Illumio Core®

Version 22.2

Endpoint Installation and Usage Guide

November 2022

45000-100-22.2

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: 22.2

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.

Endpoint Installation and Usage Guide

This guide describes how to visualize and segment workloads running on Windows domain-joined endpoints from a single Illumio Core PCE. It includes requirements, guidelines, and configuration instructions.

Historically, Illumio documentation has referred to server workloads as simply "workloads" and to endpoint workloads as simply "endpoints." This guide expands the term "workload" to refer to both "server workloads" and "endpoint workloads."

Prior to this release, Illumio supported installing VENs on server workloads. Starting in Illumio Core 21.3.0 and later releases, you can manage and segment Windows domain-joined endpoints along with server workloads from the Illumio Core.

For information about creating policy for server workloads and endpoints, see the *Security Policy Guide* in this documentation portal.

For information about installing and managing VENs, see the VEN Installation and Upgrade Guide and the VEN Administration Guide in this documentation 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

From Illumio Endpoint, you'll be able to 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.

What's New in This Release

Illumio Endpoint Scales to 25,000 Workloads

The scale limits for Illumio Endpoint visibility and segmentation for servers and endpoints have increased to 25,000 total workloads. To achieve this, policy may be written using labels but must additionally use the **Use Workload Subnets** option. The PCE auto-detects the subnets based on the IP address and netmask reported by the VEN. This method of rule writing allows for less PCE load when processing changes caused

by the endpoints. The capacity of the on-prem 2x2 PCE (10,000) or the 4x2 PCE (25,000) is used for supporting servers and endpoints. There is no lower limit on the number of endpoints for on-prem PCEs.

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.

Create Rulesets that Use Workload Subnets for Endpoints

To 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**.

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 and 22.2.0-VEN.

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	

OS Management		On-prem Domain Controller (DC) or DC/Azure AD hybrid	Azure Active Directory Only (AAD)	Notes
Endpoint OS	Feature			
Windows 10	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 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:

- How to Install VENs By Using a Pairing Script
- How to Install 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.

Create 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.

How to Install VENs By Using a Pairing Script

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

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`.

How to Install VENs By Using an EXE Package

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

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
```

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.