Illumio Core®

Version 21.5

VEN

Version 21.5

Illumio Endpoint Segmentation

November 2022

45000-100-21.5

Legal Notices

Copyright © 2022 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.

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: 21.5 (LTS Release)

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 Segmentation

This guide describes how to visualize and segment workloads running on Windows domain-joined endpoints from a single Illumio Core PCE formerly referred to as "Single Pane of Glass." 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 Illumio Endpoint.

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.

About Illumio Endpoint Segmentation

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

Benefits of Illumio Endpoint Segmentation

From Illumio Endpoint, you'll be able to perform these 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 Core 21.5.10

In this release, you can use Illumio Endpoint when installing the PCE in your own data center as an Illumio On Premises customer.

Illumio Endpoint Configurations

The following configurations are supported for endpoints in the Illumio Core.

Illumio Environment

- Illumio Component Versions
  - Illumio Cloud: Illumio Core PCE 21.5.0 and later releases
  - Illumio Core VEN 21.5.0 and later releases
- VEN Maximums

> NOTE:
> These limits for VEN maximums are not convertible; for example, you can't add more server VENs by reducing endpoint VENs.

  - Illumio Core Cloud customers: 1000 server VENs + 4000 endpoint VENs.
  - Illumio Core On Premises customers:

MNC Type	VENs
2x2 (small)	200 server VENs + 800 endpoint VENs
2x2	1,000 server VENs + 4,000 endpoint VENs
SNC	200 total VENs

> IMPORTANT:
> Currently, Illumio has validated this feature for 2x2 deployments only. If you're interested in deploying larger use cases, contact the Illumio Sales channel.

Customer Environment

For Illumio Endpoint Segmentation, Illumio 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.
- 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.

Typical Workflow

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

- **Task 1:** Create an IP list for providers.
- **Task 2:** Create labels for endpoints.
- **Task 3:** Create or modify a ruleset for endpoints.
- **Task 4:** Install and activate VENs in Endpoint mode.

Task 1: Create an IP List for Providers

Create an IP list that specifies the trusted IP addresses that your endpoints can communicate with.

For more information, see IP Lists in the *Security Policy Guide*.

Task 2: 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 3: Create or Modify a Ruleset for Endpoints

Create or modify a ruleset to define the allowed communication between endpoints and their Providers. When you select Providers, select IP List and then select the IP list you created in Task 1.

IMPORTANT:
See Create Rulesets that Specify IP Lists for Providers in this guide for guidance on creating rulesets for endpoints. For general information about creating rulesets, see Create a Segmentation Ruleset in the *Security Policy Guide.*

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.

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 Specify IP Lists for Providers

When you create policies that allow endpoints to communicate with destination servers, Illumio recommends that you specify the server's IP address, not its label. In general, take this approach:

1. Create IP lists that correspond to the destination servers that your endpoints need to access.
2. Create rulesets that specify those IP lists as Providers.
3. Be careful with broad, label-based rulesets, 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. In this label-to-label policy scenario involving endpoints, any change in endpoint connectivity will trigger policy updates on the AD servers. Because the network connections on endpoints tend to change frequently, firewall policy on the AD servers will also change frequently. Depending on the size of your implementation, churn could be significant.

Create Rulesets That Allow Inbound Traffic to the Server

To create a policy that allow an endpoint subnet to communicate with destination servers, you must do the following:

1. Create the endpoint subnet.
2. Allow inbound traffic to the server from the subnet by creating a ruleset that specifies the server labels and the endpoint subnet as consumer.

How to Install VENs By Using a Pairing Script

For more information, see Pairing Profiles and Scripts in the *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. From PowerShell, open an SSH connection to the endpoint, paste the pairing script at the command prompt, and then press **Enter**.

   The VEN is installed and paired (activated) in **endpoint mode**. The message "`VEN has been successfully paired with Illumio`" appears.
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
```

Illumio Endpoint and Scale

The Illumio Endpoint and Scale feature is a method of writing policy for endpoints so the PCE can scale its support of workloads from 5,000 (1,000 servers and 2,000 endpoints) to 25,000 workloads. Instead of using individual IP addresses of the endpoints, the PCE makes scaling possible by using the subnets of the workloads. The subnets are determined by the IP address and netmask reported by the VEN. This method alleviates overload of CPU processing. You must select the **Use Workload Subnets** option to make use of the scaled performance. To do so, you must add or edit a rule. To add or edit a rule, go to **Rulesets and Rules** > **Rulesets** > *click on a ruleset* > **Rules** > *locate a consumer and click the edit (pencil) icon* > under **Consumers**, *click the down arrow and choose* **Use Workload Subnets**.

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 in the *Illumio Endpoint Installation and Usage Guide*:

- 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.