Illumio Core®

Version 22.1.3

Single Pane of Glass Segmentation

June 2022

45000-100-22.1.3

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 Versions

PCE Version: 22.1.3 (Standard release) | Illumio Core Cloud customers only

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.

About Single Pane of Glass Segmentation

This guide describes how to use a single Illumio Core PCE to visualize and segment Windows endpoints from within the Illumio Core.

Benefits of Single Pane of Glass Segmentation

From this single pane of glass, 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 This Release

In Illumio Core, the PCE supports endpoints that are joined only to Azure Active Directory (Azure AD). Prior Illumio Core releases required that the endpoints be joined to a local on-premises domain controller.

In this release, the VENs running on Azure AD joined endpoints perform network profile detection to determine whether endpoint interfaces are connected to corporate networks. 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. In this release, you configure the corporate public IP addresses by using the PCE web console.

Single Pane of Glass Configurations

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

Illumio Environment

- Illumio Component Versions
  - Illumio Cloud: Illumio Core PCE 22.1.0 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.

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

Customer Environment

For Single Pane of Glass 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, 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.

Azure AD Support for Endpoints

In Core 21.5.10, Illumio provides 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.

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 VEN 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 22.1.1-PCE and 21.5.10-VEN.
- Endpoints must be running Windows 10 for this feature.
- Customers must be Illumio Core Cloud customers to use this feature.
- You can configure this feature for a maximum of 5,000 endpoints
- 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 not supported.

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 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
```

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.