Illumio Core®

Version 22.2

VEN

Version 22.2

VEN Installation and Upgrade Guide

November 2022

40000-100-22.2

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.

Product Version

VEN Version: 22.2

For the complete list of Illumio Core compatible PCEs for this VEN release, 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.

Resources

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

Trademarks statements, see https://www.illumio.com/trademarks

Patent statements, see https://www.illumio.com/patents

License statements, see https://www.illumio.com/eula

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

Contact Information

To contact Illumio, go to https://www.illumio.com/contact-us

To contact the Illumio legal team, email us at legal@illumio.com

To contact the Illumio documentation team, email us at doc-feedback@illumio.com

Contents

Chapter 1

Overview of VEN Installation

This chapter contains the following topics:

This section introduces you to installing the VEN on your hosts. In particular, it explains the two ways to install the VEN. Based on the method you choose, you can skip to the content that describes your preferred installation method.

About This Installation Guide

Before installing VENs on the hosts in your environment, ensure that you meet the necessary technical background.

How to Use This Guide

This guide explains how deploy the Virtual Enforcement Node (VEN) on your distributed, on-premises systems.

The guide provides the details to complete the following tasks:

- An explanation of the VEN installation methods, namely, by using the VEN Library in the PCE versus the VEN Control Interface (CTL)
- How to install VENs using the VEN Library
- How to install VENs using packaging technology and the workload operating systems' native command line interface
- How to uninstall, upgrade, activate, and deactivate VENs by using the VEN CTL

- How to set up the PCE to install VENs by using the PCE web console and the VEN Library

Before Reading This Guide

Illumio recommends that you be familiar with the following topics before you follow the procedures in this guide:

- Your organization's security goals
- The Illumio Core platform
- General computer system administration of Linux and Windows operating systems, including startup/shutdown, and common processes or services
- Linux/UNIX shell (bash) and Windows PowerShell
- TCP/IP networks, including protocols and well-known ports

Notational Conventions in This Guide

- Newly introduced terminology is italicized. Example: *activation code* (also known as pairing key)
- Command-line examples are monospace. Example: `illumio-ven-ctl --activate`
- Arguments on command lines are monospace italics. Example: `illumio-ven-ctl --activate` *`activation_code`*
- In some examples, the output might be shown across several lines but is actually on one single line.
- Command input or output lines not essential to an example are sometimes omitted, as indicated by three periods in a row. Example:

```
...
some command or command output
...
```

Ways to Install the VEN

You can install the VEN two ways. These two ways are nearly identical and achieve the same goal: VEN installation and upgrade.

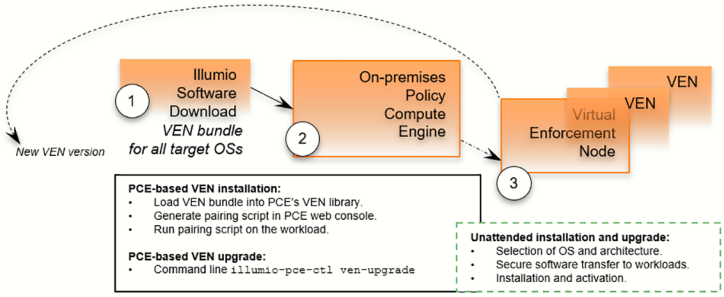
- Using the VEN Library integrated into the PCE: This method is documented in the topics about installing and upgrading the VEN Library.

- Manual VEN installation on individual workloads with your own software deployment tools: This method is documented in the topics about installing and upgrading the VEN using the VEN CTL.

VEN Installation Using the VEN Library

NOTE:
The VEN Library installation and upgrade feature in the PCE is available for the RPM, Debian, and Windows distributions of the VEN software. Other workload operating systems are not supported.

Using the VEN Library in the PCE to install the VEN is a more automated approach than installing the VEN CTL but it gives you less control over optional aspects of VEN installation and upgrade.



The VEN Library method of installation utilizes a *VEN software bundle*. A VEN software bundle is a collection of a particular VEN software version for all supported workload operating systems.

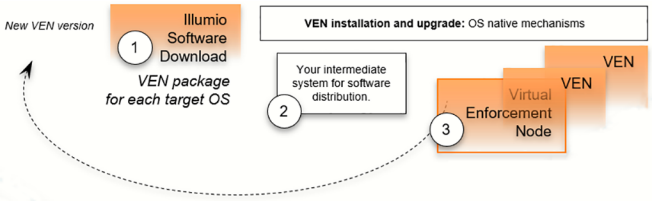
- In the PCE, you load a VEN software bundle into the *VEN library*. The VEN library is a collection of all VEN software versions you have loaded.
- For VEN installation:
  - In the PCE web console, you set a default VEN version.
  - In the PCE web console, you generate a pairing script to install and activate the VEN on target workloads.
  - You copy the pairing script to the target workload and run it.
  - The pairing script:
    - Determines the OS and CPU architecture of the target workload.
    - Securely transfers the VEN software to the target workloads.
    - Installs the VEN software.
    - Pairs the VEN with its PCE.

- For VEN upgrade, use the VEN Library in the PCE to upgrade all workloads or selective workloads.
- Some features are not available with VEN Library method, such as Kerberos-based authentication and custom settings with environment variables.

NOTE:
Setting up the VEN Library in the PCE is required only for Illumio On-premises customers. If you are an Illumio Cloud customer, Illumio Operations performs this task for you.

VEN Installation Using the VEN CTL

This method gives you greater control over optional aspects of VEN installation, pairing, and upgrade.



The VEN installation method using the CTL starts with downloading a *VEN package*. A VEN package is the VEN software for a single supported workload OS and CPU architectures. Installation and upgrade rely on package managers, which are standard, native OS tools.

- For VEN installation with this method:
  - Determine the OS and CPU architecture of the target workloads.
  - Download the appropriate VEN packages.

    For example, installing a VEN on CentOS 8 x86-64 requires you to download the VEN package `illumio-ven-XXX.c8.x86_64.rpm`.

    NOTE:
    You are responsible for securely transferring the VEN software to the target workload with your own software deployment mechanisms.

  - Optionally, set the following environment variables or command-line options:

        - Custom installation directories
        - Custom user and group names
        - Kerberos-based authentication for VEN-to-PCE communications
    - Run the native OS installation mechanism.

      For example: `rpm -ihv illumio-ven*.rpm`
    - Pair the VEN with its PCE.
        - You can pair the VEN during installation or after installation using the VEN CTL activate command (`illumio-ven-ctl activate <options>`)
        - You can use a "prepare script" to install the VEN software on machine images and activate it at the next boot.
- If you installed the VEN with the VEN CTL and packaging CLI and customized installation options (such as, a custom installation directory or alternate VEN user), you cannot later upgrade the VEN by using the VEN Library in the PCE. You must upgrade the VEN using the workload's OS package upgrade process.

TIP:
If you try to upgrade a VEN using the VEN Library in the PCE but nothing happens, verify whether the VEN was installed by using the VEN CTL.

When to Use Which Method

You can use both methods at different stages of your VEN installation.

Installation Method	Use Cases
VEN Library in the PCE	• To demonstrate the ease of VEN installation and assess installing Linux VENs using the VEN Library • To evaluate and certify new versions of the VEN
VEN CTL	To obtain more control over VEN installation and upgrade with a proprietary software distribution method

VEN-to-PCE Authentication

Illumio Core has the following mechanisms for authentication between the VEN and the PCE:

- VEN pairing with the PCE
- Kerberos authentication with the PCE

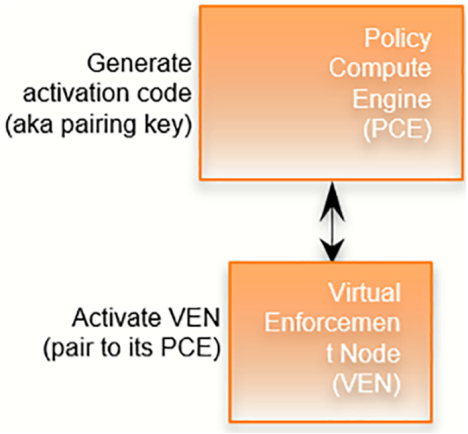
Use one or both mechanisms across your organization, but they are mutually exclusive for the same workload.

> IMPORTANT:
> This guide assumes that you already have a functional Kerberos service with which to authenticate.

VEN Authentication by Pairing with PCE

This is the default mechanism. When you install a VEN on a workload, the VEN is activated with an activation code generated by the PCE. The activation code is an identifier passed to the VEN software at activation.

After the VEN is activated, it communicates with the PCE over a secure connection. This process of activating a VEN is referred to as pairing it with the PCE. The term *activation* also applies when installing the VEN package directly on a workload by using the VEN CTL.



About the VEN Activation Code

The activation code is an identifier passed to the VEN software at activation. It is obtained from the pairing key. An activation code can be created for one-time use for a single workload or multiple uses for many workloads.

You can get an activation code in the following ways:

- In the PCE web console, create a Pairing Profile. In the profile, you can specify one-time use or unlimited use for the activation code.
- With the REST API. For information, see Create a Pairing Key in the *REST API Developer Guide.*

Activation Details

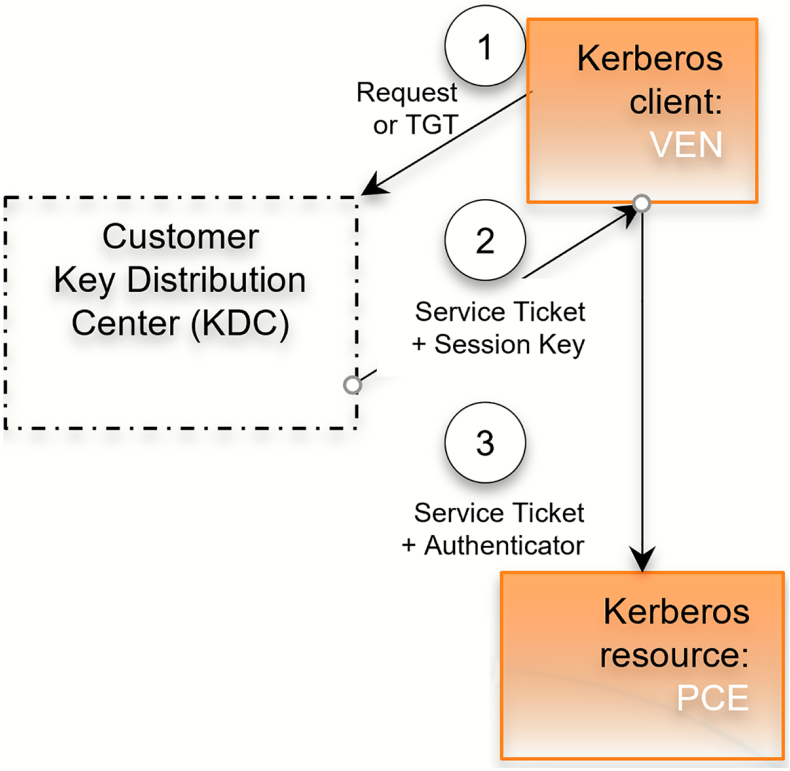
An activation code is used only after initially installing the VEN. During activation, the PCE generates an agent token. The VEN stores the agent token in a local file on the workload. The PCE stores the hash of the agent token. The VEN uses the agent token to uniquely authenticate itself to PCE. Only the agent token is used in VEN-to-PCE communication from that point on.

The VEN communicates with the PCE using HTTPS over Transport Layer Security (TLS) for REST calls and TCP over TLs for the events channel. Additionally, a clone token is generated. When an agent token is mistakenly or maliciously reused on another workload, the clone token is used to detect the condition and disambiguate the hosts. The clone token is periodically rotated. The agent token is never rotated.

VEN Authentication via Kerberos

You can configure the PCE and VEN to rely on authentication by a pre-configured Kerberos-based system, such as Microsoft Active Directory.

NOTE:
Kerberos-based authentication is supported when you install the VEN by using the VEN CTL. It is not supported when you use the VEN Library in the PCE to install the VEN.



The Key Distribution Center (KDC) is your pre-configured Kerberos service; the VEN is a Kerberos client; and the PCE is a Kerberos resource.

1. The VEN requests a session key or passes its ticket granting ticket (TGT).
2. The KDC returns a service ticket and session key.
3. The VEN passes the authenticated service ticket to the Kerberos-protected PCE.

For information about setting up Kerberos for VEN authentication with the PCE, see Set up Kerberos Authentication on PCE.

For information about pairing workloads via Kerberos for each operating system, see the following topics:

- Kerberos for Windows VEN-to-PCE Authentication
- Kerberos for Linux VEN-to-PCE Authentication

Additionally, you can use the Illumio Core REST API to set up VEN authentication with the PCE via Kerberos. See the following topics in the *REST API Developer Guide* for information:

- Workload Operations
- Bulk Traffic Loader

VEN-unactivated Golden Masters

When you create machine images for faster deployment of the VEN, consider preparing them to pair the VEN with the PCE the first time the workload is booted. See Prepare Golden Image for Workload Installationfor information.

Upgrading From pre-20.2 to Later Versions

When upgrading from a PCE version pre-20.2 to a later version, stopped VENs that have sent a *goodbye* message to the PCE will have their status value set to *stopped*. During the upgrade, this procedure can cause a burst of events to be emitted to the PCE event stream.

Reduced Banners During VEN Upgrades

The user interface experience on VENs has been enhanced. You will no longer see multiple banners during VEN upgrades. In lieu of an additional banner being displayed, a tally will indicate current upgrade status, show what process is suspended, or display what process is experiencing issues during the upgrade.

MSI to EXE Package Format

Starting with the 21.2.1 Illumio Core release, the Windows VEN installer will switch from MSI to EXE package format. Customers using the PCE-based VEN deployment must take an extra step for the transition. Specifically, Illumio Core customers running older, MSI-based Windows VENs must upgrade to 19.3.6+H1-VEN or 21.2.0+H2-VEN before upgrading to their VENs to 21.2.1 or a later version. The 21.2.0+H2-VEN release contains the necessary VEN changes to handle the transition in the VEN packaging from MSI to EXE.

Chapter 2

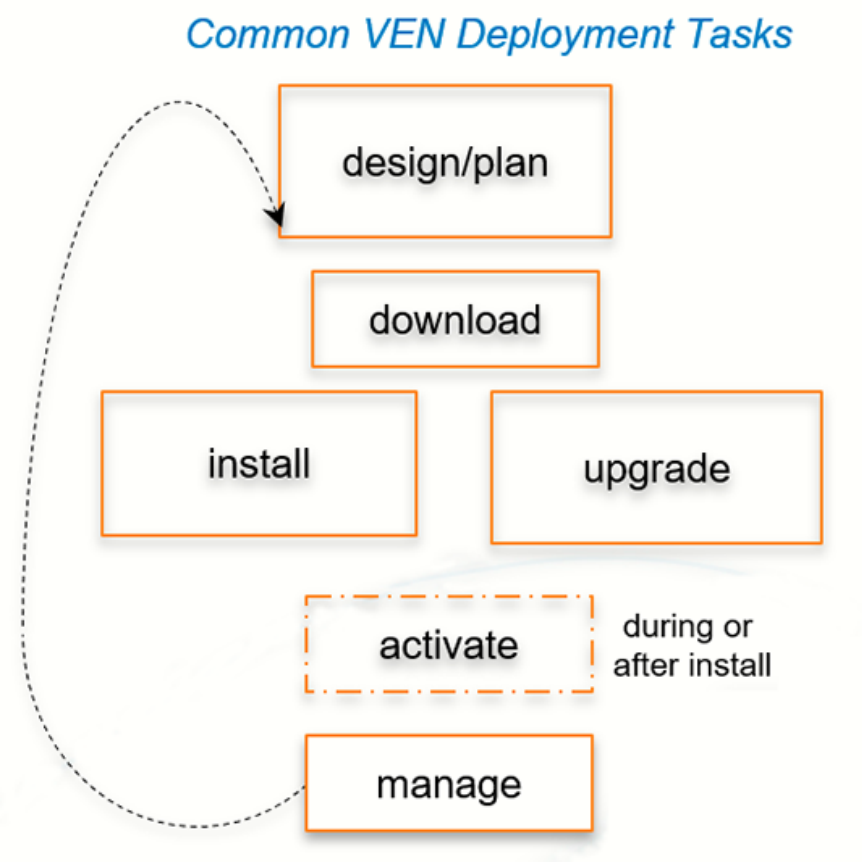
Prepare for VEN Installation

This chapter contains the following topics:

This section provides information that you need to know before installing the VEN software. For a smooth and successful installation of the VEN in your environment, meet the prerequisites outlined in this section.

Workflows for VEN Installation

The following diagram explains at a high level the workflow for performing common VEN installation and upgrade tasks.



VEN Installation Planning Checklist

This checklist summarizes VEN planning considerations and requirements detailed in this guide. It compares the requirements and considerations of both deployment methods.

Tasks	VEN Library	VEN CTL
1. Select VEN installation method.	✓	✓
2. Select VEN-to-PCE authentication mechanism: Activation Code or Kerberos.		✓
3. Select whether to activate the VEN to the PCE during or after VEN installation.		✓
4. Select whether to use a single-use or unlimited-use pairing key		✓
5. Review VEN-to-PCE communication requirements.	✓	✓
6. Review VEN workload disk sizing requirements for hosts.	✓	✓
7. Review OS and package dependencies.		✓

Tasks	VEN Library	VEN CTL
8. Determine VEN software package for workload CPU architecture.	✓ (Automatic)	✓
9. Remove parameters `ven_repo_url` and `ven_repo_ips` from PCE `runtime_env.yml`.	✓	
10. (Linux only) Configure mount `tracefs` or `debugfs`.	✓	✓
11. Download the VEN software: ◦ VEN Library: All VEN versions in a VEN software bundle ◦ Installation using the CLI and VEN CTL: All VEN versions in a package of VEN software for specific OS versions and CPU architectures	✓	✓
12. (Optional) Verify signature of downloaded packages against Illumio's public key.		✓
13. Generate VEN pairing profiles and pairing key.	✓	✓
14. Securely copy VEN paring script to workload.	✓	
15. (Optional) Prepare VEN-unactivated golden master machine Images.		✓

Prerequisites for VEN Installation

Before installing VENs on the workloads in your environment, you must understand and meet the following prerequisites.

PATH Environment Variable for `illumio-ven-ctl`

For easier invocation of `illumio-ven-ctl` and other control scripts, set your `PATH` environment variable to the directories where they are located:

- Linux: default location is `/opt/illumio_ven`
- Windows: default location is `C:\Program Files\Illumio`

For more information about using the VEN CTL, see illumio-ven-ctl General Syntax in the *VEN Administration Guide*.

VEN OSs and Package Dependencies

Some packages, such as SecureConnect StrongSwan for enforcing IPsec, are included as part of the VEN package. For example, when the `ipset` kernel module is not

installed, the VEN downloads and installs it on the workload.

Other packages are installed on the workload itself if they are not already present. When these required packages are not installed on the workload, the VEN downloads and installs them via package dependencies, such as RPM dependencies.

For the complete list of package dependencies by operating system, see the VEN OS Support and Package Dependencies page on the Illumio Support portal.

VEN-to-PCE Communication

Illumio Core uses Transport Layer Security (TLS) version 1.2 by default for VEN-to-PCE communications.

- The PCE default minimum version is TLS 1.2.
- For VEN versions 18.1 and later, all VENs use TLS 1.2.

For more information about the TLS requirements for VEN-to-PCE communication, see Negotiation of TLS Versions for Communications in the *PCE Installation and Upgrade Guide*.

Before installing a VEN, the workload must meet the following requirements for VEN-to-PCE communication:

- The workload can validate its certificate's chain of trust back to the root Certificate Authority (CA) of the server certificate on the PCE.
- The VEN can reach the PCE on the ports configured for the PCE in the PCE Runtime Environment File `runtime_env.yml`. See Port Ranges for Cluster Communication and Reference: PCE Runtime Parameters in the *PCE Installation and Upgrade Guide*.
- To prevent time drift between the PCE and VENs, Network Time Protocol (NTP) must be installed and working on the PCE and the VENs.

Workload Disk Size Requirements

Illumio recommends that you reserve the following disk space on workloads for the VEN:

- Minimum: 500MB
- Recommended: 1.5GB to 2.0GB

Application logs are rotated from primary to backup when their size reaches 15 MB. Application log files are preserved at reboot, because application logs are stored in files on a workload.

IP Address Support

In Illumio Core 20.2.0 and later releases, the VEN supports both IPv4 and Ipv6 address versions and the IP address version appears correctly in the PCE; for example, in the Workload section of the VEN summary page in the PCE web console.

You can configure how the PCE treats IPv6 traffic from workloads. For more information, see Allow or Block IPv6 Traffic in the *PCE Administration Guide*.

Obtain the VEN Packages

PCE-based VEN software bundle

If you are an Illumio On-premises customer (you are running the PCE in your corporate data center), download the VEN packages to your PCE by running the `illumio-pce-ctl` from your PCE. For more information, see VEN Library Setup in the PCE.

> NOTE:
> Illumio Cloud customers you do not have shell access to the PCE; therefore, the Illumio Operations team downloads and sets up the PCE-based VEN software bundle for customers. They download all necessary VEN packages for customers.

CLI-based VEN software packages

All VEN software is available for download from the Illumio Support portal. A VEN package is downloadable from the Illumio Support portal for each version of the VEN. Illumio provides the package as a tar file that contains a version of the VEN for all supported operating systems.

To download the VEN package:

1. Go to the Illumio Support site (login required).
2. Select **Software** > **Download** under the VEN section > VEN version.

   The Download VEN page appears.
3. In the VEN Packages row of the VEN table, click the filename for the VEN tar file.
4. Download the file to a convenient location.

VEN Package CPU Architecture

For VEN installation using the VEN CTL, after you have downloaded and unpacked the software, determine the VEN appropriate for your operating systems and hardware architecture.

See the Supported Operating Systems for Illumio VEN table - CPU Architecture Identifier in Filename column on the Illumio Support portal.

(Optional) Verify Package Signature

For additional security, verify the identity of the downloaded VEN packages against the Illumio public key.

NOTE:

- You can verify the signature of the VEN RPM packages for CentOS, Red Hat Enterprise Linux (RHEL), Ubuntu, and SUSE Linux Enterprise Server.
- Signature verification is not support for AIX, Debian, Solaris, and Windows VEN packages.

The Illumio public key is available on the Download VEN page of the Illumio Support portal (login required).

For information about using a public key to verify package signatures, see Checking a Package's Signature on the Red Hat Customer Portal.

Firewall Tampering Protection on Linux

To enable faster host firewall tampering protection (within approximately three seconds) for Linux firewalls, make sure that:

- `tracefs` is mounted (newer Linux distributions)
- `debugfs` is mounted (older Linux distributions that include `tracefs` in `debugfs`)

For information, see VEN Firewall Tampering Detection in the *VEN Administration Guide*.

NOTE:
Faster host firewall tampering protection is enabled for Windows automatically.

VEN Compatibility Check

In additional to meeting the requirements in this topic and being aware of the limitations for installing VENs on workloads, you can use the VEN Compatibility Check feature to verify the functionality of the VEN on a workload. The compatibility information for the VEN is available only while the VEN is in Idle mode.

For information about this feature, see VEN Compatibility Check.

SecureConnect Setup on Workloads

For information about SecureConnect requirements for VENs, see SecureConnect in the *Security Policy Guide.*

MSI to EXE Package Format

Starting with the 21.2.1 Illumio Core release, the Windows VEN installer will switch from MSI to EXE package format. Customers using the PCE-based VEN deployment must take an extra step for the transition. Specifically, Illumio Core customers running older, MSI-based Windows VENs must upgrade to 19.3.6+H1-VEN or 21.2.0+H2-VEN before upgrading to their VENs to 21.2.1 or a later version. This release contains the necessary VEN changes to handle the transition in the VEN packaging from MSI to EXE.

VEN Proxy Support

This section describes how to enable proxy support for the VEN on all supported operating systems: Windows, Linux, AIX, and Solaris.

CAUTION:
For both platforms (Windows and Unix-based operating systems), the VEN does not automatically add IP addresses of proxy servers to the allowlist. Instead, be sure to write allow rules for proxy server IP addresses on the PCE. When the VEN is moved into Enforced mode, failure to write allow rules will result in permanent loss of connectivity between the VEN and the PCE. If that were to happen, the PCE will not be able to apply rules to the VEN to help restore connectivity.

NOTE:
Proxy support setup for the VEN is different between Unix-based versus Windows operating systems due to platform differences.

On Unix-based operating systems, the VENs do not require system-wide proxy setting. For Unix-based VENs, each application obtains the proxy settings from the user, for example, `curl --proxy myproxy:80`.

On Windows, the operating system provides proxy settings; for example, the Chrome browser uses the same proxy setting as Microsoft Edge. Alternatively, you can use the Core 22.2.32-VEN Preview feature to explicitly configure the Windows proxy for the VEN.

VEN Connections via Windows Proxy Servers

For Windows workloads only, Illumio Core supports a VEN-to-PCE connection through proxy servers.

- The default proxy configuration on the OS is used and proxy configuration might not be required or available on the VEN.
- Only non-authenticated proxy is supported, which might require you that add an exception for the PCE address.
- Only HTTP proxy is supported. The VEN will detect the proxy automatically and configuration or mode change will not be required.

Configuration for a Windows Proxy Server

- If the network environment supports WPAD protocol, the VEN will automatically use WPAD to discovery proxies and no special configuration is required.
- If proxy configuration is done via a PAC file, you will have to import Internet Explorer's (IE) proxy setting with the PAC file URL to the LocalSystem user (S-1-5-8). The VEN only supports `http://` PAC file URL. It does not support `file://` URLs.
- If proxies are statistically configured, you can configure using one of the following two methods:
  - Using `netsh winhttp set proxy` command. This method takes precedence. For `netsh winhttp` usage, refer to https://docs.microsoft.com/en-us/-previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc731131(v=ws.10).
  - Importing IE setting with static proxies setting to the LocalSystem user. For importing IE settings for the VEN, refer to https://server-fault.com/questions/34940/how-do-i-configure-proxy-settings-for-local-system.

NOTE:
Both IE-based proxy setting and `netsh winhttp` can be pushed to the endpoints (PCs) using Group Policy.

For information about the proxy string format to use for Windows proxy servers, see also WINHTTP_PROXY_INFO (winhttp.h) - Win32 apps in the Microsoft documentation for information.

VEN Connections via Unix-based Proxy Servers

Release 21.1.0 and later releases extend VEN proxy support from Windows to Linux, AIX, and Solaris systems.

In comparison with Windows, the following limitation affects this feature for Unix-based proxy servers. This release doesn't support the Web Proxy Auto Discovery (WPAD) protocol or proxy discovery via the Proxy Auto Discovery (PAC) file for Unix-based proxy servers. This limitation occurs because VENs use LibCurl as the HTTP transport library, but LibCurl does not provide JavaScript execution capability needed to run proxy scripts. For a workaround, see Proxies - Everything curl.

Configuration for Unix-based Proxy Servers

To set up your environment for a Unix-based proxy server, perform the following steps:

1. Set the proxy string during activation using the `--proxy-server` option. For example, use `illumio-ven-ctl activate --proxy-server proxy-string` as shown:

```
root@qual-solaris11-L:/opt/illumio# /opt/illumio_ven/illumio-ven-ctl activate
--management-server example.com:8443 --activation-code <code> --proxy-server
172.24.88.114:3128
Checking Runtime Environment.....              Activating Illumio
             ------------------
Storing Activation Configuration .....
Starting Illumio Processes.....                  Pairing Status
               --------------
Pairing Configuration exists ......SUCCESS
VEN Manager Daemon running ........SUCCESS
Master Configuration retrieval ....SUCCESS
VEN Configuration retrieval .......SUCCESS
VEN has been SUCCESSFULLY paired with Illumio
root@qual-solaris11-L:/opt/illumio# /opt/illumio_ven/illumio-ven-ctl show-
proxy
proxy_server: 172.24.88.114:3128
```

2. Set or modify the proxy string using `illumio-ven-ctl set-proxy proxy-string` and clear the proxy setting using `illumio-ven-ctl reset-proxy` as shown:

```
[root@ven-rhel illumio_ven]# ./illumio-ven-ctl set-proxy
http://proxy.example.com:3128

Updating proxy to http://proxy.example.com:3128. VEN restart needed.
[root@ven-rhel illumio_ven]# ./illumio-ven-ctl restart
Shutting down illumio-control:
 - venAgentMonitor Stopping venAgentMonitor:                [  OK  ]
<snip>

Starting illumio-control:
 - Environment Setting up Illumio VEN Environment:         [  OK  ]
```

```
<snip>

[root@ven-rhel illumio_ven]# ./illumio-ven-ctl show-proxy
proxy_server: http://proxy.example.com:3128
[root@ven-rhel illumio_ven]# ./illumio-ven-ctl reset-proxy
Resetting proxy. VEN restart needed.
[root@ven-rhel illumio_ven]# ./illumio-ven-ctl restart
Shutting down illumio-control:
 - venAgentMonitor Stopping venAgentMonitor:               [  OK  ]
<snip>
Starting illumio-control:
 - Environment Setting up Illumio VEN Environment:        [  OK  ]
<snip>
[root@ven-rhel illumio_ven]# ./illumio-ven-ctl show-proxy
No proxy is set
```

3. Restart the VEN after the proxy is set, modified, or cleared, except when the proxy is enabled using `--proxy-server` during activation. Query your current proxy setting using the `illumio-ven-ctl show-proxy` command.
4. Use the proxy string format: `[<scheme>"://"]<server>[":"<port>]`

   In the string format, `[]` indicates optional values in the command and `<>` indicates required values in the command; therefore, specifying either `--proxy-server 172.24.88.114:3128` or `http://172.24.88.114:3128` are both valid.

NOTE:
When specified, only the “http” scheme is supported. Schemes such as “https” or any other schemes are not supported. For example, `http://myproxy:8080` or `http://10.0.0.2:80`.

For Linux RPM (or AIX `installp`) installation, you can set the proxy string by setting and exporting the proxy string from the `VEN_PROXY_SERVER` shell variable before invoking the RPM (or `installp`) command.

For Solaris `pkgadd`, you can set the proxy string by setting the `VEN_PROXY_SERVER` variable to an answer file (typically created using the `pkgask` command).

Linux Pairing Script Activation for Proxy Servers

Typically, VENs are paired with the PCE directly. However, if a workload is behind a Web Proxy, you must follow these steps to enable your Linux/Unix VEN to

successfully pair to your PCE:

1. From the PCE web console menu, choose **Workloads and VENs > Pairing Profile**.
2. Copy the pairing line from the Linux/Unix OS Pairing Script window.
3. Paste this pairing line into a text file so that you can edit it.
4. Edit the pairing line to make the following two changes (displayed in **bold**):
   a. Add **–x <proxy-string>** to the curl command to indicate the proxy string.
   b. Add **--proxy-server <proxy-string>** to the switch to pass the proxy string to the pairing script.

   ```
   rm -fr /opt/illumio_ven_data/tmp && umask 026 && mkdir -p /opt/illumio_ven_data/tmp && curl –x <proxy-string> --tlsv1 "https://example.-com:8443/api/v18/software/ven/image?pair_script=pair.sh&profile_id=1" -o /opt/illumio_ven_data/tmp/pair.sh && chmod +x /opt/illumio_ven_data/t-mp/pair.sh && /opt/illumio_ven_data/tmp/pair.sh --management-server <server fqdn> --proxy-server <proxy-string>
   ```

5. Paste the revised script into the Linux/Unix terminal and press **Enter**.

The workload starts the pairing process. As the pairing script runs, you will see success messages appear. Wait until you see the message “Workload has been SUCCESSFULLY paired with Illumio,” which means your VEN (behind a proxy server) and the PCE are paired.

Chapter 3

Set up PCE for VEN Installation

This chapter contains the following topics:

When you plan to install or upgrade the VENs in your environment by using the PCE web console, be sure that you complete the PCE setup tasks described in this section before logging into the PCE web console to install VENs.

VEN Library Setup in the PCE

You can use your PCE cluster as a centralized mechanism for distributing, installing, and upgrading VENs in your environment.

NOTE:
If you are an Illumio Secure Cloud customer, you do not need to set up the VEN Library in the PCE. Illumio Operations performs these tasks and upgrading VENs using the PCE web console and REST API is available for your environment. See VEN Upgrade Using the PCE Web Console for information.

About the VEN Library in the PCE

You can use the PCE web console to install and upgrade VENs in your environment in the following scenarios:

- To install or upgrade RPM, Debian, and Windows distributions of the VEN software. Other workload operating systems are not supported.
- The PCE and VEN versions are 18.2 and later.

VEN installation from the PCE does not affect any processes you might already have for installing or upgrading VENs directly on workloads, such as installation or activation/pairing with `illumio-ven-ctl`. Those processes can continue until and after you decide to use the PCE to install and upgrade VENs.

This topic primarily describes how to use the PCE web console to install and upgrade VENs. However, you can also use the Illumio Core REST API to upgrade (but not install) VENs. See the *REST API Developer Guide* for information.

VEN Library

Previously, VENs could be deployed from an external VEN repository (VEN repo) or by manually installing the VEN packages directly on your workloads.

From the 18.2.0 release onwards, the PCE can act as a repository for distributing, installing and upgrading the VEN software. The PCE can host multiple VEN versions, allowing you to evaluate and certify new versions of the VEN while continuing to deploy older versions in production.

PCE-based installation and upgrade of VENs replaces the use of the external VEN repo, which is no longer supported for VEN version 18.2.0 or higher. A migration path is available for Illumio Secure Cloud customers and on-premises customers with VEN repos upgrading VENs to 18.2.0.

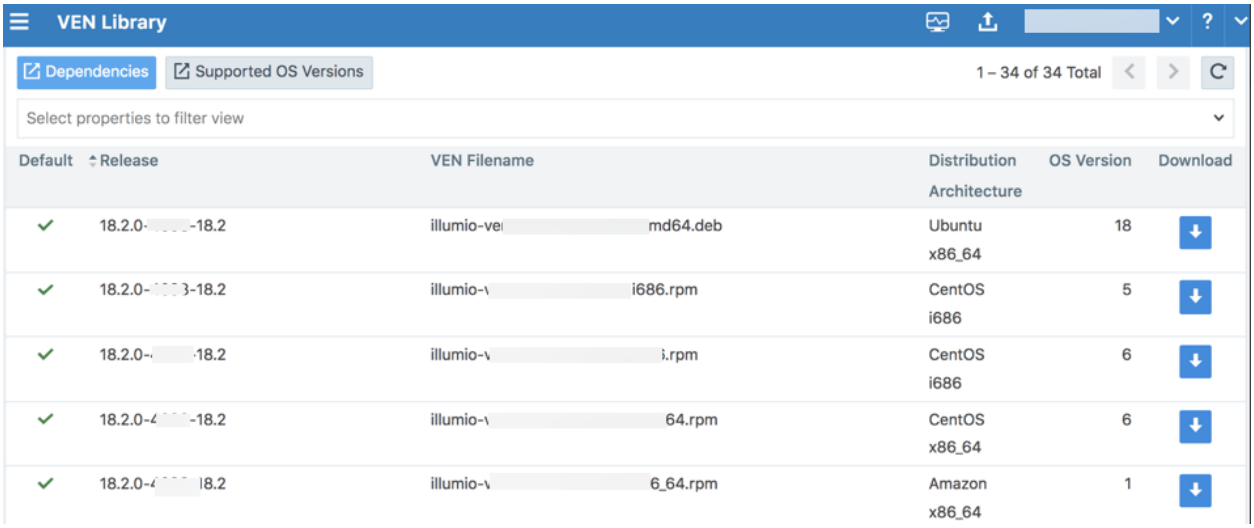
Using the VEN Library to install and upgrade VENs on your workloads has the following benefits:

- The VEN software bundle loaded on a PCE is replicated to all PCE core nodes.
- You can view VEN versions from the VEN Library page in the PCE web console.
- You can download software on workstations.
- Multiple versions of VEN software can exist on the PCE.
- You can specify an initial VEN version in pairing profiles.
- You can specify a default VEN version when the PCE has multiple VEN versions uploaded.
- You can add and remove VEN versions from the PCE.
- You can use the PCE to upgrade all VENs or selected VENs in your environment.

After setting up the VEN software bundle using the PCE control interface `illumio-pce-ctl`, the VEN Library page is available in the **Workloads and VENs > VEN Library** menu

. From this page, you can download individual VEN packages and view the dependencies and supported OS versions.

NOTE:
You must set an initial VEN version when there is no system default version or an external repository has not been configured. If your PCE has existing pairing profiles created without versions, pairing will fail when use those un-versioned profiles.



Migration to PCE-Based VEN Library

Migration from the central VEN repo or an on-premises VEN repo to the VEN Library should be thoroughly planned and timed to not impact your current operations. Contact Illumio Customer Support for assistance.

PCE Runtime Parameters for PCE-based Installation

After you have migrated from any external VEN repo you might have, remove the following parameters from the PCE `runtime_env.yml` file:

- `ven_repo_url`
- `ven_repo_ips`

These parameters are not needed for the PCE-based installation of the VEN. They are deprecated and should no longer be used.

Workflow for VEN Library Setup

You do not have to make any configuration changes or other settings to enable the VEN Library on the PCE.

Loading the VEN bundle into the PCE VEN Library enables the using the PCE web console or Illumio Core REST API to install and upgrade VENs in your environment.

To set up the VEN Library, perform the following high-level tasks:

1. Upload the VEN upgrade compatibility matrix to the PCE. See Upload VEN Upgrade Compatibility Matrix.

   NOTE:
   The compatibility matrix must be uploaded to the PCE before you upload any VEN software bundles or you will get an error.

2. Download the version of the VEN software bundle from the Illumio Support site.
   a. On the Illumio Support site (login required), go to **Software** > **Download** > **VEN – Download**.
   b. In the Download VEN page, select the radio button for the VEN version you want to set up. From the table, click the filename link for the "VEN Bundle for PCE-based deployment."

      TIP:
      Illumio recommends that you verify the checksum of the VEN software bundle after downloading it.

   The VEN software for PCE-based deployment is a zipped tarball (tar file) of a version of VEN software for all supported workload platforms. This tarball is known as a VEN *software bundle*. The tar file downloads to your local drive.

3. Repeat step 1 for all the VEN versions you want to distribute to your workloads.

   Additionally, when Illumio releases new versions of the VEN software, plan on repeating these steps when you are ready to deploy that VEN version.

4. Copy or move the VEN software bundle tar file to a convenient directory on your PCE core node or to any system that your PCE can reach with HTTP, SFTP, or SCP.

   You do not need to unpack the VEN software bundle tar file.

5. Load the VEN software bundle into one of the PCE core node's VEN Library. From this node, the VEN software bundle is automatically copied to the other nodes.

   See Upload VEN Software Bundle into PCE VEN Library for information.

6. Install or upgrade VENs:
   a. To install the VEN software on workloads, with the PCE web console, generate a pairing script. See Pairing Profiles and Scripts for information.
   b. To upgrade all VEN workloads or selective workloads, use the PCE web console. See VEN Upgrade Using the PCE Web Console for information.

Upload the VEN Upgrade Compatibility Matrix

NOTE:
The compatibility matrix must be uploaded to the PCE before you upload any VEN software bundles or you will get an error.

Alternatively, you can run the compatibility matrix upload command in one line with the command to install a VEN software bundle; for example:

```
sudo -u ilo-pce illumio-pce-ctl ven-software-install bundle_path --
compatibility-matrix matrix_file_path
```

As part of setting up the VEN Library in the PCE, you must upload the VEN upgrade compatibility matrix to the PCE. The compatibility matrix contains information about valid VEN upgrade paths and VEN to PCE version compatibility. To use the PCE web console and the Illumio Core REST API, you must upload this matrix for VEN upgrades to be successful.

In Supercluster, VENs are managed from the PCE they are paired to. You must upload VEN bundles and the compatibility matrix to each PCE.

The compatibility is a zipped tarball (tar file). You do not need to unpack the tar file to install it. The tarball contains a set of JSON files specifying the rules for upgrading VENs in your environment.

You can also view these VEN upgrade rules on the Illumio Support site (log in required). Go to **Software** > **Upgrade > VEN – Upgrade**. In the Upgrade VEN page, select your current VEN version and the version you want to upgrade to. Click **Find My Upgrade Path**.

IMPORTANT:
Until you upload this file, you can only install VENs on workloads when the VEN version is the same as the version of the PCE managing those VENs. Attempting to upgrade a VEN version, will return the message: “No valid upgrade paths were found for this release.”

To install the compatibility matrix:

1. Download the VEN upgrade compatibility matrix tar file from the Illumio Support site (log in required). Go to **Software** > **Download** > **PCE – Download**.and select the version for this releases. In the table, click the link for the “PCE-VEN Compatibility Matrix.” The file downloads to your local drive.

   TIP:
   Illumio recommends that you verify the checksum of the compatibility matrix file after downloading it.

2. Copy or move the tar file to a convenient directory on your PCE core node.
3. To upload the file to the PCE, run this command on the PCE:

   ```
   sudo -u ilo-pce illumio-pce-ctl compatibility-matrix-install matrix_file_path
   ```

Upload VEN Software Bundle into PCE

NOTE:
Before you upload a VEN software bundle into the PCE, you must first have uploaded the VEN upgrade compatibility matrix. See Upload the VEN Upgrade Compatibility Matrix for information.

Loading the VEN software bundle consists of running `illumio-pce-ctl` on the PCE command line to load the VEN software bundle into the PCE's VEN Library. The VEN Library is then replicated to the other PCE core nodes.

Loading the VEN software bundle into the PCE's VEN Library is what configures the PCE as the VEN installation and upgrade method.

In Supercluster, VENs are managed from the PCE they are paired to. You must upload VEN bundles and the compatibility matrix to each PCE.

You can only upload VEN software bundles into a PCE that are compatible with that PCE. For example, you cannot upload VEN version 21.5.0 software bundles into a PCE version 21.2.0.

To load a VEN software bundle:

1. Copy the downloaded VEN software bundles to a convenient location on your PCE core node or to any system that the PCE can access via HTTP, SFTP, or SCP.
2. To load the VEN software bundle, run the following command on the core node's command line.

   ```
   sudo -u ilo-pce illumio-pce-ctl ven-software-install bundle_path
   ```

   For example:

   ```
   sudo -u ilo-pce illumio-pce-ctl ven-software-install
   protocolAndFqdnOfVenBundleHost/nameOfVenSoftwareBundleFile.tar.bz2
   ```

   Where:

   - *bundle_path* is any of the following locations of the VEN software bundle tar file:
     - The absolute or relative path to the directory on the PCE
     - The HTTP URL to the host and file
     - The SFTP URL to the host and file
     - The SCP URL to the host
   - The filename of the VEN software bundle tar file uses the following format:

     `illumio-ven-repo-someVersionStamp.tar.bz2`

     Where `someVersionStamp` is the version and build number of the Illumio Core release.

Example

The following example assumes you have copied the VEN software bundle into `/var/tmp` on you PCE:

```
# sudo -u ilo-pce illumio-pce-ctl ven-software-install /var/tmp/illumio-ven-repo-
someVersionStamp.tar.bz2
Reading /opt/pce_config/etc/runtime_env.yml.
```

```
Validating VEN release tarball file contents:
     Valid.
Deploying VEN release tarball to 'PCE's IP address' .

Committing tarball manifest information to database.
Are you sure you want to continue? [yes/no]: yes

Release version_of_bundle Successful.
```

HTTP and SCP Examples

These examples show HTTP and SCP URLs on the `illumio-pce-ctl ven-software-install` command:

- HTTP:

```
sudo -u ilo-pce illumio-pce-ctl ven-software-install
http://myVENrepohost.BigCo.com/myRepoDir/pcerepo/illumio-ven-repo-
someVersionStamp.tar.bz2
```

- SCP:

```
sudo -u ilo-pce illumio-pce-ctl ven-software-install
scp://albert.einstein@myhost.BigCo.com:illumio-ven-repo-
someVersionStamp.tar.bz2
```

Set Default VEN Version in Library

You can set a default version of the VEN software for all workloads or for selected pairing profiles. You can use both methods simultaneously. For example:

- Set a default VEN version for all workloads when you are ready to roll out that specific version.
- Create a separate pairing profile with a specific VEN version for test, evaluation, and certification before general rollout.

Set Default VEN Version for All Workloads

To define the default VEN version for all workloads, run this command on the PCE:

```
sudo -u ilo-pce illumio-pce-ctl ven-software-release-set-default release
```

Where:

`release` is a release identifier like 19.3.0-6623. The PCE uses the default release to determine what release of the VEN to install when you pair a VEN with a workload. You can override the default release for specific pairing profiles. To obtain release IDs, run the `sudo -u ilo-pce illumio-pce-ctl ven-software-releases-list` command.

Set Default VEN Version for Specific Pairing Profile

You can selectively set a VEN version for specific pairing profiles. The profiles that have a defined VEN version create pairing profiles that install that specific VEN version on the workload. Other pairing profiles that have no VEN version set are unaffected.

To set a pairing profile's VEN version, see Configure a Pairing Profile.

For information about pairing scripts, see prepare Scripts.

Remove a Release from the VEN Library

To remove a VEN version from the VEN Library on the PCE, run this command on the PCE:

```
sudo -u ilo-pce illumio-pce-ctl ven-software-release-delete release
```

Where:

`release` is a release identifier like 19.3.0-6623. To obtain release IDs, run the `sudo -u ilo-pce illumio-pce-ctl ven-software-releases-list` command.

IMPORTANT:
To remove a VEN version from the PCE database, the PCE cannot be using that VEN version in pairing profiles and it cannot be set as the default VEN version for pairing with workloads. When your orgs no longer use that VEN version, the `ven-software-release-delete` command will remove the VEN software bundle from the PCE file system.

View the VEN Library in the PCE

The VEN loading process with `sudo -u ilo-pce illumio-pce-ctl ven-software-install` prints its success or failure when it completes. You can also verify the successful loading in the following ways:

- In the PCE web console, look at the VEN Library. Navigate to **Workloads and VENs > VEN Library** to see that the bundle has been loaded.
- On the PCE command line, run the following command:

```
sudo -u ilo-pce illumio-pce-ctl ven-software-releases-list
```

PCE Maintenance for VEN Library

These are some points to consider about backing up and modifying your PCE cluster for the PCE-based deployment model.

About PCE Backups

Be sure that your backup included the PCE's VEN library and is not earlier than when you loaded the VEN software bundles into the PCE's VEN Library. If you restore from an earlier backup, you need to either reload the VEN library or redeploy from an existing core node.

About Complete PCE failure

In case of a catastrophic failure of the PCE cluster, after rebuilding or reinstalling the cluster, reload the VEN software bundles into a PCE core node's VEN library.

VEN-related Maintenance Commands on PCE

The `illumio-pce-ctl` control script has options for VEN maintenance, such as add new VEN software bundle, remove VEN version, and delete VEN version. See the `illumio-pce-ctl --help` details.

Some of the options for distributing VENs from the PCE show org-id, org-list, and other organization-related arguments. None of the organization-related options or arguments options are needed for distributing VENs from your on-premises PCE and do not need to be specified.

Set up Kerberos Authentication on PCE

You can configure the PCE and VEN to rely on authentication by a pre-configured Kerberos-based system, such as Microsoft Active Directory.

About Enabling Kerberos Authentication

1. Enable Kerberos on the PCE. See About Enabling Kerberos Authentication.
2. Configure Kerberos-based authentication of the VEN at installation. Illumio Core supports Kerberos authentication for Linux, Windows, Solaris, and AIX VENs.

   For information, see the following topics:

   - Kerberos for Linux VEN-to-PCE Authentication
   - Kerberos for Windows VEN-to-PCE Authentication

Requirement for Kerberos Authentication

For all VENs to be paired via Kerberos, be sure to add policy rules allowing access to the required Kerberos servers.

Obtain an activation code for the VEN. When installing the VEN by using the VEN CTL, you can use the activation code either during installation or after installation. For information about activation codes for the VEN, see About the VEN Activation Code.

About Kerberos Authentication on the PCE

To use Kerberos authentication to pair a workload, you must enable Kerberos authentication on the PCE. Kerberos authentication requires configuring the following parameters in your PCE's runtime_env.yml file:

PCE Runtime Environment File Parameter	Description
`kerberos_device_auth_service_name:` `kerberos_device_auth_keytab_file`	Kerberos authentication for VENs on devices. These parameters enable Kerberos authentication for the VENs and other devices and provide a Kerberos service name and keytab file. These parameters are only used when the PCE node's role is set to `agent_service`. • The `kerberos_device_auth_service_name` must contain the complete Service Principal Name (SPN); for example, `servicename/fqdn@realm`.
`kerberos_user_auth_service_name:` `kerberos_user_auth_keytab_`	Kerberos user authentication for the Login Service. These parameters enable Kerberos authentication for the Login Service and provide a Kerberos service name and keytab. • The `kerberos_user_auth_service_name` must contain the complete Ser-

PCE Runtime Environment File Parameter	Description
`file`	vice Principal Name (SPN); for example, `servicename/fqdn@REALM`. Kerberos requires that the `REALM` be in all capital letters. • The `kerberos_user_auth_service_name` is the path to the PCE's Kerberos keytab file. Any key included in keytab can be used for authentication

`prepare` Scripts

The `prepare` script is used for creating golden images to activate the VEN the first time the image is booted.

Prepare Golden Image for Workload Installation

Many organizations use "golden images" for faster deployment. When using a golden image to install a VEN, you have two options for pairing with the PCE:

- Use a modified version of the Illumio Core pairing script called `prepare` to ensure these golden images have the VEN pre-installed.
- Use the `illumio-ven-ctl` control script.

IMPORTANT:

- You should enable your images with the `prepare` script as *the last step* in building the image. The `prepare` script takes effect at the next system boot, which means the VEN might be activated prematurely on the image itself. If you have other software to install on the image and the image requires reboot, the VEN is activated at once, which is probably not desirable.
- In the PCE web console, the pairing profile has two types of activation codes: one-time use or unlimited use. Be sure to specify the correct type for your needs. For more information, see Configure Pairing Key Usage and Lifespan.

Prepare Using the Pairing Profile/Pairing Script

This option relies on the pair script displayed in the PCE web console.

1. In the PCE web console, create a pairing profile or select an existing pairing profile. For information, see Pairing Profiles and Scripts
2. Copy the pairing script.
3. In the copy of the script, change all occurrences of `pair` to `prepare`.
4. Run the modified script on the image.

   The `prepare` script installs the VEN on the image. When the prepare scripts finishes, the VEN is stopped. The script configures the VEN to start the next time the workload is booted.

Prepare the Workload with `illumio-ven-ctl`

Instead of the `prepare` script, you have several options:

- Use `illumio-ven-ctl` to set the image into "prepare" mode:

  ```
  # /opt/illumio_ven/illumio-ven-ctl prepare –management-server <pce_fqdn:port>
  --activation-code <activation_key>
  ```

- Use an activation file that contains the activation code and management server name and port. The configuration file is read when the VEN is started when the image is booted.
  - On Windows, by default, the file is `C:\ProgramData\Illumio\etc\agent_activation.cfg`
  - On Linux, by default, the file is `/opt/illumio_ven_data/etc/agent_activation.cfg`

  Contents of `agent_activation.cfg`:

  ```
  activation_code: <your_activation_code>
  masterconfig_server: <your_pce_fqdn:your_port>
  ```

Example activation configuration file:

```
activation_code:
11bbbe89962159ffe7f0b7e71a532910aa47171f97bc0ad3a0219a780f559006a320587bba966a854
masterconfig_server: pce.example.com:8443
```

Auto Scaling Linux Workloads

The process for enabling Illumio Core to enable auto scaling for Linux workloads follows this general process:

1. Select an existing VM instance that you want to create a new instance for.
2. Inside the PCE web console, create a pairing profile (or select an existing pairing profile).
3. Copy and edit the Linux pairing script:

```
rm -fr /opt/illumio_ven_data/tmp && umask 026 && mkdir -p /opt/illumio_ven_
data/tmp && curl --tlsv1
"https://pce.example.com:8443/api/v18/software/ven/image?pair_
script=pair.sh&profile_id=1" -o /opt/illumio_ven_data/tmp/pair.sh && chmod +x
/opt/illumio_ven_data/tmp/pair.sh && /opt/illumio_ven_data/tmp/pair.sh --
management-server pce.example.com:8443 --activation-code
11a12969c511197eb7ae1e175b9b49382fe1bc011b2a2228c8a184cc6c9f75663325146e5d5ac
7c5d
```

   Change all occurrences of the script where `pair.sh` is used and replace with `prepare.sh`.

   So that the script looks like this:

```
rm -fr /opt/illumio_ven_data/tmp && umask 026 && mkdir -p /opt/illumio_ven_
data/tmp && curl --tlsv1
"https://pce.example.com:8443/api/v18/software/ven/image?pair_
script=prepare.sh&profile_id=1" -o /opt/illumio_ven_data/tmp/prepare.sh &&
chmod +x /opt/illumio_ven_data/tmp/prepare.sh && /opt/illumio_ven_
data/tmp/prepare.sh --management-server pce.example.com:8443 --activation-
code
11a12969c511197eb7ae1e175b9b49382fe1bc011b2a2228c8a184cc6c9f75663325146e5d5ac
7c5d
```

The `prepare.sh` script installs the VEN on the new workload and configures it so the VEN will start running as soon as the new workload is instantiated.

1. Run the modified script on the Linux instance.
2. Configure your auto scaling policy to use an image that contains the `prepare` script.

Auto Scaling for Windows Workloads

The process for enabling Illumio Core to enable auto scaling on Windows workloads follows this general process:

1. Select an existing VM instance that you want to create a new instance for.
2. In the PCE web console, create a pairing profile (or use an existing pairing profile).
3. Copy and edit the Windows pairing script:

```
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:8443/api/v18/software/ven/image?pair_
script=pair.ps1&profile_id=1', (echo $env:windir\temp\pair.ps1)); &
$env:windir\temp\pair.ps1 -management-server pce.example.com:8443 -
activation-code
11a12969c511197eb7ae1e175b9b49382fe1bc011b2a2228c8a184cc6c9f75663325146e5d5ac
7c5d;}"
```

Change all occurrences of the script where `pair.ps1` is used and replace with `prepare.ps1`.

So that the script looks like this:

```
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:8443/api/v18/software/ven/image?pair_
script=prepare.ps1&profile_id=1', (echo $env:windir\temp\prepare.ps1)); &
$env:windir\temp\prepare.ps1 -management-server pce.example.com:8443 -
activation-code
11a12969c511197eb7ae1e175b9b49382fe1bc011b2a2228c8a184cc6c9f75663325146e5d5ac
7c5d;}"
```

The `prepare.ps1` script installs the VEN and configures it such that the VEN will start running as soon as the new workload is instantiated.

1. Run the modified script on the Windows instance.
2. Configure your auto scaling policy to use the prepared image.

Chapter 4

VEN Installation & Upgrade Using VEN Library

This chapter contains the following topics:

The following topics describe how to install and upgrade the VEN by using the VEN Library in the PCE.

NOTE:
Before you perform the tasks described in this section, the PCE must be set up with the VEN Library. For information, see VEN Library Setup in the PCE

Pairing Profiles and Scripts

A pairing profile contains the configuration for workloads so that you can apply certain properties to workloads as they pair with the PCE, such as applying labels, setting workload policy state, and more.

When you configure a pairing profile, the pairing script contains a unique pairing key at the end of the script (an activation code) that identifies the VEN securely so it can authenticate with the PCE. The pairing key can be set to be used one time or several times, and you can configure its time and use limit.

In the PCE web console, you create a pairing profile with the characteristics to create a script called a pairing script to run on workloads. The pairing script installs the VEN software, activates it, and gets the workloads ready to accept security policy from the PCE. “Pairing” is also known as “installation and activation.”

Workflow for Using Pairing Profiles

Creating and using pairing profiles follows this general workflow:

1. Create a pairing profile.
2. Generate a pairing script.
3. Copy the script to the workload and run it.

The following conditions apply when installing VENs by using pairing profiles:

- An activation code/pairing key is required. In the PCE web console, you can specify either a single, one-time activation code or an unlimited, multi-use activation code.
- The pairing script is not absolutely required. It is an alternative to installing VEN software installation and activation with the VEN CTL (`illumio-ven-ctl`).

Which VEN Version is Installed

A particular version of the VEN is only installed on a workload when it is activated.

- In the PCE web console if you have set a **Current Default** VEN version for all workloads, that default version gets installed on all workloads.
- If you set a specific VEN version for a pairing profile in the PCE web console, that specific VEN version gets installed on the workload regardless of the **Current Default**.

Last Pairing Key Generation Information

The last pairing key generation information can be found in the PCE Web Console Pairing Profile details page by clicking a profile name and in the API.

The Default Pairing Profile

Item	Description
Name	Default
Labels	Role=<Blank> Application=<Blank> Environment=Production

Item	Description
	Location=<Blank>
Workload State	Visibility Only
Uses per Key	Unlimited
Maximum Key Age	Unlimited
Command Line Overrides	Unlocked (CLI can override anything)

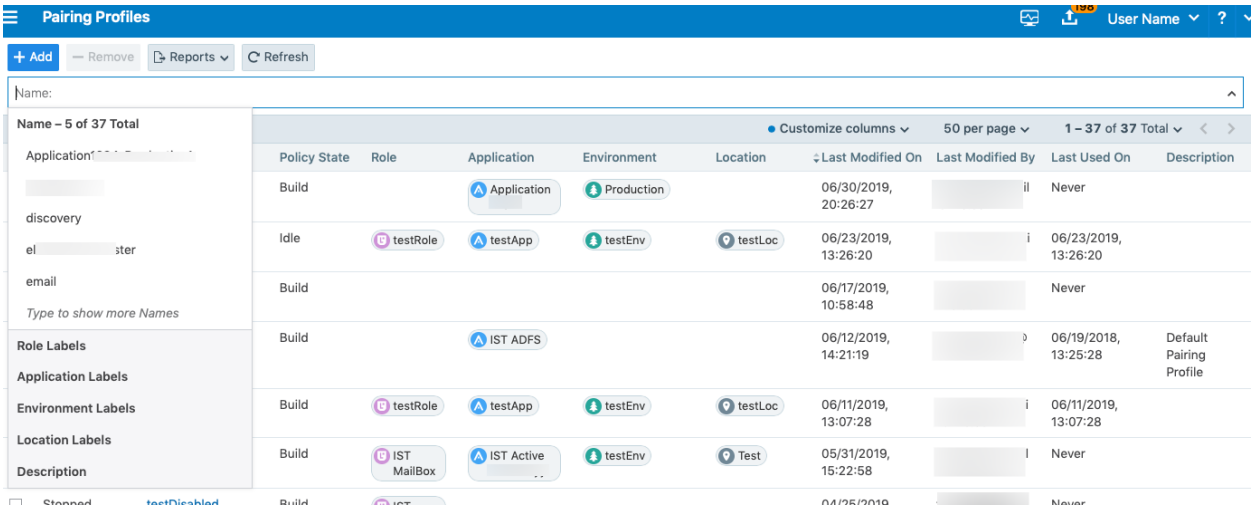
Last Pairing Key Generation Information

For each pairing profile, the PCE Web Console now shows on the pairing profile details page:

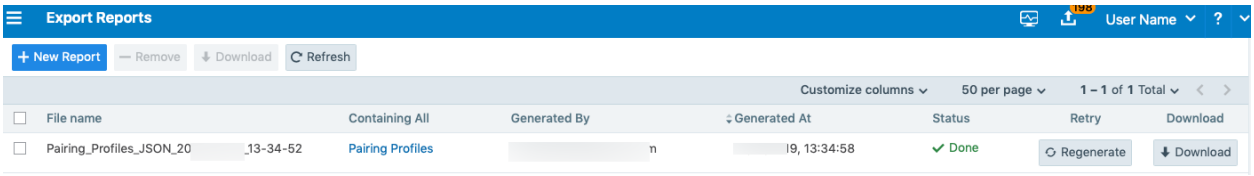
- Last time a pairing key was generated using this pairing profile.
- Last time a VEN was paired using this pairing profile.

Filter the Pairing Profiles List

You can filter the pairing profiles list using the properties filter at the top of the list. You can filter the list by entering a label type to show only those pairing profiles that use the selected labels. You can further filter the list by selecting specific properties of the pairing profiles. For example, you can filter the list by a pairing profile's name.



Click the **Reports** button and select JSON or CSV format to generate the pairing profiles report. Once generated, you can either click the download icon next to Reports to download the generated report or select **Reports > All Export Reports** to view the report details.



Configure a Pairing Profile

You can configure a pairing profile to set the initial workload policy state at the time of pairing. For example, you might want to pair workloads in the Visibility state so you can view network traffic to build policies before enforcing them.

On the other hand, if you are configuring an auto-scale policy and want to pair workloads automatically based on application demands, you can choose to have workloads paired in Full enforcement state.

To configure a pairing profile:

1. From the PCE web console menu, choose **Policy Objects** > **Pairing Profiles**.
2. Click **Add**.

   The Pairing Profile page appears.
3. Enter a name and description (optional) for the pairing profile.
4. Select the *Initial VEN Version*. This is the VEN version that will be installed initially. You can later edit the pairing profile and select another VEN version.
5. Configure the following options for the pairing profile and click **Save**.

Enforcement Mode for Policy

You can choose one of the enforcement modes for workloads when you pair them:

- **Idle**: A state in which the VEN does not take control of the workload's iptables (Linux) or WFP (Windows), but uses workload network analysis to provides the PCE relevant details about the workload, such as the workload's IP address, operating system, and traffic flows. This snapshot is taken every ten minutes.

  NOTE:
  SecureConnect is not supported on workloads in the Idle policy state. If you activate SecureConnect for a rule that applies to workloads that are in both Idle and non-Idle policy states, it could impact the traffic between these workloads.

- **Visibility:** In the Visibility Only state, the VEN inspects all open ports on a workload and reports the flow of traffic between it and other workloads to the PCE. In this state, the PCE displays the flow of traffic to and from the workload, providing insight into the datacenter and the applications running in it. No traffic is blocked in this state. This state is useful when firewall policies are not yet known. This state can be used for discovering the application traffic flows in the organization and then generating a security policy that governs required communication.
- **Selective:** Segmentation rules are enforced only for selected inbound services when a workload is within the scope of a Selective Enforcement Rule.
- **Full:** Segmentation Rules are enforced for all inbound and outbound services. Traffic that is not allowed by a Segmentation Rule is blocked.

For information about how these enforcement modes impact workload security policy, see Enforcement States and Enforcement States for Rules in the *Security Policy Guide*.

You can choose one of three modes for the traffic visibility for workloads:

- **Off (no detail)**: The VEN does not collect any details about traffic connections. This option provides no Illumination detail and utilizes the least amount of resources from workloads. This state is useful when you are satisfied with the rules that have been created and do not need additional overhead from observing workload communication.
- **Blocked:** The VEN only collects the blocked connection details (source IP, destination IP, protocol and source port and destination port), including all packets that were dropped. This option provides less Illumination detail but also demands fewer system resources from a workload than high detail.
- **Blocked + Allowed:** The VEN collects connection details (source IP, destination IP, protocol and source port and destination port). This applies to both allowed and blocked connections. This option provides rich Illumination detail but requires some system resources from a workload.

Assign Workload Labels

You can specify in the pairing profile which labels you want the to assign to workloads when they are paired. Labels group workloads into logical categories for use in rulesets.

The PCE provides four types of labels:

- **Role**: The role or function of a workload. In a simple two-tier application consisting of a web server and a database server, there are two roles: Web and Database.
- **Application**: The type of application the workload is supporting (for example, HRM, SAP, Finance, Storefront).
- **Environment**: The stage in the development of the application (for example, production, QA, development, staging).
- **Location**: The physical, geographic location of the workload (for example, Germany, US, Europe, Asia).

For information on creating labels, Labels and Label Groups in the *Security Policy Guide*.

Configure Pairing Key Usage and Lifespan

You can control the usage and lifespan of the pairing key in the pairing profile.

- **Uses Per Key**: Choose if you want the key generated from this pairing profile to be used an unlimited number of times or only once.
- **Key lifespan:** Specify how long you want the pairing key to be valid, either unlimited (forever) or for a specified time frame.

You can choose from these options to define how you want the pairing profile to be used:

- **Unlimited**: This option provides a pairing script that can be used to pair as many workloads in the organization as you want. Each user in an organization is given the pairing script from this profile regardless of the workload, the application the workload is a part of, the location of the workload (data center or country), or the environment (development, testing, QA, production). Unlimited use pairing profiles can present a security risk because they never change; however, if a pairing script is stolen, a workload could be paired into your environment by an untrusted user.

IMPORTANT:
Illumio recommends against configuring unlimited usage of pairing profiles from a security perspective. Instead, determine the appropriate lifespan for the pairing profile to minimize any security risk.

- **Custom Time Range**: If you do not want an unlimited use pairing profile, you can specify that the pairing profile can only be used to pair a workload one time, after which the pairing key cannot be used to pair more workloads.

Key Usage Requirements

The certification Key Usage requirements have changed to `CERT_DIGITAL_SIGNATURE_KEY_USAGE`, `CERT_KEY_ENCIPHERMENT_KEY_USAGE`, and `CERT_DATA_ENCIPHERMENT_KEY_USAGE`, so that the endpoint certificates can be set in the x.509 Windows environment.

Choose Command Line Overrides

For each of these Workload states, you can choose to either allow or block modifications to these settings when the pairing script is executed from the command line:

Workload Policy State

- **Lock Workload policy state assignment**: The policy state of the workloads being paired cannot be changed when the pairing script is run.
- **Allow Workload policy state assignment**: The policy state of the workloads being paired can be changed when the pairing script is run.

Label Assignment

- **Lock Label assignment**: This option prevents a user running the pairing script from assigning labels to workloads during pairing except for what is configured with the pairing profile.
- **Allow custom Labels**: This option permits the user running the pairing script to assign labels to the workloads during pairing using this pairing profile. Selecting this option selects all the Label checkboxes. You can deselect any before saving.

Start/Stop Pairing

To enable or disable the pairing profile, click the pairing profile. The pairing profile details page opens and you can click **Stop Pairing** or **Start Pairing** .

Generate Key

Click **Generate Key** at the top of the page to create a unique pairing key that can be used with the pairing script. The key will not be accessible once you close the Pairing Profile details panel.

Every key that is generated under a pairing profile inherits the properties set in the pairing profile. The script can be used to pair Workloads, according to the parameters and time limits set in the pairing profile.

Pairing Script

Regardless of how you choose to install VENs on workload (either by using the VEN Library or by using the packaging CLI and VEN CTL), you create the pairing profile in the PCE web console and run the pairing script on workloads.

Add Options to the Pairing Script

You can add additional pairing options to the pairing profile, such as assign labels to the workload, set the workload policy state, and set logging levels for VEN traffic.

For the complete list of options to use with the pairing script, see VEN Activate Command Reference.

Linux Pairing Script for VEN Library Installation

For example, if you want to add an Environment label to the workload, such as `--env Production`, include the option at the end of the pairing script as shown below.

```
rm -fr /opt/illumio_ven_data/tmp && umask 026 && mkdir -p /opt/illumio_ven_
data/tmp && curl "https://example.com:8443/api/v18/software/ven/image?pair_
script=pair.sh&profile_id=<pairing_profile_id>" -o /opt/illumio_ven_
data/tmp/pair.sh && chmod +x /opt/illumio_ven_data/tmp/pair.sh && /opt/illumio_
ven_data/tmp/pair.sh --management-server example.com:8443 --activation-code <code>
--env Production
```

Windows VEN Installation without the VEN Library

```
Set-ExecutionPolicy -Scope process remotesigned -Force; Start-Sleep -s 3; (New-
Object System.Net.WebClient).DownloadFile
("https://repo.illum.io/Z3JldGVsbHVuZHl0aGF0Y2hlcjg1dGgK/pair.ps1",
"$pwd\Pair.ps1"); .\Pair.ps1 -repo-host repo.illum.io -repo-dir
Z3JldGVsbHVuZHl0aGF0Y2hlcjg1dGgK/ -repo-https-port 443 ` -management-server
pce.example.com:8443 -activation-code <code> –env Production; Set-ExecutionPolicy
-Scope process undefined -Force;
```

Delete a Pairing Profile Key

If you want to completely disable the pairing keys generated with a pairing profile, delete the pairing profile.

To delete a pairing profile and its pairing keys:

1. From the PCE web console menu, choose **Policy Objects** > **Pairing Profiles**.
2. Select the checkbox of the pairing profiles you want to delete.
3. Click **Remove**.

All pairing keys that were associated with this pairing profile are no longer be valid for pairing workloads.

The same process applies if you are instantiating new VMs in vSphere or Microsoft Azure. You can use the modified Illumio PCE pairing script for preparing your new VMs for auto scaling.

VEN Installation Using VEN Library in PCE

Installing VENs by using the VEN Library in the PCE is only available for Windows and Linux hosts. You install VENs on AIX and Solaris hosts by downloading the VEN packages for those platforms and using the VEN CTL.

About VEN Installation, Pairing, and Upgrade

These are some general considerations for installing and upgrading VENs by using the VEN Library in the PCE web console.

- The target VENs can be in any state for installation or upgrade.
- Environment variables supported by the VEN CTL are not supported with when using the VEN Library to install VENs.
- Exact time to install or upgrade a VEN depends on many factors, including the speed of the workload hardware, the speed of its network connections, and its performance load.
- Before installation or upgrade, ensure that all the workloads on which you want to install or upgrade the VEN are online and reachable from the PCE. If they are not reachable when the installation or upgrade is running, they will be skipped.

About Installing VENs by Using the VEN Library

Installing the VEN by using VEN Library in the PCE web console is a two-step process. For each workload, perform the following high-level steps:

1. In the PCE web console, generate a pairing profile. Generating a pairing profile generates a pairing script.
2. Copy that pairing script to the workload and run it.

About Pairing Workloads

Pairing is the process of installing a VEN on a workload.

When you pair a workload, you run a script that installs the VEN on the workload. The VEN then reports detailed workload information to the PCE, such as all services running on the workload, all of its open ports, details about the operating system, workload location, and more.

When you configure and then provision rules, the PCE calculates and configures policy for each paired workload.

When you pair workloads, you can choose to place those workloads in one of these policy states:

Enforcement Mode for Policy

You can choose one of the enforcement modes for workloads when you pair them:

- **Idle**: A state in which the VEN does not take control of the workload's iptables (Linux) or WFP (Windows), but uses workload network analysis to provides the PCE relevant details about the workload, such as the workload's IP address, operating system, and traffic flows. This snapshot is taken every ten minutes.

  NOTE:
  SecureConnect is not supported on workloads in the Idle policy state. If you activate SecureConnect for a rule that applies to workloads that are in both Idle and non-Idle policy states, it could impact the traffic between these workloads.

- **Visibility:** In the Visibility Only state, the VEN inspects all open ports on a workload and reports the flow of traffic between it and other workloads to the PCE. In this state, the PCE displays the flow of traffic to and from the workload, providing insight into the datacenter and the applications running in it. No traffic is blocked in this state. This state is useful when firewall policies are not yet known. This state can be used for discovering the application traffic flows in the organization and then generating a security policy that governs required communication.
- **Selective:** Segmentation rules are enforced only for selected inbound services when a workload is within the scope of a Selective Enforcement Rule.
- **Full:** Segmentation Rules are enforced for all inbound and outbound services. Traffic that is not allowed by a Segmentation Rule is blocked.

For information about how these enforcement modes impact workload security policy, see Enforcement States and Enforcement States for Rules in the *Security Policy Guide*.

You can choose one of three modes for the traffic visibility for workloads:

- **Off (no detail)**: The VEN does not collect any details about traffic connections. This option provides no Illumination detail and utilizes the least amount of resources from workloads. This state is useful when you are satisfied with the rules that have been created and do not need additional overhead from observing workload communication.
- **Blocked:** The VEN only collects the blocked connection details (source IP, destination IP, protocol and source port and destination port), including all packets that were dropped. This option provides less Illumination detail but also demands fewer system resources from a workload than high detail.
- **Blocked + Allowed:** The VEN collects connection details (source IP, destination IP, protocol and source port and destination port). This applies to both allowed and blocked connections. This option provides rich Illumination detail but requires some system resources from a workload.

To start the Workload pairing process, you need to:

- Create a Pairing Profile or use the default pairing profile
- Pair workloads: Linux or Windows

VEN Package Format Changes (Windows only)

In Illumio Core 21.2.1, the Windows VEN installer switched from MSI to EXE package format. Customers using the PCE-based VEN deployment must take an extra step for the transition. Specifically, Illumio Core customers running older MSI-based Windows VENs must upgrade to 19.3.6+H1-VEN or 21.2.0+H2-VEN before upgrading to their VENs to 21.2.1 or a later version. Older VEN versions are not EXE package aware and cannot upgrade themselves without manual intervention on the CLI.

For the detailed steps required for this transition, see New Windows VEN Installer Starting with 21.2.1, Knowledge Base Article 3561 (login required).

Pair a Windows Workload

Pairing a workload requires running the pairing script on it to install the VEN.

When you first log into the PCE web console, a default pairing profile containing a pairing script is provided so you can begin pairing workloads. You also have the option to

create a new pairing profile if you want to configure your own workload pairing settings.

NOTE:
When the Illumio VEN is installed on a Windows workload and paired with the PCE in the Full enforcement policy state, all Internet Group Management Protocol (IGMP) traffic will be blocked unless you add a rule to allow it. Windows servers typically use IGMP for things like Windows Internet Name Service (WINS), Windows Deployment Services (WDS), IGMP Router/Proxy mode, and Network Load Balancing (NLB) in multicast mode.

WARNING:
Your pairing script to install a Windows VEN on a workload cannot contain colons in the values for command options. Including a colon in a option value causes VEN activation to fail. For example, including the following values in the `-role` option, causes VEN activation to fail:

```
-role "R: UNKNOWN" -app "A:UNKNOWN" -env "E: UNKNOWN"
```

Activation fails because Windows uses the colon as a special character and cannot interpret the value even when you include quotation marks around the value.

NOTE:
You must be logged in as an Administrator user on the Windows workload to run the Illumio pairing script.

To pair a workload on Windows:

1. From the PCE web console menu, choose > **Workloads and VENs > Workloads.**
2. Click **Add** > **Pair Workload with Pairing Profile**.

   The Pairing Profiles page appears.
3. From the drop-down list, select a pairing profile. The list contains the default pairing profile and the pairing profiles you've added.

   To create a new pairing profile, see Configure a Pairing Profile.
4. From the *Windows OS Pairing Script* field, copy the Windows pairing script.
5. On the Windows workload you want to pair, open the Windows PowerShell as an Administrator user.

6. Paste the pairing script you copied into the PowerShell command prompt.

   When the script finishing running, the following output appears:

```
PS C:\Program Files> 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:8443/api/v18/software/ven/image?pair_
script=pair.ps1&profile_id=1', '.\Pair.ps1'); .\Pair.ps1  -management-server
example.com:8443 -activation-code <code>;}"

             Installing Illumio
             ------------------
Setting up Illumio Repository ........
Retrieving Illumio Package ...........
Installing Illumio Package ...........
Validating Package Installation ......
Pairing with Illumio ..................
               Pairing Status
               --------------
Illumio Package installation ......SUCCESS
Pairing Configuration exists ......SUCCESS
VEN Manager Service running .......SUCCESS
Master Configuration retrieval ....SUCCESS
VEN Configuration retrieval .......SUCCESS
VEN has been SUCCESSFULLY paired with Illumio

PS C:\Program Files> cd .\Illumio\
PS C:\Program Files\Illumio> .\illumio-ven-ctl.ps1 status
Service venAgentMgrSvc:                 Running
Service venPlatformHandlerSvc:          Running
Service venVtapServerSvc:               Running
Service venAgentMonitorSvc:             Running
Service venAgentMgrSvc:                 Enabled
Service venPlatformHandlerSvc:          Enabled
Service venVtapServerSvc:               Enabled
Service venAgentMonitorSvc:             Enabled
Agent State: illuminated
```

7. To view the workload after it has finished pairing, choose **Workloads and VENs > Workloads** from the PCE web console menu.

Unpair a Windows Workload

Unpairing is the process of uninstalling the VEN from a workload so that it no longer reports any information to the PCE and can no longer receive any policy information. After uninstalling the VEN, the PCE will no longer maintain control over the workload.

NOTE:
After you remove a workload from the PCE using the PCE web console or REST API (but not by using the VEN CTL), it remains in policy computation and can continue to appear (for example, in auto complete fields or API responses) until the VEN confirms that it has been uninstalled or a one-hour delay has passed.

Windows Unpair Options

Carefully consider the security state you want to return the Windows workload to after the VEN is uninstalled:

- **Remove Illumio policy**: (Recommended) Remove Illumio Windows Filtering Platform (WFP) filters and activate the Windows firewall.
- **Open all ports**: Uninstalls the VEN and leaves all ports on the workload open to traffic.
- **Close all ports except remote management**: Temporarily allow only RDP/3389 and WinRM/5985, 5986 until the system is rebooted.

NOTE:
When you unpair a workload that uses a Windows GPO policy, the GPO policy overrides local WFP rules.

To unpair a Windows workload:

1. From the PCE web console menu, choose **Workloads and VENs > Workloads**.
2. Select the Windows workload you want to unpair. You can select as many workloads as you want to unpair.
3. Click **Unpair**.
4. Select an unpair option, and then click **Remove**.

Remove VEN Using Windows Control Panel

You can also use the Windows Control Panel Programs and Features utility to remove the VEN. When you use this utility to remove the VEN, the Windows workload is returned to the “Recommended” state.

Pair a Linux Workload

Pairing a workload requires running the pairing script on it to install the VEN.

When you first log into the PCE web console, a default pairing profile and corresponding pairing script is provided. You can use the default pairing profile to assess installing Linux VENs using the VEN Library.

Or, you can create a new pairing profile to configure your own workload pairing settings. Ultimately, you should create your own Linux pairing profile to designate your own workload pairing settings.

Before you begin, open an SSH connection to the workload you want to pair.

NOTE:
You must be logged in as a user with root permissions to run the Illumio pairing script.

To pair a workload on Linux:

1. From the PCE web console menu, choose **Workloads and VENs > Workloads**.
2. Click **Add** > **Pair Workload with Pairing Profile**.

   The Pairing Profiles page appears.
3. From the drop-down list, select a pairing profile. The list contains the default pairing profile and the pairing profiles you've added.

   To create a new pairing profile, see Configure a Pairing Profile.
4. From the *Linux/Unix OS Pairing Script* field, copy the Linux pairing script.
5. In a shell window on the workload you want to pair, paste the script you copied from the pairing profile.

   When the script finishing running, the following output appears:

```
[root@ven-rhel tmp]# rm -fr /opt/illumio_ven_data/tmp && umask 026 && mkdir -
p /opt/illumio_ven_data/tmp && curl --tlsv1
"https://pce.example.com:8443/api/v18/software/ven/image?pair_
```

```
script=pair.sh&profile_id=1" -o /opt/illumio_ven_data/tmp/pair.sh && chmod +x
/opt/illumio_ven_data/tmp/pair.sh && /opt/illumio_ven_data/tmp/pair.sh --
management-server pce.example.com:8443 --activation-code <code>

  % Total  % Received  % Xferd  Average Speed  Time  Time  Time  Current
Dload  Upload   Total   Spent    Left  Speed
  100  40891  100  40891  0  0  93526  0 --:--:-- --:--:-- --:--:-- 93572

             Installing Illumio
             ------------------
Retrieving Illumio Packages [x86_64][CentOS][7.4] ..........
Validating sha256 ..................
Installing Illumio Packages ..........
EXPECTED_VERSION: <ven_version>
INSTALLED_VERSION: <ven_version>
Starting Illumio processes .................
Starting illumio-control:
- Environment Setting up Illumio VEN Environment:         [  OK  ]
- venAgentMgr Starting venAgentMgr:                       [  OK  ]
- IPSec Starting IPSec: feature not enabled               [  OK  ]
- venPlatformHandler Starting venPlatformHandler:         [  OK  ]
- venVtapServer Starting venVtapServer:                   [  OK  ]
- venAgentMonitor Starting venAgentMonitor:               [  OK  ]
Pairing with Illumio .................

               Pairing Status
               --------------
Pairing Configuration exists ......SUCCESS
VEN Manager Daemon running ........SUCCESS
Master Configuration retrieval ....SUCCESS
VEN Configuration retrieval .......SUCCESS
VEN has been SUCCESSFULLY paired with Illumio

[root@ven-rhel tmp]#
```

Unpair a Linux Workload

Unpairing is the process of uninstalling the VEN from a Wworkload so that it no longer communicates with the PCE. Once unpaired, the PCE no longer controls the workload.

NOTE:
After you remove a workload from the PCE using the PCE web console or REST API (but not by using the VEN CTL), it remains in policy computation and can continue to appear (for example, in auto complete fields or API responses) until the VEN confirms that it has been uninstalled or a one-hour delay has passed.

Linux Unpair Options

Carefully consider the security state you want to return the Linux workload to after the VEN is uninstalled.

- **Remove Illumio policy**: (Recommended) Revert firewall rules to the state previous to pairing.
- **Open all ports**: Uninstalls the VEN and leaves all ports on the workload open to traffic.
- **Close all ports except remote management**: Temporarily allow only SSH/22 traffic until system is rebooted.

NOTE:
If the Workload you are unpairing is offline during the unpairing process, the Workload may still appear in the Workloads list in the PCE web console, even though the Workload has been unpaired. The unpaired Workload will be removed within 30-35 minutes.

To unpair a Linux Workload:

1. From the PCE web console menu, choose **Workloads and VENs** > **Workloads**.
2. Select the Linux workload you want to unpair.
3. Click **Unpair**.
4. Select an unpair option, and then click **Remove**.

Ignored Interfaces

You can now set interfaces from “managed” to “ignored” in the PCE web console. Use this option when you want the workload to ignore visibility and enforcement specific interfaces; for example, on the interconnected interfaces of database clusters, such as Oracle RAC. You can set one or more interfaces to “ignored” during pairing. Using this setting causes the first downloaded firewall to ignore those interfaces. An ignored interface is not be included in the policy configuration and traffic will flow

uninterrupted through it without any change in latency. You can see which interfaces are marked as “ignored” on the Workload details page.

IMPORTANT:
Illumio recommends that you designate all private (non-routable) interfaces as ignored interfaces.

To set an interface to ignored:

1. From the PCE web console menu, choose **Workloads and VENs > Workloads**.
2. Select the workload that has interface you want to ignore.
3. Click **Edit.**
4. In the Network Interfaces section, change the interface to Ignored in the **PCE Action** drop-down menu.
5. Click **Save**.

NOTE:
After you set an interface to Ignored, it will not be included in policy configuration provided by the PCE and traffic will continue to flow uninterrupted through that interface.

VEN Installation Troubleshooting

This topic provides information about troubleshooting VEN installation issues you might encounter when using the PCE web console. For general troubleshooting, see VEN Troubleshooting.

Troubleshoot Pairing Errors

If you execute the pairing script and it fails, the system displays an error message indicating failure.

If the script fails to install the VEN, the following output displays:

```
Pairing Status
              --------------
Secureware Package installation ......SUCCESS
Pairing Configuration exists .........SUCCESS
```

```
VEN Manager Daemon running ..........SUCCESS
Master Configuration retrieval .......SUCCESS
VEN Configuration retrieval ..........FAILED
2014-01-23T18:43:50Z AgentManager 13088
Verify activation code and retry pairing
Workload has FAILED pairing with Illumio
```

Possible Causes of Failure

- An invalid pairing profile is being used.
- The wrong pairing script was copied and run on the workload.
- In the pairing script section, the pairing profile contains invalid pairing keys.
- The pairing profile was disabled.
- The use limit for the pairing key has been exceeded.
- The pairing key has expired.

Check the pairing profile in the PCE web console to verify the cause of the failure.

The VEN Library is available in the PCE web console. You can download VEN software bundle and also view the dependencies and supported OS versions.

VEN Upgrade Using VEN Library in PCE

You can use your PCE cluster as a centralized mechanism for upgrading VENs in your environment.

From the 20.2.0 release on, you can upgrade one or more VENs by using the PCE web console. From the PCE web console menu, go to the **Workloads and VENs** > **VENs** > **Upgrade**.

You can also use the Illumio Core REST API to upgrade (but not install) VENs. See the *REST API Developer Guide* for information.

NOTE:
Before you use this feature, you must set up the VEN Library in the PCE. See VEN Library Setup in the PCE for information.

If you are an Illumio Cloud customer, Illumio Operations set up the VEN Library in the PCE.

IMPORTANT:
For Illumio Core Cloud customers, the VEN Library only provides the option to upgrade to VENs that Illumio designated as a Long Term Support (LTS) release. See Versions and Compatibility in the Illumio Support Portal (login required) for information.

About VEN Upgrade

You can upgrade all VENs, upgrade a selected subset of VENs, or upgrade all VENs that match a set of filters. After you confirm an upgrade from the PCE web console, the VEN will download the new VEN image from the PCE and upgrade itself. The upgrade on the workload host only takes on average a few minutes.

If the VEN does not successfully upgrade within a certain amount of time (approximately 1 hour), the upgrade will time out and the PCE will put the VEN in a warning state. However, in most cases, the upgrade will complete within this window. To clear this warning, just start another upgrade on the VEN.

You can upgrade up to 25,000 VENs in a single PCE region. Selecting this large a number of VENs in one upgrade will result in some CPU and memory spikes and increased network bandwidth because the VENs will be communicating with the PCE to request new firewalls and downloading new software versions.

The VEN upgrade feature includes upgrade validation; namely, the PCE will validate that the VEN upgrade path is allowed and that the version of the VEN you are upgrading to is compatible with the version of the PCE. If you attempt to upgrade VENs to a version incompatible with the PCE or Illumio does not support that upgrade path, the PCE web console provides feedback on which VENs can be upgraded.

VEN Package Format Changes

Starting with the 21.2.1 release, the Windows VEN installer switched from MSI to EXE package format. This package format change primarily affects Illumio Core On-Premises customers running older MSI-based Windows VENs. For information about using the VEN Library in the PCE to install Windows VENs on workloads, see Pair a Windows Workload.

Prerequisites and Limitations for VEN Upgrade

Prerequisites

- The PCE must be a version 20.2.0 or later.
- The VENs selected for upgrade must be version 18.2.0 or later.
- The VEN Library must be set up in the PCE. See Upload VEN Software Bundle into PCE VEN Library for information.
- The VEN upgrade compatibility matrix must be installed on the PCE. See Upload VEN Upgrade Compatibility Matrix for information.

Limitations

- You must update the VENs in your environment using a supported upgrade path.
- You cannot upgrade a VEN to a later version than the PCE's current version.
- The VEN Upgrade feature does not support upgrading AIX or Solaris VENs or upgrading the C-VEN.
- If a VEN has been installed with custom RPM installation options, you cannot use the VEN upgrade feature to upgrade it.

  For example, you cannot upgrade VENs installed with a custom `--prefix` option because options like that aren't persisted when a VEN is upgraded from the PCE, and the VEN will be installed in the default directory. This outcome might cause data loss or operational issues with the VEN, depending on your environment.
- You cannot use the feature to downgrade a VEN to an earlier version.
- Using the PCE CLI to upgrade VENs is no longer supported in Illumio Core 21.2.0 and later releases.
- If you installed the VEN with the VEN CTL and packaging CLI and customized installation options (such as, a custom installation directory or alternate VEN user), you cannot later upgrade the VEN by using the VEN Library in the PCE. You must upgrade the VEN using the workload's OS package upgrade process.

VEN Package Format Changes (Windows only)

Starting with the Illumio Core 21.2.1 release, the Windows VEN installer switched from MSI to EXE package format. This package format change affects Illumio Core On-Premises customers running older MSI-based Windows VENs.

Customers using the VEN Library in the PCE to install or upgrade VENs must take an extra step for the transition. Specifically, Illumio Core customers running older MSI-

based Windows VENs must upgrade to Illumio Core 19.3.6+H1-VEN or 21.2.0+H2-VEN before upgrading to their VENs to 21.2.1 or a later version. The 21.2.0+H2-VEN release contained the necessary VEN changes to handle the transition in the VEN packaging from MSI to EXE.

For the detailed steps required for this transition, see New Windows VEN Installer Starting with 21.2.1, Knowledge Base Article 3561 (login required).

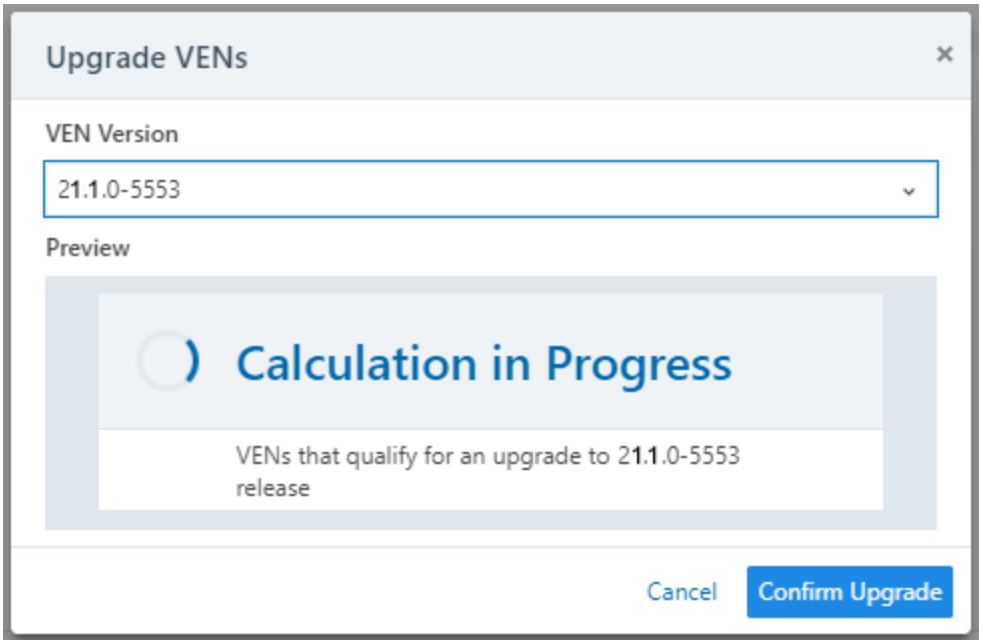
Upgrade All VENs to the Current Version

When you select "Upgrade All," the PCE upgrades all your deployed VENs and not just the VENs that appear in that page of the list (for example, you have 10 pages in the list, the VENs in all 10 pages are upgraded.)

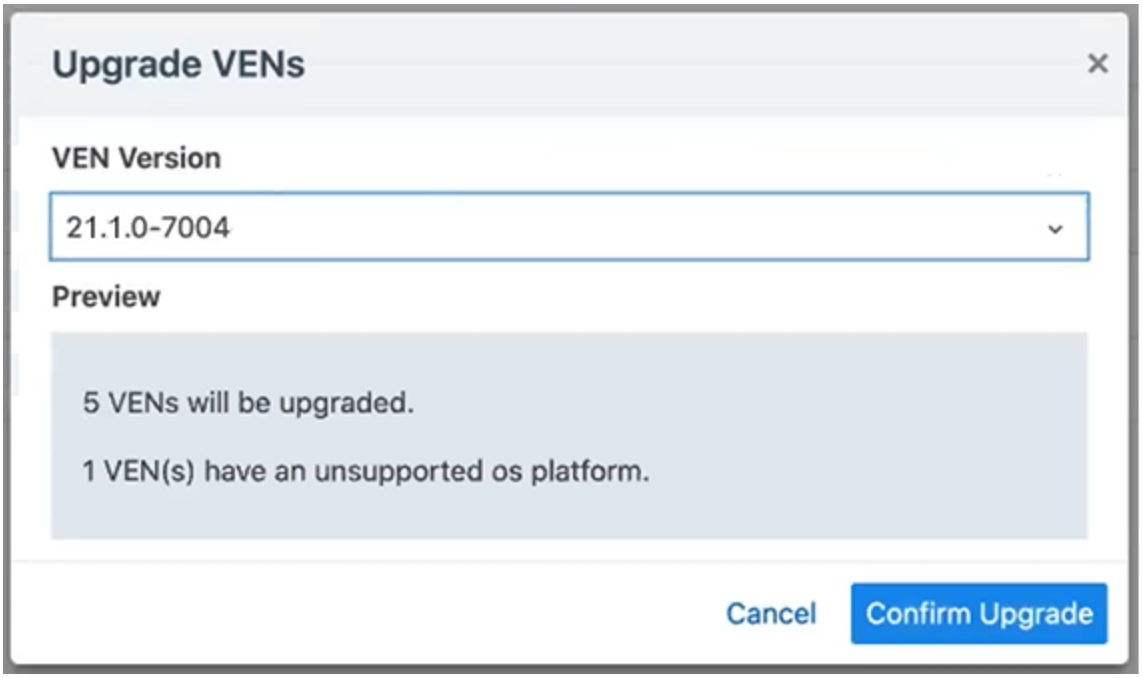
1. From the PCE web console menu, choose **Workloads and VENs** > **VENs**. The Workloads and VENs – VENs page appears.
2. From the **Upgrade** drop-down menu, choose **Upgrade All**.

   The Upgrade VENs dialog box appears. By default, the most current VEN version in the VEN Library is selected.
3. (Optional) To upgrade to a version other than the current version, select the VEN version from the drop-down menu.

   The PCE calculates the scope of the upgrade.



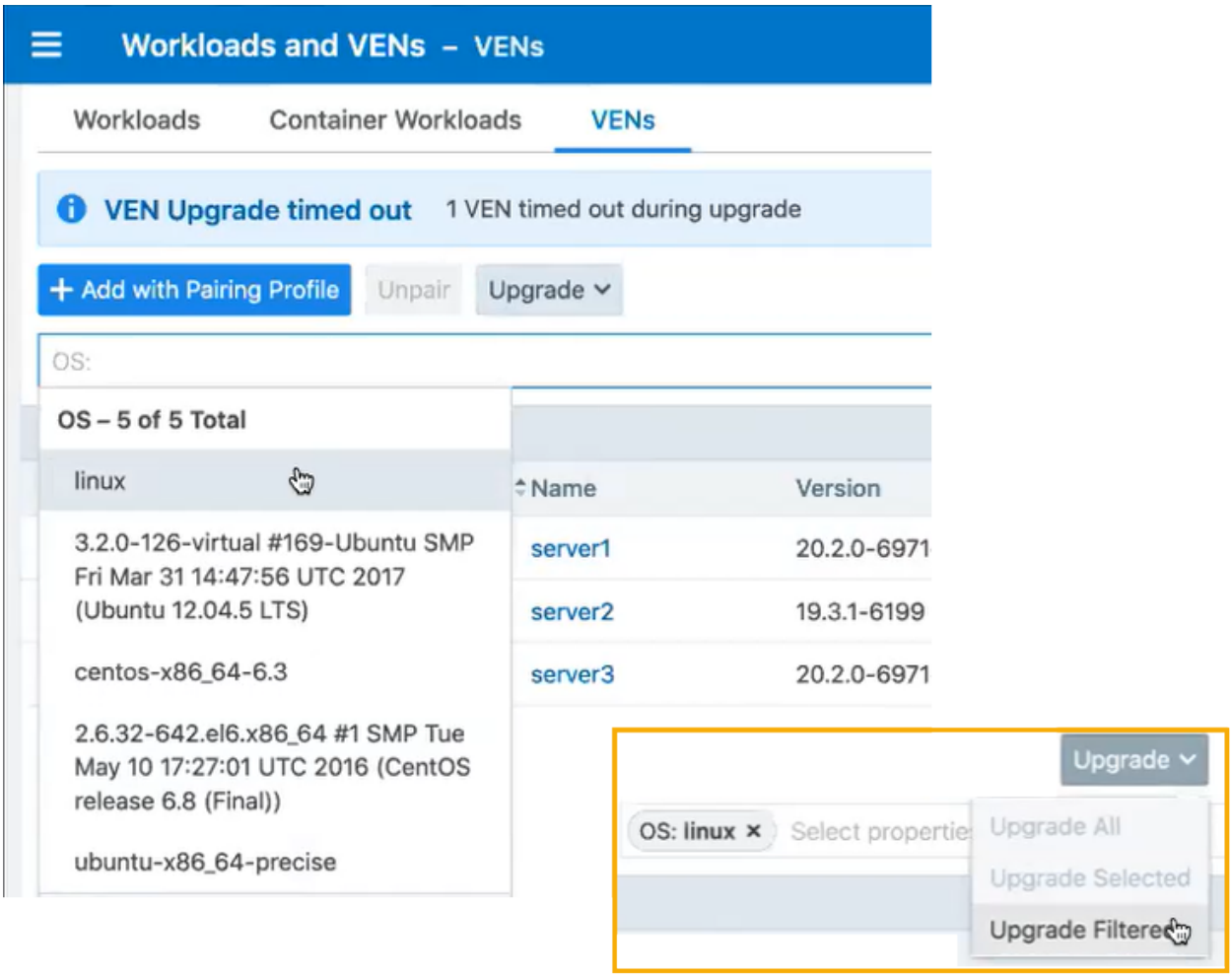
When the calculation is complete, the dialog box refreshes and informs you which VENs in your environment can be upgraded to the selected version. In this example, one VEN has an unsupported OS platform because it's a VEN running on Solaris, which cannot be upgraded using this feature in this release.



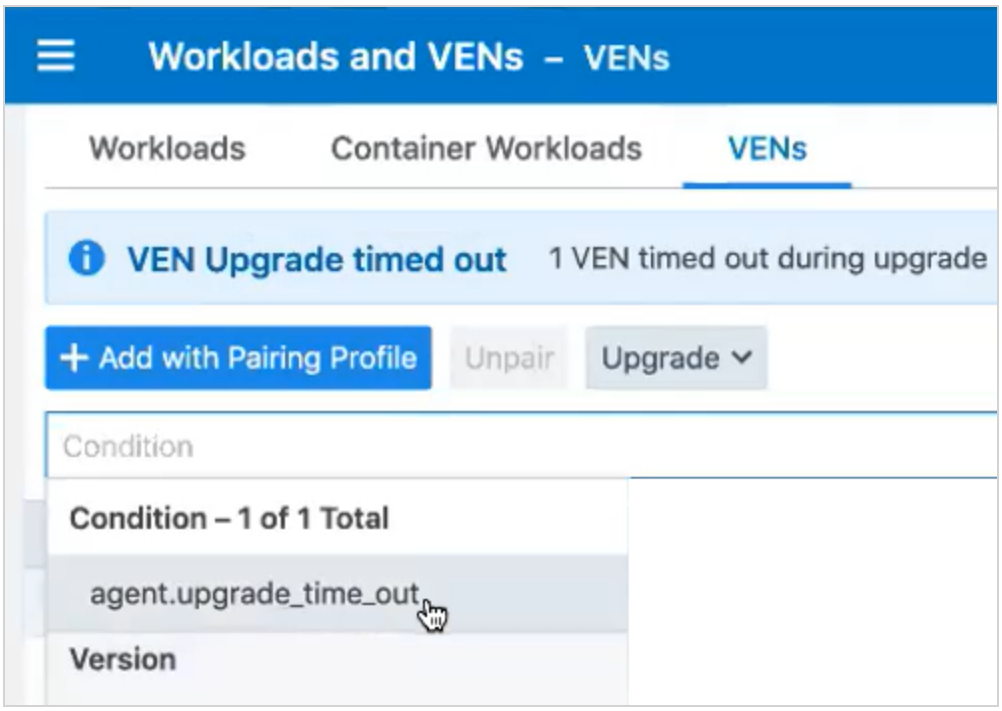
4. Click **Confirm Upgrade**.

Upgrade Selective VENs

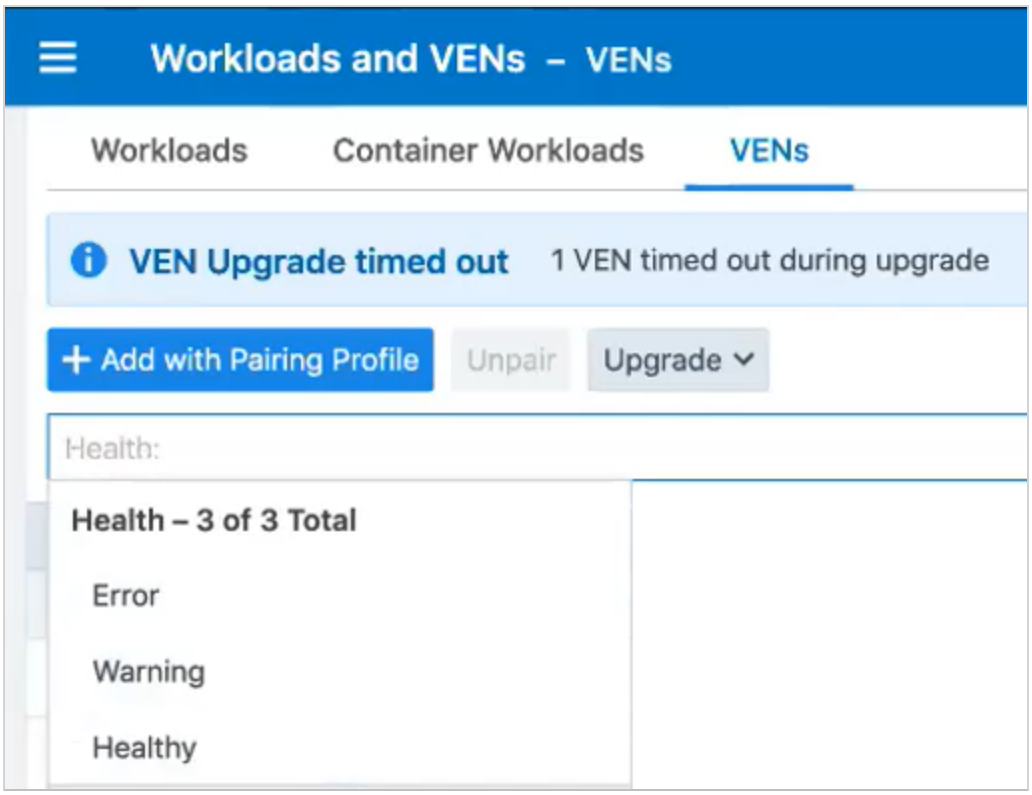
When upgrading, you can use all the filters available in the VEN list to manage the upgrade. For example, you could filter VENs by the location label to only upgrade VENs in a specific datacenter or you can filter the VENs in your environment by their operating systems and upgrade just those VENs.



You can filter and upgrade VENs based on specific conditions. For example, you can locate the VENs that weren't upgraded in your first attempt to upgrade all VENs to the default version; for example, these VENs might have been offline when you ran your first upgrade and the upgrade timed out for those VENs but succeeded on all the others in your environment.

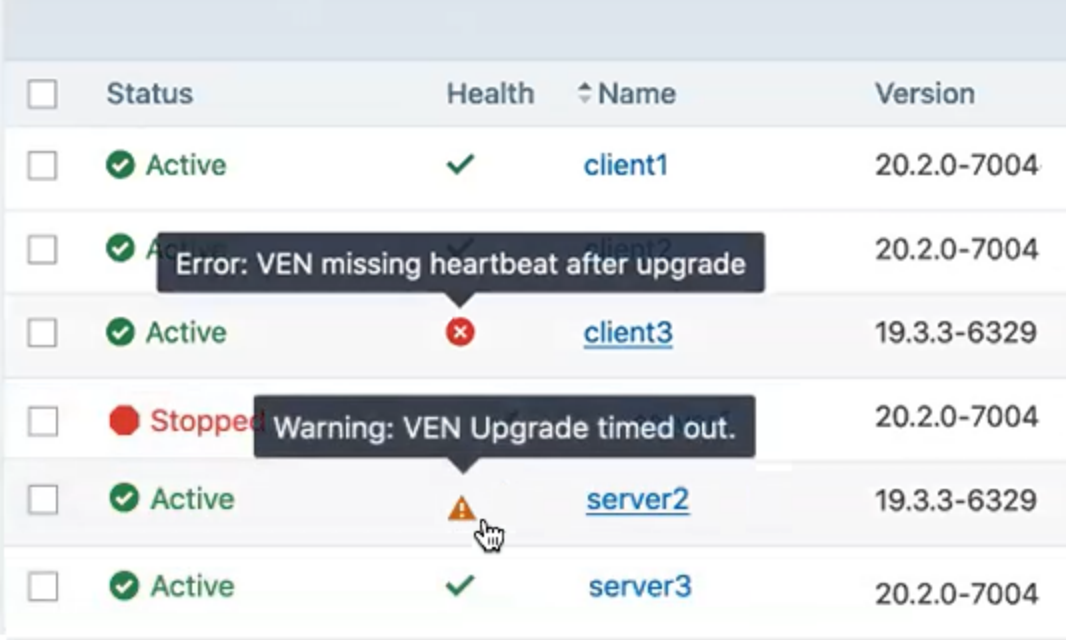


You can filter and upgrade VENs based on their Health status in the PCE.



VENs can have one of three Health statuses that you can filter for:

- **Healthy:** The VEN has no Health conditions.
- **Warning:** The VEN has one or more Warning conditions.
- **Error:** The VEN has one or more Error conditions or has both Error and Warning conditions.

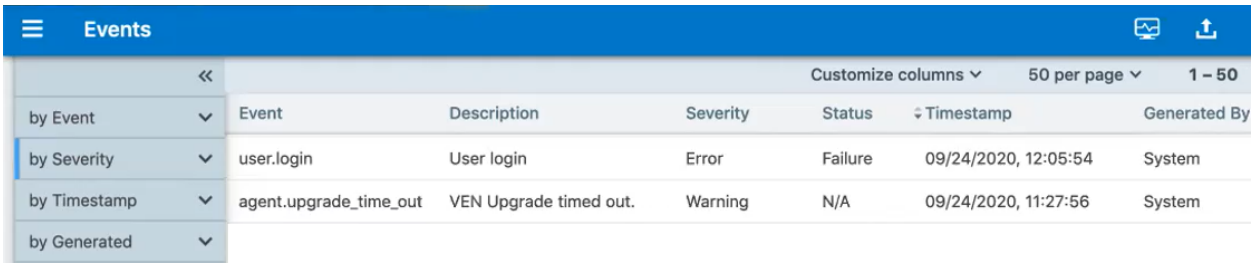


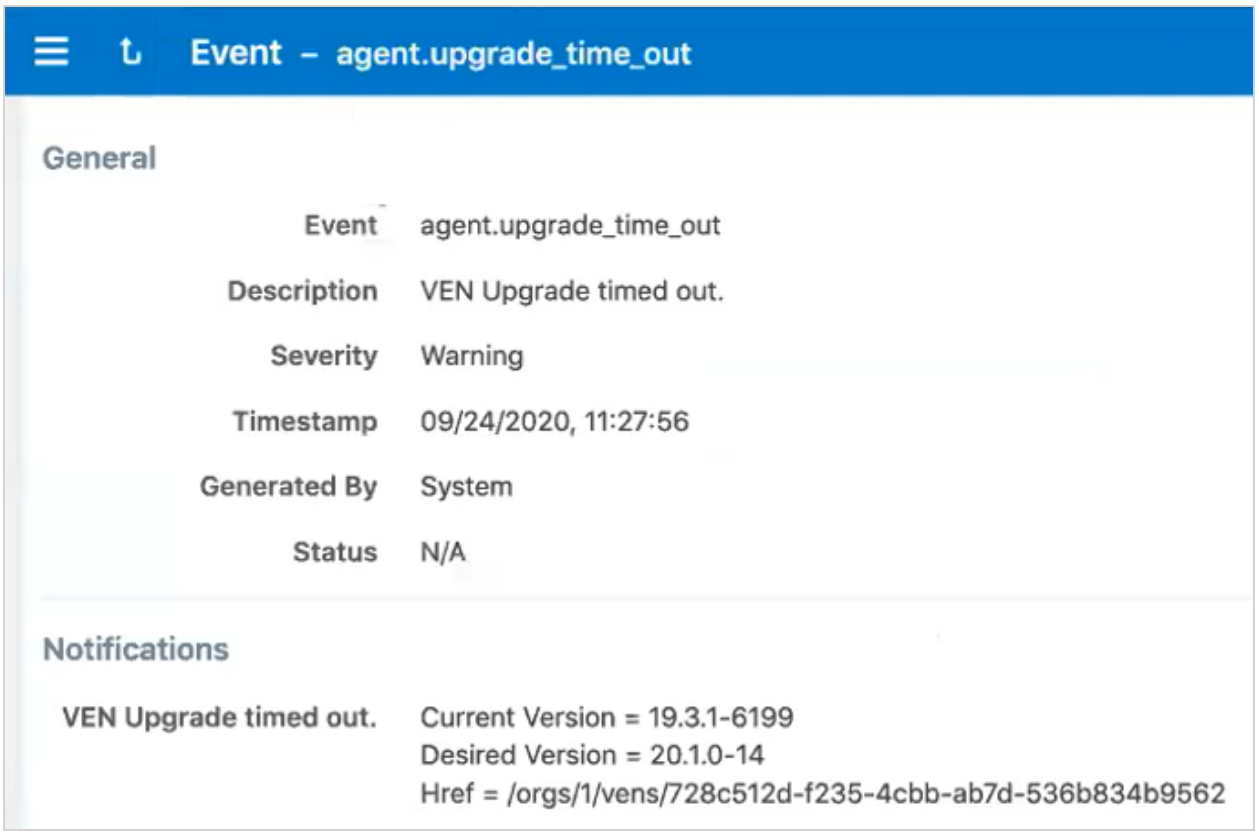
View VEN Upgrade Events

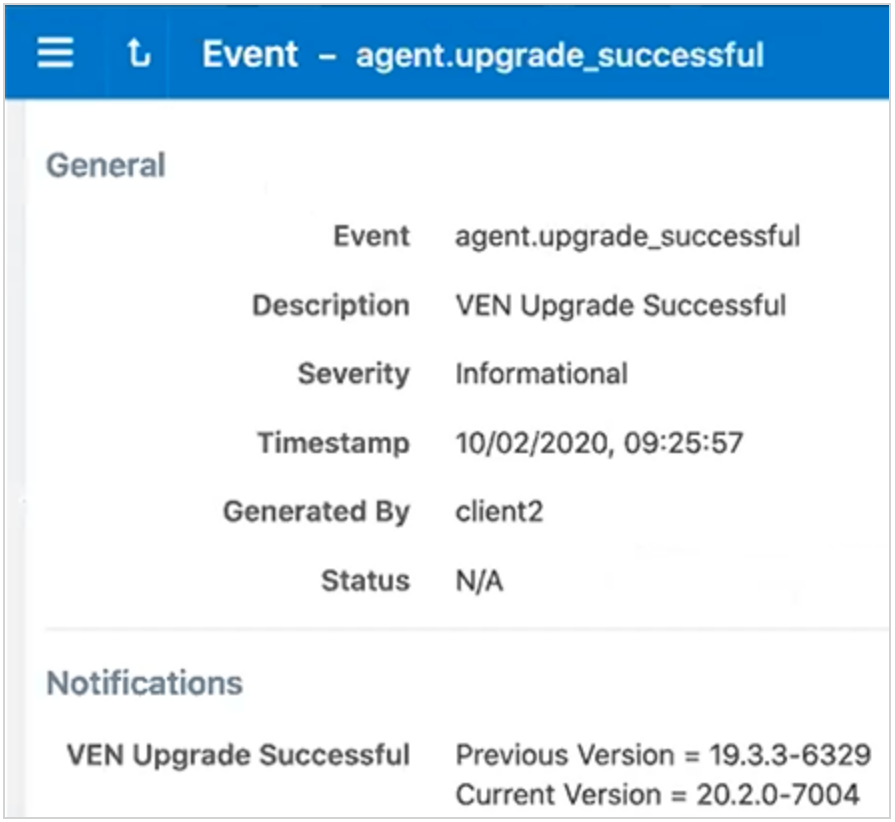
Upgrading VENs using the PCE web console or the REST API generate events that you can view in the Events page.

From the PCE web console menu, choose **Troubleshooting** > **Events**.

You can find events indicating when upgrades succeeded and when they failed. If you are using the *Upgrade All* option to upgrade large numbers of VENs in your environment, the PCE aggregates the event for `agent.upgrade_requested`; however, the PCE still generates a separate event for each successful upgrade.




Event – agent.upgrade_time_out
General
Event agent.upgrade_time_out
Description VEN Upgrade timed out.
Severity Warning
Timestamp 09/24/2020, 11:27:56
Generated By System
Status N/A
Notifications
VEN Upgrade timed out.
Current Version = 19.3.1-6199
Desired Version = 20.1.0-14
Href = /orgs/1/vens/728c512d-f235-4cbb-ab7d-536b834b9562


Event – agent.upgrade_successful
General
Event agent.upgrade_successful
Description VEN Upgrade Successful
Severity Informational
Timestamp 10/02/2020, 09:25:57
Generated By client2
Status N/A
Notifications
VEN Upgrade Successful
Previous Version = 19.3.3-6329
Current Version = 20.2.0-7004

Chapter 5

VEN Installation & Upgrade with VEN CTL

This chapter contains the following topics:

The following topics describe how to use packages and the VEN CTL to install the VEN on hosts in your environment. To perform the tasks in this section, you must log into the Illumio Support portal to download the VEN software to your local environment.

Windows: Install and Upgrade with CLI and VEN CTL

This section discusses installing and upgrading the VEN for Windows by using packaging technology commands and the VEN CTL.

With the Windows VEN MSI, you have the option of activating (pairing) the VEN either during installation or after installation.

Windows VEN Installation Directories

By default, the Windows VEN is installed in the following directories:

- Installation: `C:\Program Files\Illumio`
- Data: `C:\ProgramData\Illumio`

VEN Package Format Changes

Starting with the Illumio Core 21.2.1 release, the Windows VEN installer switched from MSI to EXE package format. This package format change primarily affects Illumio Core On-Premises customers running older MSI-based Windows VENs.

For information about using the VEN Library in the PCE to install Windows VENs on workloads, see Pair a Windows Workload.

Run PowerShell as Administrator

Use Windows PowerShell to run the VEN installation program.

Run PowerShell as Administrator with Execution Policy, because the installation affects the operating system.

Right-click the PowerShell icon and select **Run as Administrator**.

In addition, the VEN control scripts require the proper execution permissions on Windows. In PowerShell, run the following command before installation:

```
Set-ExecutionPolicy -ExecutionPolicy RemoteSigned
```

Install the Windows VEN Using EXE Package

Starting with the version 21.2.1, the Windows VEN installer format changed from an MSI package to an EXE bundle. The installation file is now executable and `msiexec.exe` is no longer used to install the Windows VEN in Illumio Core 21.2.1 and later releases.

Command Line Interface

The Windows VEN installer supports following command line options:

- `/install`
- `/uninstall`
- `/quiet`

  Disables the interactive installer so that you don't respond to installation prompts.
- `/passive`

  Still displays a minimal user interface but does not provide installation prompts.
- `/norestart`

  Suppresses any attempts at restart.

- `/log`

  Logs installation information to a specific file.

The following installation command lines show how to install the VEN EXE bundle and activate the VEN after installation. See Windows VEN Activation After Installation.

Quiet VEN Installation

```
Start-Process -FilePath "<directory_path>\illumio-ven-<ven_version>.<os_
platform>.exe" -ArgumentList "/install","/quiet","/norestart","/log" "<directory_
path>\VENInstaller.log" -Wait -PassThru
```

For example:

```
Start-Process -FilePath "$env:WinDir\temp\illumio-ven-21.5.0-xxxx.win.x64.exe" -
ArgumentList
"/install","/quiet","/norestart","/log","$env:WinDir\temp\VENInstaller.log" -Wait
-PassThru
```

Quiet VEN Installation with Custom Directories

```
Start-Process -FilePath "$env:WinDir\temp\illumio-ven-<version>-
<build>.win.x64.exe" -ArgumentList
"/install","/quiet","/norestart","/log","$env:WinDir\temp\VENInstaller.log"
INSTALLFOLDER="c:\illumio\ven" DATAFOLDER="c:\illumio\ven_data" -Wait -PassThru
```

CAUTION:
The VEN EXE installer supports custom installation directories; however, you should only specify the `INSTALLFOLDER` and `DATAFOLDER` parameters when installing the Windows VEN the first time. Do not specify these parameters when upgrading the Windows VEN using the EXE installer or the upgrade will fail.

Interactive VEN Installation

```
Start-Process -FilePath "<directory_path>\illumio-ven-<ven_version>.<os_
platform>.exe" -ArgumentList "/install","/log" "<directory_path>\VENInstaller.log"
```

Windows VEN Activation After Installation

Be sure that you have the proper administrative permissions. See Run PowerShell as Administrator .

To activate the Windows VEN after installation, run the following command:

```
PS C:\Program Files\Illumio> .\illumio-ven-ctl.ps1 activate -activation-code
<activation_code> -management-server <pce_fqdn:pce_portnumber> <activation_
options>
```

Windows VEN Activation Options

You have several activation options you can set while pairing. You can set the workload policy state and apply labels at the time of activation.

This example shows how to activate a Windows workload with the following options:

- Set the VEN policy state to `illuminated` with no traffic logging: `-log_traffic false`
- Set the role as Web service: `-role Web`
- Set the application to HRM: `-app HRM`
- Set the environment to development: `-env Dev`
- Set the location of the VEN to New York City: `-loc NYC`

```
PS C:\Program Files\Illumio> .\illumio-ven-ctl.ps1 activate -management-server
yourPCE.example.com.8443 -activation-code <activation_code> -visibility_level
flow_summary -log_traffic false -role Web -app HRM -env Dev -loc NYC
```

Kerberos for Windows VEN-to-PCE Authentication

To enable Kerberos authentication at installation, set the command-line variable `KERBEROS_PCE_SPN` on the installation program. Use the following value for this variable:

```
illumio-device-auth/<fqdn_of_your_pce>
```

Where:

- The literal `illumio-device-auth/` is required.
- `fqdn_of_your_pce` is the fully qualified domain name (FQDN) of your PCE.

Example:

```
C:\> msiexec.exe /i illumio-ven-<ven_version>.<os_platform>.msi KERBEROS_PCE_
SPN=illumio-device-auth/pce.example.com
```

Activation with Kerberos

On the `illumio-ven-ctl --activate` or in the pairing script, do *not* use any option that sets a label. That is, do not use the `--env`, `--loc`, `--role`, or `--app` options. Labels should be set in the PCE web console. See the *Security Policy Guide*for information.

After installation with the command-line variable, when you activate the VEN, a message similar to the following is displayed:

```
# illumio-ven-ctl activate

      Activating Illumio
...
Enabling Kerberos Authentication .....
...
```

Windows VEN Upgrade for the MSI Package Format

IMPORTANT:
Illumio strongly recommends that you upgrade VENs only during maintenance windows.

NOTE:
If the VEN was activated prior to the upgrade, it does not need to be activated again after the upgrade completes.

To upgrade the VEN, run this command:

```
PS C:\> msiexec /i illumio-ven-<ven_version>.<os_platform>.msi /qn
```

Windows VEN Uninstallation Using CLI

To uninstall the Windows VEN by using the VEN CTL, see Deactivate and Unpair VENs in the *VEN Administration Guide*.

Offline VEN During Unpairing

If the workload you are unpairing is offline, the workload might still appear in the workloads list in the PCE web console, even though the workload has been unpaired. The unpaired workload is removed from the PCE web console within 30-35 minutes.

Alternative: Remove Windows VEN Using Control Panel

You can also use the Windows Control Panel Programs and Features utility to remove the VEN. When you remove the Windows VEN with the Windows Control Panel, the VEN unpairs the workload with the **Unpair and remove Illumio policy** option. This method removes any current Illumio policy and activates the Windows firewall.

Linux: Install and Upgrade with CLI and VEN CTL

This section discusses installing and upgrading the VEN for Linux by using packaging technology commands and the VEN CTL.

- Installing the VEN on Linux relies native package management commands:
  - For Debian and Ubuntu (referred to as “Debian”): `dpkg`
  - For Red Hat and CentOS (referred to as “Red Hat”): `rpm`
- Root access on the workload is required for installation of the Linux VEN.
- Some of the optional installation features in the RPM are not available with the Debian package. These cases are marked in section titles below with “RPM only.”

About iptables Versions for Red Hat and CentOS

Red Hat Version 6 VENs

If the iptables version already on the workload is older than iptables version 1.4.7-16 or ipsets is older than version 6.11-4, the VEN installation process installs more recent versions of iptables and ipset, including libmnl. These unmodified distribution files (RPMs) are packaged with the VEN itself and installed in `/opt/illumio_ven/etc/extras`.

About Red Hat 8 Support and nftables

In 18.2.x, the VEN supported iptables. In 19.3.0 and later releases, the VEN supports nftables, which is the default host-based firewall used by Red Hat 8. Supporting nftables, which is used by Red Hat 8, simplifies rule writing and allows developers to write fewer rules and do so much more efficiently. The new support for nftables does not change VEN functionality or the VEN feature set because the underlying net filter cap-

abilities are the same. Support for nftables provides the following usability enhancements for the VEN:

- **Simpler syntax:** Uses a simpler syntax, which is very similar to TCP dump.
- **Combined rules:** Rather than write 2 rules for every enforcement point, you can combine them into a single rule; such as combining multiple ports into a single rule, and IPv4 and IPv6 into a single rule.
- **Multiple actions:** A single rule can have multiple actions, such as LOG and DROP.
- **Built in tracing:** Includes built-in support for named sets. To use lists or sets with `iptables`, you need to install `ipset.nftables` has integrated set support and can be used more naturally within the configuration.

Notes:

- Native support for `nftables` in Red Hat 8 does not change the VEN installation or upgrade process; if you've written installation scripts, they don't require updates.
- `nftables` does not impact Firewall Coexistence and it is still supported.
- Using the `nftrace` tool on Illumio created tables is not supported because it requires specific filtering rules.
- `nftables` support does not impact the PCE; viewing a workload that is running Red Hat 8 in the PCE web console does not change. You can view all the workload details. Creating policy for workloads running Red Hat 8 does not change.

IMPORTANT:
In 19.3.0 and later releases, the VEN continues to support earlier versions of Red Hat with no changes. For the complete list of Red Hat versions supported by the VEN by release, see OS Support and Package Dependencies on the Illumio Support portal.

Linux Default Installation Directories

The Linux VEN is installed into two directories by default:

- `/opt/illumio_ven`
- `/opt/illumio_ven_data`

Directory Ownership Pre- and Post-activation

- All directories are created with mode 0750.
- Post-activation user/group `ilo-ven:ilo-ven` allows processes running as that user to write to the VEN installation directory and VEN data directory.
- At installation, you can set various environment variable to override default settings. See Linux Installation with Environment Variables.

VEN Package Format	Path	Default Pre-Activation Owner	Default Post-Activation Owner
RPM	`/opt/illumio_ven`	`root:ilo-ven`	`root:ilo-ven`
	`/opt/illumio_ven_data`	`ilo-ven:ilo-ven`	`ilo-ven:ilo-ven`
DPKG	`/opt/illumio_ven`	`root:ilo-ven`	`root:ilo-ven`
	`/opt/illumio_ven_data`	`root:ilo-ven`	`ilo-ven:ilo-ven`

Dependency Check for Certificates

If your PCE-to-VEN SSL certificate was signed by a private CA and the signing CA's credentials have already been added to the workload's trusted certificate store, the ca-certificates package is not needed. To install the VEN without the dependency check, follow these examples:

- Red Hat: `rpm -vh -nodeps illumio-ven-<ven_version>.<os_platform>.rpm`
- Debian: `dpkg --ignore-depends=illumio-ven-<ven_version>.<os_platform>.deb`

RPM Only: Installation in Non-Default Directory

If you want to change the installation directory during installation or upgrade, you can use environment variable or use the `--prefix` option on the RPM command line.

```
# rpm -ivh <illumio-ven-pkg>.rpm --prefix=/opt/foo/bar
```

CAUTION:
The Linux VEN does not support installing the VEN in a directory where the directory is a symbolic link.

Linux Installation with Environment Variables

The following table lists VEN environment variables that you can set for the package installation on Linux.

NOTE:
Before installation, set any of the following environment variables.

Variable	Description
`VEN_ACTIVATION_CODE`	The activation code; see Example: Linux Environment Variables and About the Command Options.
`VEN_DATA_DIR`	Directory where the `illumio_ven_data` directory is created. This option can also be used when you are upgrading a VEN with RPM or Debian.
`VEN_DISABLE_MONITOR_RESTART`	Disable the VEN agent monitor process. See Disable Agent Monitor cronjob .
`VEN_INSTALL_ACTION`	Activate or prepare the VEN during installation. Valid values: • `activate`: Requires an activation code on the `illumio-ven-ctl` control script or set in the `VEN_ACTIVATION_CODE` environment variable. • `prepare`: Used to defer activation until after installation. For example, see Prepare Golden Image for Workload Installation.
`VEN_KERBEROS_WORKLOAD_SPN`	See Kerberos for Linux VEN-to-PCE Authentication.
`VEN_KERBEROS_MANAGEMENT_SERVER_SPN`	See Kerberos for Linux VEN-to-PCE Authentication.
`VEN_KERBEROS_LIBRARY_PATH`	See Kerberos for Linux VEN-to-PCE Authentication.
`VEN_MANAGEMENT_SERVER`	The FQDN of the PCE server and its port.
`VEN_NONPRIV_UID`	If `VEN_NONPRIV_USER` is not set, create the `ilo-ven` user with the specified UID.
`VEN_NONPRIV_GID`	If `VEN_NONPRIV_USER` is not set, create the `ilo-ven` group with the specified GID.
`VEN_NONPRIV_`	Existing username to override the default username `ilo-ven`. The

Variable	Description
USER	group name of the specified user is the primary existing group name of the specified user. • If VEN_NONPRIV_USER is set, any values for VEN_NONPRIV_UID and VEN_NONPRIV_GID are ignored. • Conversely, if VEN_NONPRIV_USER is not set, any values for VEN_NONPRIV_UID and VEN_NONPRIV_GID take effect.
ILLUMIO_RUNTIME_ENV	If ILLUMIO_RUNTIME_ENV is set, read the runtime_env.yml from this file path. This environment variable is unique because it is relevant during and after installation.

Kerberos for Linux VEN-to-PCE Authentication

The illumio-ven-ctl command does not have any options for Kerberos, but when you activate the VEN with illumio-ven-ctl, at installation it honors the Kerberos values that have been set in environment variables.

Before installing the Linux VEN, set the following environment variables.

Environment variable	Value	Notes
VEN_KERBEROS_WORKLOAD_SPN	(Optional) See notes. The default host principal set in the Kerberos keytab file. The SPN of the server for renewing Ticket Granting Tickets (TGT) for Linux workloads. Format: `host/fqdn_of_ven@REALM` Where: • The literal host/ is required. • fqdn_of_ven is the FQDN of the workload	A workload might have more than one host principal in its keytab file, one of them the principal needed for PCE authentication. In this case VEN_KERBEROS_WORKLOAD_SPN must be set so that the VEN software knows which principal to use to acquire a TGT. The VEN relies on the default Kerberos keytab file, typically /etc/krb5.keytab. Therefore, the host SPN for PCE authentication must be added to the default keytab file. Before deploying Kerberos authentication, you can use kinit to verify that a TGT for the workload's SPN can be acquired: `kinit -k`

Environment variable	Value	Notes
	where the VEN is installed. • `@REALM` is optional. If not specified, the default realm is used.	If the command is successful, use `klist` to verify the TGT has been acquired for the correct host SPN. If the default SPN is not what you want for PCE authentication, use the following command to verify that you can reach the desired SPN: `kinit -k host/fqdn_of_ven@REALM` If the command is successful, set `VEN_KERBEROS_WORKLOAD_SPN` to `host/fqdn_of_ven@REALM`.
`VEN_KERBEROS_MANAGEMENT_SERVER_SPN`	SPN for the PCE Example: `illumio-device-auth/pce.example.com`	GSSAPI Authentication
`VEN_KERBEROS_LIBRARY_PATH`	Absolute path to `libgssapi_krb5.so` Example: `/usr/lib/libgssapi_krb5.so`	The exact path can vary by type of Linux OS. If `libgssapi_krb5.so` does not exist on your system, create a symlink of the same name to point to the `libgssapi_krb5.so.n` file, where `n` is the number on the actual installed shared object library on your workload, like `libgssapi_krb5.so.2`

Activation with Kerberos

On the `illumio-ven-ctl --activate` or in the pairing script, do *not* use any option that sets a label. That is, do not use the `--env`, `--loc`, `--role`, or `--app` options. Labels should be set in the PCE web console. See the *Security Policy Guide*for information.

After installation with the command-line variable, when you activate the VEN, a message similar to the following is displayed:

```
# illumio-ven-ctl activate
```

```
      Activating Illumio
...
Enabling Kerberos Authentication .....
...
```

Example: Linux Environment Variables

To activate the VEN during installation, set the following environment variables before running the installation command.

- `VEN_MANAGEMENT_SERVER`
- `VEN_ACTIVATION_CODE`
- `VEN_INSTALL_ACTION`

For example, to activate a VEN during installation of a VEN package:

```
# VEN_MANAGEMENT_SERVER=pce.example.com:8443 VEN_INSTALL_ACTION=activate VEN_
ACTIVATION_CODE=<activation_code> rpm -ivh illumio-ven-<ven_version>.<os_
platform>.rpm
```

Or

```
# VEN_MANAGEMENT_SERVER=pce.example.com:8443 VEN_INSTALL_ACTION=activate VEN_
ACTIVATION_CODE=<activation_code> dpkg -i illumio-ven-<ven_version>.<os_
platform>.deb
```

Change Default Name of User at Installation

The default username for the VEN installation is `ilo-ven`. With the package installation, you can specify an environment variable to set a different, existing username to override this default. The group name is the specified user's primary group and does not need to be specified.

```
# VEN_NONPRIV_USER=desired_existing_username rpm -ivh illumio-ven-<ven_
version>.<os_platform>.rpm
```

Or

```
# VEN_NONPRIV_USER=desired_existing_username dpkg -i illumio-ven-<ven_
version>.<os_platform>.deb
```

Disable Agent Monitor cronjob

You can disable the agent monitor cronjob before or after VEN installation. When failing to hook into existing `init` systems like `systemd`, `upstart`, or `SysV`, the Linux VEN installation creates a cronjob to check the VEN agent monitor process and restart it if necessary. This cronjob runs every 10 minutes.

Some organizations prefer to rely on their own VEN agent monitoring processes. The Illumio-supplied VEN-checking cronjob might create logs whose size you consider excessive or whose frequency is not right for your needs.

To disable the Linux VEN monitoring cronjob before installation:

Set the following environment variable:

```
export VEN_DISABLE_MONITOR_RESTART=true
```

Any value other than `true` does not have any effect.

To modify or disable the Linux VEN monitoring cronjob after installation:

You have several options:

- Edit your crontab to decrease the cronjob's frequency.
- In your crontab, completely comment out the VEN agent monitoring cronjob.

To substitute your own VEN agent monitor checking process, consider the following points:

- Rely on your own organization's standard mechanisms for monitoring processes.
- Make sure your monitoring restarts the VEN if necessary.
    - Do not restart only the VEN agent monitoring process. Restart the entire VEN:

      ```
      # illumio-ven-ctl restart
      ```

    - Be sure that your monitoring process has sufficient permissions to restart the VEN.

Linux VEN Activation After Installation

To activate the VEN after installation, use the `illumio-ven-ctl` control script with the `activate` argument to activate the workload and pair the VEN with the PCE.

At a minimum, to activate the VEN using the VEN control script, you need the host-name or IP address of the PCE, an activation code (called a pairing key in the PCE web console) generated from a pairing profile, and any other required options, such as the workload policy state, label assignment, and workload name. For example, the following command shows how to activate the VEN that places the workload into the Illumination policy state (`--mode`).

```
# /opt/illumio_ven/illumio-ven-ctl activate --management-server
pce.example.com:8443 --activation-code <activation_code>
```

Upgrade Linux VEN Using CLI

IMPORTANT:
Illumio strongly recommends that you upgrade VENs only during maintenance windows.

NOTE:
If the VEN was activated prior to the upgrade, it does not need to be activated again after the upgrade completes.

Custom Username, Installation Directory, VEN Data Directory

If you installed the VEN with your own username, for upgrade you need to specify that same username with the `VEN_NONPRIV_USER` environment variable.

If you previously installed the VEN to non-default installation (RPM only) and data directories with environment variables, specify the same values before upgrade.

See Linux Installation with Environment Variables.

RPM Upgrade

```
# rpm -Uvh illumio-ven-<ven_version>.<os_platform>.rpm
```

IMPORTANT:
If the `VEN_DATA_DIR` environment variable and the `--prefix` option are not specified during the RPM installation, then the `illumio_ven` and `illumio_ven_data` directories are created in the `/opt` directory.

This information is important because if you previously installed the VEN to non-default installation and data directories, and if you upgrade without specifying those non-default directories, the VEN will not upgrade to your custom directories.

Therefore, if you specified non-default installation (RPM only) and data directories when you installed the VEN, you need to specify those same directories in the upgrade command.

This example also includes a custom username that was used during VEN installation.

For example, if you installed the VEN with this type of command:

```
# VEN_NONPRIV_USER=ven_install_username VEN_DATA_DIR=/opt/my_data_dir rpm -ivh
<orig-illumio-ven-pkg>.rpm --prefix=/opt/my_ven_dir
```

Then, upgrade the VEN with the following command:

```
# VEN_NONPRIV_USER=ven_install_username VEN_DATA_DIR=/opt/my_data_dir rpm -Uvh
<new-illumio-ven-pkg>.rpm --prefix=/opt/my_ven_dir
```

Debian Upgrade

```
# dpkg -i illumio-ven-<ven_version>.<os_platform>.deb
```

IMPORTANT:
If the `VEN_DATA_DIR` environment variable is not specified during VEN installation, then the `illumio_ven_data` directory is created in the `/opt` directory.

This information is important, because if you specified a custom data directory during installation, and if you upgrade the VEN without specifying the custom data directory, the VEN will not upgrade using your custom data directory.

Therefore, if you specified a non-default data directory when you installed, you need to specify the same non-default data directory during upgrade.

This example also includes a custom username that was used during VEN installation.

NOTE:
Using `--prefix=/opt/my_ven_dir` to specify a custom installation directory is not supported with Debian.

For example, if you installed the VEN with this type of command:

```
# VEN_NONPRIV_USER=ven_install_username VEN_DATA_DIR=/opt/my_data_dir dpkg -i
<orig-illumio-ven-pkg>.deb
```

Then, upgrade the VEN with the following command:

```
# VEN_NONPRIV_USER=ven_install_username VEN_DATA_DIR=/opt/my_data_dir dpkg -i
<new-illumio-ven-pkg>.deb
```

Uninstall Linux VEN Using CLI

Unpair a Linux VEN before uninstalling it. See Deactivate and Unpair VENs in the *VEN Administration Guide*.

SUSE Linux: If a SUSE workload is unpaired in the Full enforcement policy state, the uninstallation might not complete when the workload does not have rules that allow it to connect to SUSE repositories. To avoid this issue, change the policy state to Visibility before unpairing the VEN. For more information see Workload Policy States in the *VEN Administration Guide*.

Uninstall the VEN

Security Implications: Production applications on this workload could break because after uninstalling the VEN this workload will no longer allow any connections to it other than SSH on port 22.

To uninstall the VEN, see Deactivate and Unpair VENs in the *VEN Administration Guide*.

AIX: Install and Upgrade with CLI and VEN CTL

The following topic describes how to install and upgrade the AIX VEN by using packaging technology commands and the VEN CTL.

Limitations and Considerations

General:

- AIX 5.3 is not supported.

  See VEN OS Support and Package Dependencies for the list of supported operating systems for AIX VENs.

- AIX native IPsec is not supported while the VEN is installed.
- The AIX VEN does not support SecureConnect and SecureConnect Gateway.
- The following directories must be present on the AIX host or the AIX VEN installation will fail. These directories are commonly present on AIX hosts.
  - `/var/lib`
  - `/var/log`
- By default, the AIX VEN is installed in the following directories:
  - `/opt/illumio_ven`
  - `/opt/illumio_ven_data`

  Installing the AIX VEN in a custom directory is not supported. Do not change the default installation directory for the AIX VEN or the AIX VEN installation will fail.

IPFilter:

- Illumio provides a custom IPFilter package for managing the packet filtering rules. Before you install the AIX VEN, install the Illumio-provided IPFilter package.

  CAUTION:
  You must use the Illumio customized IPFilter package with the AIX VEN. Do not use IBM's IPFilter package or the AIX VEN will not function correctly.

- Avoid any changes to packet filtering with `genfilt`, `mkfilt` and other such network tools. Do not perform any such operation while VEN software is installed.
- The AIX system firewall's state table limit is 65,536 entries. When that limit is reached, IPFilter drops packets. If you anticipate a high number of network connections, configure higher limits in the IPFilter state table. See Tuning the IPFilter State Table for Solaris and AIX workloads in the *VEN Administration Guide*.

Change Default Username Before Installation

Before installing the VEN on AIX, you can set an environment variable to change the username that owns the non-privileged portions of the installed software. The privileged portions of the installed software are always owned by root, and the software can only be run as root.

Environment Variable	Description
`VEN_NONPRIV_USER`	Existing username to override the default username `ilo-ven`. The group name of the specified user is the primary existing group name of the specified user.

Boot Scripts Installed at VEN Installation

As part of installation, the VEN creates RC scripts ("run commands") in `/etc/rc3.d` to start the VEN at boot.

Illumio Support for IPFilter

IBM has discontinued support and development of IPFilter and has put IPFilter on GitHub as an open source project. Consequently, Illumio provides its own version of IPFilter for the Illumio AIX VEN version 17.1.2 and later.

NOTE:
Illumio supports *only* its provided version of IPFilter. We do not support installing the AIX VEN with the OEM version of IPFilter. Before installing the AIX VEN, you must install the Illumio-provided IPFilter package.

Illumio supports its version of IPFilter in the following ways:

- The Illumio IPFilter package will not be made public. Permissive licensing of IPFilter does not require that modifications of open source software be made public.
- Illumio can provide IPFilter source code patches for bug-fixes and improvements on request to your Illumio representative.

About the Illumio-provided IPFilter for AIX

The Illumio custom IPFilter package (Version 5.3.0.5001 and later) resolves the following issues in the OEM IPFilter versions 5.3.0.4 and 5.3.0.6:

- Removes a former limit of a maximum 68 IP addresses per IPset.
- Resolves an issue in the OEM `ipflt` extension.

Download AIX VEN Tar File and IPFilter Package

Download the VEN Packages tar file from the Illumio Support site. The tar file contains the AIX VEN in Backup File Format (BFF) format.

Additionally, you must download the Illumio-provided IPFilter package from the Illumio Support site. The VEN package does *not* contain the required Illumio-provided IPFilter package.

To download the AIX VEN files:

1. Go to the Illumio Support site (login required).
2. Select **Software** > **Download** under the VEN section > the VEN version.

   The Download VEN page appears. The page contains two tables: “VEN” and “Other”
3. In the VEN Packages row of the VEN table, click the filename for the VEN tar file.
4. In the Other table, click the AIX IPFilter filename (`ipf1.5.3.0.5002.bff`) to download the Illumio-supported IPFilter 5.3.0.5002 package.

Upgrade to Illumio IPFilter

This procedure describes how to perform either of these tasks:

- Upgrade from the IBM IPFilter package to the current Illumio IPFilter 5.3.0.5002 package
- Upgrade from the previous version of the Illumio IPFilter 5.3.0.5001 package to the current 5.3.0.5002 package

The steps in this procedure apply to both of these IPFilter upgrades except for step #4, which applies only when upgrading from IBM IPFilter to the Illumio IPFilter 5.3.0.5002 package.

To upgrade to Illumio IPFilter:

1. Download the Illumio-supplied IPFilter package. See Download AIX VEN Tar File and IPFilter Package.
2. Stop the VEN if it's running:

   ```
   llumio-ven-ctl stop
   ```
3. Stop the IBM ipf kernel extension using the following command:

```
/lib/methods/cfg_ipf -u
```

Run this command repeatedly until it fails with the following error: `No such device.`

If the command fails with the error `Device Busy`, before continuing these steps, reboot the system.

4. [For Upgrades from IBM IPFilter Only] If IBM iFIX or ipfl is installed on the host, uninstall them. (In an earlier release, Illumio had recommended installation of some iFIXes.)

   NOTE:
   Depending on your installed AIX version, you might have installed iFIX version IV89793s5a or IV89793s3a. Remove the version corresponding to the version already installed on your AIX server. Neither version is needed and must be removed with the appropriate `emgr` command. The following command uninstalls only version IV89793s5a.

   ```
   emgr -r -L  IV89793s5a.161102.epkg.Z
   ```

5. Change directory to where you downloaded the AIX VEN and the IPFilter package.
6. Upgrade the version of IPFilter with the Illumio custom IPFilter:

   ```
   inutoc . && installp -acYd . ipfl
   ```

7. Proceed to installing or upgrading the AIX VEN.

Install the AIX VEN

1. Download the VEN package from the Illumio Support site. See Download AIX VEN Tar File and IPFilter Package.
2. Log in to the AIX host and become superuser.
3. If necessary, upgrade IPFilter on the AIX host to Illumio's custom IPFilter. See Upgrade to Illumio IPFilter.

IMPORTANT:
You must upgrade to Illumio's custom IPFilter before installing the AIX VEN.

4. Copy your trusted root CA certificate in the following directory with a filename `ca-bundle.crt`. This path must be exactly as shown.

```
/var/ssl/certs/ca-bundle.crt
```

5. Make `ca-bundle.crt` world-readable.

```
# chmod 644 /var/ssl/certs/ca-bundle.crt
```

6. Install the VEN package on the AIX host by entering the following commands, where `path_to_bff_file` is the directory where you copied the AIX VEN BFF file.

```
# inutoc <path_to_bff_file>
# installp -acXgd path_to_bff_file illumio-ven
```

AIX VEN installation is complete. The next step is Activate AIX VEN After Installation.

Optional: If you anticipate a high number of network connections, you can configure higher limits in the IPFilter state table. See Tuning the IPFilter State Table for Solaris and AIX Workloads.

Activate AIX VEN After Installation

IMPORTANT:
If you're using the GRE and IPIP protocols, before activating the VEN on AIX, edit the file in the `/etc/protocols` directory to support the GRE and IPIP protocols. If the GRE and IPIP protocol lines are commented out, un-comment them.

After installing the VEN package on the AIX host, activate the VEN. Use the Illumio VEN control script (`illumio-ven-ctl`) with the `activate` option to activate the workload and pair the AIX VEN with the PCE.

At a minimum, to activate the AIX VEN using the VEN control script, you need the hostname or IP address of the PCE, an activation code (called a pairing key in the PCE

web console) generated from a pairing profile, and any other available options, such as the workload policy state, label assignment, workload name, and more.

For information about obtaining an activation code from the PCE web console, see "Pairing Profiles" in the *Security Policy Guide*.

```
# /opt/illumio_ven/illumio-ven-ctl activate --management-server <pce_fqdn:port> --
activation-code <code>
```

See the following example command:

```
# /opt/illumio_ven/illumio-ven-ctl activate --management-server
pce.example.com:8443 --activation-code <code>
```

Upgrade the AIX VEN

IMPORTANT:
Illumio strongly recommends that you upgrade VENs only during maintenance windows.

NOTE:
If the VEN was activated prior to the upgrade, it does not need to be activated again after the upgrade completes.

For the supported upgrade paths for the AIX VEN, see Upgrade VEN on the Illumio Support portal (login required).

1. Download the new version of the VEN package from the Illumio Support site. See Download AIX VEN Tar File and IPFilter Package.
2. If necessary, upgrade the Illumio-supported IPFilter package to version 5.3.0.5002.

   If you are upgrading the AIX VEN from an earlier release, such as 17.1.x, you might be running the Illumio-supported AIX IPFilter package version 5.3.0.5000. See Upgrade to Illumio IPFilter.
3. Stop the VEN if it's running:

   ```
   llumio-ven-ctl stop
   ```

4. Upgrade the VEN package on the AIX host by entering the following commands, where `path_to_bff_file` is the directory where you copied the new version of the AIX VEN BFF file.

```
# inutoc <path_to_bff_file>
# installp -acXgd path_to_bff_file illumio-ven
```

Solaris: Install and Upgrade with CLI and VEN CTL

The following topic describes how to install the Solaris VEN by using packaging technology commands and the VEN CTL.

The VEN for Solaris supports two different Solaris machine architectures: SPARC and x86_64. The installation and upgrade steps for both machine architectures are identical but each architecture uses its own VEN package file.

Limitations and Requirements

General

- In Illumio Core 19.3.1 and later releases, the Solaris VEN supports Solaris zones.

  All Solaris zones use the same underlying kernel networking stack. This design can result in undesirable interaction between global and non-global Solaris zones. The VEN only operates reliably in global Solaris zones. Please contact your Illumio Customer representative for assistance if you are using non-global Solaris zones.

- By default, the Solaris VEN is installed in the following directories:
  - `/opt/illumio_ven`
  - `/opt/illumio_ven_data`

  Installing the Solaris VEN in a custom directory is not supported. Do not change the default installation directory for the Solaris VEN or the Solaris VEN installation will fail.

- Installing or activating the Solaris VEN on a workload running an LDAP client can take longer than on other workloads without an LDAP client.
- The Solaris VEN requires the bash shell and the Solaris XCU4 utilities (POSIX-compliant tools) be installed on the Solaris host. Verify that both are installed on the host. The XCU4 utilities are installed using the Solaris SUNWxcu4 package, typically in the `/usr/xpg4/bin/` directory. See the Oracle Solaris documentation for information about installing the XCU4 utilities.

IP Filter (Solaris version 11.3 and earlier)

- Avoid making any changes to packet filtering with Packet Filter. Do not use Packet Filter while VEN software is installed.
- The Solaris system's firewall state table limit is 65,536 entries. When that limit is reached, IP Filter drops packets. If you anticipate a high number of network connections, configure higher limits in the IP Filter state table. See Tuning the IP Filter State Table for Solaris and AIX workloads in the *VEN Administration Guide*.

> IMPORTANT:
> In Solaris 11.4, Packet Filter replaces IP Filter. When installing the VEN on Solaris 11.4, Illumio only supports Packet Filter. IP Filter is not supported in branded zones starting with Solaris 11.4.

Change Default Username

You can set an environment variable to change the username that owns the non-privileged portions of the installed software. The privileged portions of the installed software are always owned by root, and the software can only be run as root.

Environment Variable	Description
`VEN_NONPRIV_USER`	Existing username to override the default username `ilo-ven`. The group name of the specified user is the primary existing group name of the specified user.

You can reset this environment variable in your customized Solaris Response file or at a prompt during interactive installation.

About Solaris 11.4 Support

Prior to 11.4, Solaris used IP Filter as the firewall. In Solaris 11.4, Packet Filter is the only supported firewall.

The following details apply to Solaris 11.4 support by the VEN:

- Support for Solaris 11.4 does not change the VEN installation or upgrade process on Solaris workloads; if you've written installation scripts, they don't require updates. Package installation remains the same for 11.4 as for earlier supported versions of Solaris.
- Packet Filter support does not impact the PCE; viewing a workload that is running Solaris 11.4 in the PCE web console does not change. You can view all the

workload details. Creating policy for workloads running Solaris 11.4 does not change.

- Packet Filter does not support customizable table sizes. However, state tables in Solaris 11.4 use a 1 million state table size.

IMPORTANT:
For the complete list of all Solaris versions supported by the VEN in this release, see OS Support and Package Dependencies on the Illumio Support portal.

About the Solaris Response and Admin Files

In addition to the Solaris VEN, the VEN package includes two files to help with VEN installation on Solaris hosts: the Solaris Administration and Response files. For more information about these files, see Avoiding User Interaction When Adding Packages (pkgadd) in the *Oracle Solaris Administration Guide*.

Solaris Administration File

The Solaris Administration contains information about how the VEN installation or upgrade should proceed on the Solaris host. To perform a non-interactive VEN installation or upgrade (the VEN installation script will *not* prompt for settings when it runs), you must customize the Administration file.

In addition to settings, the file contains commented-out instructions for changing the settings.

CAUTION:
If you choose to provide custom values in the Administration file, you must delete these commented-out lines or the VEN installation or upgrade will fail. Commented-out lines in a Solaris Administration file are not supported with the Solaris `pkgadd` command.

```
# This file is used in case of upgradation
# instance=ask allows multiple instance of the same software to be installed
# and hence the UPDATE flag is passed to us in procedural scripts of IPS.
mail=
instance=ask
partial=ask
runlevel=ask
```

```
# Require that our dependencies are met when installing.
idepend=quit
# However, if someone tries to uninstall us but another package depends on us,
# we should just warn them & ask if they want to proceed anyway.
rdepend=ask
space=ask
setuid=ask
conflict=ask
action=nocheck
networktimeout=60
networkretries=3
authentication=quit
keystore=/var/sadm/security
proxy=
basedir=default
```

Solaris Response File

The VEN package includes a template for the Solaris Response file. The template contains the environment variables that you can set when installing and upgrading the Solaris VEN.

In addition to the available environment variables, the template contains commented-out instructions for providing custom values for variables.

CAUTION:
If you choose to provide custom values in the Response file, you must delete these commented-out lines or the VEN installation or upgrade will fail. Commented-out lines in a Solaris Response file are not supported with the Solaris `pkgadd` command.

```
#Parameter : VEN_NONPRIV_USER
#Type : String
#Description : VEN non-privileged user. If unspecified (VEN_NONPRIV_USER=""), then
the default account "ilo-ven" is used. If that account does not exist on the
system, it is created automatically. If specified (VEN_NONPRIV_USER="foo"), the
provided account is used. If that account does not exist on the system, then the
installer fails. All non-root-owned files that the VEN creates are owned by that
user and that user's primary group. For further information about this feature,
```

```
refer to the Illumio VEN deployment documentation.
VEN_NONPRIV_USER=""
#Parameter : VEN_PKI_CLIENT_CERT
#Type : String
#Description : PKI (public key infrastructure) authentication certificate. Use
with VEN_PKI_CLIENT_KEY. When specified, these fields are appended to runtime_
env.yml. Then, they may be used to activate the VEN. I.e., ``$ /opt/illumio_
ven/illumio-ven-ctl activate'' uses these fields to authenticate the VEN with the
PCE.
VEN_PKI_CLIENT_CERT=""
VEN_PKI_CLIENT_KEY=""
VEN_KERBEROS_MANAGEMENT_SERVER_SPN=""
VEN_KERBEROS_LIBRARY_PATH=""
VEN_ACTIVATION_CODE=""
VEN_MANAGEMENT_SERVER=""
VEN_INSTALL_ACTION=""
#Parameter : VEN_NO_SUSPEND
#Type : Number
#Description : Custom setting to disable suspend. 1 - disable, 0 - default
VEN_NO_SUSPEND=0
```

If you leave the Response file as is, the VEN installation script uses the default values for these environment variables by displaying them at the prompts during an interactive installation or silently during installation (because you're using the Administration file).

To Use Customized Response and Administration Files

To customize the Response and Administration file for your Solaris VEN installation or upgrade, perform these steps:

1. Extract the Response and Administration files from the VEN package. See Installation Preparation for information.
2. Copy and rename the files from the following directories for your machine architecture:

```
$ sudo bash
# cp illumio-ven/root/opt/illumio_ven/etc/templates/admin /tmp/admin.custom
```

```
# cp illumio-ven/root/opt/illumio_ven/etc/templates/response
/tmp/response.custom
```

This command example suggests copying the files to the `/tmp` directory; however, you can copy the files to any directory.

3. Edit the files to set your own values. See Solaris Response File and Solaris Administration File for the requirements when customizing these files.

Installation Preparation

1. Download the VEN package from the Illumio Support portal. See Obtain the VEN Packages for information.

   The Solaris VEN software downloaded from the Illumio Support portal is provided as a compressed tar archive file that contains one file for each of the supported Solaris machine architectures: SPARC and x86_64:

   - `illumio-ven-<ven_version>.sol5.sparc.pkg`
   - `illumio-ven-<ven_version>.sol5.i386.pkg`

2. Extract the Solaris VEN software:

```
# gunzip illumio-ven-<ven_version>.<architecture>.pkg.tgz
# tar -xvf illumio-ven-<ven_version>.<architecture>.pkg.tar
```

3. Install your trusted root CA certificate in the following directory with this exact specified filename:

```
/etc/certs/ca-certificates.crt
```

Ways to Install the Solaris VEN

You can install the Solaris VEN by specifying the Solaris `pkgadd` command and running the interactive VEN installation script; referred to as a “basic” installation in this topic.

Alternatively, you can use a Solaris Administration file or Solaris Response file (or both) to perform a non-interactive installation or set custom installation values (or both); referred to as an “advanced” installation in this topic.

Behavior During Each Type of Installation

SOLARIS FILES	BEHAVIOR
None	The VEN installation script performs a basic installation wherein you are prompted to set installation values or accept the default values.
Administration file only	The VEN installation script runs without prompting you for installation values (non-interactive) and uses only the default installation values; you cannot specify custom values.
Response file only	The VEN installation script launches an interactive installation; however, the prompts contain your custom values or the default value if not set. Press **Enter** to accept.
Both Administration and Response files	The VEN installation script runs without prompting you for installation values (non-interactive) and uses your custom values or the default value if not set. This method is the most automated of all the ways to install the Solaris VEN.

Basic Installation

1. Complete the tasks to prepare for Solaris VEN installation. See Installation Preparation for information.
2. To install the Solaris VEN, enter the following command:

```
# pkgadd -d . illumio-ven-<ven_version>.<architecture>.pkg
```

> IMPORTANT:
> When installing the Solaris VEN, enter the correct package for the Solaris machine architecture (SPARC or x86_64) you want to install:
>
> - `illumio-ven-<ven_version>.sol5.sparc.pkg`
> - `illumio-ven-<ven_version>.sol5.i386.pkg`

   The interactive VEN installation scripts starts.
3. Provide custom VEN installation and configuration values at the prompts or accept the defaults.

Solaris VEN installation is complete. The next step is to activate the Solaris VEN.

Advanced Installation

1. Complete the tasks to prepare for Solaris VEN installation. See Installation Preparation for information.
2. Prepare the Solaris Administration and Response files for use in the installation. See To Use Customized Response and Administration Files for information.
3. Enter the following command to perform a customized, non-interactive installation:

```
# pkgadd -d . -a pkgadd -a /tmp/admin.custom -r /tmp/response.custom illumio-ven-<ven_version>.<architecture>.pkg
```

Where the paths to the customized Administration and the Response files are the same ones you created when you extracted and copied them locally or to a network share. See To Use Customized Response and Administration Files for information.

IMPORTANT:
When installing the Solaris VEN, enter the correct package for the Solaris machine architecture (SPARC or x86_64) you want to install:

- `illumio-ven-<ven_version>.sol5.sparc.pkg`
- `illumio-ven-<ven_version>.sol5.i386.pkg`

Solaris VEN installation is complete. The next step is to activate the Solaris VEN.

Activate a Solaris VEN After Installation

After installing the VEN package on the Solaris host, activate the VEN with the Illumio VEN CTL (`illumio-ven-ctl`). The `--activate` option activates the workload and pairs the Solaris VEN with the PCE.

TIP:
You can activate the Solaris VEN by using the VEN CTL or by specifying the values in the appropriate environment variables in the Solaris Response file. See Solaris Response File for information.

NOTE:
Activating the Solaris VEN on a workload that is running an LDAP client can take longer than on workloads not using LDAP.

At a minimum, to activate the Solaris VEN using the VEN CTL, you need the hostname or IP address of the PCE, an activation code (called a pairing key in the PCE web console) generated from a pairing profile, and any other available options, such as the workload policy state, label assignment, workload name, and more.

The following example shows how to activate the VEN and set its policy state to Illuminated:

```
# /opt/illumio_ven/illumio-ven-ctl activate --activation-code  <code> --
management-server <fqdn:port>
```

Upgrade the Solaris VEN

IMPORTANT:
Illumio strongly recommends that you upgrade VENs only during maintenance windows.

NOTE:
If the VEN was activated prior to the upgrade, it does not need to be activated again after the upgrade completes.

Illumio supports both Solaris machine architectures: SPARC and x86_64. The upgrade steps for both machine architectures are identical but each architecture uses its own VEN package file.

For the supported upgrade paths for the Solaris VEN, see Upgrade VEN on the Illumio Support portal (login required).

Requirement: To upgrade the Solaris VEN, you must perform the upgrade by using the Solaris Administration file. Using the Response file with the upgrade is optional.

1. Download the new version of the VEN package from the Illumio Support site. See Obtain the VEN Packages for information.
2. Extract the Solaris VEN software. See Installation Preparation for information.
3. Prepare the Solaris Administration file for the upgrade. See To Use Customized Response and Administration Files for information.

   At a minimum, you must set the following values in the Administration file for the upgrade:

```
mail=
instance=overwrite
conflict=nocheck
action=nocheck
```

4. Stop the VEN if it's running:

```
llumio-ven-ctl stop
```

5. Enter the following command to perform a non-interactive installation:

```
# pkgadd -d . -a /tmp/admin.custom illumio-ven-<ven_
version>.<architecture>.pkg
```

Where the path to the customized Administration file is the same one you created when you extracted and copied it locally or to a network share.

NOTE:
If you also need to customize settings for the upgrade, use a customized Response file for the upgrade and include the `-r` argument in the upgrade command; for example: `-r /tmp/response.custom`. See Solaris Response File for information.

Uninstall the Solaris VEN

IMPORTANT:
Before you uninstall the VEN software from a Solaris workload, unpair the VEN running on the workload from the PCE. See Deactivate and Unpair VENs in the *VEN Administration Guide*.

1. Enter the following commands to uninstall the VEN:

```
$ sudo bash
# cd /tmp
# pkgrm illumio-ven
```

2. The following command output and prompts appear in the command window. Respond to the required prompts to uninstall the VEN:

```
The following package is currently installed:
   illumio-ven  illumio-ven
                (i386) <ven_version>.sol5.i386

Do you want to remove this package? [y,n,?,q] y

## Removing installed package instance <illumio-ven>

This package contains scripts which will be executed with super-user
permission during the process of removing this package.

Do you want to continue with the removal of this package [y,n,?,q] y
## Verifying package <illumio-ven> dependencies in global zone
## Processing package information.
## Executing preremove script.
VEN_DATA : /opt/illumio_ven_data
Stopping venAgentMonitor: ...done
Stopping venAgentMgr:    ...done
Stopping venVtapServer:    ...done
Stopping venPlatformHandler:    ...done
## Removing pathnames in class <none>
.
.
.
## Executing postremove script.
## Updating system information.

Removal of <illumio-ven> was successful.
```

Chapter 6

Reference

This chapter contains the following topics:

This section contains useful reference information for installing and upgrading VENs on workloads in your organization.

VEN Activate Command Reference

The following topic describes the commands for activating the VENs either during or after installation, and the ways that you can configure the VEN during activation.

About the Command Options

You use the `activate` options in these ways:

- When pairing a VEN with a pairing script and you activate the VEN during installation:
  - `pair.sh` (Linux)
  - `pair.ps1` (Windows)
- When activating a VEN (all supported operating systems) after VEN installation by using the `illumio-ven-ctl` control script

If you are activating with a PCE that has a pairing profile configured to block changes to policy state (the `illumio-ven-ctl` option `--mode`) or label assignment (the `illumio-`

`ven-ctl` options `--env`, `--loc`, `--role`, `--app`), you must not use these options on these blocked configurations or the activation will fail.

WARNING:
When you use the VEN CTL or a pairing script to install a Windows VEN on a workload, you cannot include colons in the values for the options. Including a colon in a command value causes VEN activation to fail. For example, including the following values in the `-role` option, causes VEN activation to fail:

```
-role "R: UNKNOWN" -app "A:UNKNOWN" -env "E: UNKNOWN"
```

Activation fails because Windows uses the colon as a special character and cannot interpret the value even when you include quotation marks around the value.

Description of the `activate` Command Options

The options and arguments are the same for Windows and Unix (Linux, Solaris, and Solaris), except the options with two dashes on Unix should be replaced with a single dash on Windows (for example, `--loc` on Linux should be replaced with `-loc` on Windows).

NOTE:
The following options are optional unless noted in the description.

Option	Arguments	Description
`activation-code | -a`	`<activation_code>`	**REQUIRED:** Inputs the activation code of the VEN into the pairing script. This code is auto-generated by the pairing profile. Activation code: one-time use or unlimited use In the PCE web console, you can specify that an activation code is for one-time use or for unlimited uses. Be sure you have generated the correct type for your needs. Do not use a single one-time use activation code for more than one workload. Example: `--activation-code 1234567890abcdef`
`management-server | -m`	`<PCE_FQDN:port> | <IPaddress:port>`	**REQUIRED:** Sets the domain name or IP address and port of the host where the VEN can retrieve master configuration information.

Option	Arguments	Description
		Example: `--management-server mypce.example.com:8443`
`name | -n`	`<server_friendly_name>`	Sets a friendly name that will be used for this workload when it appears in the PCE web console. Example: `--name "Web Server 1"`
`env`	`<environment_label>`	Assigns an Environment label for this workload. Example: `--env Production`
`loc`	`<location_label>`	Assigns a Location label for this workload. Example: `--loc "US"`
`role`	`<role_label>`	Assigns a Role label for this workload. Example: `--role "Dev Group"`
`app`	`<application_label>`	Assigns an Application label for this workload. Example: `--app "Web Service"`
`proxy_server`	`<proxy-string>`	**[Linux, Solaris, AIX only]** You only need to specify this option when configuring a proxy server for a Linux, Solaris, or AIX workload. Windows automatically detects a proxy server; therefore, you do not need to specify this option when installing a VEN on a Windows workload. For information about configuring a proxy server, see VEN Proxy Support.
`log-traffic`	`true | false`	Enables or disables traffic logging. If not specified, logging is set to true by default. Default: `true` Interacts with the `visibility-level` option. See Allowable Combinations of log-traffic and visibility-level.
`mode`	`illuminated | enforced | idle`	Sets the policy state for the workload. For an explanation of the various states, see "Workload Policy States" in the *VEN Administration Guide*.
`enforcement_mode`	`full | visibility_only | selective | idle`	Default: `visibility_only` Enables the new `selective` mode for the VEN.

Option	Arguments	Description
`visibility-level`	`flow_summary` | `flow_drops` | `flow_off`	Default: `flow_summary` Defines the extent of the data the VEN collects and reports to the PCE from a workload in the Full enforcement or Visibility policy states, so you can control resource demands on workloads. The higher levels of detail are useful for visualizing traffic flows in greater detail in the Illumination map inside the PCE web console. Interacts with the `--log-traffic` option. See Allowable Combinations of log-traffic and visibility-level.

`visibility-level` Arguments

Argument	Value in Policy States	Notes
`flow_summary`	Included in all policy states	Default. The VEN collects traffic connection details for both *allowed* and *blocked* connections: source and destination IP address and port and protocol. This argument creates traffic links in the Illumination map and is typically used initially after installing the VEN to determine the full scope of potential policy impact on the workload.
`flow_drops`	Valid only in full policy state	The VEN collects connection details only for *blocked* traffic: source and destination IP address and port and protocol. This argument produces less detail for Illumination but demands fewer workload system resources than `flow_summary`.
`flow_off`	Valid in all policy states	The VEN does not collect any details about traffic connections. This option produces no details for the Illumination map but requires the fewest number of workload resources. Useful when you are satisfied with policy rules and do not need additional detail.

Allowable Combinations of `log-traffic` and `visibility-level`

The following rules apply to using the `log-traffic` and `visibility-level` options together with the activate command:

- The `visibility-level` argument takes precedence over the `log-traffic argument`.
- `visibility-level flow_off` and `--log-traffic true` is an invalid combination.
- `visibility-level flow_drops` is invalid in Illuminated policy state.

VEN Modes in Illumio Core 20.2.0 and later

In Illumio Core 20.2.0, Illumio introduced a new feature called Selective Enforcement. For an explanation of how this feature changed policy functionality in the release, see Selective Enforcement in *What's New in This Release, 20.2.0*.

NOTE:
This change to the VEN modes affects the VEN in Illumio Core 20.2.0 and later releases.

In particular, the feature changed the workload policy states. To further understand how the policy state changed between releases, see these topics:

- Workload Policy State in the *Security Policy Guide*, 19.3.x releases
- Workload Enforcement States in the *Security Policy Guide*, 21.2.0 release

The changes to policy states in 20.2.0 impacted the VEN `mode` option that you specify with the `activate` command in the following ways.

CAUTION:
Do not use both the `mode` and `enforcement_mode` options together on the command line because you could specify contradictory options. Specify one or the other. To specify the new Selective Enforcement option, enter the `enforcement_mode selective` option and argument.

- Adds a new option for the `activate` command: `enforcement full|visibility_only|selective|idle`
- Retains the `mode` option from the previous release for backward compatibility
- The arguments for the `mode` option map to those for the `enforcement_mode` option in this way:
  - `illuminated` maps to `visibility_only`
  - `enforced` maps to `full`

  - `idle` is the same in both options
  - `enforcement_mode` option adds the `selective` argument

    Use the `selective` argument to set the VEN mode as Selective Enforcement state. For information about using Selective Enforcement in policy, see Enforcement Modes for Rules in the *Security Policy Guide*.

- The `visibility-level` option and argument are unchanged in Illumio Core 20.2.0 and later releases; however, the Selective Enforcement feature separated the workload policy visibility state from the policy enforcement state; in particular, the PCE web console has separate drop-down menus (**Enforcement** and **Visibility**) in the **Workloads** page for these two options.

  The arguments for the `visibility-level` option map to the new visibility states in 20.2.0 and later releases in this way:

  - `flow_off` maps to Off
  - `flow_drops` maps to Blocked
  - `flow_summary` maps to Blocked + Allowed

VEN Compatibility Check

This topic explains how to use the VEN Compatibility Check feature after installing VENs on workloads.

About Compatibility Checks

When you pair a 19.3.*x* VEN or later release in the Idle state or change the VEN state to Idle, the VEN performs several compatibility checks and sends the results to the PCE. This process occurs every 24 hours and checks whether the preexisting workload state will have issues when the VEN is moved out of the Idle state.

After reviewing the results of the VEN Compatibility Check, you can determine if the VEN is ready to moved out of the Idle state or resolve any detected issues, such as backing up any system firewall rules.

NOTE:
The VEN Compatibility Check is per-workload and is only available for VENs in the Idle state and is not available for the Visibility, Selective, or Full states. If a workload reverts from any of these states to the Idle policy state, the VEN Compatibility Check is performed.

All detected issues are categorized as:

- **Red:** Major incompatibility detected
- **Yellow**: A potential incompatibility detected
- **Green**: No major incompatibilities detected

The Compatibility Check results are displayed in the PCE web console. To view the results, select the workload's details page, then select the **Compatibility Report** tab.

If no incompatibilities have been detected on the VEN, the page displays "No incompatibilities found."

After viewing the results, you can export them as a text file by clicking **Export**.

The compatibility checks vary by the workload's operating system.

Linux Operating Systems

Incompatibility Type	Reason for incompatibility with Illumio Core	Results
IPv4 forwarding enabled	At least 1 iptables forwarding rule is detected in the forwarding chain. VEN removes existing iptables rules in the non-Idle policy state.	Yellow
IPv4 forwarding packet count	Complementary check whether IPv4 forwarding is enabled.	
iptables rule count	At least 1 iptables filter rule is detected. VEN removes existing iptables rules in the non-Idle policy state.	Yellow
IPv6 global scope enabled	IPv6 is enabled for the workload.	Yellow
IPv6 active connection count	Complementary check whether IPv6 global scope is enabled.	
ip6tables rule count	At least 1 iptables filter rule is detected. VEN removes existing ip6tables rules in the Visibility policy state	Yellow
IPsec service enabled	UDP port 500/4500 is in use by other services. Do not enable SecureConnect for the workload.	Red
Routing table conflict	The StrongSwan routing table setting conflicts with existing networking routing tables. Do not enable SecureConnect for the workload.	Red

Windows Workloads

Incompatibility Type	Reason for incompatibility with Illumio Core	Results
IPv6 enabled	IPv6 is enabled for the workload.	Yellow

Incompatibility Type	Reason for incompatibility with Illumio Core	Results
Virtual loop-back interfaces	Virtual loopback interface is detected. Untested and unsupported configuration.	Yellow
Firewall GPO	Windows firewall Group Policy Object (GPO) is detected. For more information, see KB Article #3545, Firewall GPO Warning Under Compatibility Report (login required).	Yellow
IPsec service enabled	IKEEXT service is disabled. Do not enable SecureConnect for the workload.	Yellow

AIX and Solaris Workloads

Incompatibility Type	Reason for incompatibility with Illumio Core	Results
IPv4 forwarding enabled	IPv4 is enabled for the workload.	Yellow
IPv4 forwarding packet count	Complementary check whether IPv4 forwarding is enabled.	
iptables rule count	At least 1 iptables filter rule is detected. VEN removes existing iptables rules in the non-Idle policy state.	Yellow
IPv6 global scope enabled	IPv6 is enabled for the workload.	Yellow
IPv6 active con-nection count	Complementary check whether IPv6 global scope is enabled.	
ip6tables rule count	At least 1 iptables filter rule is detected. VEN removes existing ip6tables rules in the Visibility policy state	Yellow
IPsec service enabled	IPsec service is already in use. Do not enable SecureCon-nect for the workload.	Red

Pairing Script and Package Installation (Linux & Windows)

The following information is provided for your reference so that you understand the process and events that occur when you install a VEN by using a pairing script in the PCE or by installing a package with the CLI.

Linux Pairing Script for VEN Library

The following example shows a typical Linux pairing script. The pairing script works with the VEN Library in the PCE web console:

```
rm -fr /opt/illumio_ven_data/tmp && \
umask 026 && mkdir -p /opt/illumio_ven_data/tmp && \
curl --tlsv1 "https://example.com:8443/api/v18/software/ven/image?pair_
script=pair.sh&profile_id=2" -o /opt/illumio_ven_data/tmp/pair.sh && \
chmod +x /opt/illumio_ven_data/tmp/pair.sh && \
/opt/illumio_ven_data/tmp/pair.sh \
--management-server example.com:8443 \
--activation-code <code>
```

This pairing script performs the following actions on the workload:

1. Deletes the `/opt/illumio_ven_data/tmp` directory, if it already exists.
2. Changes `umask` to `026` to prevent the `group-write` and `others-read,write` permissions as it creates the `/opt/illumio_ven_data/tmp` directory.
3. Uses curl to download the pairing script from the VEN repository and store it in the `/opt/illumio_ven_data/tmp` directory.
4. Changes the script permissions to allow execution.
5. Runs the `opt/illumio_ven_data/tmp` script with the following command line options:

    6. `--management-server` to communicate with the PCE

    7. `--activation-code` to authenticate the VEN to the PCE and authorize the VEN to pair with the PCE

The pair script installs the VEN packages on the workload and pairs the VEN with the PCE. The output of pair is captured in `/var/log/illumio_install.log`.

Next, the script performs the following operations:

1. Detects OS release and CPU architecture. Ensure the combination is supported.
2. Downloads the package to `/opt/illumio_ven_data/tmp`.
3. Uses native OS package manager (detected by line 1) to install the package.

    Using native package managers is simpler for newer operating systems. For example, Illumio can use yum to manage package dependencies for the VEN and

workloads. For older operating systems, customers have to manage dependencies by manually installing packages.

4. Verifies installation by invoking installed scripts.
5. Invokes `/opt/illumio_ven/bin/init_Platform start`.
6. Generates the activation file `/opt/illumio_ven_data/etc/agent_activation.cfg`.
7. Invokes `/opt/illumio_ven/bin/agent_status.sh` to activate the VEN.

RPM Installation

RPM installation performs the following operations:

1. Creates the `ilo-ven` user and group, unless a custom username is specified at installation.
2. Prepares and then starts the Illumio Core to perform the following actions:
   a. Loads the necessary kernel modules: `ip_tables`, `iptable_filter`, `nf_conntrack`, `nf_conntrack_ipv4`, `nf_conntrack_ftp`, `ipt_LOG`, `ip_set`, `ip6_tables`, `ip6table_filter`, `nf_conntrack_ipv6`, `ip6t_LOG`
   b. Sets `net.netfilter.nf_conntrack_tcp_timeout_established` to 8 hours (28,800 seconds). See Linux nf_conntrack_tcp_timeout_established.
   c. Takes control of the system firewall.
   d. Disables and stops the system firewall service iptables.

      This action is acceptable because the Illumio services act in place of the iptables service.

   e. Saves existing iptables rules if any.
   f. Loads iptables rules computed from PCE firewall policy.
   g. Starts the VEN components described in Description of VEN Components in the *VEN Administration Guide*.

      This step includes monitoring system iptables configuration (similar to the service iptables performed).

Windows Pairing Script

The following example shows a typical Windows pairing script. The pairing script works with the VEN Library in the PCE web console. (*Line breaks have been added for readability only.*)

```
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://example.com:8443/api/v18/software/ven/image?pair_
script=pair.ps1&profile_id=1', (echo $env:windir\temp\pair.ps1)); &
$env:windir\temp\pair.ps1
-management-server example.com:8443 -activation-code <code> }"
```

This pairing script performs the following actions on the workload:

1. Changes execution policy of the host PowerShell process to RemoteSigned.
2. Configures the .NET framework `System.Net` class to negotiate TLS 1.2.

   The Windows VEN uses “3072” instead of “Tls12” because the `enum` value is not defined in older Windows operating systems. When `system.net` does not support TLS 1.2, the script fallbacks to using the system default.
3. Using the .NET framework `WebClient` class, downloads `pair.ps1` from the VEN repository and stores it in the `$env:windir\temp` directory.
4. Runs the `pair.ps1` script with the following command line options:
   - `-management-server`: Used by the VEN to communicate with the PCE
   - `-activation-code`: Used by the PCE to authenticate and authorize the VEN during the pairing process
5. The pairing script installs the VEN packages on the workload and pairs the VEN with the PCE. The output of `pair.ps1` is captured in `$env:windir\temp\illumio.log` or `$env:tmp\illumio.log`.

   The script performs the following actions:

   a. Retrieves VEN MSI package from the VEN repository using .NET framework `WebClient` class.
   b. Launches `msiexec.exe` to install the downloaded package.
   c. Generates `agent_activation.cfg` file with PCE information
   d. Retrieves agent activation status and displays it.

FIPS Compliance for VEN

This section describes the operational requirements for compliance with Federal Information Processing Standard (FIPS) 140-2 for the VEN.

FIPS Prerequisites

- Red Hat 7.9.
- Red Hat 8.2.
    - The VEN will be FIPS compliant on later versions of Red Hat 8.x as Red Hat completes the FIPS certification process.
- Windows Server 2012 R2, 2016, and 2019.

Enable Red Hat Linux VEN FIPS Compliance

All VEN OpenSSL communications by default operate in a FIPS-compliant mode.

1. Before activating the VEN, configure FIPS mode as described in RHEL 8, Section 9.1 ("Crypto Officer Guidance") of Red Hat Enterprise Linux 8 OpenSSL Cryptographic Module v8.0.
2. After the system starts, check that FIPS mode is enabled:

    ```
    $ fips-mode-setup --check

    FIPS mode is enabled.
    ```

3. Activate the VEN.

NOTE:
OpenSSL 3.0 module used on Red Hat 7 is in process for FIPS validation, but is not yet certified. The VEN will become FIPS compliant as soon as the OpenSSL module is certified.

NOTE:
The SecureConnect feature is not FIPS compliant with RHEL 7.4 or RHEL 7.9.

Enable Windows VEN FIPS Compliance

Windows Server 2012, Windows Server 2016, Windows 7, and Windows 10 must be configured according to the following vendor documents:

- Windows 2012 conforming with Section 2 of the Windows Server 2012 NIST Security Policy
- Windows 2016 conforming with Section 2 of the Windows Server 2016 NIST Security Policy

FIPS-related Government and Vendor Documentation

- Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules
- Red Hat Enterprise Linux OpenSSL Cryptographic Module NIST Security Policy
- RHEL v8.x Red Hat Enterprise Linux 8 OpenSSL Cryptographic Module v8.0
- Windows Server 2012 NIST Security Policy
- Windows Server 2016 NIST Security Policy

Enable FIPS Compliance for Windows VENs

Windows VEN is FIPS compliant when installed on Windows Server 2012 or Windows Server 2016.

1. Before activating the VEN, configure FIPS mode as described in the documentation provided by Microsoft. See "Step 3: Enable the FIPS security policy" in FIPS 140-2 Validation on the Microsoft Learn website.
2. Activate the VEN.

VENs on RHEL8 and OpenSSL CVEs

VENs installed on RHEL 8 use the OpenSSL package that is installed as part of the OS. There are known security vulnerabilities on several OpenSSL versions. The vulnerabilities CVE-2022-1292, CVE-2022-2068, and CVE-2022-2274 are defined by NIST U.S. Department of Commerce. The OpenSSL `c_rehash` script does not properly handle shell metacharacters to prevent command injection. The recommended action is to upgrade to the latest OpenSSL v3.0.5 or v1.1.1q or later. Please note that based on its usage of OpenSSL, VENs are not impacted by CVE-2022-1292, CVE-2022-2068, and CVE-2022-2274.

Supporting OpenSSL 3.0 on Linux Systems

strongSwan, the IPSec subsystem for the Linux OS, must be updated to support OpenSSL 3.0. VENs with OpenSSL 3.0 during a FIPS certification migration breaks the PKCS12_*xxx* API. The PKCS12KDF security algorithm that is used for the PKCS12 MAC binary storage format is not FIPS compliant (although it supports older FIPS

standards with OpenSSL 1.0.2). Illumio uses PKCS12 for easy management of certificates and key pairing and not for security purposes.

NOTE:
Adding another algorithm for PKCS12 MAC would fix this issue, however it would require changing the FIPS standard. This is because the non-compliant PKCS12KDF algorithm is hardcoded into the PKCS12 standard as the key derivation function (KDF) that generates the MAC key from the password.

To support OpenSSL 3.0, Illumio recommends generating the PKCS12 container for Linux systems.

Enter the following commands in the CLI.

For any Linux VEN version before 22.2.10:

- Without FIPS:
  ```
  openssl pkcs12 -export -out certificate.p12 -inkey mykey.pem -in mycert.pem -password pass:
  ```
- With FIPS:
  ```
  openssl pkcs12 -export -out certificate.p12 -inkey mykey.pem -in mycert.pem -password pass: -descert -des3
  ```

For any 22.2.10 VEN Linux version and after:

- With OpenSSL 3.0 supported or VEN with OpenSSL 3.0 with FIPS:
  ```
  openssl pkcs12 -export -out certificate.p12 -inkey mykey.pem -in mycert.pem -password pass: -provider fips -nomac
  ```
- With any version of OpenSSL without FIPS:
  ```
  openssl pkcs12 -export -out certificate.p12 -inkey mykey.pem -in mycert.pem -password pass:
  ```