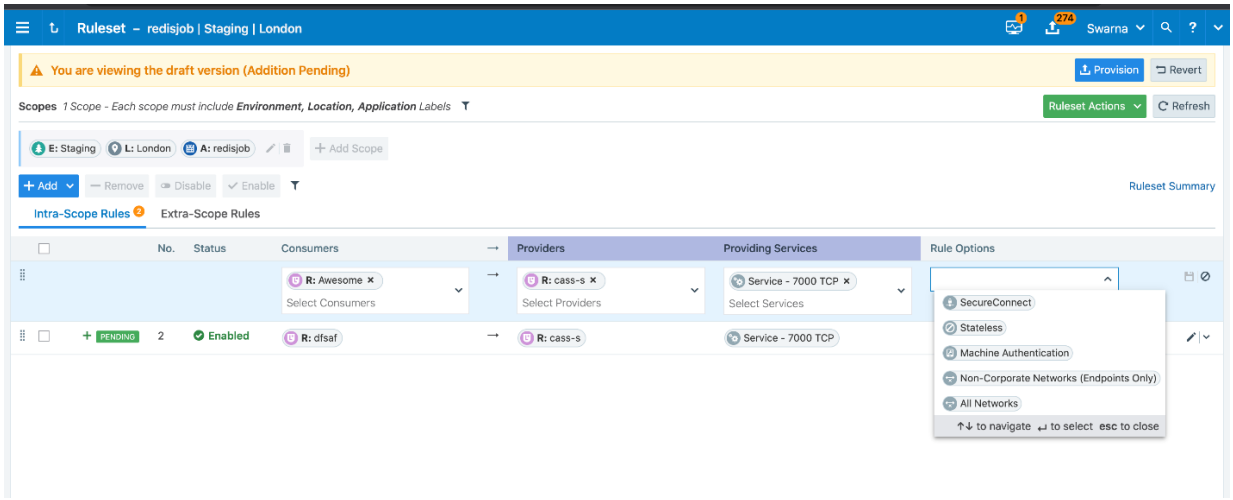
Writing Rules with Network Profiles

You can use network profiles on rules and Enforcement Boundaries to specify the endpoint interfaces affected by the rRule or Enforcement Boundary. If you don't specify a network profile, the default network profile on a rule or Enforcement Boundary is **Corporate**, which applies to all servers and corporate interfaces on endpoints. You have the option to choose **Non-Corporate Networks (Endpoints only)**. The rule or Enforcement Boundary applies only to non-corporate interfaces on endpoints. Servers cannot have non-corporate interfaces.

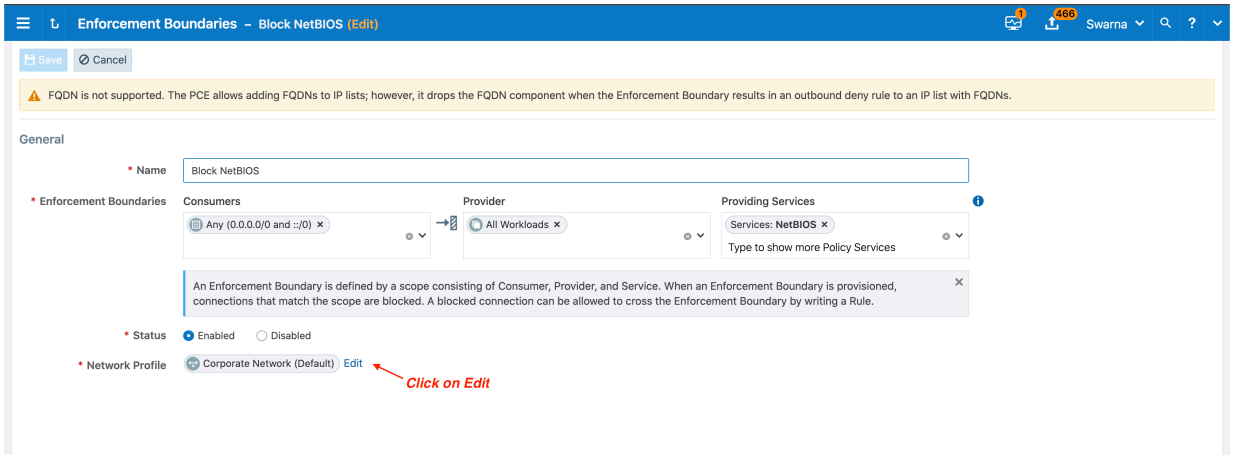
When either the **Non-Corporate Networks** or **All Networks** option is selected, the rule must only use IP lists in either the provider or the consumer.

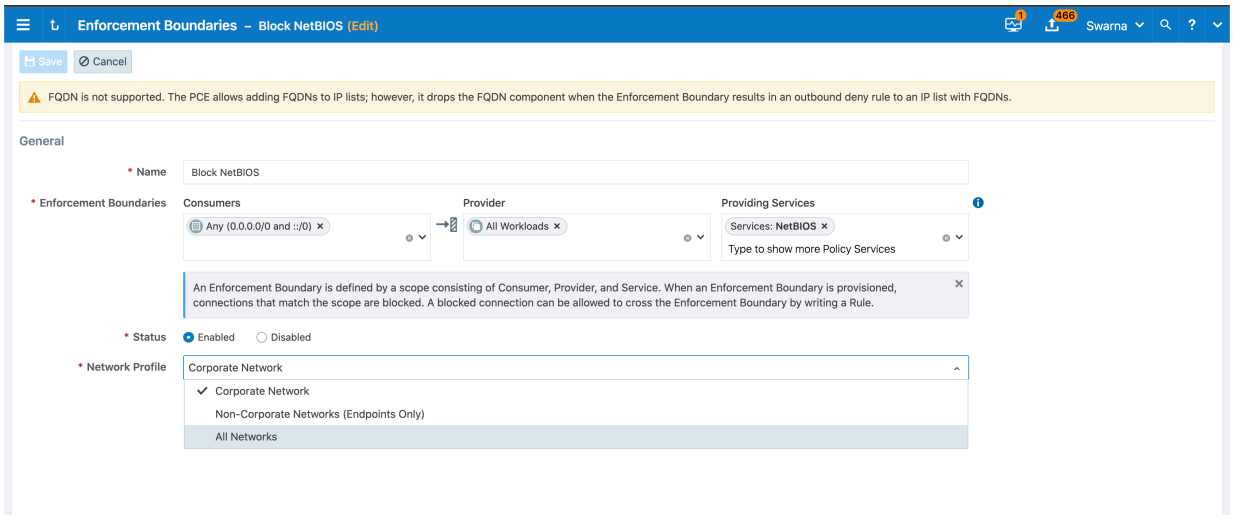


When writing a rule through the **Ruleset** page on the PCE web console, you can specify that the rule applies to **Non-Corporate Networks (Endpoints Only)** or **All Networks** via the **Rule Options** menu.



When writing an Enforcement Boundary, the Network Profile can be selected when editing the Enforcement Boundary.





For more information, see the following topics:

- "Create Labels for Endpoints" in the Endpoint User Guide.
- "Labels and Label Groups" in the *Security Policy Guide*
- "Rule Writing" *Security Policy Guide*
- "The Illumio Policy Model" *Security Policy Guide*

Troubleshooting

To troubleshoot the corporate and non-corporate interfaces, go to the **Workloads and VENs** page. Corporate interfaces specify **Corporate** after the interface name and address, while Non-corporate interfaces specify **External**.