Illumio Core®

Version 21.5

VEN

Version 21.5

VEN Administration Guide

November 2023

50000-100-21.5

Legal Notices

Copyright © 2022 Illumio 920 De Guigne Drive, Sunnyvale, CA 94085. All rights reserved.

The content in this documentation is provided for informational purposes only and is provided "as is," without warranty of any kind, expressed or implied of Illumio. The content in this documentation is subject to change without notice.

Product Version

PCE Version: 21.5 (LTS Release)

For the complete list of Illumio Core components compatible with Core PCE, see the Illumio Support portal (login required).

For information on Illumio software support for Standard and LTS releases, see Versions and Releases on the Illumio Support portal.

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 Administration 6

About This Administration Guide 6
How To Use This Guide 6
Before Reading This Guide 7
Notational Conventions in This Guide 7
VEN Architecture and Components 7
Basic Concepts for Illumio Core Software 8
Activation or Pairing 8
VEN Architectural Diagram 9
Main Components of the VEN 10
VEN Interactions with Files and Components 11
Management Interfaces for the VEN and PCE 12
About VEN Administration on Workloads 14
VEN Software Management from PCE 14
VEN Proxy Support on Linux, AIX, and Solaris 14
Support on IBM Z With RHEL 7 and RHEL 8 15
Support on SLES 11 SP2 15
Debian 11 Support 15
VEN Support on Rocky Linux 15
Workload Policy States 15
VEN Enforcement Characteristics 16
VEN Policy Sync 19
VEN Health Status on Workloads 20
VEN Process Health 20
Workload Clone Alerts 20
Stopped VEN Status 20
Aggressive Tampering Protection for nftables 21
Uninterrupted Traffic Between the VEN and the PCE 21
VEN File Settings Option 21
Windows VEN Proxy Fallback Enhancement 21
Label-based Security Setting for IP Forwarding 22
Uninterrupted Traffic Between the VEN and the PCE 22
IPv6 Support and Features for the VEN 22
illumio-ven-ctl General Syntax 24
Set PATH Environment Variable 24

Command Line Syntax by Platform 24
Linux/AIX/Solaris Command Line Help 25
Windows Command Line Help 25
Useful VEN and OS Commands 25
Verify VEN Version Number 25
Commonly Used VEN Commands 26
illumio-ven-ctl Command Options by OS 27
Chapter 2 VEN State 29
VEN Startup and Shutdown 29
VEN Startup and Shutdown (illumio.com) 29
Start Up VENs 29
Shut Down VENs 31
Disable and Enable VENs (Windows only) 31
VEN Suspension 32
About VEN Suspension 32
Linux VEN: Back Up Custom iptables/NAT Rules 33
Suspend and Unsuspend Commands 34
Mark VEN as Suspended Using the PCE Web Console 34
Disable VEN Suspension on Workloads 35
Rollback, Deactivate, or Uninstall VENs 38
Backup, Restore, and Rollback VENs 38
Downgrading versus Rolling Back VENs 38
Back Up Current VEN Version 39
Roll Back to Previous VEN Version 39
Manual Rollback 41
Deactivate and Unpair VENs 43
Deactivate Using VEN Command Line 43
Unpair Using VEN Command Line 44
Unpair Using System Commands 45
VEN Unpairing Details 46
Linux/AIX/Solaris 46
Windows 47
Support Report During Unpairing 47
Chapter 4 Monitor and Diagnose VEN Status 48
VEN-to-PCE Communication 48

Details about VEN-to-PCE Communication 48
VEN Connectivity 49
Communication Frequency 50
VEN Heartbeats and Lost Agents 51
VEN Offline Timers and Isolation 52
Sampling Mode for VENs 52
Wireless Connections and VPNs 53
Show Amount of Data Transfer 53
VEN Status Command and Options 55
The VEN Status Command 55
Policy Option for VEN Status 57
Health Option for VEN Status 57
Status Connectivity Option for VEN Status 58
VEN Logging 60
VEN Traffic Logging 60
List of Local Processes 62
Tuning the IPFilter State Table (AIX/Solaris) 62
About State Table Tuning 62
Set a Custom IPFilter State Table Size 63
Manage Conntrack Table Size (Linux) 65
About Managing the State Table 65
Customizing the VEN Adjustment Behavior 66
VEN Firewall Tampering Detection 67
Automatic History of Firewall Changes 67
Host Firewall Tampering Protection 67
Host Firewall Tampering Alerts 68
VEN Support Reports 71
Generate Support Report from PCE 71
Generate Linux/AIX/Solaris Support Report Using CLI 71
Generate Windows Support Report Using CLI 72
VEN Troubleshooting 73
Windows: Enable Base Filtering Engine (BFE) 73
Linux: ignored_interface 74
VEN Troubleshooting Tools 74
Commands to Obtain Firewall Snapshot 74
Troubleshooting Tips 75

Chapter 1

Overview of VEN Administration

This chapter contains the following topics:

About This Administration Guide 6

VEN Architecture and Components 7

About VEN Administration on Workloads 14

illumio-ven-ctl General Syntax 24

Useful VEN and OS Commands 25

This section describes the VEN characteristics and the VEN commands that you use to administer the VEN on the workloads in your environment after you have installed the VEN and the workloads are managed by Illumio Core.

About This Administration Guide

This guide shows you how use `illumio-ven-ctl` (for Linux, AIX, and Solaris) and `illumio-ven-ctl.ps1` (for Windows) 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.

How To Use This Guide

The VEN Administration 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.

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
...
```

VEN Architecture and Components

This topic describes the basic concepts relevant to the VEN and for Illumio Core software. Additionally, it explains the VEN architecture and components.

Basic Concepts for Illumio Core Software

- A *workload* is bare metal server, virtual machine (VM), or a container.
- The *VEN* is a lightweight, multiple-process application with a minimal footprint that runs on a workload.
- *Native network interfaces* are also know as the OS's firewall platform.

The VEN manages firewalls at an OS level, so you must install a VEN on every bare-metal server or virtual machine you want to secure. However, you only need to install a single VEN to secure all the containers on a machine. A secured workload is known as a *managed workload*.

Once installed, the VEN performs the following tasks:

- Interacts with the native networking interfaces to collect traffic flow data.
- Enforces policy received from the PCE.
- Only consumes CPU as needed to calculate or optimize and apply the firewall, and so on, while remaining idle in the background as much as possible.
- Uses configurable operational modes to minimize the impact to workloads.
- Summarizes the collected traffic-flow data, then reports it to the PCE.

You control the VEN's operations through the PCE web console or from the command line on the machine with the installed VEN itself.

Activation or Pairing

The terms “activation” and “pairing” indicate the same function from different perspectives, namely putting the workload under managed control by the PCE:

- The VEN sees itself as *activated* or *deactivated*.
- The PCE sees a VEN as *paired* or *unpaired*.

Pairing and Activating the VEN

1	The VEN is installed.	The PCE remains unaware the VEN is present.
2	The VEN and the PCE are paired.	The PCE uses a pairing key (activation code) to pair with the VEN. After pairing, the PCE becomes aware of the VEN.
3	The VEN is activated.	The VEN uses an activation code generated by the PCE. After

activation, the VEN is ready to function.

Unpairing or Deactivating the VEN

- When the PCE is unpaired with the VEN, the VEN is deactivated and uninstalled.
- When the VEN is deactivated, it remains installed and can be reactivated.
- Use the `illumio-ven-ctl` command to deactivate the VEN. You can't deactivate a VEN by using the PCE UI; you may only unpair it.

VEN Architectural Diagram

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

VEN Logical Software Architecture

1. The VEN reports to the PCE the status of the workloads.
2. The PCE computes a unique security policy for each managed workload and transmits it to the VEN.
3. The VEN receives the policy and it programs a firewall by using the firewall platform of the OS. The VEN supports the following firewall platforms:
   a. iptables (older Linux)
   b. Nftables (newer Linux)
   c. Packet Filter (newer Solaris)

   d. Ipfilter (older Solaris)
   e. Windows Filtering Platform (Windows)
4. When the VEN is finished programming a firewall for each workload, it reports back to the PCE. The PCE then considers these workloads as having a *synced* policy.

Main Components of the VEN

VEN Process	Description	Linux/AIX/Solaris User	Windows User
AgentManager	• Manages PCE-driven uninstallation and upgrades. • All actions relating to active service reporting. • Mines the workload's system information, such as network interfaces, and listening processes, and sends them to the PCE. • Sends heartbeats to the PCE. • Calls netstat periodically for connection status through a shell script or with a direct program call.	`root`	LOCAL SYSTEM
PlatformHandler	• Firewall configuration via native OS mechanisms. • Tamper detection and protection. • Upgrades and uninstallation.	`root`	LOCAL SYSTEM
VtapServer	• Windows: VTAP runs under the "Local System" account. • Retrieves traffic flow data from the ilowfp ker-	`root`	LOCAL SYSTEM

VEN Process	Description	Linux/AIX/Solaris User	Windows User
	nel mode driver (Windows) or firewall (other platforms) and generates flow logs in a database. • Receives events from the firewall on blocked packets and allowed connections. • Checks on the connection status of all listening services on the system for the default gateway, on connections, for open ports, etc.		
AgentMonitor	• Service account: NT Authority/Local System • Monitors VEN processes or services and restarts them when necessary.	`root`	LOCAL SYSTEM

SecureConnect Architecture

Illumio's optional SecureConnect feature configures Internet Protocol Security (IPsec), a set of protocols to enforce security for IP networks. IPsec can be configured to use cryptography.

IPsec runs as root in LOCAL SYSTEM.

VEN Interactions with Files and Components

The VEN interacts with files and components for installation, root tasks, and initialization tasks. Minor tasks include working with install logs, the registry key, and read-only access to machine resources.

The VEN interacts with the following files and components:

Linux/AIX/Solaris

Function	Description	File/Location
Root file	DATA_ROOT is a variable that points to a filepath.	`/opt/illumio_ven_data` (by default)
Package repository	INSTALL_ROOT is a variable that points to a filepath.	`/opt/illumio_ven` (by default)
System initialization	Initializes system	`/etc/illumio_ven` (typically)
Persistent install log	Persistent install log	`/var/log/illumio.log`
Firewall	Dynamically addS IPs to ipsets:	Snoop on special packets.
	Strongswan IPSec system.	Snoop on Security Associations.
	Read system files (e.g., netstat).	`/proc`

Windows

Function	Description	File/Location
Runtime data files	DATAFOLDER is an installer parameter that points to a filepath.	`c:\ProgramData\Illumio` (by default)
Executable program files	INSTALLFOLDER is an installer parameter that points to a filepath.	`c:\Program Files\Illumio` (by default)
Install log	Persistent install log.	`c:Windows\Temp\illumio.log` (by default) `c:Windows\Temp\Illumio_VEN_Install.log` (by default) `c:Windows\Temp\Illumio_VEN_Uninstall.log` (by default)
System initialization	N/A	N/A
Firewall	For network filtering.	Windows Filtering Platform

Management Interfaces for the VEN and PCE

The diagram below is a logical view of the management interfaces to the PCE and VEN.

Interface	Notes	See...
PCE web console	With the PCE web console, you can perform many common tasks for managing Illumio Core.	*Security Policy 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 the Illumio Core on the PCE command line, including installing and updating the VEN.	*PCE Administration 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 rule-	*PCE CLI Tool Guide*

Interface	Notes	See...
	sets, labels, and other resources.	
REST API	With the Illumio Core 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 Developer Guide*
VEN command line	A primary management tool on the VEN command line is the `illumio-ven-ctl` control script.	*VEN Administration Guide*

About VEN Administration on Workloads

The following topic explains the VEN states and characteristics necessary to understand when administering the VEN on workloads.

VEN Software Management from PCE

The ability to manage VEN software and install the VEN by using the PCE has been enhanced in this release in the following ways:

- You can upgrade all VENs or just a subset of VENs from the PCE.
- You can upgrade VENs by using filters, such as for labels, OSs, VEN health, IP address, current VEN version.
- When upgrading, the PCE informs you of the version the VENs will be upgraded to.
- You can monitor and troubleshoot VEN upgrade issues.
- You can perform VEN version reporting and compatibility.

VEN Proxy Support on Linux, AIX, and Solaris

This release extends VEN proxy support to include Linux, AIX, and Solaris devices, in addition to Windows.

For more information, see VEN Proxy Support in *VEN Installation and Upgrade Guide.*

Support on IBM Z With RHEL 7 and RHEL 8

IBM Z® is a family of modern z/Architecture hardware that runs z/OS, Linux, z/TPF, z/VM and IBM Z systems software.

Illumio supports installing and operating the VEN on IBM Z systems running Red Hat Enterprise Linux 7 (RHEL 7) and RHEL 8. Additionally, Illumio supports the VEN running on IBM Z systems using both KVM and z/VM as hypervisors.

Support on SLES 11 SP2

The VEN can be installed on systems running SLES 11 SP2 when the following packages are installed:

From the SLES 11 SP2 Latest Updates:

- libipset2-6.12-0.7.7.1
- ipset-6.12-0.7.7.1
- libmnl0-1.0.3-0.5.4
- kernel-default-3.0.101-0.7.17.1
- kernel-default-base-3.0.101-0.7.17.1

From the SLES 11 SP4 DVD:

- libxtables9-1.4.16.3-1.37
- libiptc0-1.4.16.3-1.37
- iptables-1.4.16.3-1.37
- libnfnetlink0-1.0.0+git1-9.5.56

Debian 11 Support

Starting from Release 21.2.3, Illumio supports installing and operating the VEN on the Debian 11 operating system.

VEN Support on Rocky Linux

Beginning in the 21.5.10 release, the VEN is supported on the Rocky Linux OS.

Workload Policy States

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

Change the policy state of the VEN by modifying settings in the PCE or by making calls to the REST API.

VEN Enforcement Characteristics

Policy enforcement is managed through both enforcement states and visibility states to specify how much data the VEN collects from a workload.

The following table summarizes the key enforcement characteristics of the VEN:

Workload Enforcement State	VEN Mode	VEN Visibility Level	Log Traffic
Idle	Idle	Limited	Limited
Visibility Only	Illuminated	Off Blocked Blocked+Allowed Enhanced Data Collection	VEN does not log traffic connection information VEN logs connection information for blocked and potentially blocked traffic only VEN logs connection information for allowed, blocked, and potentially blocked traffic VEN logs byte counts in addition

Workload Enforcement State	VEN Mode	VEN Visibility Level	Log Traffic
			to connection details for allowed, blocked, and potentially blocked traffic
Selective	Selective	Off Blocked Blocked+Allowed Enhanced Data Collection	VEN does not log traffic connection information VEN logs connection information for blocked and potentially blocked traffic only VEN logs connection information for allowed, blocked, and potentially blocked traffic VEN logs byte counts in addition to con-

Workload Enforcement State	VEN Mode	VEN Visibility Level	Log Traffic
			nection details for allowed, blocked, and potentially blocked traffic
Full	Enforced	Off Blocked Blocked+Allowed Enhanced Data Collection	VEN does not log traffic connection information VEN logs connection information for blocked and potentially blocked traffic only VEN logs connection information for allowed, blocked, and potentially blocked traffic VEN logs byte counts in addition to connection

Workload Enforcement State	VEN Mode	VEN Visibility Level	Log Traffic
			details for allowed, blocked, and potentially blocked traffic

For more information, see Ways to Enforce Policy in the *Security Policy Guide*.

VEN Policy Sync

To help you administer and troubleshoot the VEN, it reports many Policy Sync states. Here are the Policy Sync states and their definitions:

- **Active (Syncing)**: Policy is currently being applied to the workload.
- **Active**: The most recent policy provisioning was successful, no unwanted changes to the workload's firewall have been reported, none of the configured SecureConnect connections are in an erroneous state, and all VEN processes are running correctly.
  - For more information on SecureConnect see Security Policy Guide.
- **Staged**:The PCE has successfully sent policy to the VEN, and it is staged and scheduled to be applied at a later time. This state only appears when you have configured the Policy Update Mode for the workload to use Static Policy. See Static Policy and Staged Policy for information. For information, see Types of Illumio Policy in the *Security_Policy_Guide.*
- **Error**: One of the following errors has been reported by the VEN:
  - The most recent policy provisioning has failed.
  - Unwanted changes to the workload's firewall have been reported.
  - At least one VEN process is not running correctly.
  - There is a SecureConnect or Machine Authentication policy, but leaf certificates are not set up properly.
- **Warning**: At least one SecureConnect connection is in an erroneous state, and either the most recent policy provisioning was successful or no unwanted changes to the workload's firewall have been reported.

- **Suspended**: Used by admins to debug. Rules programmed into the platform firewall (including custom iptables rules) are removed completely. No Illumio-related processes are running on the workload.

VEN Health Status on Workloads

The VEN health status on the workload's details page displays information related to the current state of VEN connectivity, the most recently provisioned policy changes to that workload, and any errors reported by the VEN.

These errors include any unwanted changes to the workload's firewall settings, any SecureConnect functionality issues, or any VEN process health errors.

To view a workload's VEN health status, view the VEN section on the **Summary** tab for the workload's details page.

VEN Process Health

The health status of the VEN can be monitored from the PCE web console. If for any reason one or more Illumio processes on the workload are not running, the VEN reports the error to the PCE. The PCE marks the workload as in an error state and adds a notification on the Workloads page. It also logs an audit event that includes the Illumio processes which were not running on the workload.

Workload Clone Alerts

Workloads can be filtered according to whether a cloned node has been detected. On Windows, Linux, and Mac OS systems, when the PCE detects a cloned node, it notifies the VEN through a heartbeat. The VEN verifies that a clone exists, prevents it from being activated, and deletes it.

In the Illumio REST API, detection is done by using the `clone_detected` state. In the PCE web console UI, search the workloads list by filtering on, "clone detected." If there are workloads in the `clone_detected` state, a red banner (similar to *workloads in suspension*) is displayed at the top of the workload list page.

Stopped VEN Status

The addition of the `stopped` status has the following affect on the PCE web console UI:

- On the Workload list page, the "Connectivity" column is replaced with "Status."
- On the Workload details pages, "VEN Connectivity" is changed to "VEN status."
- You can filter the Workload list page by the new VEN stopped status.

Aggressive Tampering Protection for nftables

Firewall changes that are not explicitly configured by the VEN are logged as tampering attempts. This feature extends Release 19.3 nftables support with the inclusion of aggressive tampering protection.

Uninterrupted Traffic Between the VEN and the PCE

> IMPORTANT:
> This feature requires the Illumio Core VEN version 21.2.0 or later.

The current VEN implementation in Release 21.2.0 provides an extra layer of self-protection that prevents any erroneous policy from being applied to the VEN. The VEN employs a defensive approach that reviews policies before applying them. In case the VEN detects that the new policy may disrupt communications between the VEN and the PCE, the VEN automatically isolates that policy and logs an error in the event log. The VEN then continues to communicate with the PCE using the existing functional policy.

Prior to Release 21.2.0, if an erroneous policy was inadvertently propagated from the PCE to the VENs, it caused a permanent disruption in communications. All VENs and all workloads were impacted and would remain in an undesirable state until the correct policies were reapplied. Manual intervention was required to reload the correct policy to resume communications between the VEN and the PCE. This is no longer required.

VEN File Settings Option

In 21.2.1, the VEN IPFilter state table supports a new option for AIX workloads to support traffic from NFS servers:

VEN File Setting:`IPFILTER_TCPCLOSED=<value>`

ipfilter Setting:`fr_tcpclosed=<value>`

For more information about this option, see VEN Activate Command Reference in the *VEN Installation and Upgrade Guide.*

Windows VEN Proxy Fallback Enhancement

Starting from Illumio Core 21.2.1 and 21.2.2, the VEN automatically detects a web proxy. However, it always attempts to connect directly to the PCE first. In this release, Illumio enhanced the heuristic in the VEN for falling back to the configured web proxy.

After an attempt fails to connect to the PCE directly due to an HTTPS intercepting proxy, the VEN falls back to use the configured web proxy.

Label-based Security Setting for IP Forwarding

In Illumio Core 21.5.10, Illumio enabled IP forwarding to hosts running Linux. A container networking solution routes the traffic to the VMs. To configure IP forwarding, use the new IP Forwarding tab in the PCE web console. In this tab, you can use labels and label groups to enable IP forwarding for the workloads that match the label combination.

To enable this feature, contact Illumio Support. For details about how to set up IP forwarding for workloads, see Connectivity Settings in the PCE Administration Guide.

Uninterrupted Traffic Between the VEN and the PCE

> IMPORTANT:
> This feature requires the Illumio Core VEN version 21.2.0 or later.

The current VEN implementation in Release 21.2.0 provides an extra layer of self-protection that prevents any erroneous policy from being applied to the VEN. The VEN employs a defensive approach that reviews policies before applying them. In case the VEN detects that the new policy may disrupt communications between the VEN and the PCE, the VEN automatically isolates that policy and logs an error in the event log. The VEN then continues to communicate with the PCE using the existing functional policy.

Prior to Release 21.2.0, if an erroneous policy was inadvertently propagated from the PCE to the VENs, it caused a permanent disruption in communications. All VENs and all workloads were impacted and would remain in an undesirable state until the correct policies were reapplied. Manual intervention was required to reload the correct policy to resume communications between the VEN and the PCE. This is no longer required.

IPv6 Support and Features for the VEN

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*.

The VEN supports IPv6 in the following ways.

IPv6 is Enabled by Default on Datacenter VENs

Release 20.2.0 and later support configuring inbound or outbound IPv6 traffic by organization (ORG). In previous releases, you are only able to block all, or allow all IPv6 traffic by organization.

The default settings are as follows:

- If the previous ORG-wide IPv6 policy is to *block all* IPv6 traffic, then this setting is *preserved*.
- If the previous ORG-wide IPv6 policy is to *allow all* IPv6 traffic, then this setting is *not preserved*.

IPv6 Support for Linux and Windows VENs

Beginning with Release 20.1, the Linux and Windows VENs support IPv6 rules.

VEN Compatibility Report for IPv6 Support

Illumio supports IPv6 for workloads. This includes providing a warning in the Compatibility Report. The Compatibility Report is used to detect the possible issues before moving VEN out of idle state. See VEN Compatibility Check in the *VEN Installation and Upgrade Guide*. In this release, Illumio updated the options in the Compatibility Report to increase it's usability.

The following command and command options are supported:

- On Linux and SunOS, this command option is available regardless of whether IPv6 is enabled:
  - ipv6_forwarding_enabled
    - At least 1 iptables forwarding rule is detected in the IPv6 forwarding chain. VEN removes existing iptables rules in the non-Idle policy state.
- On Windows, we do not support all IPv6 transition tunnels that is a part of the IPv6 transition technology (RFC 4213). The following options are available:
  - teredo_tunneling_enabled
    - Teredo tunneling allows for IPv6 connectivity.
    - Teredo is an IPv6 transition tunnel.

        - We do not report on Teredo adapters.
    - IPv6 enabled
        - Continues to be supported.
        - Detects potential transition technology usage on Windows.

`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.

Set PATH Environment Variable

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`

Command Line Syntax by Platform

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

Linux/AIX/Solaris Command Line Help

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

Windows Command Line Help

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

Useful VEN and OS Commands

This topic provides is a short description of the VEN command-line tools that you commonly use for various operations, and some useful native OS commands. Syntax for the VEN-provided commands is detailed throughout this guide, and in the help of the commands themselves.

Additionally, this topic lists the availability of the VEN commands across operating systems.

Verify VEN Version Number

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

- View the VEN version in the PCE web console.
- Run the following command on the workload:

  ```
  # /opt/illumio_ven/illumio-ven-ctl
  version 21.5.0-xxxx
  ```

- Run the following command on a Windows workload:

  ```
  PS C:\Users\Administrator> & 'C:\Program Files\Illumio\illumio-ven-ctl.ps1'
  version
  21.5.0-xxxx
  ```

- Examine the columns in **Add or remove programs** or Task Manager.

- Examine the **Properties** > **Details** tab of `venAgentMgr.exe` or `venPlatformHandler.exe`.
- Use the Illumio Core REST API. With the REST API, the `agent-version` key and value are returned in the payload of every response.

Commonly Used VEN Commands

Platform	Command	Description
Linux	`/opt/illumio_ven/illumio-ven-ctl`	VEN Linux shell control script to control VEN control VEN settings and functions
	`/opt/illumio_ven/bin/agent_status.sh`	Alternative to `illumio-ven-ctl status`
	`ps`	Native OS command to list all system processes
	`chkconfig`	Native OS command to update and query runlevel information for system services
Windows	`C:\Program Files\Illumio\illumio-ven-ctl.ps1`	VEN PowerShell script to control VEN settings and functions
	`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
AIX/Solaris	`/opt/illumio_ven/illumio-ven-ctl`	VEN AIX/Solaris shell control script to control VEN control VEN settings and functions
	`/opt/illumio_ven/bin/agent_status.sh`	Alternative to `illumio-ven-ctl status`
	`/opt/illumio_ven/bin/agent_status.sh`	Alternative to `illumio-ven-ctl status`
	`ps`	Native OS command to list all system processes
AIX	`lssrc`	Native OS command to list OS subsystem status
Solaris	`svcs`	Native OS command to list OS service status

illumio-ven-ctl Command Options by OS

The following tables details the `illumio-ven-ctl` command support by operating system:

Command	Description	AIX	CentOS	Debian	RHEL	Solaris	SUSE	Ubuntu	Windows
`activate <options>`	Activate VEN.	Y	Y	Y	Y	Y	Y	Y	Y
`backup`	Backup VEN data.	—	Y	Y	Y	—	Y	Y	Y
`check-env`	Check VEN `runtime_env.yml` settings.	Y	Y	Y	Y	Y	Y	Y	Y
`conncheck`	Query VEN policy.	Y	Y	Y	Y	Y	Y	Y	
`connectivity-test`	Test connectivity with PCE.	Y	Y	Y	Y	Y	Y	Y	Y
`deactivate <options>`	Deactivate VEN without uninstalling.	Y	Y	Y	Y	Y	Y	Y	Y
`gen-supportreport <options>`	Generate VEN support reports.	Y	Y	Y	Y	Y	Y	Y	Y
`prepare`	Prepare VEN image.	Y	Y	Y	Y	Y	Y	Y	Y
`restart`	Restart VEN services.	Y	Y	Y	Y	Y	Y	Y	Y
`restore`	Restore VEN `datail-lumio-ven-ctl`.	—	Y	Y	Y	—	Y	Y	Y
`start`	Start VEN services.	Y	Y	Y	Y	Y	Y	Y	Y

Command	Description	AIX	CentOS	Debian	RHEL	Solaris	SUSE	Ubuntu	Windows
`status`	Report VEN status.	Y	Y	Y	Y	Y	Y	Y	Y
`stop`	Stop VEN services.	Y	Y	Y	Y	Y	Y	Y	Y
`suspend`	Suspend VEN (enter emergency state).	Y	Y	Y	Y	Y	Y	Y	Y
`unpair <options>`	Unpair VEN.	—	Y	Y	Y	Y	Y	Y	Y
`unsuspend`	Unsuspend VEN (exit emergency state).	Y	Y	Y	Y	Y	Y	Y	Y
`version`	Display VEN version.	Y	Y	Y	Y	Y	Y	Y	Y
`workloads`	Report VEN workload status.	—	Y	Y	—	—	Y	Y	—

Chapter 2

VEN State

This chapter contains the following topics:

VEN Startup and Shutdown 29
Disable and Enable VENs (Windows only) 31
VEN Suspension 32

This section describes all the VEN's states and how you can manage them. VEN state refers to the active state of the VEN on a workload; basically, is it running, stopped, enabled, disabled, or suspended.

VEN Startup and Shutdown

This topic provides information on starting and stopping VENs.

VEN Startup and Shutdown (illumio.com)

- AIX and Solaris: Start up the VEN.
- AIX and Solaris: Shut down the VEN and send a Goodbye message.

Start Up VENs

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

Automatic Startup

The VEN starts when the workload is booted from system boot files:

Platform	Command	Notes

Linux/AIX/Solaris	`/etc/rc.d/init.d/illumio-ven`
	Or
	`/etc/init.d/illumio-ven`
		Installs firewall kernel modules if necessary, sets firewall to the desired state.

	CentOS/RHEL 7+, starting from 19.3.2 `/usr/lib/systemd/system/illumioven.service`	Initializes and starts the daemon processes needed for VEN operation. IMPORTANT: This command is only supported in Illumio Core 19.3.2-VEN and later.
Windows	None needed.	The Service Control Manager (SCM) starts all VEN services at boot.

Manual Startup

The VEN can also be started manually with `illumio-ven-ctl start`.

Platform	Command
Linux/AIX/Solaris/RHEL/CentOS	`/opt/illumio_ven/illumio-ven-ctl start`
Windows	`C:\Program Files\Illumio\illumio-ven-ctl.ps1 start`

Shut Down VENs

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/AIX/Solaris Workload Shutdown

Platform	Command	Notes
Linux/AIX/Solaris/RHEL/CentOS	`illumio-ven-ctl stop`	• Stops all VEN processes. • The VEN sends a “goodbye” message to the PCE.
Windows	None needed.	• Service Control Manager (SCM) stops all VEN services. • The VEN sends a “goodbye” message to the PCE.

Disable and Enable VENs (Windows only)

If you want to install the VEN but activate it later, you can disable the VEN after you first install it. This is only available on the Windows platform.

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

Platform	Action	Command

Windows	• Enable
	• Disable:
		`PS C:\Program Files\Illumio> .\illumio-ven-ctl.ps1 enable`
		
		`PS C:\Program Files\Illumio> .\illumio-ven-ctl.ps1`

Platform	Action	Command
		`disable`

VEN Suspension

If users are not able to reach an app on a workload, you can suspend the VEN to see if the VEN was causing the issue. The VEN suspension feature allows you to isolate a VEN on a workload to troubleshoot any communication issues with that workload, and to determine if the VEN is the cause of the anomalous behavior.

> IMPORTANT:
> **Security Implications:** When the VEN is suspended, the workload firewall rules are removed leaving the VEN open and all traffic is allowed.

About VEN Suspension

When a VEN is suspended, the following is true:

- Any rules programmed into the workload's iptables (including Custom iptables rules), Windows Filtering Platform (WFP), or ipfilter, or pf firewalls are removed completely, and all VEN software processes are shut down.
- The VEN connectivity and policy sync status are changed to **Suspended**.
- The VEN informs the PCE that it is in the suspended state. If the PCE does not receive this notification, you must mark the workload as **Suspended** in the PCE web console.
- If the PCE does not receive the VEN suspension notification and 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 the policy, which effectively isolates the workload from the network. For example, users will not be able to reach apps on the workload.
- Workloads communicating with the suspended VEN continue to have their rules programmed into iptables or WFP.
- The SecureConnect policy continues to be in effect while the VEN is suspended.
- An organization event (`server_suspended`) is logged. This event is exportable to CEF/LEEF and has a severity of WARNING.

Properties of a suspended VEN:

- The workload continues to appear in the PCE in the workloads list page and Illumination map.
- You can unpair a workload while its VEN is suspended.
- You can change the policy state of the workload in the PCE Web Console while the VEN is suspended.
- When the VEN is unsuspended, the new policy state is applied.
- Heartbeats or other communication is not expected, but if one is received, any communication is logged by the PCE.
- If the PCE is rebooted, the VEN remains suspended.

When a VEN is unsuspended:

- The PCE is informed that the VEN is no longer suspended and can now receive policy from the PCE.
- If existing Rules affect the unsuspended workload, the PCE will reprogram those Rules.
- An organization event (`server_unsuspended`) is logged. This event is exportable to CEF/LEEF and has a severity of WARNING.
- The workload will revert to its policy state prior to Suspended.
- Custom iptables Rules are configured back into the iptables.

You can manage VEN suspension by using these features of the Illumio Core:

- The REST API

  For more information on this method, see VEN Operations in the REST API Developer Guide.

- The command line
- The PCE web console

  For more information, see Mark VEN as Suspended Using the PCE Web Console in this topic.

Linux VEN: Back Up Custom iptables/NAT Rules

NOTE:
Before suspending a Linux VEN, back up the workload PCE custom iptables filter or NAT rules.

After a workload is suspended, restore the rules on the workload because all custom iptables filter or NAT rules will have been removed from the workload.

Suspend and Unsuspend Commands

Platform	Action	Command	Notes

Linux/-Unix	• 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.`
			On Linux, be sure to backup your custom configuration.
			See Linux VEN: Back Up Custom 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.`	

Mark VEN as Suspended Using the PCE Web Console

In addition to using the command explained in the previous section, you can mark a workload as **Suspended** using the PCE web console.

NOTE:
Marking a workload as **Suspended** in the PCE web console does **not** actually suspend the VEN. It should only be used if the VEN went offline before it could be suspended. Marking the workload as **Suspended** is a way to keep the PCE from removing the VEN from the policy and isolating it from the rest of the network.

1. Select a workload from the Workloads list page.
2. Click **Edit**.
3. Click **Mark as Suspended**.
4. Click **OK** to confirm the VEN suspension.

The number of suspended workloads is displayed at the top of the page and the suspended workload is displayed on the Workloads page with a red "Suspended" icon.

To unsuspend a VEN:

1. Select a workload from the Workloads list page.
2. Click **Edit**.
3. Click **Clear Suspension**.
4. Click **Clear** to confirm.

Disable VEN Suspension on Workloads

You can disable the ability to suspend a VEN on a workload. To disable the VEN suspension feature, define the following environment variable for the VEN. How you set the variable varies by VEN platform. See the procedures to set the environment variable for each platform.

Environment Variable	Values
`VEN_NO_SUSPEND`	1 – Disable VEN suspension 0 – VEN suspension is enabled

NOTE:
Disabling VEN suspension is not supported for Illumio Secure Cloud customers.

Linux VENs

Before installing or upgrading the Linux VEN, enter the following command line syntax to set the environment variable:

```
# VEN_NO_SUSPEND=1 <ven_install_or_upgrade_command>
```

Examples:

```
# VEN_NO_SUSPEND=1 rpm -i <illumio-ven-pkg>.rpm
```

```
# VEN_NO_SUSPEND=1 dpkg -i <illumio-ven-pkg>.deb
```

```
# VEN_NO_SUSPEND=1 rpm -U <illumio-ven-pkg>.rpm
```

Windows VENs

Pass the environment variable as a command line option when using the Windows VEN package to install or upgrade the VEN:

```
PS C:\> msiexec /<options> <ven_installation_filename>.msi VEN_NO_SUSPEND=1
```

Example:

```
PS C:\> Set-ExecutionPolicy -ExecutionPolicy RemoteSigned
PS C:\> msiexec /i  ven_install_filename.msi VEN_NO_SUSPEND=1
```

AIX VENs

Before installing or upgrading the AIX VEN, enter the following command line syntax to set the environment variable:

```
# VEN_NO_SUSPEND=1 <ven_install_or_upgrade_command>
```

Example:

```
# VEN_NO_SUSPEND=1 installp -acXgd <path_to_bff_package> illumio-ven
```

Solaris VENs

When you install the Solaris VEN by interactively responding to installer prompts, enter `n` at the following prompt:

```
"Do you want to disable VEN suspend? [y,n] ", enter as required : y - disable, n -
default/no-action
```

When you use the template file in the VEN package to pre-load responses to installer prompts, copy the following file:

```
illumio-ven/root/opt/illumio_ven/etc/templates/response
```

Change the copied file in the following way:

```
/usr/xpg4/bin/sed 's/^VEN_NO_SUSPEND=0/VEN_NO_SUSPEND=1/g’ \
< illumio-ven/root/opt/illumio_ven/etc/templates/response \
> illumio-ven/root/opt/illumio_ven/etc/templates/response.custom
```

Chapter 3

Rollback, Deactivate, or Uninstall VENs

This chapter contains the following topics:

Backup, Restore, and Rollback VENs 38
Deactivate and Unpair VENs 43
VEN Unpairing Details 46

This section describes all the ways that you can change the VEN software running on a workload, from reverting it to an earlier release, deactivating the software, to uninstalling it completely.

Backup, Restore, and Rollback VENs

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.
- Perform an automatic rollback while re-installing the previous version.

  –Or–

  Manually rollback by running `illumio-ven-ctl restore`.

Downgrading versus Rolling Back VENs

Do not downgrade the VEN by 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, uninstall the current version and then install the older version.

Back Up 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 below for the default paths to the data directory.

- Linux: `<installation_root_dir>/illumio_ven_data/backup`
- Windows: `%PROGRAMDATA%\Illumio\backup`
- AIX/Solaris: Not available

> CAUTION:
> 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

> NOTE:
> 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`
- AIX/Solaris: Not available

Roll Back to Previous VEN Version

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.

NOTE:
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

NOTE:
A rollback procedure using the Windows EXE Installer is not available in this release.

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.

AIX/Solaris

Rollback to the previous VEN version is not available on AIX or Solaris.

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_install-ation_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

Value	Description
	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 Deactivate and Unpair VENs.

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	Description
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 Deactivate and Unpair VENs.
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"
```

AIX/Solaris

Manual rollback is not available on AIX or Solaris.

Deactivate and Unpair VENs

This topic discusses how to deactivate and unpair VENs by operating system.

Additionally, it explains the security implications for performing these tasks and makes recommendations on how to properly deactivate and unpair VENs.

See also VEN Unpairing Details for further information.

Deactivate Using VEN Command Line

To deactivate the VEN, you must use the `illumio-ven-ctl` command.

`deactivate` breaks the PCE-to-workload connection but doesn't uninstall the VEN software (as `unpair` would).

After deactivation, the workload reverts to its pre-Illumio native firewall settings.

Linux/AIX/Solaris

```
# /opt/illumio_ven/illumio-ven-ctl deactivate
```

Windows

```
PS C:\Program Files\Illumio> .\illumio-ven-ctl.ps1 deactivate
```

Unpair Using VEN Command Line

The `unpair` command breaks the PCE-to-workload connection, and uninstalls the VEN software. The `unpair` command gives you control over the post-unpair state, as described below.

Linux/AIX/Solaris

With `illumio-ven-ctl unpair`, specify the post-unpair state for the VEN:

```
# /opt/illumio_ven/illumio-ven-ctl unpair [recommended | saved | open]
```

> NOTE:
> On Linux, the `unmanaged` option is not available.

Unpair Options on Linux/AIX/Solaris

- `recommended`: Uninstalls the VEN and temporarily allows only SSH/22 until reboot.

  > IMPORTANT:
  > **Security implications**: When the 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`: Uninstalls the VEN and reverts to pre-Illumio policy to the state before the VEN was first installed. Revert the state of the workload's iptables to the state before the VEN was installed. The dialog displays the amount of time that has passed since the VEN was installed.

  > IMPORTANT:
  > **Security implications**: Depending on how old the iptables configuration is on the workload, VEN removal could impact the application.

- `open`: Uninstalls the VEN and leaves all ports on the workload open.

  > IMPORTANT:
  > **Security implications**: When iptables or Illumio are the only security being used for the workload, the workload is open to anyone and becomes vulnerable to attack.

Windows

With `illumio-ven-ctl.ps1` unpair, specify the post-deactivation state for the VEN:

```
PS C:\Program Files\Illumio> .\illumio-ven-ctl.ps1 unpair [recommended | saved |
open | unmanaged]
```

Unpair Options on Windows

- `recommended`: Temporarily allow only RDP/3389 and WinRM/5985,5986 until reboot.

  > IMPORTANT:
  > **Security implications**: If the workload is running a production application, the application could break because the workload no longer allows any connections to it.

- `saved`: Restores firewall rules and configuration to the state it was in at the time the workload was paired. Reverts the state of the firewall to before Illumio was installed.

  > IMPORTANT:
  > **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.

  > IMPORTANT:
  > **Security implications**: When WFP or the PCE are the only security being used for the workload, the workload is open to anyone and becomes vulnerable to attack.

- `unmanaged`: Uninstalls the VEN and reverts to the workload's currently configured Windows Firewall policy.

Unpair Using System Commands

You can use the `illumio-ven-ctl` (Linux/AIX/Solaris) or `illumio-ven-ctl.ps1` (Windows) to unpair the VEN.

> **IMPORTANT:**
> As an alternative, you can use the `system uninstall` command to unpair the VEN, however it is not recommended. This command should only used as a fallback if there are issues with unpairing with `illumio-ven-ctl` or `illumio-ven-ctl.ps1`.

Linux

- RPM: `rpm -e illumio-ven`
- DPKG: `dpkg -P illumio-ven`

Windows

- Use the Control Panel to uninstall the VEN.

AIX

- `installp -u illumio-ven`

Solaris

- `pkgrm illumio-ven`

VEN Unpairing Details

During unpairing, the VEN performs the following actions. These actions are specific to the workload operating system.

Linux/AIX/Solaris

- Unpairs the VEN from the PCE.
  - Sends a "deactivate" message to 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: The firewall is restored to its state just before the VEN was installed.
- Uninstalls the `illumio-ven` package.
  - Removes program and data files.
  - Removes repo and GPG files and package.

Windows

- 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.

Support Report During Unpairing

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 is uninstalled.

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

Chapter 4

Monitor and Diagnose VEN Status

This chapter contains the following topics:

VEN-to-PCE Communication 48
VEN Status Command and Options 55
VEN Logging 60
Tuning the IPFilter State Table (AIX/Solaris) 62
Manage Conntrack Table Size (Linux) 65
VEN Firewall Tampering Detection 67
VEN Support Reports 71
VEN Troubleshooting 73

This section provides you with the necessary information to monitor VEN status on your workloads and to troubleshoot any problems that might occur.

VEN-to-PCE Communication

This topic discusses how the VEN communicates with the PCE for both Illumio Core Cloud customers and Illumio Core On-Premises customers.

Details about VEN-to-PCE Communication

The VEN, by default, communicates with the PCE when installed in customers data centers (On-Premises) over the following ports:

- Port 8443 using HTTPS for REST calls.
- Port 8444 using TLS-over-TCP for the lightning bolt channel.

The VEN, by default, communicates with the Illumio Core Cloud PCE over the following ports:

- Port 443 for REST calls.
- Ports 443/444 for lightning-bolt channels.

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:

- Regular heartbeat with the latest hostname and other properties of the workload
- Traffic log
- Network interfaces
- Processes
- Open ports
- Interactive users (Windows only)
- Container workload information (C-VEN only)

The VEN receives the following details from the PCE:

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

VEN Connectivity

- **Online**: The workload is connected to the network and can communicate with the PCE.
- **Offline**: The workload is *not* connected to the network and cannot communicate with the PCE.
- **Suspended**: The VEN is in the suspended state and any rules programmed into the workload's IP tables (including custom iptables rules) or Windows filtering platform firewalls are removed completely. No Illumio-related processes are running on the workload.

VEN offers limited IPv6 policy support. On a per- organization basis, the PCE can send *allow-all-ipv6* or *block-all-ipv6* policy enforceable by the VEN.

Communication Frequency

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

Function	Frequency	Notes
Firewall policy updates	Real-time if lightning bolts are enabled.	If lightning bolts are displayed or the channel is not functional, policy updates are communicated to the VEN by a heartbeat action.
Active service reporting	See note.	• AgentManager performs all active service reporting tasks. • At start-up, a snapshot of processes and ports is sent to the PCE. • Every 24 hours, a snapshot of *all* listening processes is taken and sent to the PCE.
Interface reports and changes	Event driven.	Only if there are changes to the interfaces; otherwise, no data are sent.
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

Function	Frequency	Notes
		is written to the PCE's event log. See also VEN Heartbeats and Lost Agents.
Dead-peer interval	Configurable	Default is 60 minutes (or 12 heartbeats). See also VEN Offline Timers and Isolation.
VEN tampering detection	Within a few seconds on Windows and Linux.	For more information, see Host Firewall Tampering Protection.

VEN Heartbeats and Lost Agents

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 fails to send a heartbeat, check the workload where the VEN is installed and investigate any connectivity issues. If the VEN continues to fail to send a heartbeat, it eventually is marked Offline, which means it can no longer communicate with the PCE or other managed workloads.

PCE down or network issue and the VEN degraded state

- 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 three heartbeats, the VEN enters the *degraded state*. In the degraded state, the VEN ignores all the asynchronous commands received as lightning bolts from the PCE, except the commands for software upgrades and support reports.
- After connectivity to the PCE is restored, the VEN comes out of the degraded state after three successful heartbeats.

Failed authentication and the VEN minimal state

- If the VEN enters the degraded state because of failed authentications, the VEN enters a state called *minimal*. In the minimal state, the VEN only attempts to connect with the PCE every four hours through a heartbeat.
- If the authentication failure was temporary, the VEN exits the minimal state after its first successful connection to the PCE. Whenever the VEN enters the minimal state, it stops the VTAP service. VTAP is then restarted when the VEN exits the minimal state.

- If Kerberos authentication is used, the VEN attempts to refresh the agent token with a new Kerberos ticket before sending a heartbeat. If the authentication error is not recovered after four hours, the VEN sends a lost-agent message to the PCE which then logs a message in the Organization Events. The message informs the user that the VEN needs to be uninstalled or reinstalled manually on this workload.

VEN Offline Timers and Isolation

When the VEN on a workload is stopped, the VEN makes a "best effort" REST API goodbye call to the PCE. After a delay, specified by the "workload goodbye timer" (a default of 15 minutes), the PCE marks the workload as offline and removes it from the policy.

If the REST API call (goodbye) fails, or 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.

Sampling Mode for VENs

If the VEN receives a sustained amount of high traffic per second from many individual connections, the VEN enters Sampling Mode to reduce the 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`

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

The Illumio Core VEN supports wireless connections for VENs installed on endpoints in the Illumio Core.

For more information about installing the VEN on an endpoint, and supporting a wireless network connection, see *Illumio Endpoint Installation and Usage Guide*.

> NOTE:Wireless network support is only available for endpoints in Illumio Core. It is not available for other support server types, such as bare-metal servers, virtual machines (VMs), or container hosts.

Show Amount of Data Transfer

The operation of 'show amount of data transfer' capability on the PCE is a preview feature available with the 20.2.0 release. The PCE now reports amount of data transferred in to and out of workloads and applications in a datacenter. The number of bytes sent by and received by the provider of an application are provided separately. These values can be seen in traffic flow summaries streamed out of the PCE. This capability can be enabled on a per-workload basis in the Workload page. It can also be enabled in the pairing profile so that workloads are directly paired into this mode.

After the feature is enabled, the VEN starts reporting the number of bytes transferred over the connections. The PCE collects this data, adds relevant information, such as, labels and sends the traffic flow summaries out of the PCE.

The direction reported in flow summary is from the viewpoint of the provider of the flow.

- Destination Total Bytes Out (`dst_tbo`): Number of bytes transferred out of provider (Connection Responder)
- Destination Total Bytes In (`dst_tbi`): Number of bytes transferred in to provider (Connection Responder)

The number of bytes includes:

1. L3 and L4 header sizes of each packet (IP Header and TCP Header)
2. Sizes of multiple headers that may be included in communication (when SecureConnect is enabled)
3. Retransmitted packets.

The bytes transferred in the packets of a connection are included in measurement. This is similar to various networking products such as firewalls, span-port measurement tools, and other network traffic measurement tools that measure network traffic.

Term	Description
dst_tbi	**Destination Total Bytes** In Total bytes received till now by the destination over the flows included in this flow-summary in the latest sampled interval. This is the same as bytes sent by the source. Present in 'A', 'C', and 'T' flow-summaries. source = client = connection initiator, destination = server = connection responder.
dst_tbo	**Destination Total Bytes** Out Total bytes sent till now by the destination over the flows included in this flow-summary in the latest sampled interval. This is the same as bytes received by the source. Present in 'A', 'C', and 'T' flow-summaries. source = client = connection initiator, destination = server = connection responder.
dst_dbi	**Destination Delta Bytes** In Number of bytes received by the destination in the latest sampled interval, over the flows included in this flow-summary. This is the same as bytes sent by the source. Present in 'A', 'C', and 'T' flow-summaries. source = client = connection initiator, destination = server = connection responder.
dst_dbo	**Destination Delta Bytes** Out Number of bytes sent by the destination in the latest sampled interval, over the flows included in this flow-summary. This is the same as bytes received by the source. Present in 'A', 'C', and 'T' flow-summaries. source = client = connection initiator, destination = server = con-

Term	Description
	nection responder.
interval_sec T	**Time Interval in Seconds** Duration of latest sampled interval over which the above metrics are valid.

Connection State	Description
A	**Active:** The connection is still active at the time the record was posted. Typically observed with long-lived flows on source and destination side of communication.
T	**Timed Out:** Flow does not exist any more. It has timed out. Typically observed on destination side of communication.
C	**Closed:** Flow does not exist any more. It has been closed. Typically observed on source side of communication.
S	**Snapshot:** Connection was active at the time VEN sampled the flow. Typically observed when the VEN is in Idle state.

VEN Status Command and Options

This topic describes various commands for determining the status of a VEN. Log in as root to run these commands.

The VEN Status Command

`illumio-ven-ctl status`

Returns the status of the VEN on the workload.

Linux/AIX/Solaris

```
# /opt/illumio_ven/illumio-ven-ctl status
```

Example Linux VEN Status return parameters

```
Status for illumio-control:
 - Environment Illumio VEN Environment is setup
 - venAgentMgr venAgentMgr (pid 23598) is running...
 - IPSec IPSec feature not enabled
 - venPlatformHandler venPlatformHandler (pid 23676) is running...
 - venVtapServer venVtapServer (pid 23737) is running...
 - venAgentMonitor active(running)

Agent state: enforced
```

Linux/AIX/Solaris VEN status field definitions

Name	Definition
`Environment`	Whether or not the Illumio VEN environment is setup
`venAgentMgr`	`venAgentMgr` status, and if running its `pid`
`IPSec`	Whether or not the IPSec feature is enabled
`venPlatformHandler`	`venPlatformHandler` status, and if running its `pid`
`venVtapServer`	`venVtapServer` status, and if running its `pid`
`venAgentMonitor`	`venAgentMonitor` status
`Agent state`	For example, `enforced`

Windows

Example Windows PowerShell VEN status command:

```
C:\Program Files\Illumio> .\illumio-ven-ctl.ps1 status
```

Example Windows VEN status return parameters

```
Service venAgentMgrSvc:         Running
Service venPlatformHandlerSvc:  Running
Service venVtapServerSvc:       Running
Service venAgentMonitorSvc:     Running
Service venAgentMgrSvc:         Enabled
Service venPlatformHandlerSvc:  Enabled
Service venVtapServerSvc:       Enabled
Service venAgentMonitorSvc:     Enabled
```

Policy Option for VEN Status

`illumio-ven-ctl status policy`

Returns the timestamp, ID, and state of the current security policy the VEN received from the PCE.

Linux/AIX/Solaris

```
# /opt/illumio_ven/illumio-ven-ctl status policy
```

Windows

Example Windows PowerShell VEN status policy command:

```
C:\Program Files\Illumio> .\illumio-ven-ctl.ps1 status policy
```

Return Description

Example

```
{
   "timestamp" : "2019-06-14T00:41:41Z",
   "id" : "xxxxxxxx940d0f4c2531b0d44400523dae055674-
xxxxxxxx7a6796c210fb846b0321847bc22d701e",
   "state" : "enforced"
}
```

VEN status policy field definitions

Policy Field Name	Definition
`timestamp`	Time the policy was received from the PCE (Local time + UTC offset)
`id`	ID of the security policy (computed locally)
`state`	Policy state (for example, `enforced`)

Health Option for VEN Status

`illumio-ven-ctl status health`

Returns whether or not the VEN can write logs locally.

NOTE:
This is not the same as PCE health.

Linux/AIX/Solaris

```
# /opt/illumio_ven/illumio-ven-ctl status health
```

Windows

Example Windows PowerShell VEN status health command:

```
# /opt/illumio_ven/illumio-ven-ctl status health
```

Return Description

Example

```
{
  "results": [
    {
      "test": "VEN has write access to the log directory",
      "result": "pass"
    }
  ],
  "state": "healthy"
}
```

Linux/AIX/Solaris VEN status health field definitions

Field Name	Definition
`results`	Array of test results
`test`	VEN has write access to the log directory
`result`	"`pass`" or an error
`state`	VEN health status ("healthy" or "unhealthy"); "`healthy`" means the VEN can write logs locally

Status Connectivity Option for VEN Status

`illumio-ven-ctl status connectivity`

Returns the status of the VEN connectivity with the PCE.

Linux/AIX/Solaris

```
# /opt/illumio_ven/illumio-ven-ctl status connectivity
```

Windows

Example Windows PowerShell VEN status connectivity command:

Return Description

Example

```
{
   "connectivity" : {
      "ips_returned" : 1,
      "pce" : "someName.someDomain",
      "port" : 8443,
      "results" : [
         {
            "ip" : "xx.xx.xxx.xxx",
            "result" : "pass",
            "http_code" : 204
         }
      ]
   },
   "last_successful_hb" : "2019-06-14T04:10:28Z",
   "time_now" : "2019-06-14T04:14:06Z"
}
```

VEN status connectivity field definitions

Field Name	Definitions
`connectivity`	JSON object containing most of the connectivity status fields
`ips_returned`	Number of IP addresses returned for the PCE name
`pce`	PCE name
`port`	PCE port number
`results`	Array containing the PCE IP address, the test result, and the HTTP code
`ip`	PCE IP address

Field Name	Definitions
`result`	Result of test ("`pass`" or an error message)
`http_code`	HTTP code received when the VEN attempted to connect to the PCE IP address
`last_successful_hb`	Timestamp of the last VEN heartbeat received by the PCE
`time_now`	Timestamp of the current local time

VEN 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. 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.

VEN Traffic Logging

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, which comes with the VEN, is used to query the flow log databases.

Linux/AIX/Solaris Database Query Examples

Query Type	Example
Non-aggregated accepted flows	`/opt/illumio_ven/bin/sqlite3 /opt/illumio_ven_data/log/flow.db "select * from flow_view"`

Query Type	Example
Non-aggregated dropped flows	`/opt/illumio_ven/bin/sqlite3 /opt/illumio_ven_data/log/flow.db "select * from drop_flow_view"`
Aggregated accepted flows	`/opt/illumio_ven/bin/sqlite3 /opt/illumio_ven_data/log/flowsum.db "select * from flow_view"`
Aggregated dropped flows	`/opt/illumio_ven/bin/sqlite3 /opt/illumio_ven_data/log/flowsum.db "select * from drop_flow_view"`

Window Database Query Examples

Query Type	Example
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 droppe-	`"c:\Program Files\Illumio\bin\sqlite.exe" c:\Program Data\Illumio\log\flowsum.db "select * from drop_flow_view"`

Query Type	Example
d flows	

List of Local Processes

The names of local process are captured in traffic flow data and stored in the PCE.

OS	Description
Windows	Indicates whether auto resize of the Conntrack table is required.
Linux, AIX, and Solaris	The VEN monitors the list of all processes with listening ports on TCP and UDP inbound connections, then matches process names to the list. Refreshes occur every 30 seconds. This process allows for a lower impact on the CPU.

The data can be exported in near-real-time to a Security Information and Event Management (SIEM) or another collector.

Tuning the IPFilter State Table (AIX/Solaris)

In versions 11.3 and earlier, you can tune the IPFilter state table for AIX and Solaris workloads. Solaris versions before 11.4, you must tune the IPFilter state table. In version 11.4 and after, you must tune the packet filter.

About State Table Tuning

In most environments, the state table default values are sufficient to handle the number of network connections encountered by Solaris and AIX workloads. However, if your system has a very large number of network connections, you might need to tune the state table. You can do so either before or after VEN activation. Tuning the state table values persists through rebooting, restarting, and suspending the VEN. For more information, see KB Article #2731, *IPFilter State Table Size in AIX* (login required).

By default, Solaris and AIX VENs are installed with the following state table values:

- `fr_statemax`: 1,000,000
- `fr_statesize`: 250,007

- `fr_state_maxbucket`: 256
- `fr_tcpclosed`: 120

Set a Custom IPFilter State Table Size

1. Create the following file on your Solaris or AIX workload as `root` or the Illumio VEN user, `ilo-ven`.

> NOTE:
> The file must be created by the `root` user or the Illumio VEN user, `ilo-ven`, and cannot be world readable or writeable.

2. Add the following settings and values to the file. Do not include spaces in the settings or values.

VEN File Setting	ipfilter Setting	Description
`IPFILTER_STATE_MAXX=<value>`	`fr_statemax`	Maximum number of network connections stored in the state table. You must also set `IPFILTER_STATE_SIZE`.
`IPFILTER_STATE_SIZEE=<value>`	`fr_statesize`	Size of the hash table. Must be a prime number. You must also set `IPFILTER_STATE_MAX`. **Recommended:** Set the hash table size to 1/4 of the number in `fr_statemax`. This setting allows each hash bucket to contain about 4 states.
`IPFILTER_STATE_MAXBUCKET=<value>`	`fr_state_maxbucket`	Number of allowed hash collisions before the VEN starts dropping network connections **Recommended:** Increase this value beyond the default value to avoid dropping network connections.
`IPFILTER_TCPCLOSEDD=<value>`	`fr_tcpclosed`	Option introduced and supported for Illumio Core 21.2.1

VEN File Setting	ipfilter Setting	Description
		VEN and later. To support NFS traffic so that the workload does not drop this traffic even when a rule exists in the PCE allowing the traffic. This issue occurs due to TCP port number reuse. **Recommended:** Illumio customers have found that setting the value for the IPFILTER_TCPCLOSED option to 2 (2 equals 1 second) resolved the issue.

NOTE:
If you set `IPFILTER_STATE_MAX`, you must also set `IPFILTER_STATE_SIZE`. If you add only one of these settings in the `illumio-agent` file, the VEN ignores the value and uses default values for both settings.

3. This step depends on whether the VEN has been activated.
   - If the VEN has not yet been activated, skip this step.
   - If the VEN has been activated, restart the VEN by entering the following command:

     ```
     /opt/illumio_ven/illumio-ven-ctl restart
     ```

4. Enter the following command to confirm the new values are configured for the state table:

   ```
   /usr/sbin/ipf -T fr_statemax,fr_statesize,fr_state_maxbucket
   ```

   The command output displays the values from the state table. In this example, the settings are still at the default values:

```
fr_statemax min 0x1 max 0x7fffffff current 1000000
fr_statesize min 0x1 max 0x7fffffff current 250007
fr_state_maxbucket min 0x1 max 0x7fffffff current 256
```

Manage Conntrack Table Size (Linux)

This topic explains how to manage the kernel firewall state table.

About Managing the State Table

Conntrack is only supported on Linux systems, and IPFilter is supported on AIX and Solaris before version 11.4. Both are system-specific names for the *Kernel Firewall State Table*.

- Linux workloads: Manage the Conntrack table.
- AIX or Solaris workloads, versions 11.3 and earlier: Manage the IPFilter state table.

  For more information about AIX and Solaris, see Tuning the IPFilter State Table (AIX/Solaris).

On Linux workloads, the VEN automatically increases and decreases the size of the Conntrack table as needed based on the number of active connections on the workload.

The VEN automatically increases the size to minimize the possibility of the workload running out of space in the Conntrack table and blocking valid connections.

The VEN uses the following behavior to manage the Conntrack table size:

- By default, the size of the Conntrack table starts at 1M. This is the baseline value. The baseline value is used as the starting point for automatically resizing the Conntrack table.
- Every 10 seconds, the VEN polls the table size to check the fill percentage.
- When the table reaches 80% of the maximum size, the VEN doubles the value set for the maximum size.
- The VEN doubles the maximum size value only 3 times (8x of the baseline value).
- For a 1M baseline value, the maximum table size after adjustment is 8M.

Customizing the VEN Adjustment Behavior

If the Conntrack table is experiencing issues with the size limit, you can adjust the way by which the VEN automatically manages the table size. Adjust the VEN behavior by setting the following values in the VEN configuration file `/etc/default/illumio-agent`.

Setting	Default	Description
`FW_STATE_TABLE_AUTO_RESIZE`	True	Indicates whether auto resize of the Conntrack table is required.
`CONNTRACK_MAX`	1000000	• Defines the maximum number of Conntrack table entries. • Configures the system value for `/proc/sys/net/nf_conntrack_max`
`CONNTRACK_HASH_SIZE`	256000	• Defines the starting size of the Conntrack hash table. • Configures the system value for `/sys/module/nf_con-`

Setting	Default	Description
		`ntrack/parameters/hashsize`

NOTE:
When you install a VEN on a Linux workload, this feature is enabled by default using the default values. If you customize the values in the `illumio-agent` configuration file before installing the VEN, the custom values will apply on installation. If you customize the values after installing the VEN, you must restart the VEN for the values to take effect in runtime.

Restrictions for VEN Adjustment

Customizing the VEN adjustment behavior has the following restrictions:

- The value you set for `CONNTRACK_HASH_SIZE` should be 25% of the value of `CONNTRACK_MAX`.
- You must set the values to 512 or higher. If you set a value below 512, the Linux kernel will automatically adjust the value to 512.

VEN Firewall Tampering Detection

The PCE distributes the latest policy applicable to each workload to ensure that the VEN receives the latest policy updates. The VEN internally creates and maintains a set of meta information of these rules, which it uses to detect tampering.

Automatic History of Firewall Changes

Changes to the firewall on a workload are historically recorded for an audit trail. Up to 10 changes to the firewall history are saved. The history is viewable via the PCE Support Reports.

Host Firewall Tampering Protection

If a host firewall is tampered with, firewall tampering protection start firewall validation procedure. If the outcome detects any of the Illumio-added rules have been tampered, then the restoration procedure starts.

The procedure attempts to fetch a new security policy from the PCE, but if it fails due to a network connectivity issue, you can try to recover your last known good copy of a policy stored locally. The last step is validating the policy against the meta information of the policy. The tampering attempt is reported to the PCE as an `agent.tampering` event.

A host firewall tampering event occurs when another administrator or an attacker:

- Adds a firewall rule to the Illumio firewall compartment.
- Modifies a firewall rule added by Illumio.
- Deletes a firewall rule added by Illumio.
- Deletes all firewall rules (flush) added by Illumio.

The norm is that Illumio tries to detect tampering attempts only to Illumio firewall policy only and not to others.

Workload OS	Tampering Detection
Linux	The VEN monitors any underlying iptables and ipset changes. Once the VEN detects a tampering attempt, it validates the snapshot of iptables/ipset against the firewall policy validation meta information.
Windows	The VEN monitors any changes in Windows Filtering Platform (WFP) layer. If it detects a change, it starts the validation and restore procedure.
AIX/Solaris	On AIX (all versions) and Solaris (versions before 11.4) , the VEN monitors any underlying ipfilter changes. Once the VEN detects a tampering attempt, it validates the snapshot of ipfilter against the firewall policy validation meta information. On Solaris versions 11.4 and later, the VEN checks packet filter. On AIX and Solaris, the feature is enabled by default and updated every 10 minutes.

Host Firewall Tampering Alerts

Host firewall tampering alerts can be viewed:

- On the host VEN.
- In the PCE web console.
- In the return from a call to the `/events` Illumio Core REST API.
- In the return from a query in Splunk or other SIEM software.

View Tampering Alerts on VEN Host

Workload OS	Procedure
Linux	As root, separately execute the following commands:

Workload OS	Procedure

	Tail the VEN log file to see suspected tampering events and hash comparisons:
	`$ tail -f /opt/illumio_ven_data/log/platform.log`
	`INFO: Possible tamper detected...`
	`INFO: FW iptables checksums ... (compares security policy hashes to see if anything changed)`

Windows	Check `\programdata\illumio\log\platform.log` and search "`!!!Tampering detected`" NOTE: This alter displays "Filtering Platform Policy Change" when a tampering event is detected. Double-click the alert for detailed information.

View Tampering Alerts Sent to PCE

PCE Web Console

To view `agent.tampering` events in the PCE web console, navigate to **Troubleshooting > Events**.

Double-click an `agent.tampering` event to see its details.

Illumio Core REST APIs

To return all tampering events for an organization, execute the following command using your organization URI. For more information, see Events in the *REST API Developer Guide*.

Example Curl Command to Get Information for All `agent.tampering` Events:

```
$ curl -i -X GET https://pce.example.com:8443/api/v2/orgs/1/events/?event_type=agent.tampering -H "Accept: application/json" -u $KEY:$TOKEN
```

Example Curl Command to Get Information for a Specific `agent.tampering` Event:

```
$ curl -i -X GET https://pce.example.com:8443/api/v2/orgs/1/events/some_
event_ID -H "Accept: application/json" -u $KEY:$TOKEN
```

Example JSON Response Body from Getting an `agent.tampering` Event:


```
{
    "href": "/orgs/1/events/some_event_ID",
    "timestamp": "2019-06-17T05:42:10.419Z",
    "pce_fqdn": "someName.someDomain",
    "created_by": {
        "agent": {
            "href": "/orgs/1/agents/xxxxx",
            "hostname": "someHostname"
        }
    },
    "event_type": "agent.tampering",
    "status": "success",
    "severity": "err",
    "action": {
        "uuid": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
        "api_endpoint": "FILTERED",
        "api_method": "PUT",
        "http_status_code": 204,
        "src_ip": "xx.xxx.xx.xx"
    },
    "resource_changes": [],
    "notifications": [
        {
            "uuid": "yyyyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyyyy",
"notification_type": "workload.oob_policy_changes",
            "info": {
                "tampering_revert_succeeded": true,
                "beginning_timestamp": "2019-06-17T05:42:10Z",
                "ending_timestamp": "2019-06-17T05:42:10Z",
                "num_events": 1
            }
        }
```

```
    ]
}
```

Splunk or Other SIEM Software

If you send VEN events received by the PCE to Splunk or other SIEM software, query for `agent.tampering` events in accordance with the SIEM vendor's query procedures.

VEN Support Reports

A VEN support report provides diagnostic information for selected workloads. To troubleshoot issues with your workloads, you can generate a support report and send it to Illumio support.

> NOTE:
> Your PCE user account must have the Organization Owner or Admin user role to perform this task and the workload should be an active, managed workload.

Generate Support Report from PCE

To generate a VEN support report from the PCE web console:

1. In the PCE web console, go to **Workloads and VENs**, then **VENs**. The page displays your installed VENs.
2. Click the **Workloads** tab.
3. Click a workload and scroll to the bottom of its **Summary** page.
4. Click **Generate Report**. This process can take up to 10 minutes.
5. To view the status of the report, click the **Support Reports** link, which opens the **Support Reports** page. Displays the 50 most recent reports that you have generated.
6. Click the **Download** to download a report.

Generate Linux/AIX/Solaris Support Report Using CLI

If you need to troubleshoot VEN issues, you can generate a support report from the command line for any workload and then send the report to Illumio support.

On Linux, AIX, and Solaris, the generated report is saved to the `/tmp` directory and overwrites any previously generated copy of the same report.

NOTE:
You must have root privileges on the workload to run the support report command.

You can also run a support report when you unpair a workload.

To generate a VEN support report for a Linux workload:

1. Establish a secure shell connection (SSH) to the Linux workload.
2. Execute the following command as root to generate the support report.

```
/opt/illumio_ven/illumio-ven-ctl gen-supportreport
```

3. Type Y when asked if you want to run the report.
4. Optionally, if you want to bypass the confirmation prompt, you can execute the script with a `-y` or `-Y` option:

```
/opt/illumio_ven/illumio-ven-ctl gen-supportreport -y
```

5. To view the report generation log, enter the following command:

```
more -n 10 -f /opt/illumio_ven_data/log/report.log
```

6. The support report generation is complete when "Successfully created report" or "Failed to create report" is logged. After the report is successfully generated, the report is sent to the PCE.

Generate Windows Support Report Using CLI

If you need to troubleshoot VEN issues, you can generate a VEN support report from the command line for any workload and then send the report to Illumio Customer Support.

On Windows, the generated report is saved to the `C:\Windows\Temp` directory and overwrites any previously generated copy of the same report.

You can also run a support report when you unpair a workload.

To generate a VEN support report for a Windows workload:

1. Open PowerShell on a Windows workload.
2. Enter the following command to set the PowerShell execution policy:

```
Set-ExecutionPolicy -Scope process remotesigned -Force; Start-Sleep -
s 3
```

3. Run the support report command:

```
& "${Env:ProgramFiles(x86)}\Illumio\Admin\supportreport.ps1"
```

4. Optionally, if you want to bypass the confirmation prompt, you can execute the script with the `yes` option:

```
& "${Env:ProgramFiles(x86)}\Illumio\Admin\supportreport.ps1" yes
```

5. To monitor the status of the report, enter the following command:

```
Get-Content "${Env:ProgramData}\Illumio\log\report.log" -Wait
```

6. The support report generation is complete when "Successfully created report" or "Failed to create report" is logged. After the report is successfully generated, the report is sent to the PCE.
7. To reset the PowerShell execution policy, enter the following command:

```
Set-ExecutionPolicy -Scope process undefined -Force
```

VEN Troubleshooting

This topic describes some important system administration considerations on Windows, useful tools, and a generalized set of actions to troubleshoot VEN operations.

Windows: Enable Base Filtering Engine (BFE)

Windows BFE is a Windows subsystem that determines which packets should be allowed to the network stack. BFE is enabled by default. If you disable BFE on your Windows workload, all packets are sent to the TCP/IP stack bypassing BFE which can result in different behavior from one system to another. The worst case scenario is all the ingress and egress packets get dropped.

If you have disabled BFE on your Windows workload, re-enable it.

Linux: ignored_interface

The Linux `ignored_interface` inhibits PCE policy updates.

Transitioning an enforced workload's interface from or to `ignored_interface` might drop the dynamic, long-lived connections maintained by the system.

When a VEN interface is placed in the `ignore_interface` list, the any flow state over the interface won't be kept by conntrack an longer. (The conntrack table on Linux stores information on 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 implements any policy sent by lightning bolt from the PCE.

VEN Troubleshooting Tools

Illumio provides the following tools for VEN connectivity checking and troubleshooting VEN issues on workloads:

- 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 VEN Compatibility Check in the VEN Installation and Upgrade Guide.

Commands to Obtain Firewall Snapshot

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

Linux

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

Windows

- `netsh wfp show state`

Solaris

```
ipfstat -ionv
```

AIX

```
ipfstat -ionv
```

Troubleshooting Tips

Connectivity Issues

Perform the following actions to identify why a workload is unreachable, cannot reach other workloads, or cannot communicate with the PCE:

- Determine if all workloads are unable to communicate or just a subset of the workloads are reported as disconnected. If the PCE reports that all workloads are offline, check if PCE is reachable from workloads.
- 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.
- Check if any workloads that are unable to communicate are located behind NAT devices, firewalls, or remote data centers.
- Ensure that outbound TCP port 443 and 444 on the workloads are opened to the PCE.
- If running in a public cloud instance:
  - For AWS, ensure security groups permit TCP ports 443 and 444.
  - For Azure, ensure that Endpoints are configured to allow traffic.

VEN Process Issues

Check the status of the VEN-specific processes and ensure that they are running and active:

- **Linux:** Run `/opt/illumio/illumio-ven-ctl status`
- **Windows:** Execute `get-service` in the PowerShell

Ensure the following processes are running and active:

- **Linux:** `venAgentManager`, `venPlatformHandler`, `venAgentLManager`, `VtapServer`, and `AgentMonitor`
- **Windows:** `venAgentLogMgrSvc`, `venPlatformHandler`, `venVtapServerSvc`, and `ilowfp`

Errors in the VEN Logs

Review the VEN 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 *`

To check for firewall updates, view the `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
```

- Check heartbeat logs for records related to update messages from the PCE. See the following 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 "0x800000000000025f " --
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
```

Policy Sync Might Require Reboot

Persistent errors with policy sync on a workload can be cleared by rebooting the VEN.

Event Viewer Stops Logging

After you upgrade the VEN, **Event Viewer** can stop logging so that the support report does not include `windows_evt_application`, `windows_evt_system`, and the system directory (e.g.: `msinfo32`). To correct the issue, close **Event Viewer** before upgrading the VEN. Then reopen **Event Viewer**.