Illumio Core®

Version 23.2

Endpoint Installation and Usage Guide

June 2024

45000-100-23.2

Legal Notices

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.

For legal information, see https://www.illumio.com/legal-information.

Open source software utilized by the Illumio Core and their licenses, see Open Source Licensing Disclosures

Product Version

PCE Version: 23.2

For the complete list of Illumio Core components compatible with Core PCE, see the Illumio Support portal (login required).

For information on Illumio software support for Standard and LTS releases, see Versions and Releases on the Illumio Support portal.

Illumio Endpoint Installation and Usage Guide

This guide describes how to use Illumio Endpoint feature in Core, a single Illumio Core PCE, formerly referred to as "Single Pane of Glass," to visualize and segment Windows endpoints.

Benefits of Illumio Endpoint

For the Illumio Endpoint, you perform the following tasks:

- View all server and endpoint workloads (wired and wireless).
- Author policy for servers and endpoints.
- View events and traffic for servers and endpoints.

Illumio Endpoint on macOS

Illumio Core Cloud customers can now install the VEN for the Illumio Endpoint on these versions of macOS

- 14.0, 14.1, 14.2, and 14.3 (Sonoma)

  > NOTE:
  > macOS 14.3 is supported only with VEN 23.2.22. In this use case, you may see the following failure message if you `issue /opt/illumio_ven/illumio-ven-ctl restart` to restart the ven:
  >
  > `Stopping venAgentMonitor: ...fail!`
  >
  > This failure message appears in error in this case and you can safely ignore it.

- 12.*x* (Monterey)
- 11.0 (formerly 10.16) (Big Sur)
- 10.15 (Catalina)

About a third of all endpoint platforms within an enterprise are running macOS. Not protecting this platform leaves organizations vulnerable to ransomware and malware. To prevent breaches and lateral movement in your organization, install the Illumio Endpoint on macOS and create full enforcement policies for your Mac endpoints.

For the steps to install the Illumio Endpoint on macOS, see Endpoint on macOS. For information about creating full enforcement policies, see Ruleset and Labeling Guidelines for Endpoints.

For an overview of the Illumio solution for endpoints, see Illumio Endpoint on the Illumio website.

Illumio Endpoint Configurations

The following configurations are supported for Illumio Endpoint in Illumio Core.

Illumio Environment

- Illumio Cloud: Illumio Core PCE 22.2.0 and later releases.
- Illumio Core 21.5.11 or 21.5.20 VEN and later releases.

Customer Environment

Illumio Endpoint supports the following customer environments:

- Endpoints running Windows 7 or Windows 10.
- Endpoints can be on-premises domain joined or on-premises Azure AD-hybrid joined, or joined with Azure AD only.
- Supported domain-joined endpoint interfaces:
    - Wired
    - Wireless
    - PPP/VPN
- Endpoint segmentation is not compatible with hypervisors such as Windows Hyper-V. The connectivity to or from virtual machines might be blocked in Enforced mode.

Wireless Connections and VPNs

The Illumio Core VEN supports wireless connections for VENs installed on endpoints in the Illumio Core.

To install a VEN on an endpoint and to support a wireless network connection, you must include the `-endpoint` option in the VEN CTL command line or in the VEN pairing script.

> NOTE:When installing the VEN by using the `-endpoint` option, the Illumio VEN detects two additional interface types on the endpoint; namely, 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.)

For more information about installing the VEN on an endpoint, and supporting a wireless network connection, see the following topics:

- How to Install VENs by using a Pairing Script
- How to Install VENs by Using an EXE Package

> NOTE:
> Wireless network support is only available for endpoints in Illumio Core. It is not available for other support server types, such as bare-metal servers, virtual machines (VMs), or container hosts.

Azure AD Support for Endpoints

In Core 21.5.11, Illumio began Azure AD support for endpoints. So that your endpoints can detect interfaces connected to your corporate network, you must specify in the PCE the public IP addresses that are used by your corporate network for endpoints in an AD setup, such as when using Azure AD. Once configured, the VENs on the endpoints send network profile detection requests to the PCE. These requests appear to originate from your organization's public IP addresses.

When those IP addresses fall within the range of the corporate public IP addresses you configured in the PCE, the PCE recognizes that endpoint interface as a corporate interface. When an IP address is outside the range, the PCE recognizes the endpoint interface as an external interface.

On endpoints, the VENs report to the PCE and enforce the corporate firewall policies that are created in the PCE. The VENs enforce the policy from the PCE 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. You can configure the corporate public IP addresses by using the PCE Web Console.

NOTE:
The Workloads page in the PCE Web Console displays a "public IP" field for endpoint workloads. The IP address in this field represents the public IP address of the endpoint as observed by the PCE at the time of endpoint activation. The displayed IP address isn't necessarily the corporate public IP address of the endpoint. Also, the IP address isn't guaranteed to be the latest public IP address used by the endpoint.

Requirements and Limitations

- You must be running Illumio Core 22.2.0-PCE or later releases and 22.2.0-VEN or later releases.

OS Management		On-prem Domain Controller (DC) or DC/Azure AD hybrid	Azure Active Directory Only (AAD)	Notes
Endpoint OS	Feature			
Windows 7 SP1	Domain policy	Yes	N/A	
	AUS	Yes	N/A	
Windows 10, Windows 11	Domain policy	Yes	Yes	PCE Network Location Detection is required for AAD-only endpoint
	AUS	Yes	No	

- You must configure your corporate public IP addresses in the PCE.
- Only IPv4 addresses or CIDR blocks are supported for corporate public IP addresses.
- Policies for Adaptive User Segmentation (AUS) are supported, but not supported on Azure AD.

Configure Corporate Public IP Addresses in the PCE

> NOTE:
> You must be an Illumio Organization Administrator to perform this task.

1. From the PCE web console main menu, choose **Settings > Corporate Public IPs**.

   The Corporate Public IPs page appears.

2. Click **Edit**.

   The page refreshes with a field to enter IP addresses.

3. Enter individual IPv4 addresses or CIDR blocks.
4. Click **Save**.

Typical Workflow

Illumio suggests this typical workflow for deploying and segmenting VENs on your endpoints:

- **Task 1:** Create labels for endpoints.
- **Task 2:** Add corporate public IPs if using Azure AD.
- **Task 3:** Create or modify a ruleset for endpoints.
- **Task 4:** Install and activate VENs in Endpoint mode.

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 in this guide 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 Configure Corporate Public IP Addresses in the PCE

Task 3: Create or Modify a Ruleset for Endpoints

Create or modify a ruleset to define the allowed communication between endpoints and servers.

See To Create Rulesets that Use Workload Subnets for Endpoints.

Task 4: Install and Activate VENs in Endpoint Mode

This task describes how to install and activate VENs on endpoints by invoking endpoint mode from a command prompt (installing VENs in endpoint mode from the PCE Web Console is not yet supported). Endpoint mode is required for visualizing and segmenting endpoints from the Core PCE.

For simplicity, this task shows how to manually install and activate the VEN onto a single endpoint. You can also install VENs remotely on multiple endpoints using a network provisioning tool. You can now use subnets instead of IP lists.

There are two installation methods:

- Install Windows Endpoint VENs By Using a Pairing Script
- Install Windows Endpoint VENs By Using an EXE Package

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.

To 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**.

Install Windows Endpoint VENs By Using a Pairing Script

For more information, see Pairing Script in *VEN Installation and Upgrade Guide* for 22.2.

Copy a pairing script from the PCE Web Console, edit it in a text editor, and then run the script.

1. From the PCE web console menu, go to **Workloads and VENS** > **VENs**.
2. Click **Add with Pairing Profile**.
3. Scroll to **Pairing Scripts > Windows OS Pairing Script** and then copy the script.
4. Paste the script into a text editor and enter `-endpoint true` in an appropriate place in the script. In this example, note that the endpoint argument is placed between `$env:windir\temp\pair.ps1` and `-management-server`:

```
PowerShell -Command "& {Set-ExecutionPolicy -Scope process remotesigned -
Force; Start-Sleep -s 3; Set-Variable -Name ErrorActionPreference -Value
SilentlyContinue; [System.Net.ServicePointManager]::SecurityProtocol=
[Enum]::ToObject([System.Net.SecurityProtocolType], 3072); Set-Variable -Name
ErrorActionPreference -Value Continue; (New-Object
System.Net.WebClient).DownloadFile
('https://pce.example.com/api/v18/software/ven/image?pair_
```

```
script=pair.ps1&profile_id=1', (echo $env:windir\temp\pair.ps1)); &
$env:windir\temp\pair.ps1 -endpoint true -management-server pce.example.com -
activation-code <code>;}"
```

5. Copy the edited pairing script.
6. Execute the pairing script on the target endpoint.

   The VEN is installed and paired (activated) in **endpoint mode**. This message appears: "`VEN has been successfully paired with Illumio`".
7. **(Optional)** Verify that the VEN is installed in endpoint mode by checking for `endpoint: true` in the runtime file located at `c:\ProgramData\Illumio\config\runtime_env.yml`.

Install Windows Endpoint VENs By Using an EXE Package

For more information, see Install the Windows VEN Using EXE Package in the *VEN Installation and Upgrade Guide* for 22.2.

Make sure to include the argument `ENDPOINT=true` as shown in the following examples:

Interactive Mode

```
PS C:\windows\Temp> .\illumio-ven-<version>-<build>.win.x64.exe ENDPOINT=true
```

Silent Mode

```
PS C:\Program Files\Illumio> Start-Process -FilePath "$env:WinDir\temp\illumio-
ven-<version>-<build>.win.x64.exe" -ArgumentList
"ENDPOINT=true","/install","/quiet","/norestart","/log","$env:WinDir\temp\VENInsta
ller.log" -Wait -PassThru
```

Install macOS Endpoint

In Release 22.5.0, the Endpoint VEN supports macOS versions 10.15 (Catalina), 10.16 (Big Sur), and 12.x (Monterey). The macOS VEN software package is a universal binary and can be installed on Intel and ARM Mac platforms. Using macOS VEN, you can 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

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

Installation and Upgrade

You install the macOS VEN software and pair it by using the macOS pairing line. The Illumio Core Cloud release installation package is also available through the PCE web console.

Jamf Installation and Deployment Procedure

1. Download the installation package through the PCE web console.
2. Go to the Jamf Pro console. Locate and upload the package and the registration script.
3. Through the registration script, register the VEN to the PCE.
   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.

To install or upgrade to the 22.3.*x*-VEN release, follow these steps through the macOS UI.

The release consists of a single package.

1. Double-click the package:

   `illumio-ven-<version>-<build#>.mac.universal.pkg`

2. Follow the instructions in the installation dialogs.

   When the installation is complete, a dialog appears.

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`

Uninstallation

To uninstall the macOS VEN software, issue the following command in a user-interactive terminal:

```
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.

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.

The 23.2 Endpoint VEN for Windows recognizes both corporate and non-corporate interfaces in on-premises AD, Azure AD, and hybrid AD environments.

The 23.2 Endpoint VEN for macOS recognizes 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.

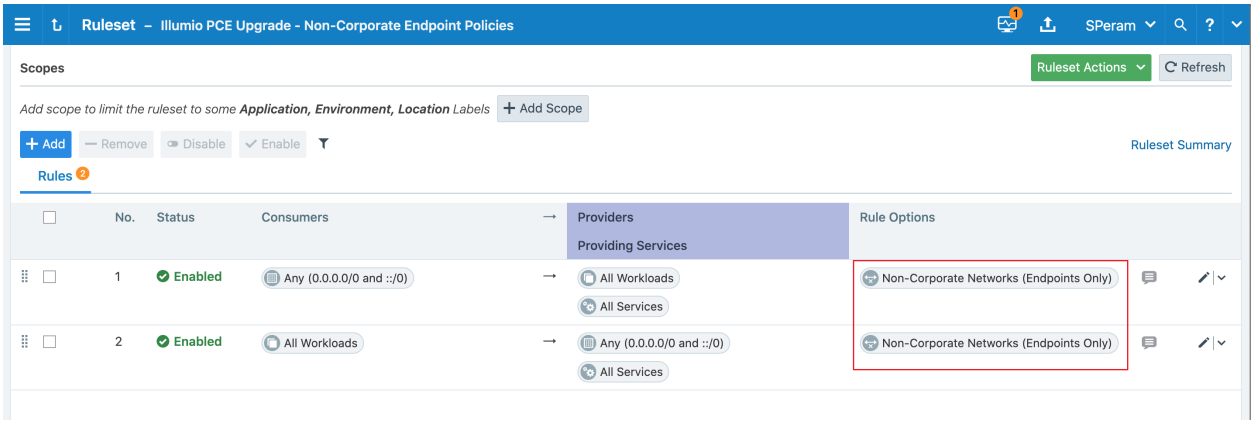
Backward Compatibility

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.

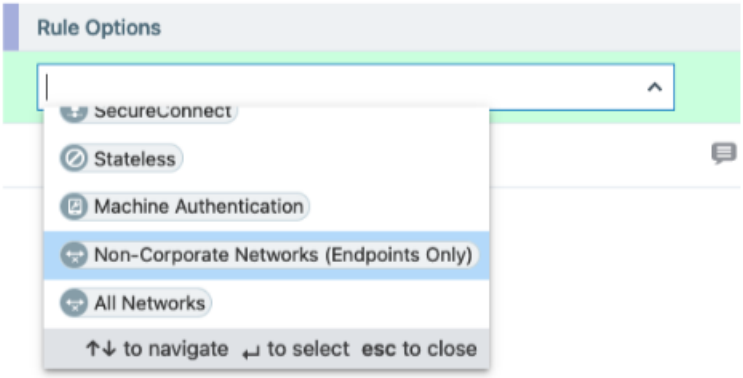


Writing Rules with Network Profiles

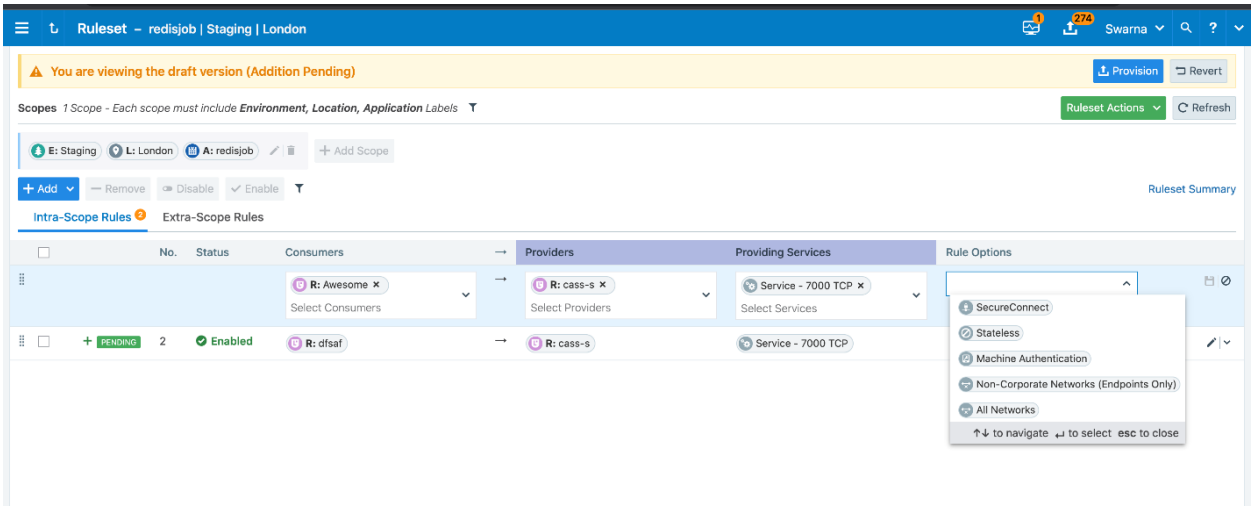
Network profiles can be used on rules and Enforcement Boundaries to specify the endpoint interfaces affected by the rRule or Enforcement Boundary. If unspecified, the default network profile on a rule or Enforcement Boundary is **Corporate**, which applies to all servers and corporate interfaces on endpoints. 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.

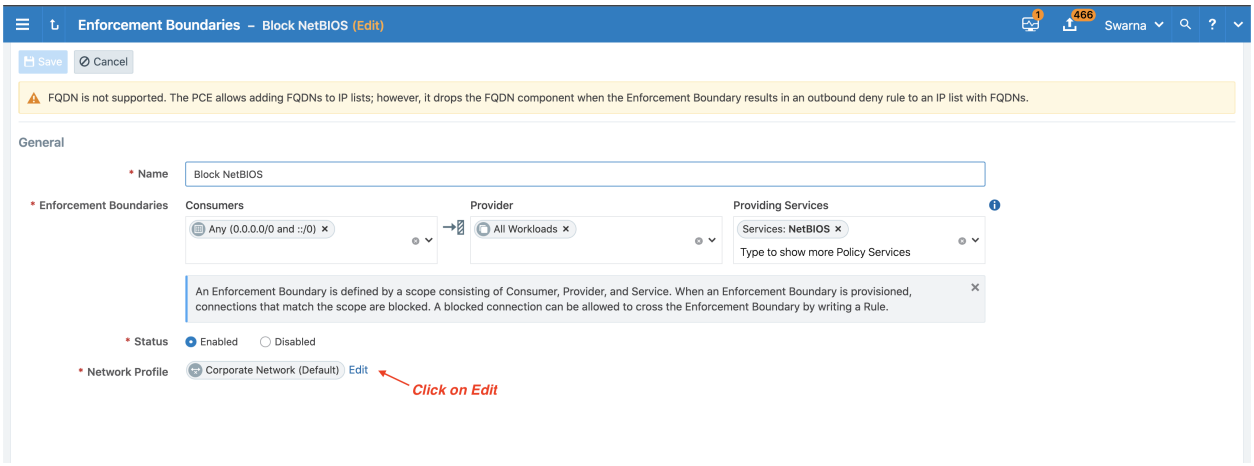
When either the **Non-Corporate Networks** or **All Networks** option is selected, the rule must only use IP lists in either the provider or the consumer.

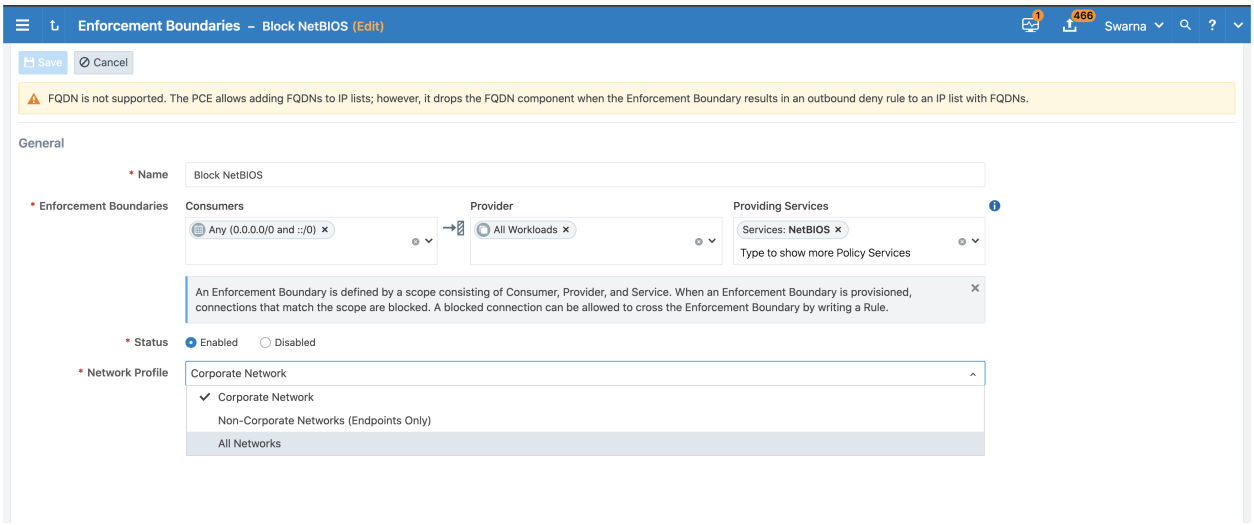


When writing a rule through the **Ruleset** page on the PCE web console, you can specify that the rule applies to **Non-Corporate Networks (Endpoints Only)** or **All Networks** via the **Rule Options** menu.



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



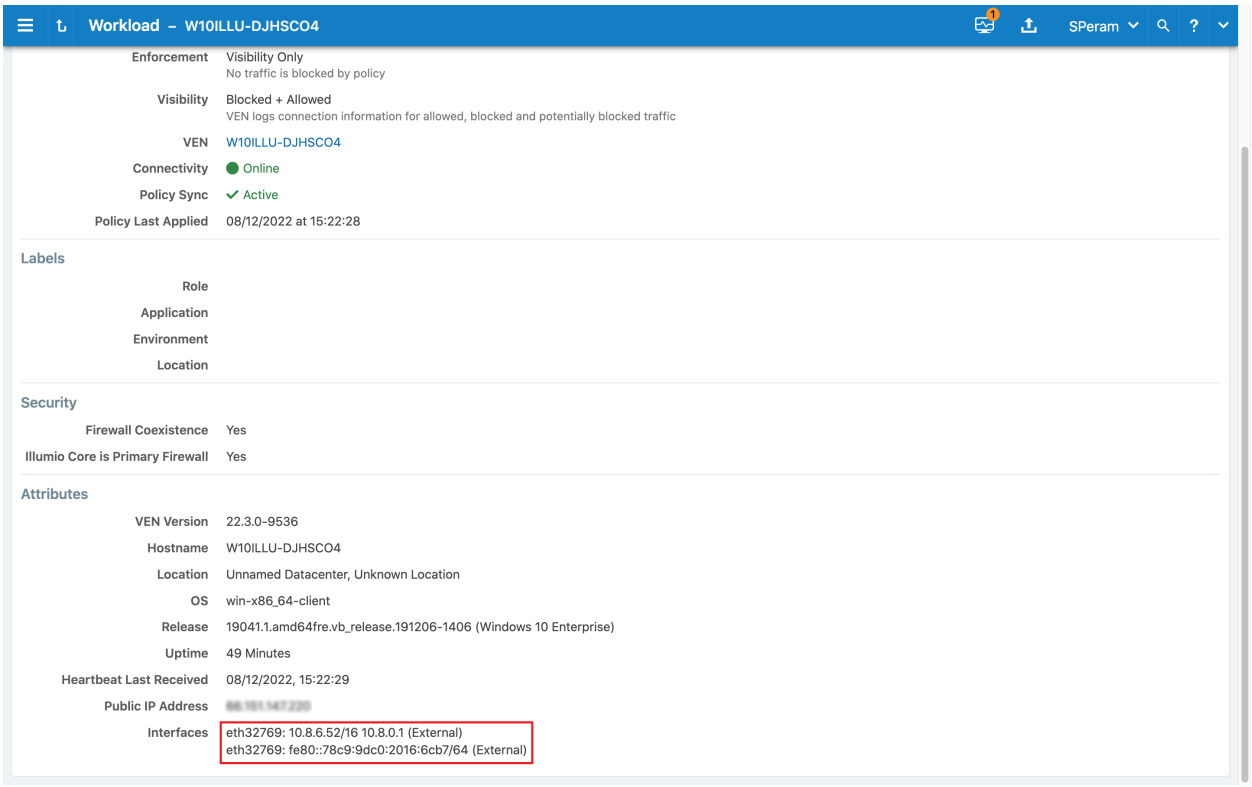


For more information, see the following topics:

- Create Labels for Endpoints
- Labels and Label Groups (*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**.


Workload – W10ILLU-DJHSCO4
SPeram
Enforcement
Visibility Only
No traffic is blocked by policy
Visibility
Blocked + Allowed
VEN logs connection information for allowed, blocked and potentially blocked traffic
VEN
W10ILLU-DJHSCO4
Connectivity
Online
Policy Sync
Active
Policy Last Applied
08/12/2022 at 15:22:28
Labels
Role
Application
Environment
Location
Security
Firewall Coexistence
Yes
Illumio Core is Primary Firewall
Yes
Attributes
VEN Version
22.3.0-9536
Hostname
W10ILLU-DJHSCO4
Location
Unnamed Datacenter, Unknown Location
OS
win-x86_64-client
Release
19041.1.amd64fre.vb_release.191206-1406 (Windows 10 Enterprise)
Uptime
49 Minutes
Heartbeat Last Received
08/12/2022, 15:22:29
Public IP Address
Interfaces
eth32769: 10.8.6.52/16 10.8.0.1 (External)
eth32769: fe80::78c9:9dc0:2016:6cb7/64 (External)