Illumio Adaptive Security Platform 18.2.1 VEN Operations Guide

01/24/2019

50000-100-18.2.1

Table of Contents

Product Version

Illumio® Adaptive Security Platform®

Current PCE Version: 18.2.1

Current VEN Version: 18.2.1

Note: 18.2.1 has not been designated as a Long Term Support (LTS) release. In the future an 18.2.x LTS release will be designated.

About Illumio

Illumio products and services are built on Illumio's patented technologies. For more information, see Illumio Patents.

Illumio Professional Services for Deployment

To ensure optimal deployment of the Illumio Adaptive Security Platform, contact your Illumio Professional Services representative.

Preview Features Only for Evaluation Before General Availability

Any preview features in this release of Illumio Adaptive Security Platform are for your evaluation only.

> **Do not deploy preview features in a production environment**
> Be sure to install these preview features only on non-production systems. To avoid inadvertently impacting your current operations, do *not* install the preview features on production systems.
> The purpose of preview features is to make them more useful for your needs before general availability.

Illumio welcomes your comments and suggestions for improving preview features and documentation. For more information and to send feedback, contact Illumio Customer Support.

Illumio Adaptive Security Platform Training

Illumio offers a wide yet focused training curriculum for Illumio Adaptive Security Platform, from beginning to advanced topics.

To see available courses, log into your Illumio support account and select the **Training** tab.

Search Knowledge Base and Documentation

For useful short articles about Illumio Adaptive Security Platform, log into your Illumio support account and select the **Knowledge Base** or **Documentation** tab.

Illumio Adaptive Security Platform Support

If you cannot find what you are looking for in this document or in support Knowledge Base and Documentation, contact us at:

- support@illumio.com
- +1-888-631-6354
- +1-408-831-6354

Recommended Skills

Illumio recommends that you be familiar with the following:

- Your organization's security goals
- Solid understanding of Illumio Adaptive Security Platform
- General computer system administration of Linux and Windows operating systems, including startup/shutdown, common processes or services
- Linux shell (bash), Windows PowerShell, or both
- Understanding TCP/IP networks, including protocols and well-known ports
- Familiarity with PKI certificates

Related Documentation

Illumio® Adaptive Security Platform® documentation is available from the Support portal.

- *Policy Compute Engine (PCE) Web Console Guide*: working with Illumination®, designing security policy, and provisioning and administering VENs.
- *Policy Compute Engine (PCE) Deployment Guide*: planning and installing the PCE.
- *Policy Compute Engine (PCE) Operations Guide:* common management tasks of the PCE.
- *Advanced Command-line Tool Interface Guide*: common PCE-related tasks to use on your local computer.
- *Policy Compute Engine (PCE) Supercluster Deployment and Usage Guide*: designing, deploying, and managing the PCE Supercluster of multiple, distributed standard PCE clusters.
- *Policy Compute Engine (PCE) REST API Guide*: web-programming Illumio Adaptive Security Platform.

- *Virtual Enforcement Node (VEN) Deployment Guide:* installing and activating the VEN, including PCE-based distribution of the VEN and on-worload installation and management
- *Virtual Enforcement Node (VEN) Operations Guide*: common management tasks of the VEN.
- *Auditable Events and SIEM Integration Guide*: analyzing significant events on the PCE and VEN and securely transferring event records to analytics or Security Information and Event (SIEM) systems.

Notational Conventions

- 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:
  ```
  ...
  some command or command output
  ...
  ```
- References to section titles in this guide are in double quotation marks. Example: See "Basic Theory of Operation".
- Reference to other guides in the Illumio library are *italicized*. Example: See the *PCE Web Console User Guide*.

How To Use This Guide

This document shows you how use `illumio-ven-ctl` and other commands to administer the Virtual Enforcement Node (VEN) on a managed workload for operational tasks such as start/stop, suspend, and other functions on the VEN and with the Policy Compute Engine (PCE) in an on-premise deployment.

The *VEN Operations Guide* has several main divisions:

- Overview of VEN Software Architecture and Description of Components.
- VEN deployment models
- Command-line-oriented sections with syntax examples for `illumio-ven-ctl` for on-workload managing the VEN.
- Basic Theory of VEN Operations.

Terminology: Activation or Pairing

These following terms indicate the same function: putting the workload under managed control by the PCE:

- The terms *activation/deactivation a VEN* is used for the single package deployment model, which is downloaded and installed on the workload and then the `illumio-ven-ctl` command.
- The term *pairing/unpairing* a VEN is used for the Illumio Repo deployment model and also in the PCE Web Console, which relies on the `pair` or `pair.ps1` script.

VEN Logical Software Architecture and Description of Components

A *workload* with an installed VEN is a computer system you want to secure. A secured workload is known as a *managed workload*. You control the VEN's operations through the PCE user console or from the command-line on the VEN itself.

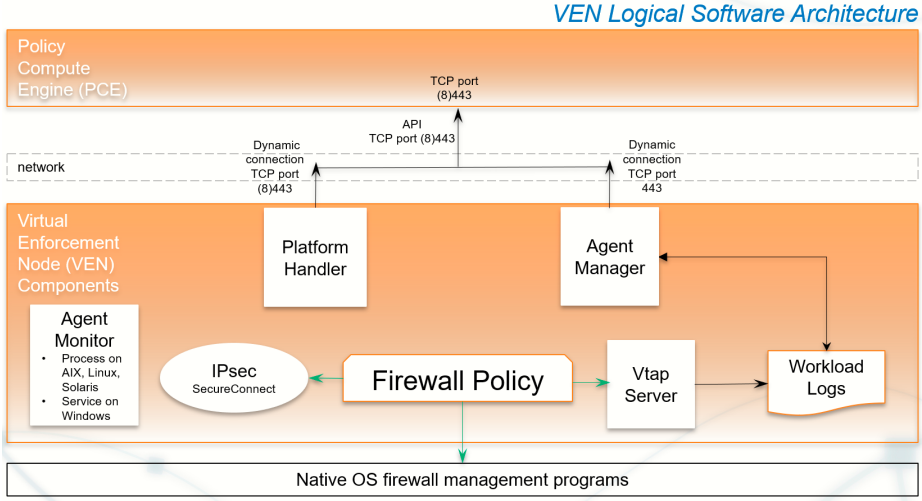
The VEN resides in the guest OS as a lightweight, multiple-process application with a minimal footprint.

- It interacts with the native networking interfaces to enforce policy received from the PCE.
- It operates periodically at maximum speed, remaining in the background as much as possible.
- It uses configurable operational modes to minimize the impact to workloads.
- It provides details of traffic flow data collected via logging, summarized by the VEN, and viewable in the PCE's Support Reports.

VEN Architectural Diagram

At startup, the VEN instantiates the following processes or services.

VEN Logical Software Architecture



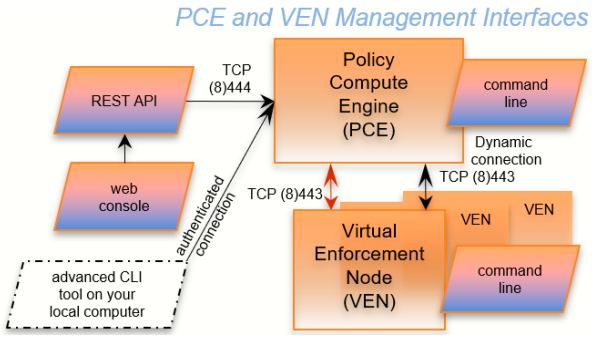
1. The VEN reports the managed workload's context (status and attributes) to the PCE.
2. The PCE computes a unique security policy for the workload and transmits it to the VEN.
3. The VEN receives the policy and programs native OS mechanisms on the workload.
4. The PCE lets those mechanisms enforce that policy.

Description of VEN Components

VEN Process	Description	Linux User	Windows User
AgentManager	• Manages uninstallation and upgrades. • Mines the workload's system information, such as network interfaces, and listening processes, to send to the PCE. • Uploads logs to the PCE for events and traffic flows. • Sends heartbeats to the PCE.	`root`	Administrator
PlatformHandler	Handles: • Sending VEN events to the PCE. • Firewall configuration via native OS mechanisms. • Tamper detection and protection. • Upgrades and uninstallation.	`root`	Administrator
vtapServer	Receives traffic flow data logs and records them in a SQLite database.	root	LOCAL SERVICE
AgentMonitor	Monitors VEN processes or services and restarts them when necessary.	root	LOCAL SERVICE
IPsec	The optional SecureConnect configures Internet Protocol Security (IPsec), a set of protocols to enforce security for IP networks. IPsec can be configured to use cryptography.	root	LOCAL SERVICE

Management Interfaces for the PCE and VEN

You can manage the PCE and the VEN via several interfaces.



Interface	Notes	See...
PCE web console	With the PCE web console, you can perform many common tasks for managing Illumio® Adaptive Security Platform®.	*PCE Web Console Guide*
PCE command line	Use of the command line directly on the PCE. A primary management tool on the PCE is the command line `illumio-pce-ctl` control script. You can perform many common tasks for managing Illumio® Adaptive Security Platform® on the PCE command line, including installing and updating the VEN.	*PCE Operations Guide*
PCE advanced command-line tool	From your own local computer, you can run the PCE advanced CLI tool for many management tasks on the PCE's resource objects: • Importing vulnerability data for analysis with Illumination®. • Importing/exporting security policy rules. • Managing security policy rules and rulesets, labels, and other resources.	*PCE Advanced Command-line Tool Guide*
REST API	With the Illumio® Adaptive Security Platform® REST API, you can perform many common management tasks. One use is to automate the management of large groups of workloads, rather than each workload individually. The endpoint for REST API requests is the PCE itself, not the workload; the REST API does not communicate directly with the VEN.	*REST API Guide*
VEN command line	A primary management tool on the VEN command line is the `illumio-ven-ctl` control script.	*VEN Operations Guide*

illumio-ven-ctl General Syntax

The `illumio-ven-ctl` is a primary tool for managing VENs on individual workloads. The script varies slightly by platform.

illumio-ven-ctl: Linux Two Dashes, Windows One Dash

Platform	Command	Notes
Linux	`illumio-ven-ctl`	⚠ Parameters for the script are preceded by *two* hyphens: *`--option1 var --option2 var ...`*
Windows	`illumio-ven-ctl.ps1`	In Windows PowerShell, the `.ps1` extension is *optional*. ⚠ Parameters for the script are preceded by a *single* hyphen: *`-option1 var -option2 var ...`*

Set PATH Environment Variable for illumio-ven-ctl

For easier invocation of the script, you might want to set your `PATH` variable to the directory where the VEN commands are located:

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

VEN Installation, Uninstallation, Upgrade, Activation, and Deactivation

How you install, uninstall, upgrade, activate, and deactivate the VEN is highly configurable. This extensive topic is detailed in the *VEN Deployment Guide*.

Verify VEN Version Number

You can verify the version of the VEN software in several different ways:

- In the PCE Web Console
- On the Workload itself.

  - Windows: Any of the following:
    - Examine the columns in **Uninstall or change a program** or Task Manager
    - Examine the **Properties > Details** tab of the `venAgentMgr.exe` or `venPlatformHandler.exe`
- With the REST API, the `agent-version` key and value are returned in the payload of every response.

VEN Startup

Via system boot files, the VEN starts when the workload is booted. The VEN can also be started manually.

Platform	Command	Notes
Linux	• `/etc/init.d/illumio-firewall` • `/etc/init.d/illumio-ven-ctl start`	• Installs ipset kernel module if necessary, sets iptables/ipsets to desired state. • Initializes and starts the daemon processes needed for VEN operation.
Windows	None needed	The Service Control Manager (SCM) starts all VEN services at boot.

VEN Shutdown

At shutdown, the VEN sends a “goodbye” message to the PCE. The PCE marks the Workload as offline and initiates a policy recomputation. After the new policy is distributed throughout the network, the Workload without the VEN is effectively isolated from the network.

Linux Workload Shutdown

- `illumio-ven-ctl stop` stops all VEN processes.
- The VEN sends a “goodbye” message to the PCE.

Windows Workload Shutdown

- Service Control Manager (SCM) stops all VEN services
- The VEN sends a “goodbye” message to the PCE

VEN Status

To see the status of the VEN on the workload, run this command.

```
$ illumio-ven-ctl status
```

VEN Disable/Enable

If you want to install the VEN but activate it at a later time, you can disable the VEN after you first install it.

For example, you can load the VEN on machine image and disable the VEN. See considerations regarding preparing a "Golden Master" in the *VEN Deployment Guide*.

Platform	Action		Notes

Linux	• Enable
	• Disable
		`$ illumio-ven-ctl enable`
		
		`$ illumio-ven-ctl disable`	

Windows	• Enable
	• Disable
		`$ illumio-ven-ctl.ps1 enable`
		
		`$ illumio-ven-ctl.ps1 disable`
			When you disable the VEN, all Illumio Adaptive Security Platform-based filters are removed from the Windows Filtering Platform (WFP).

VEN Suspend/Unsuspend

Suspending a VEN isolates a VEN on a workload so you can troubleshoot possible communication issues to determine the cause of any anomalous behavior.

- When you suspend a VEN, any rules programmed into the workload's iptables (including Custom iptables rules) or Windows Filtering Platform (WFP) firewalls are removed completely and all VEN software processes are shut down. The VEN's connectivity and policy sync status are changed to **Suspended**.
- Workloads communicating with the suspended VEN continue to have rules programmed into iptables or WFP.
- You can unpair a workload while its VEN is suspended.
- With the PCE Web Console you can change the policy state of the workload while the VEN is suspended. When the VEN is unsuspended, the new policy state is applied.

Linux - Before Suspending, Backup iptables/NAT rules

Before you suspend a Linux VEN, back up the workload's custom iptables rules or NAT rules.

After a workload is suspended, you need to restore the rules on the workload because all custom iptables or NAT rules are removed from the workload. At the time of suspension, the VEN informs the PCE that it is in suspended state.

If the PCE does not receive this notification, you must mark the workload as "suspended" in the PCE web console. See the *PCE Web Console Guide*.

If you do not mark the VEN as suspended in the PCE, after one hour the PCE assumes the Workload is offline and removes it from policy, which effectively isolates the workload from the network.

Suspend/Unsuspend Commands

Platform	Action	Command	Notes

Linux	• Suspend
	• Unsuspend
		`$ illumio-ven-ctl suspend`
		`Suspending the VEN... The VEN has been suspended. PCE was notified.`
		
		`$ illumio-ven-ctl unsuspend`
		`Unsuspending the VEN... The VEN has been unsuspended. PCE was notified.`
			⚠ Be sure to backup your configuration See "Linux - Before Suspending, Backup iptables/NAT rules".

Windows	• Suspend
	• Unsuspend
		`PS C:\Program Files\Illumio> illumio-ven-ctl.ps1 suspend`
		`Suspending the VEN... The VEN has been suspended. PCE was notified.`
		
		`PS C:\Program Files\Illumio> illumio-ven-ctl.ps1 unsuspend`
		`Unsuspending the VEN... The VEN has been unsuspended. PCE was notified.`	

Results of Suspending/Unsuspending

- The workload still appears in the PCE in the workloads list page and Illumination® map.
- The workload can only be unpaired from the PCE.
- An organization event (`server_suspended`) is logged. This event is exportable in Common Event Format (CEF) and Log Event Extended Format (LEEF) . This event has a severity of WARNING.
- Heartbeats or other communication are not expected, but if received, communication is logged by the PCE.
- If the PCE is rebooted, the VEN remains suspended.
- Any custom iptables rules are removed and must be reconfigured manually.
- If SecureConnect has been enabled on the VEN, it is not disabled.

When a VEN is unsuspended:

- The PCE is informed that the VEN is no longer suspended and is able to receive policy from the PCE.
- If existing rules affect the unsuspended workload, the PCE reprograms those rules.
- An organization event (`server_unsuspended`) is logged. The event has a severity of WARNING. The event is exportable in Common Event Format (CEF) and Log Event Extended Format (LEEF).
- The workload revert sto its policy state prior to Suspended.
- Custom iptables rules are configured back into the iptables.

VEN Backup, Restore, and Rollback to Previous VEN Version

You can restore a previously installed version of the VEN without unpairing. "Restoring" is also called *rollback*.

The general process is as follows:

- Backup the current VEN version.
- Do an automatic rollback while re-installing the previous version.
  or
- Manually rollback with `illumio-ven-ctl restore`.

Do not downgrade the VEN: use rollback

Illumio advises that you should not downgrade the VEN by simply installing the old version while the current version is still in place.

Instead, use the rollback feature documented in this section.

If you must downgrade, the best way is to first uninstall the current version and then install the older version.

Backup Current VEN Version

You can rely on the VEN's automatic backup, or you can manually backup yourself.

Automatic Backup at Upgrade

The VEN software automatically makes a backup when the VEN is upgraded. The backup includes all information about the VEN after activation. The backup is maintained for only the immediately previous version of the VEN.

The automatic backup is stored in the `backup` subdirectory of the VEN's data directory, as shown in below for the default paths to the data directory.

- Linux: *`installation_root_dir`*`/illumio_ven_data/backup`
- Windows: `%PROGRAMDATA%\Illumio\backup`

> ⚠ Do not tamper with the automatic `backup` directory. Do not put any files in it. For security's sake, you should copy the `backup` directory to a location that is not on the workload.

Manual Backup

> **Stop currently installed VEN**
> Before you manually backup, you must first stop the currently installed VEN.

- Linux: `illumio-ven-ctl backup` *`path_to_backup_file`*
- Windows: `illumio-ven-ctl.ps1 backup` *`path_to_backup_file`*

Rollback to Previous Version – Automatic or Manual

There are two types of rollback: automatic and manual. *Automatic rollback* means that the VEN software does much of the process for you, as opposed to *manual rollback* in which you use a manually created backup as input to the restore command.

Supported VEN versions

- **Automatic:** VENs upgraded to versions later than 17.2 can be rolled back automatically to the previously-installed version.
- **Manual:** VENs upgraded to version 17.2 or later can be rolled back manually to the previously-installed version.

Linux

Automatic rollback relies on native OS mechanisms and the environment variable `ILLUMIO_VEN_ROLLBACK`. The values for this environment variable are as follows.

Syntax:

- `ILLUMIO_VEN_ROLLBACK=auto rpm -U --oldpackage` *`path_to_previous_rpm_package_to_install`*
- `ILLUMIO_VEN_ROLLBACK=`*`path_to_backup_file`* `rpm -U --oldpackage` *`path_to_previous_rpm_package_to_install`*
- `ILLUMIO_VEN_ROLLBACK=auto dpkg -i` *`path_to_previous_deb_package_to_install`*
- `ILLUMIO_VEN_ROLLBACK=`*`path_to_backup_file`* `dpkg -i` *`path_to_previous_deb_package_to_install`*

Environment Variable and Value	Description
`ILLUMIO_VEN_ROLLBACK=auto`	Rollback to the automatically backup-ed VEN version from most recent VEN upgrade. If the automatic backup does not exist, the automatic rollback fails.
`ILLUMIO_VEN_ROLLBACK=`*`path_to_backup_file`*	Rollback to the previous VEN version you manually backed-up to *path_to_backup_file*.

Windows

Automatic rollback relies on the `ROLLBACK` argument on the `msiexec` command line. The values for the arguments are described below.

Syntax:

- `msiexec.exe` *`installation_options`* `ROLLBACK=auto`
- `msiexec.exe` *`installation_options`* `ROLLBACK=`*`path_to_backup_file`*

Value	Description
`ROLLBACK=auto`	Required. Rollback to the automatically backup-ed VEN version from most recent VEN upgrade. If the automatic backup does not exist, the automatic rollback fails.
`ROLLBACK=`*`path_to_backup_file`*	Required. Rollback to the previous VEN version you manually backed-up to *path_to_backup_file*.
`installation_options`	Optional. Any of the allowed `msiexec` options for installation described in this guide. This value should be enclosed in quotation marks.

Manual Rollback

Manual rollback has the following effects:

- Uninstalls the currently installed VEN but does not deactivate it.
- Installs the specified previous VEN version, but does not activate it.
- Restores the previous VEN version backup you created.
- Sets the pre-rollback firewall state to your choice of `open` or `saved`.

Linux

Syntax:

```
illumio-ven-ctl
restore path_to_backup_file linux_rpm_or_deb_installation_command_with_path_to_previous_
VEN_version firewall_state_after_restore
```

Value	Description
`path_to_backup_file`	Required. Path to your manual backup file.
`linux_rpm_or_dpkg_installation_command_with_path_to_previous_VEN_version`	Required. The RPM or dpkg command options with the path to your manual backup file. Must be enclosed in quotation marks.
`installation_options`	Required. Any of the allowed `msiexec` options for installation described in this guide. This value should be enclosed in quotation marks.
`firewall_state_after_restore`	Required. Either `open` or `saved`. For more information, see "illumio-ven-ctl Deactivation/Unpair Options".

Examples:

- Install on RedHat and set VEN state to `open`:
  `illumio-ven-ctl restore /tmp/old-ven.backup "rpm -i /tmp/old-ven.rpm" open`
- Install on Debian, set VEN state to `saved` and log to a file:
  `illumio-ven-ctl restore /tmp/old-ven.backup "dpkg -i /tmp/old" saved 2&1>1 /tmp/log.txt`

Windows

Syntax

```
illumio-ven-ctl.ps1
restore path_to_backup_file path_to_msi_package_of_previous_VEN_version firewall_state_after_restore additional_msiexec_options
```

Value	Desscription
path_to_backup_file	Required. Path to your manual backup file.
path_to_msi_package_of_previous_VEN_version	Required. Installation options and the path to the old version of the VEN to install. Must be enclosed in quotation marks.
firewall_state_after_restore	Required. Either `open` or saved. For more information, see "illumio-ven-ctl Deactivation/Unpair Options".
additional_msiexec_options	Optional. Any other options for MSI installation, such as logging. Must be enclosed in quotation marks.

Examples:

- Install on Windows and set VEN state to open:
  `illumio-ven-ctl.ps1 restore c:\temp\old-ven.backup c:\temp\old-ven.msi open`
- Install on Windows, set VEN state to `saved`, and log to a file:
  `illumio-ven-ctl.ps1 restore auto c:\temp\old-ven.msi saved "/l*v c:\temp\log.txt"`

Diagnostics and Troubleshooting

This section describes some important System administration considerations on Windows, a useful tools, and a generalized set of steps for troubleshooting.

Enable Windows Application Layer Enforcement (ALE)

If you have disabled Windows Application Layer Enforcement (ALE), you need to re-enable it.

ALE is a Windows component to determine which packets should be sent to the TCP/IP stack.

ALE is enabled by default. If you disable it, all packets are sent to the TCP/IP stack, which marks them as illegal and drop them. You also lose visibility into the packets. Such packets can be exploited for a Denial of Service (DOS) attack on the workload.

Linux ignored_interface Inhibits PCE Policy Updates

Transitioning an enforced VEN's interface in and out of `ignored_interface` might drop the dynamic, long-lived connections maintained by the AgentManager component between the VEN and the PCE. See the description of the AgentMonitor in "Description of VEN Components".

When a VEN interface is placed in `ignore_interface` list, `conntrack` is disabled. (The `conntrack` table on Linux stores information about network connections.) If the connection on TCP port 8444 to the PCE is reinitialized, any arriving packets from the PCE are dropped, because the packets do not have any state in `conntrack`.

The VEN heartbeat eventually restores connections, but meanwhile the VEN does not implement any policy sent via lightning bolt from the PCE.

Tools for Connectivity Checking and Workload Troubleshooting

- A VEN connectivity checking tool called "venconch" for workloads is available on the Illumio Support site.
- A VEN compatibility checking feature is available in the PCE Web Console for paired workloads. See the *PCE Web Console User Guide*.

Troubleshooting Steps

Follow these steps to identify the cause of workload connectivity issues. If a workload is unreachable or cannot reach other workloads/PCE, follow these steps to troubleshoot.

1. Determine if all workloads are unable to communicate or just a subset of the workloads are reported as disconnected. If PCE reports that all workloads are offline, check if PCE is reachable from workloads.
2. If a subset of workloads are down, check if there are differences in network configuration between those and the workloads that are connected, and if they are contributing to PCE being unreachable.
3. Check If any workloads unable to communicate are located behind NAT devices, firewalls, or remote data centers. See "Tools for Connectivity Checking and Workload Troubleshooting".
4. For on-premise deployments, ensure TCP port 443 and 444 on workloads are opened to the PCE.

5. If running in a public cloud instance:
    a. For AWS, ensure security groups permit TCP ports 443 and 444.
    b. For Azure, ensure that Endpoints are configured to allow traffic.
6. Check the status of the VEN-specific processes and ensure that they are running and active:
        - On Linux: run `/opt/illumio/bin/agent_status –a or illumio-ven-ctl status`
        - On Windows: execute `get-service` in the PowerShell
    a. Ensure the following processes are running and active:
        - On Linux: AgentManager, IPSec, PlatformHandler, AgentLogManager, VtapServer, AgentMonitor
        - On Windows: venAgentLogMgrSvc, venPlatformHandler, venVtapServerSvc, ilowfp
7. Review log files to find any errors generated by the system (`sudo` required):
    - Logs in Data_Dir/log directory
    - To look for any errors in the log files, execute `grep –ir ERROR *`

9. To check for firewall updates, view `platform.log` file. Look for logs related to firewall updates; for example:

```
2014-07-26T22:20:41Z INFO:: Enforcement mode is: XXXX
2014-07-26T22:20:41Z INFO:: Is fw update yes
2014-07-26T22:20:41Z INFO:: Is ipset update yes
2014-07-26T22:20:41Z INFO:: saved fw-json
```

10. Check heartbeat logs for records related to update messages from the PCE. The following are example heartbeats:

```
2014-07-26T22:43:12Z Received HELLO from EventService.
2014-07-26T22:43:12Z Sent ACK to EventService.
Events - f/w updates etc.
014-07-26T22:34:11Z Received EVENT from EventService.
2014-07-26T22:34:11Z Added EVENT from EventService to PLATFORM handler thread message
queue
```

```
iptables-save | grep 443 | grep allow_out
        -A tcp_allow_out -d 54.185.43.60/32 -p tcp -m multiport --dports 443 -m
conntrack --ctstate NEW -j NFLOG --nflog-prefix "0x8000000000000025f " --nflog-threshold
1
        -A tcp_allow_out -d 54.185.43.60/32 -p tcp -m multiport --dports 443 -m
conntrack --ctstate NEW -j ACCEPT
        -A tcp_allow_out -d 204.51.153.0/27 -p tcp -m multiport --dports 443 -m
conntrack --ctstate NEW -j NFLOG --nflog-prefix "0x8000000000000265 " --nflog-threshold
1
        -A tcp_allow_out -d 204.51.153.0/27 -p tcp -m multiport --dports 443 -m
conntrack --ctstate NEW -j ACCEPT
iptables-save | grep 444 | grep allow_out
        -A tcp_allow_out -d 54.185.43.60/32 -p tcp -m multiport --dports 444 -m
conntrack --ctstate NEW -j NFLOG --nflog-prefix "0x8000000000000266 " --nflog-threshold
1
        -A tcp_allow_out -d 54.185.43.60/32 -p tcp -m multiport --dports 444 -m
conntrack --ctstate NEW -j ACCEPT
```

Run the following commands on the workload to get a copy of the logs and configured firewall settings.

Linux

- `iptables-save`
- `ipset -L`

Windows

- Navigate to **Start** -> **Control Panel** -> **System and Security** -> **Windows Firewall** -> **Advanced Settings**
- Navigate across inbound and outbound rules to look for relevant firewall/filtering configuration.

Basic Theory of VEN Operations

The section describes in greater detail the effects, behaviors, and other aspects of how the VEN works.

VEN Installation and Uninstallation

Illumio recommends that you reserve the following for disk sizing 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.

Linux Pairing Script for VEN Repo: pair

Below is an example of Linux pairing script with annotation. The pairing script works with the VEN Repo model of deployment, not the single-package installation (the preferred deployment model), which uses `illumio-ven-ctl --activation` option. Both mechanisms accomplish the same purpose: bring a workload under management by Illumio ASP.

```
rm -fr /opt/illumio/scripts && \
umask 027 && mkdir -p /opt/illumio/scripts && \
curl https://repo.bigcompany.com/scp2HSPFGj2C82BVDYJf2BCXlzsGWXO3/pair -o /opt/illumio/
scripts/pair && \
chmod +x /opt/illumio/scripts/pair &&  \
/opt/illumio/scripts/pair \
--repo-host repo.bigcompany.com --repo-dir scp2HSPFGj2C82BVDYJf2BCXlzsGWXO3/ --repo-
https-port 443 \
--management-server scp2.bigcompany.com:443 \
--activation-code 0123456789abcdef
```

1. Removes any existing `/opt/illumio/scripts` directory
2. Changes umask to 027 to prevent the group-write and others-read,write,execute permissions as it creates `/opt/illumio/scripts` directory
3. Uses curl to download the pair script from repo.illum.io and store it under `/opt/illumio/scripts`.
4. Changes script permissions to allow execution
5. Runs the `/opt/illumio/scripts/pair` with the following command line options:
6. Line 6 `--repo-host`, `--repo-dir`, and `--repo-port` to check for VEN software updates
7. Line 7 --management-server: to communicate with the PCE
8. Line 8 --activation code to authenticate the VEN to the PCE and authorize the VEN to pair

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

The script then performs the following:

a. For yum-based OSes, updates releaserver to release name in /etc/yum.conf using sed
b. Removes VEN files leftover from a previous failed installation
c. Downloads the VEN GnuPG public key from repo wih curl
d. Stores the key in /tmp and make it root accessible
e. Installs the key into rpm or apt-key commands
f. On Red Hat, disables the subscription manager plugin (set enabled=0 in /etc/yum/pluginconf.d/subscription-manager.conf)
g. Creates the Illumio yum repo at `/etc/yum.repos.d/illumio.repo` or apt-get repo at `/etc/apt/sources.list.d/illumio_repo.list`

h. Populates the repo file with repo URI and other information
i. Installs dependencies followed by illumio-agent-control and illumio-agent-vtapserver packages from Illumio repo
j. Places upgrade hold on VEN packages so that they don't get upgraded automatically
k. Checks if ipset kernel module is installed (if not, the process fails)
l. Runs /opt/illumio/bin/init_Platform script with "start" option
m. Generates activation file /opt/illumio/etc/agent_activation.cfg
n. Invokes /opt/illumio/bin/agent_status to activate the VEN
o. Restores releaserver=latest in /etc/yum.conf

RPM Installation

RPM installation performs the following operations:

- Creates the `ilo-ven` user and group, unless a custom username is specified at install.
- Starts the Illumio Adaptive Security Platform security service to manage the following:

  a. In Idle state, security service does nothing.
  b. Loads 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
  c. Sets `net.netfilter.nf_conntrack_tcp_timeout_established` to 8 hours (28,800 seconds). See "Linux nf_conntrack_tcp_timeout_established set to 8 Hours".
  d. Disables the system firewall service iptables
  e. Stops system firewall service iptables
  f. Saves existing iptables rules if any
  g. Loads iptables rules computed from PCE firewall policy
  h. Starts the VEN components described in "Description of VEN Components".

Packages and Kernel Modules

Some packages, such as SecureConnect StrongSwan for enforcing IPsec, are included as part of the VEN package. Other packages are installed on the host itself if they are not already present.

If the following packages are not installed on the workload, via RPM dependencies the VEN installation downloads and install them.

1. curl: Used for HTTPS client functionality
2. dnsutils: Used for DNS client functionality
3. uuid-runtime: Used for generating UUIDs
4. ipset: Used for ipset functionality
5. libnfnetlink0: Used for communicating with the Net Filter module
6. libcap2: Used for selectively enabling/disabling capabilities
7. libgmp10: Used for multi-precision arithmetic
8. bind-utils: Used for DNS client functionality
9. iptables and iptables-ipv6: Used for iptables functionality

10. apt-transport-https (for apt-based OS): Used for HTTPS transport for apt

If the following kernel modules are not installed, the VEN downloads and installs them:

- ipset

Windows Pairing Script pair.ps1

Below is an example of Windows pairing script.

```
Set-ExecutionPolicy -Scope process remotesigned -Force;
Start-Sleep -s 3;
(New-Object System.Net.WebClient).DownloadFile("https://repo.illum.io/
scp2HSPFGj2C82BVDYJf2BCXlzsGWXO3/pair.ps1", "$pwd\Pair.ps1"); .\Pair.ps1
-repo-host repo.illum.io
-repo-dir scp2HSPFGj2C82BVDYJf2BCXlzsGWXO3/
-repo-https-port 443 -management-server scp2.illum.io:443
-activation-code 0123456789abcdef;
Set-ExecutionPolicy -Scope process undefined -Force;
```

In the above example, the Windows pairing script performs the following:

- Changes execution policy of the host PowerShell process to remotesigned.
- Using .NET framework WebClient class, downloads pair.ps1 from VEN repository and stores it in the current directory
- Runs the pair.ps1 script with the following command line options:
  - repo host, repo directory, and repo port: Used by the VEN to check for VEN software updates
  - management server: Used by the VEN to communicate with the PCE
  - activation code: Used by the PCE to authenticate and authorize the VEN during pairing process
- The pair script installs the VEN packages on the application workload and pairs the VEN with the PCE. The output of pair.ps1 is captured in `%TMP%\illumio.log`. The script performs the following steps:
- Retrieves VEN MSI package from repo using .NET framework WebClient class
- Launches msiexec.exe to install the downloaded package
- Generates agent_activation.cfg file with PCE information
- Retrieves agent activation status and displays it

MSI Installation

The MSI installation performs the following:

1. Creates VEN registry key under `HKLM\Software\Illumio`

2. Adds the Illumio Adaptive Security Platform code-signing certificate to “Trusted Publisher” store for Computer
3. Registers VEN Event (Event Tracing for Windows, or ETW) providers
4. Installs Ilowfp (kernel mode driver) and the processes and services described in "VEN Architectural Diagram" as auto-start at boot and then starts them.

VEN-to-PCE Communications

For background, see "Overview of VEN Software Architecture and Description of Components".

The VEN communicates with the PCE on (8)443 using HTTPS. The VEN uses Transport Level Security (TLS) to connect to the PCE. The PCE certificate must be trusted by the VEN before communication can occur.

The VEN sends the following details to the PCE:

- Traffic logs.
- Network interfaces.
- Processes.
- Open ports.

The VEN receives the following details from the PCE:

- Firewall policy.
- Lightning bolts with action to perform, such as sending a support report.

Frequency of VEN-to PCE Communications

The following table shows the frequency of communications to the PCE for common VEN operations. The *PCE Operations Guide* includes more details about these intervals and their effects.

Function	Frequency	Notes
Firewall policy updates	Real-time if lightning bolts are enabled.	

Function	Frequency	Notes
Active service reporting	See note.	• At start-up, a snapshot of processes and ports is sent to the PCE. • Information about listening processes on a workload in build, test, idle, and enforced states is accumulated every 30 seconds. This includes only processes that are actively communicating at that time. • Every 10 mins, this accumulated information is reported to PCE. • Every 24 hours, a snapshot of *all* listening processes is taken and sent to the PCE.
Interface reports and changes	Every 5 minutes.	Only if there are changes to the interfaces; otherwise, no data are sent.
Firewall and traffic flow log	Every 10 minutes.	• The VEN checks if there are logs, and if so, sends them to the PCE. • If the PCE is inaccessible, the VEN retains flow summaries for the previous 24 hours but purges logs that are older than 24 hours, with the oldest log at every 24 hour mark. • When logs are purged, the VEN locally logs an alert, which is posted to the PCE as an event when connectivity is restored.
Heartbeat	Every 5 minutes.	• If the PCE does not receive three consecutive heartbeats, an event is written to the PCE's event log. • See also "Heartbeat mechanism and "Lost Agent" state".
Dead-peer interval	Configurable	Default is 60 minutes (or 12 heartbeats). See also "VEN Offline Timers and Isolation Mechanism".
VEN tampering detection	10 minutes	

Heartbeat mechanism and "Lost Agent" state

The VEN sends a heartbeat message every five minutes to the PCE to inform the PCE that it is up and running. If the VEN cannot connect to the PCE (either because the PCE is down or because of a network issue), the VEN continues to enforce the last-known-good policy while it tries to reconnect with the PCE.

After missing two heartbeats, the VEN enters a diminished state, sometimes called *degraded mode*. In the diminished state, the VEN ignores all the asynchronous commands received as lightning bolts from the PCE, except the commands for software upgrade and support reports. After the connectivity to the PCE is restored, the VEN comes out of the diminished state after two successful heartbeats.

If the VEN fails to communicate with the PCE because of failed authentication, the VEN enters a state called *lost agent*. In the lost agent state, the VEN only attempts to connect with the PCE every four hours. The PCE logs a message in the Organization Events to inform the user that the VEN needs to be uninstalled or reinstalled manually on this Workload. If the authentication failure was temporary, after first successful connection to the PCE, the VEN exits the lost agent state.

VEN Offline Timers and Isolation Mechanism

When the VEN on a workload is stopped, the PCE detects that the workload is offline. The PCE recomputes the policy for all the peer workloads. In the new policy, the peer workloads are not allowed to communicate with the workload where the VEN is stopped.

If the workload goes offline abruptly (for example, due to a power outage), the PCE stops receiving heartbeats from the workload. After the length of time specified by the value configured in the PCE web console **Settings > Offline Timers**, the PCE marks the workload as offline and recomputes policies for the peer workloads to isolate the offline workload. If this value has not been set, the default is 60 minutes, or 12 heartbeats.

SecureConnect

The VEN uses the StrongSwan suite to provide IPsec encryption between the host and a communicating Workload. StrongSwan is installed as part of the VEN installation. StrongSwan is used to perform the Internet Key Exchange (IKE) v2 handshake. The actual encryption of IP packets is done natively by the OS.

Sampling Mode

If the VEN receives a sustained amount of high traffic per second from many individual connections, the VEN enters Sampling Mode to reduce load. Sampling Mode is a protection mechanism to ensure that the VEN does not contribute to the consumption of CPU. In Sampling Mode, not every flow is reported. Instead, flows are periodically sampled and logged.

After CPU usage on the VEN decreases, Sampling Mode is disabled and each connection is reported to the VEN. The entry and exit from sampling-mode is automatically performed by VEN depending on the load on VEN.

Linux nf_conntrack_tcp_timeout_established set to 8 Hours

For VENs installed on Linux workloads, the VEN relies on conntrack to manage the `nf_conntrack_tcp_timeout_established` variable.

By default, as soon as the VEN is installed, it sets the `nf_conntrack_tcp_timeout_established` value to eight hours (28,800 seconds). This frequency is to manage workload memory by removing unused connections from the table and thereby increase performance.

If you change this setting via sysctl, it is reverted the next time the workload is rebooted or the next time the VEN's configuration file is read.

Wireless connections and VPNs not supported

Security policy is not enforced on wireless connections or VPNs on any of the supported platforms

VEN Activation or Pairing

The terms *activation/deactivation* of *a VEN* applies to the single-package installation directly on the workload, but the term *pairing/unpairing a VEN* is used for the VEN Repo model of deployment and also in the PCE web console. These have the same function.

A workload pairs with a PCE before it can become part of Illumio Adaptive Security Platform distributed security system. Pairing can be performed using one of these methods:

- A pairing key
- A PKI certificate
- A Kerberos service principal name (SPN)

An activation key or pairing key is used only at initial pairing. During pairing, an Agent Token is generated and stored in a local file on workload, and the hash of the token is stored on PCE. Only the agent-token is used in VEN-to-PCE communication from that point onwards.

The VEN communicates with PCE with HTTPS over Transport Layer Security (TLS). The Agent Token is used by VEN to uniquely authenticate itself to PCE. In addition, a Clone Token is generated by the VEN. If 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. Agent Token is never rotated.

VEN Startup

See the commands "VEN Startup".

For a description of the VEN architecture and software components, see "Overview of VEN Software Architecture and Description of Components".

VEN Shutdown

See the commands in "VEN Shutdown".

For a description of the VEN architecture and the software components, see "Overview of VEN Software Architecture and Description of Components".

VEN Status

The VEN status contains information related to the current state of VEN connectivity, the most recently provisioned policy changes that affect the workload, any potential firewall tampering, and any issues related to SecureConnect functionality.

See the commands in "VEN Status".

VEN Uninstallation

During uninstallation, the VEN performs the following steps.

Linux	Windows

• Unpairs from the PCE
• Restores the host firewall state to the requested or open state if no state is specified. Possible values of the state are:
  • Open: All ports are open after VEN uninstalls
  • Saved: Restore the firewall to its state just before the VEN was installed
• Uninstalls the illumio-agent-control and illumio-agent-vtap packages
  • Removes program and data files
  • Removes repo and GPG files and packages
	• Unpairs the VEN from the PCE
	• Sends a “deactivate” message to PCE
	• Stops all VEN services
	• Unregisters services from Service Control Manager
	• Restores Windows Firewall to requested state
	  • Open: All ports are open after VEN uninstalls
	  • Saved: Restore the firewall to its state just before the VEN was installed
	• Removes Program Files and ProgramData directories
	• Removes VEN registry keys
	• Removes Certificate
	• Unregisters VEN Event provider

Workload Policy States

After activation, the VEN can be in one of the following policy states. The VEN policy state determines how the rules receives from PCE affect a workload's network communication.

You change the policy state of the VEN via settings in the PCE or the REST API.

State	Description
Build	The VEN inspects all open ports on a workload and reports to the PCE the flow of traffic between it and other workloads. In this state, the PCE displays the flow of traffic to and from the workload, providing insight into the data center and the applications running in it. No traffic is blocked in this state. The Build state is useful when firewall policies are not yet known. This state can be used for discovering the Application flows in the organization and then generating a security policy that governs all desired communication.
Enforced	All ruleset rules are enforced on the workload. Any traffic flows not explicitly allowed by the rules from the PCE are blocked.
Idle	Idle state is used for installing and activating VENs on workloads without changing the workloads' firewall. A pairing profile can be used to pair workloads in Idle state. The VEN does not take control of the workloads' firewall, but uses workload network analysis to send to the PCE relevant details about the workload, such as the workload's IP address, operating system, and traffic flows. In Idle policy state, SecureConnect (IPv6 compatibility) is not supported on workloads. If you activate SecureConnect for a rule that applies to workloads that are in both Idle and non-Idle policy states, traffic between these workloads might be affected.
Test	In Test, you can visualize all of the traffic that would be blocked if you enforced rules on the workloads.

Automatic History of Firewall Changes

Changes to the firewall on a workload are historically recorded for audit trail. Up to 10 changes to the firewall history are saved. The history is viewable via the PCE Support Reports. See the *PCE Operations Guide* and *PCE Web Console Guide*.

VEN Traffic Logging

The VEN captures logs of its operation and traffic flow summaries locally on the workload. There are several different application log files, each with one backup.

Contents of Traffic Flow Logs

The VEN stores traffic flow summaries, rather than each individual traffic flow. For each connection, the traffic flow summary includes:

- Source IP
- Destination IP
- Destination Port
- Protocol
- Number of connections

Querying flow log databases

The `sqlite` command-line tool comes with the VEN, which you can use to query the flow log databases.

Linux Database Query Examples

- Non-aggregated accepted flows
  `/opt/illumio/bin/sqlite /opt/illumio/log/flow.db "select * from flow_view"`
- Non-aggregated dropped flows
  `/opt/illumio/bin/sqlite /opt/illumio/log/flow.db "select * from drop_flow_view"`
- Aggregated accepted flows
  `/opt/illumio/bin/sqlite /opt/illumio/log/flowsum.db "select * from flow_view"`
- Aggregated dropped flows
  `/opt/illumio/bin/sqlite /opt/illumio/log/flowsum.db "select * from drop_flow_view"`

Window Database Query Examples

- Non-aggregated accepted flows
  `"c:\Program Files\Illumio\bin\sqlite.exe" c:\ProgramData\Illumio\log\flow.db "select * from flow_view"`
- Non-aggregated dropped flows
  `"c:\Program Files\Illumio\bin\sqlite.exe" c:\ProgramData\Illumio\log\flow.db "select * from drop_flow_view"`
- Aggregated accepted flows
  `"c:\Program Files\Illumio\bin\sqlite.exe" c:\ProgramData\Illumio\log\flowsum.db "select * from flow_view"`

- Aggregated dropped flows
  ```
  "c:\Program Files\Illumio\bin\sqlite.exe" c:\Program Data\Illumio\log\flowsum.db
  "select * from drop_flow_view"
  ```

Summary of VEN and Useful OS commands

Below is a short description of the VEN command-line tools you commonly use for various operations and some useful native OS commands.

Syntax for the VEN-provided commands is detailed throughout this guide, in the VEN Deployment guide, and in the help of the commands themselves.

Platform	Command	Description
Linux	`illumio-firewall`	VEN Linux shell control script to start the policy-based firewall at boot.
	`illumio-ven-ctl`	VEN Linux shell control script to control VEN control VEN settings and functions
	`agent_status`	Alternative to `illumio-ven-ctl status`
	`pair`	Script to pair with the PCE
	`ps`	Native OS command to list all system processes
	`chkconfig`	Native OS command to update and query runlevel information for system services
Windows	`illumio-ven-ctl.ps1`	VEN PowerShell script to control VEN settings and functions
	`pair.ps1`	VEN PowerShell script to pair with the PCE
	`Get-Service`	Native OS PowerShell command to display system services
	`tasklist /svc`	Native OS command to display system services
	`wf.msc`	Native OS command to manage the Windows firewall

illumio-ven-ctl Syntax and Command-line Options

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/bin`
- Windows: default location is `C:\Program Files\Illumio`

Linux illumio-ven-ctl Help

```
$ illumio-ven-ctl --help
Usage:  {start|stop|restart|status|connectivity-test|check-env|gen-supportreport|
activate|prepare|unpair|version|suspend|unsuspend|backup|restore}
```

Windows illumio-ven-ctl.ps1 Help

```
illumio-ven-ctl.ps1 <action> <options>

 <action>:
activate <options> # Activate VEN
deactivate <options> # Deactivate VEN without uninstalling it
unpair <options> # Unpair VEN
upgrade [yes] # Upgrade VEN
start # Start VEN services
stop # Stop VEN services
enable # Enable VEN services
disable # Disable VEN services
restart # Restart VEN services
status # Report VEN status
check-env # Check VEN runtime_env.yml settings
gen-supportreport <options> # Generate VEN support reports
prepare # Prepare VEN image
version # Display VEN version
suspend # Suspend VEN (enter the emergency state)
unsuspend # Unsuspend VEN (exit the emergency state)
backup <options> # Backup VEN data
restore <options> # Restore VEN data
```

illumio-ven-ctl Activation Options

The following options on the `illumio-ven-ctl` control script are for activating the VEN on Linux workloads. The options and arguments generally the same for Windows.

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 of these blocked configurations or the activation will fail.

Syntax note:

- On Linux, the options below are entered with a double dash: *`--option`*
- On Windows, the options below are entered with a single dash: *`-option`*
- If the value you specify for any these arguments contain multiple , space-separated words, the must be enclosed in double quotation marks

Option	Argument	Required	Notes
`--activate | -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.
`--management-server | -m`	`PCE_FQDN:port or IPaddress:port`	Required	Sets the domain name or IP address and port of the host where the VEN can retrieve master configuration information.
`--name | -n`	`server friendly name`	Optional	Sets a friendly name that will be used for this workload when it appears in the PCE web console. Example: `--name "Web Server 1"`

Option	Argument	Required	Notes
`--env`	`environment <label_name>`	Optional	Inputs an Environment Label for this workload. Example: `--env Production`
`--loc`	`location <label_name>`	Optional	Example: `--loc "US"`
`--role`	`role <label_name>`	Optional	Assigns a Role Label for this workload. Example: `--role "Dev Group"`
`--app`	`application <label_name>`	Optional	Assigns an Application Label for this workload. Example: --app "Web Service"
`--mode`	`illuminated | enforced | idle`	Optional	Sets the policy state for the workload. For explanation of the various states, see "Workload Policy States" in the *VEN Operations Guide*.
`--log-traffic`	`true | false`	Optional	Enables or disables traffic logging. If not specified, logging is set to `true` by default. Interacts with the `--visibility-level` option. See "--visibility-level Arguments Correlated with --log-traffic Arguments".

Option	Argument	Required	Notes
`--visbility-level`	`flow_summary` | `flow_drops` | `flow_off`	Optional	Default: `flow_summary`. Defines the extent of the data the VEN collects and reports to the PCE from a Workload in the `enforced` mode (policy state), so you can control resource demands on Workloads. The higher levels of detail are useful for visualizing traffic flows in the Illumination map inside the PCE web console. Interacts with the `--log-traffic` option. See See "--visibility-level Arguments Correlated with --log-traffic Arguments".
`-wfp-optimizations-enabled`	`-wfp-optimizations-enabled true`	Optional	Use this option if you want to pair the Windows workload with the WFP_Optimization feature, which enables support for IPSets.

--visibility-level Arguments Correlated with --log-traffic Arguments

--log-traffic Argument	Effect by VEN Policy State	Description
`flow_summary`	Included in all policy states.	Default. Called **High Detail** in the PCE web console. 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 during the **build** and **test** states.

--log-traffic Argument	Effect by VEN Policy State	Description
`flow_drops`	Valid only in **enforced state.**	Called **Less Detail** in the PCE web console. 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`	No flow logging.	Called **No Detail** in the PCE web console. 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 Arguments

The following table indicates valid and invalid combinations of the arguments to the `--log-traffic` and `--visibility-level` options on `illumio-ven-ctl`.

VEN mode/ state	--log-traffic Argument	--visibility-level Argument	Notes
illuminated	false	flow_summary	This is a combination of settings called **Build and Test** in the PCE web console
	~~false~~	~~flow_drops~~	Not a valid combination
	false	flow_off	
	true	flow_summary	In the PCE web console, this combination is called "Build and Test".
	~~true~~	~~flow_drops~~	Not a valid combination
	true	flow_off	

VEN mode/ state	--log-traffic Argument	--visibility-level Argument	Notes
enforced	false	flow_summary	
	false	flow_drops	
	false	flow_off	No detail in enforced mode
	true	flow_summary	High detail in enforced mode.
	true	flow_drops	Low detail in enforced mode. - LOW DETAIL
	~~true~~	~~flow_off~~	Not a valid combination

illumio-ven-ctl Deactivation Options

With `illumio-ven-ctl unpair`, you specify the post-deactivation state for the VEN.

```
illumio-ven-ctl.ps1 unpair [recommended | saved | open | unmanaged]
```

Unpair options on Linux

- `recommended`:
  Temporarily allow only SSH/22 until reboot.
  Security implications: If this workload is running a production application, it could break because this workload will no longer allow any connections to it other than SSH on port 22.

- `saved`:
  Revert to pre-Illumio policy from when the VEN was first installed. Revert the state of the workload's iptables to the state they were in at the moment before the VEN was installed. The dialog will display the amount of time that has passed since the VEN was installed.
  Security implications: Depending on how old the iptables configuration are on the workload, VEN removal could impact the application.

- `open`:
  Uninstalls the VEN and leaves all ports on the workload open.
  Security implications: If iptables or Illumio were the only security being used for this workload, the workload will be opened up to anyone and become vulnerable to attack

On Linux, the `unmanaged` option is not available.

Unpair Options on Windows

- `recommended`:
  Temporarily allow only RDP/3389 and WinRM/5985,5986 until reboot. **Security implications**: If this workload is running a production application, the application could break because this workload will no longer allow any connections to it.

- `saved`:
  Restores firewall rules and configuration to the state it was in at the time the workload was paired. When a Windows workload is paired, a backup is made of the firewall configuration, and this option reverts the workload's firewall settings to that state. If the same Workload has been paired, and then unpaired, with the recommended or all ports open option (i.e., not the revert option), then you will need to unpair the Workload and then run this PowerShell command to import the snapshot that was taken at the time of pairing:

  ```
  PS C:\ netsh advfirewall import %HOMEPATH%\AppData\Local\Temp\illumio.fwbackup
  ```

  Note: The illumio.fwbackup file is stored in a temp directory which the PCE has no control over, so be sure to save this file elsewhere in case that temp directory gets cleared or deleted.
  Security implications: Depending on how old the WFP configuration was on the workload, VEN removal could impact the application.
- `open`:
  Uninstalls the VEN and leaves all ports on the workload open.
  Security implications: If WFP or the PCE were the only security being used for this workload, the workload will be accessible to anyone and become vulnerable to attack.

- `unmanaged`:

  Uninstalls the VEN and reverts to the workload's currently configured Windows Firewall policy.

Support Report During Deactivation

When you unpair a workload, the VEN creates a local Support Report for diagnostic purposes, in case you need a record of the VEN after it becomes uninstalled.

On Linux, the generated Support Report will be saved to the `/tmp` directory. On Windows, the generated Support Report will be saved to the `C:\Windows\Temp` directory. If a there was already an existing Support Report in this directory, it will be overwritten with the new one.

Revision History

Illumio Adaptive Security Platform VEN Operations Guide

Document ID: 50000-100-18.2.1

Date	Description
2019-01-23	Updated for Illumio Adaptive Security Platform version 18.2.1: • Description of effects of VEN disconnect setting in "About Isolation Mechanism" in "Basic Theory of VEN Operations". • For improved performance, the EventSync and AgentLogManager components of the VEN have been removed and should no longer be whitelisted. For current components, see "Description of VEN Components".
2018-11-15	Updated description of timing of VEN purge of traffic flow logs in "Frequency of VEN-to-PCE Communications".
2018-10-29	Clarified details about timing of active service reporting in "Frequency of VEN-to-PCE Communications".
2018-09-06	Updated for Illumio Adaptive Security Platform version 18.2: • Included "Tools for Connectivity Checking and Workload Troubleshooting". • Conformance of Idle mode with other states in "Illumination Maps – Increased Reporting Frequency of Workload Firewall/Traffic Flows".
2018-05-10	Updated for Illumio Adaptive Security Platform version 18.1: • Added theory of VEN operations. • Reorganization and miscellaneous corrections throughout. • Start of revision history.