Illumio Adaptive Security Platform 18.2 VEN Deployment Guide

09/19/2018

Table of Contents

Product Version

Illumio® Adaptive Security Platform®

Current PCE Version: 18.2.0

Current VEN Version: 18.2.0

Note: 18.2.0 is not a Long Term Support (LTS) release. A future 18.2.x maintenance release will be designated as a LTS release.

About Illumio

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

Illumio Professional Services for Deployment

To ensure optimal deployment of the Illumio Adaptive Security Platform you should work with Illumio Professional Services. Contact your Illumio representative.

Preview Features Only for Evaluation Before General Availability

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

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

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

Illumio Adaptive Security Platform Training

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

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

Search Knowledge Base and Documentation

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

Illumio Adaptive Security Platform Support

If you cannot find what you are looking for in this document or the support knowledge base and documentation, contact us at:

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

Recommended Skills

Illumio recommends that you be familiar with the following topics:

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

Related Documentation

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

- *Policy Compute Engine (PCE) Web Console Guide*: working with Illumination®, designing security policy, and provisioning and administering VENs.
- *Policy Compute Engine (PCE) Deployment Guide*: planning and installing the PCE.
- *Policy Compute Engine (PCE) Operations Guide:* common management tasks of the PCE.
- *Policy Compute Engine (PCE) Supercluster Deployment and Usage Guide*: designing, deploying, and managing the PCE Supercluster of multiple, distributed standard PCE clusters.
- *Policy Compute Engine (PCE) REST API Guide*: web-programming Illumio® Adaptive Security Platform®.
- *Virtual Enforcement Node (VEN) Deployment Guide:* installing and activating the VEN, including PCE-based distribution of the VEN and on-worload installation and management

- *Virtual Enforcement Node (VEN) Operations Guide*: common management tasks of the VEN.
- *Auditable Events and SIEM Integration Guide*: analyzing significant events on the PCE and VEN and securely transferring event records to a nalytics or Security Information and Event (SIEM) systems.

Notational Conventions

- Newly introduced terminology is *italicized*. Example: *activation code* (also known as *pairing key*).
- `Command-line` examples are `monospace`. Example: `illumio-ven-ctl --activate`.
- Arguments on command lines are *`monospace italics`*. Example: `illumio-ven-ctl --activate` *`activation_code`*.
- In some examples, the output might be shown across several lines but is actually on one single line.
- Command input or output lines not essential to an example are sometimes omitted, as indicated by three periods in a row:
  ```
  ...
  some command or command output
  ...
  ```
- Section titles in this guide are in double quotation marks. Example: See "Basic Theory of Operation".
- Reference to other guides n the Illumio library are *italicized*. Example: See the *PCE Web Console User Guide*.

How To Use This Guide

This guide shows you how deploy the Virtual Enforcement Node (VEN) on your distributed, on-premise systems.

The guide includes details on the following:

- Two VEN deployment models of VEN: PCE-based or standalone.
- Interactions with the ASP Policy Compute Engine (PCE).
- Standalone VEN installing, uninstalling, upgrading, activating, and deactivating the VEN.

VEN Deployment Overview

Central to Illumio Adaptive Security Platform is the Policy Compute Engine (PCE) and Virtual Enforcement Node (VEN), a lightweight software agent you install on systems to make them managed workloads.

The VEN analyzes the workload and determines the operating system, IP address details, protocols, and processes listening on ports. The VEN sends that context to the Policy Compute Engine (PCE).

The PCE computes security policies to enforce on the VEN. The PCE and VENs monitor and adapt security to changes.

You can activate VEN either during installation or after installation. The VEN reports workload information to the PCE, such as all services on the workload, all open ports, details about the operating system, and workload location.

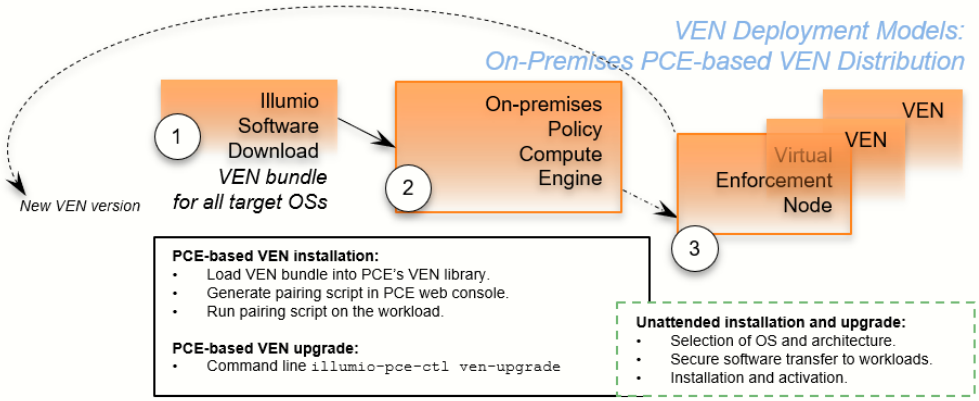
VEN Deployment Models

The VEN has two deployment models. The two models for VEN deployment are nearly identical and achieve the same goal: VEN installation and upgrade.

- Integrated VEN deployment from an on-premises PCE. This is called *PCE-based VEN deployment*.
- Manual VEN installation on individual workloads with your own software deployment tools. This is called *standalone VEN installation.*

On-Premises PCE-Based VEN Deployment

The PCE-based VEN deployment model is more automated than the standalone VEN deployment model but gives you less control over optional aspects of VEN installation and upgrade.



The PCE-based deployment model starts with a *VEN software bundle*. A VEN software bundle is a collection of a particular VEN software version for all supported workload OSs.

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

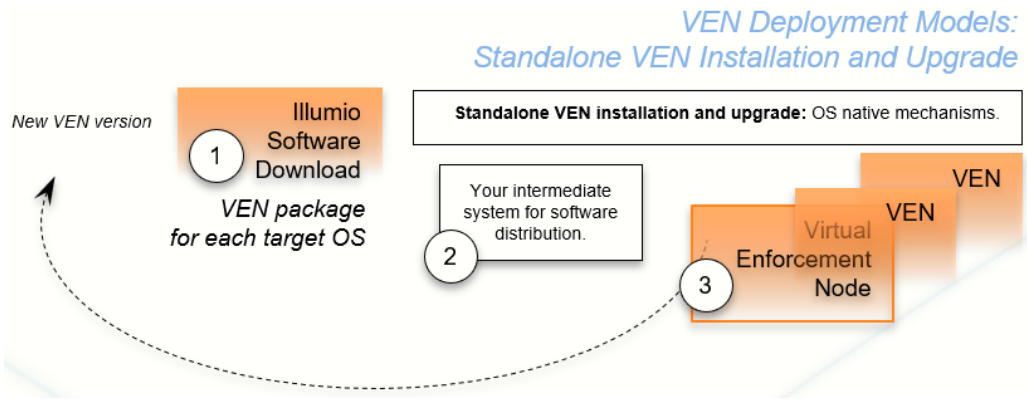
    - Installs the VEN software.
    - Activates/pairs the VEN with its PCE.
- For VEN upgrade, on the on-premises PCE command-line, you run `illumio-pce-ctl ven-upgrade` for either all workloads or selective workloads.
- Some features are not available with PCE-based deployment, such as Kerberos support and custom settings with environment variables.

The PCE-based deployment feature is:

- Optional.
- Available for the RPM, Debian, and Windows distributions of the VEN software. Other workload operating systems are not supported.
- Available only for PCE and VEN version 18.2 and later.

Standalone VEN Installation and Upgrade

It gives you great control over optional aspects of VEN installation, activation, and upgrade.



The standalone VEN installation model starts with downloading a *VEN package*. A VEN package is the VEN software for a single supported workload OS and CPU architectures. Installation and upgrade rely on standard native OS tools.

- For VEN installation with the standalone model:
    - You determine the OS and CPU architecture of the target workloads and download the appropriate single VEN packages.
    - You are responsible for securely transferring the VEN software to the target workload with your own software deployment mechanisms.
    - You can set environment variables or command-line options for custom installation directories and custom user and group names. You can also set up Kerberos-based authentication for VEN to PCE communications.
    - You run native OS mechanisms.
    - You activate/pair the VEN with its PCE either during or after installation.

    - You can use a "prepare script" to install the VEN software on machine images and activate it at the next boot.
- For VEN upgrade, with the workload command line, you run native OS mechanism.

When to Use Which Deployment Model

You can use both models at different stages of your rollout of the VEN. Here are some suggestions:

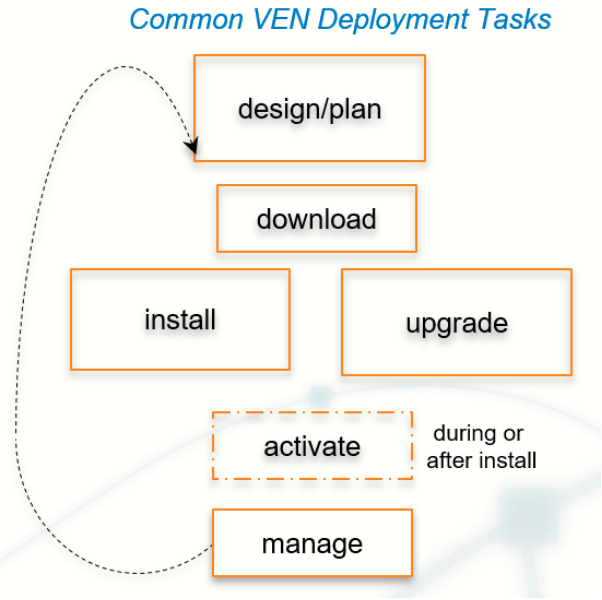
- The PCE-based VEN deployment model is suitable for proof-of-concept implementations or quick deployments.
  Use this model to evaluate and certify new versions of the VEN software.
- The standalone VEN installation model is suitable for production deployments.
  After certification, you can use your own in-house software distribution mechanism to install or upgrade individual workloads.

Migration to PCE-Based VEN Deployment

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

Common VEN Deployment Tasks

Below is a cyclical view of many common VEN deployment tasks.



VEN Logical Software Architecture and Theory of Operations

For details about the VEN logical software architecture, associated components, the basic theory of VEN operations, and other aspects of the VEN, see the *VEN Operations Guide*.

VEN Deployment Planning and Prerequisites

Before you install the VEN, consider the details in this section.

VEN Deployment Planning Checklist

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

On-premises PCE Deployment	Step	Standalone Installation and Upgrade
X	Decide on VEN deployment model.	X
X	Remove parameters `ven_repo_url` and `ven_repo_ips` from PCE `runtime_env.yml`.	

On-premises PCE Deployment	Step	Standalone Installation and Upgrade
X	Required communications between PCE and VEN.	X
	Operating system and package dependencies.	X
X	Download the VEN software: • On-premises PCE deployment: All VEN versions in a VEN software bundle. • Standalone installation/upgrade: All VEN versions in a package of VEN software for specific OS versions and CPU architectures.	X
	Optional -- Verify signature of downloaded packages against Illumio's public key.	X
Automatic	Determine VEN software package for workload CPU architecture.	X
	Decide to activate the VEN during or after VEN installation.	X
	Decide type of activation code for VENs: one-time use per workload or unlimited multiple uses.	X
X	Generate VEN pairing profiles and activation codes (pairing key).	X
X	Securely copy VEN paring script to workload.	X
	Optional -- Prepare VEN-unactivated golden master machine Images.	X

PCE-based Deployment – Remove PCE Runtime Parameters

For the PCE-based VEN deployment model, after you have migrated from any external VEN repo you might have, remove the following parameters from the PCE `runtime_env.yml` file:

- `ven_repo_url`
- `ven_repo_ips`

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

Required Communications between PCE and VEN

Before deploying the VEN, be sure your installed PCE and the VENs can communicate properly. The following requirements are only a few of the requirements detailed in the *PCE Deployment Guide:*

- The workload can validate its SSH certificate's chain of trust back to the root Certificate Authority (CA) of the server certificate on the PCE.
- The VEN can reach the PCE on the ports configured for the PCE configured in the PCE runtime environment file `runtime_env.yml`.
- To prevent time drift between the PCE and VENs, Network Time Protocol (NTP) must be installed and working on the PCE and the VENs.

Operating System and Package Dependencies

The VEN is supported on the operating systems detailed on Illumio support site.

Download the VEN

All VEN software is on Illumio support site. Go to the Software page and select the desired version of Illumio Advanced Security Platform VEN.

PCE-based VEN deployment software bundle	Standalone VEN software packages
Download the VEN software **Bundle** to a location on a PCE core node or to any system that can be reached from your PCE core node with HTTP, SFTP, or SCP.	Download the **RPM** packages to a convenient location.

Decide Type of Activation Code

For activation, you need an *activation code* for the VENs. The activation code is also known as a *pairing key*. The activation code is an identifier passed to the VEN software at activation.

An activation code can be created for one-time use on a single workload or multiple uses for many workloads.

You can get an activation code in the following ways:

- In the PCE web console, create a Pairing Profile. In the profile, you can specify one-time use or unlimited use for the activation code.
- With the REST API.

With the standalone deployment model, you can use the activation code either during installation or after installation.

Planning Considerations for the VEN Standalone Installation

These sections describe planning/prerequisite information that applies to the VEN standalone installation directly on workloads. These details are not necessary for PCE-based VEN deployment.

Optional – Verify signature of downloaded standalone packages

For security of the standalone VEN deployment, you can optionally verify the identity of the downloaded VEN packages against Illumio's public key.

- Signature verification is available for VENs delivered in RPM format for CenOS/RHEL, Ubuntu, and SUSE.
- It is not available for AIX, Debian, Solaris, or Windows.

You can get Illumio's public key from the Illumio Support site.

Steps to verify against the public key depend on what tools you want to use. See this information for RedHat.

Determine Standalone VEN Package CPU Architecture

For the standalone VEN installation, after you have downloaded and unpacked the software, determine the VEN appropriate for your OSs.

File naming conventions indicate OS and CPU architecture.

Platform	OS Variant	CPU Architecture Identifier
AIX	AIX 6.1, 7.1, 7.2	64 bit: **ppc64**
Linux	Amazon Machine Image	• 32-bit: **c6.i686** • 64-bit: **c6.x86_64**

Platform	OS Variant	CPU Architecture Identifier
	Debian 7 Wheezy, Debian 8 Jessie, Debian 9 Stretch	• 32-bit: **d7.i386** • 64-bit: **d7.amd64**
	RedHat/CentOS 5.x	• 32-bit: **c5.i686** • 64-bit: **c5.x86_64**
	RedHat/CentOS/Oracle 6.x	• 32-bit: **c6.i686** • 64-bit: **c6.x86_64**
	RedHat/CentOS/Oracle 7.x	64-bit: **c7.x86_64**
	Ubuntu 12 Precise	• 32-bit: **u12.i386** • 64-bit: **u12.amd64**
	Ubuntu 14 Trusty	• 32-bit: **u14.i386** • 64-bit: **u14.amd64**
	Ubuntu 16 Xenial	• 32-bit: **u16.i386** • 64-bit: **u16.amd64**
Solaris	• Solaris Sparc 11.1, 11.2, 11.3, 10 (U8 or later) • Solaris x86 11.1, 11.2, 11.3, 10 (U8 or later)	64-bit: **sparcv9** 64 bit: **x86_64**
Windows	Windows 2008 R2 SP1, 2012, 2012 R2	• 32-bit: **x86** • 64-bit: **x64**

Optional -- Preparing VEN-unactivated Golden Master Machine Images

If you create machine images for faster deployment of the VEN, consider preparing them to activate the VEN the first time the workload is booted. See "Preparing Golden Master Images for Workload Deployment".

PCE-based Installation and Upgrade of VEN Software

You can use your on-premises PCE cluster as a centralized mechanism for distributing, installing, and upgrading VENs in your organization.

The PCE-based deployment feature is:

- Optional.
- Available for the RPM, Debian, and Windows distributions of the VEN software. Other workload operating systems are not supported.
- Supported only for PCE and VEN version 18.2 and later.

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

The high-level process for PCE-based VEN deployment is as follows:

1. Download the version of the VEN software bundle to distribute.
2. Load the VEN deployment into one of the PCE core node's VEN Library. From this node, the VEN software bundle is automatically copied to the other nodes.
3. Install or upgrade VENs:
    a. To install the VEN software on workloads, with the PCE web console, generate a pairing script.
    b. To upgrade all VEN workloads or selective workloads, use the PCE command line.

No Explicit Configuration Necessary

You do not have to make any configuration changes or other settings to enable PCE-based VEN deployment.

Loading the VEN bundle into the PCE's VEN library enables the PCE-based deployment of the VEN. See also "Set a default VEN Version".

Decide Where to Download VEN software bundle

Decide on a system where you want to download the VEN software bundle. Download it to one of the PCE core nodes or to a system that is accessible from a PCE core node via HTTP, SFTP, or SCP.

Determine Desired VEN software bundle

Determine which VEN software versions to distribute.

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

Download VEN software bundles from Illumio Web Site

Download the VEN software bundles for all VEN versions you require to load into the PCE.

1. In your browser, navigate to Illumio's software download page.
2. Select the desired version of Illumio ASP.
3. From the VEN table, select **Linux RPM/DEB and Windows MSI**.
4. Download all the VEN software bundles you need to distribute to a convenient directory on your PCE core node or to any system that your PCE can reach with HTTP, SFTP, or SCP.

   You do not need to unpack the VEN software bundle
5. Repeat this step for all versions of the VEN versions you want to distribute.

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

Load the VEN Software Bundle into PCE VEN Library

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

Loading the VEN software bundle into the PCE's VEN library is what configures the PCE as the VEN deployment mechanism.

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

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

   where:

   - *protocolAndFqdnOfVenBundleHost/nameOfVenSoftwareBundleFile* `.` `tar.bz2` is any of the following:

    - The absolute or relative path to a directory on the PCE where you downloaded the VEN software bundle.
    - An HTTP URL to a host and file where you stored the downloaded VEN software bundle.
    - An SFTP URL to a host and file where you stored the downloaded VEN software bundle.
    - An SCP URL to a host where you stored the downloaded VEN software bundle.
- *nameOfVenSoftwareBundleFile*. `tar.bz2` follows this pattern:

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

  where *someVersionStamp* is the version and build number of the Illumio Adaptive Security Platform release.

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

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

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

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

Release version_of_bundle Successful.
```

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

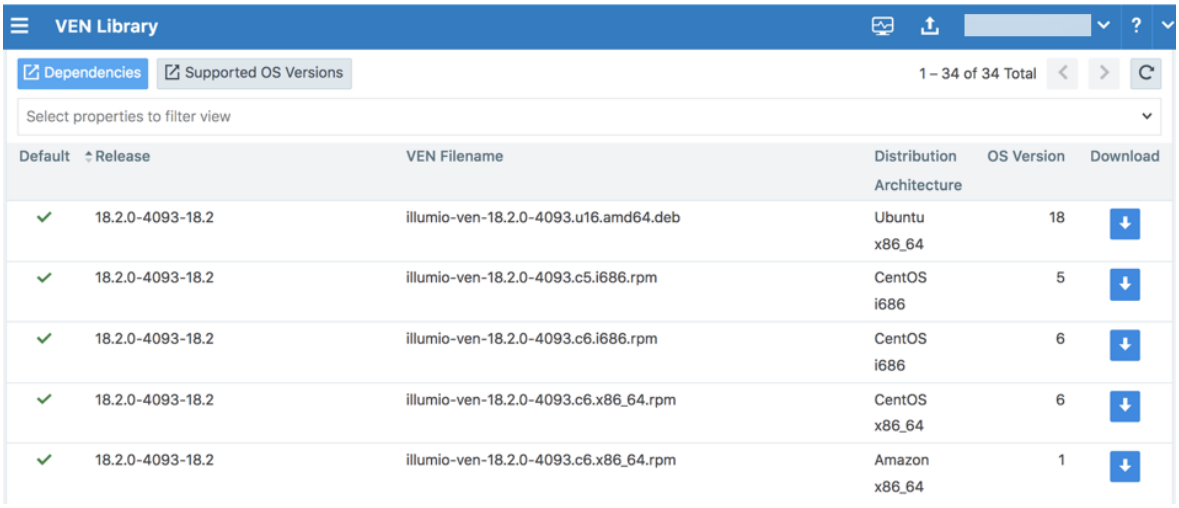
- HTTP:
  `illumio-pce-ctl ven-software-install http://myVENrepohost.BigCo.com/myRepoDir/pcerepo/illumio-ven-repo-`*`someVersionStamp`*`.tar.bz2`
- SCP:

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

View Loaded VEN Library

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

- In the PCE web console, look at the VEN library. Navigate to **Troubleshooting > VEN Library**.



- On the PCE command line, run the following command:

```
illumio-pce-ctl ven-software-releases-list
```

Setting Default VEN Version

There are to ways to set a default version of the VEN software: either for all workloads or for selected pairing profiles. These two methods can be used simultaneously. For example:

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

Set default VEN version for all workloads

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

```
illumio-pce-ctl --ven-software-release-set-default ven_release_id
```

where:

- *ven_release_id* is the release ID displayed by the `illumio-pce-ctl ven-software-releases-list` command. See "Verify Loaded VENs".

Set default VEN Version for a Specific Pairing Profile

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

To set a pairing profile's VEN version, see the PCE Web Console User Guide.

For details about pairing scripts, see "Pairing Profiles, Pairing Scripts, and Prepare Scripts".

VEN Installation/Pairing and Upgrade

These are some general considerations for installing and upgrading VENs with the PCE.

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

Installing VENs – PCE Web Console and On the Workload

Installing the VEN via the PCE is a two-step process. For each workload:

1. In the PCE web console, generate a pairing profile and its corresponding pairing script.

   See the *PCE Web Console User Guide*.
2. Copy that pairing script to the workload and run it.

   See "Pairing Profiles, Pairing Scripts, and Prepare Scripts".

Upgrading VENs – PCE command line

Upgrade is initiated on any core PCE node with the control program:

```
illumio-pce-ctl ven-upgrade
```

Upgrade All VENs with the default VEN version

To upgrade all VENs in your deployment, run the following command on a PCE core node. This example upgrades all VENs to the defined default VEN version.

```
$ illumio-pce-ctl ven-upgrade --all --default

 Reading /opt/pce_config/etc/runtime_env.yml.
VEN upgrade initiated.
```

Upgrade Selective VENs

To upgrade selective VENs, use the Illumio REST API to obtain a list of the specific VEN workload IDs and specify those workload IDs to the `illumio-pce-ctl` control script on the PCE.

1. With the following Illumio REST API URIs, get the workload IDs of the target VENs:
   - All workloads: `GET [api_version][org_href]/workloads`
   - Single workload: `GET [api_version][org_href]/workload`

     For exact syntax, see the *REST API Guide* .
2. From the response body, extract the `agent` 's `href` value to get the workload UUID. The workload UUID is the final word of the `href` value. See the example below.
3. Specify the VEN workload IDs in a comma-separated value list on the command line with `illumio-pce-ctl ven-upgrade --ven-ids` *`ven_ids`*.

Example. The following example snippet of the response shows the workload UUID `8351` :

Example of API response showing workload UUID

```
...
  "agent": {
      "config": {
        "log_traffic": false,
        "visibility_level": "flow_summary",
        "mode": "enforced"
      },
      "href": "/orgs/2/agents/8351",
      "status": {
...
```

The following example command upgrades three VENs to the defined default VEN version. The VENs are identified by workload UUIDs in a CSV list as an argument to the `--ven-ids` option:

```
illumio-pce-ctl ven-upgrade --ven-ids 8351,9944,2223
```

PCE Maintenance for VEN Deployment

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

About PCE backups

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

Addition, Deletion, or Failure of Nodes of the PCE Cluster: VEN Redeploy

If you need to add or replace one of core nodes to your PCE cluster, you need to redeploy the VEN library to the new core node. After adding or replacing a node, redeploy the VEN library with the following command on the core node that still has the VEN library:

```
illumio-pce-ctl ven-software-redeploy
```

About Complete PCE failure

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

Other VEN-related maintenance commands on PCE

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

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

Standalone Install/Upgrade AIX VEN

This section discuss the standalone model for installing and upgrading the VEN for AIX.

AIX VEN Known Limitations and Considerations

- AIX 5.3 is not supported.
- IPFilter:
    - Before you install the AIX VEN, install the Illumio-provided IPFilter package.
    - Before you install the AIX VEN, IPFilter packet filtering must be disabled. Illumio provides a custom IPFilter package for managing the packet filtering rules.
    - Before you install the AIX VEN, install the Illumio-provided IPFilter.Avoid any changes to packet filtering with genfilt, mkfilt and other such network tools. Do not perform any such operation while VEN software is installed.
    - IPsec is not supported with the required Illumo-provided IPFilter that must be installed before installation of the AIX/VEN.
- The AIX system's state table limit is 65,536 entries. If that limit is reached, IPFilter drops packets. Correct the issue by increasing the state table limit.
- The AIX VEN does not support Kerberos authentication.
- The AIX VEN does not Support SecureConnect and SecureConnect Gateway.

Contents of tar File

The tar file contains:

- The AIX VEN in Backup File Format (BFF) format.
- A custom, Illumio-supplied IPFilter.

Changing Default Username before AIX VEN Installation

Before installing the VEN on AIX, you can set an environment variable to change the username that owns and runs the installed software.

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

Write-Protected Home Directory – Pre-Create Username

At installation, the VEN attempts to create the home directory for its default username `ilo-ven` or for any custom username you specify at installation. If the VEN user's home directory is write-protected or its parent directory does not exist, the installation fails.

Some examples of this problem:

- If users' home directories are on a write-protected automounted file system, the installation fails.
- If `/home` does not exist, the installation fails because the VEN's home directory cannot be created.

Workaround:

- Before installation, create the desired username, group, and home directory.
- Make sure this user has write permission on the `/home` directory so that its own subdirectory can be created.

Illumio-provided IPFilter for AIX

For the AIX VEN version 17.1.2 and later, Illumio provides a custom IPFilter package to correct problems in IBM's IPFilter versions 5.3.0.4 and 5.3.0.6.

The Illumio-provided IPFilter version 5.3.0.5000 resolves the following issues:

- Removes a former limit of a maximum 68 IP addresses per IPset.
- Corrects a bug in IBM's ipflt extension.

Install IPFilter before the VEN
Before installing the AIX VEN, install this IPFilter package.

Support for IPFilter

IBM has discontinued support and development of IPFilter and has put IPFilter on GitHub as an open source project.

- Illumio supports the Illumio IPFilter.
    - The IPFilter is included in the AIX VEN installation package.
    - The Illumio IPFilter package will not be made public. Permissive licensing of IPFilter does not require that modifications of open source software be made public.

    - Illumio can provide the IPFiltersource code patches for bug-fixes and improvements upon request to your Illumio representative.
- IBM supports the underlying AIX operating system.

Steps to Upgrade to Illumio IPFilter version 5.3.0.5000 and Start the VEN

To install the IPFilter package on AIX, install the AIX VEN, and start the AIX VEN:

1. Illumio's custom IPFilter package is included with the VEN installation package, which is downloadable from the Illumio support site.
2. Stop the VEN:

   ```
   illumio-ven-ctl stop
   ```
3. **Mandatory:** Uninstall the IBM iFIX for `ipfl`.

   In an earlier release, Illumio had recommended installation of some iFIXes.

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

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

4. Stop the IBM ipfl kernel extension using the following command:
   `/lib/methods/cfg_ipf -u`
   Run this command repeatedly *until it fails with the following error*:

   ```
   No such device.
   ```

   If the command fails with the error `Device Busy`, before continuing these steps, reboot the system.
5. Change directory to where you downloaded the AIX VEN and the IPFilter package.
6. Upgrade with Illumio's custom IPFilter:
   ```
   inutoc . && installp -acYd . ipfl
   ```

7. Upgrade the AIX VEN:
   ```
   inutoc . && installp --acd . illumio-ven
   ```

8. Start the AIX VEN:
   ```
   illumio-ven-ctl start
   ```

Steps to install or upgrade the AIX VEN

1. Log in to the AIX host and become superuser.

2. Download https://public.dhe.ibm.com/aix/freeSoftware/aixtoolbox/RPMS/ppc/zlib/zlib-1.2.11-1.aix6.1.ppc.rpm
3. Install zlib: `rpm -ivh zlib-1.2.11-1.aix6.1.ppc.rpm`
4. Install Illumio's custom IPFilter. See "Illumio-provided IPFilter for AIX".
5. Copy your trusted root CA certificate in the following directory with a filename `ca-bundle.crt`. This path must be exactly as shown.
   `/var/ssl/certs/ca-bundle.crt`
6. Install the VEN package on the AIX host by entering the following commands, where *`path_to_bff_file`* is the directory where you copied the AIX VEN BFF file.
   ```
   # inutoc path_to_bff_file
   # installp -acXgd path_to_bff_file illumio-ven
   ```

Upgrading AIX VEN from 17.1.x releases

- **Not Supported**: VEN version 18.2 does not support direct upgrade from v17.1.0, because the packaging format changed from rpm to LPP.
- **Supported**: VEN versions 18.2 and 17.1.2 support upgrade from 17.1.1.
  - Before upgrading, be sure to stop the VEN.
  - If the upgrade fails, rollback to 17.1.1.

Boot Scripts Installed at VEN Installation

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

Activate an AIX VEN After Installation

Important: Before activating the VEN on AIX, edit the file in the /etc/protocols directory to support the GRE and IPIP protocols. If the GRE and IPIP protocol lines are commented out, un-comment them.

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

At a minimum, to activate the AIX VEN using the VEN control script, you need the hostname or IP address of the PCE, an activation code (called a pairing key in the PCE web console) generated from a Pairing Profile, and any other available options, such as the Workload policy state, Label assignment, Workload name, and more. For information about obtaining an activation code from the PCE web console, see “Pairing Profiles” in *Illumio PCE Web Console Users Guide*.

```
$ illumio-ven-ctl activate --management-server <pce_fqdn:port> --activation-code <code>
```

See the following example command:

```
$ /opt/illumio_ven/illumio-ven-ctl activate --activation-code xyzzyeb573ae7ca98bcd71eexyzzyc52077d --
management-server pce.mycompany.com:8443
```

Standalone Install Linux VEN

This section discuss the standalone model for installing and upgrading the VEN for Linux.

- Installing the VEN on Linux relies on the standard syntax on the `rpm` or `dpkg` command-lines.
- Root access on the workload is required for installation of the Linux VEN.
- Some of the optional installation features in the RPM are not available with the Debian package. These cases are marked in section titles below with "RPM only".

Linux Default Installation Directories

The Linux VEN is installed into two directories:

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

Directory Ownership Pre- and Post-activation

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

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

Optional Disable Dependency Check for ca-certificates during Installation

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

- Red Hat: `rpm -vh -nodeps illumio_ven_package_name.rpm`
- Debian: `dpkg --ignore-depends=illumio_ven_package_name`

Write-Protected Home Directory – Pre-Create Username

At installation, the VEN attempts to create the home directory for its default username `ilo-ven` or for any custom username you specify at installation. If the VEN user's home directory is write-protected or its parent directory does not exist, the installation fails.

Some examples of this problem:

- If users' home directories are on a write-protected automounted file system, the installation fails.
- If `/home` does not exist, the installation fails because the VEN's home directory cannot be created.

Workaround:

- Before installation, create the desired username, group, and home directory.
- Make sure this user has write permission on the `/home` directory so that its own subdirectory can be created.

RPM Only: Installing to a Non-Default Directory

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

```
$ rpm -ivh illumio-ven*.rpm --prefix=/opt/foo/bar
```

Linux Installation with Environment Variables

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

> Environment variables are not supported with the `illumio-ven-ctl` control script, only with the package installation.

Variable	Description
`VEN_ACTIVATION_CODE`	The activation code described in "Generate VEN Pairing Profiles and Activation Code (Pairing Key) in PCE Console".
`VEN_DATA_DIR`	Directory where the `illumio_ven_data` directory is created. This option can also be used when you are upgrading a VEN with RPM or Debian.
`VEN_DISABLE_MONITOR_RESTART`	Disable the VEN agent monitor process. See "Disable Agent Monitor cronjob Before or After Installation".
`VEN_INSTALL_ACTION`	Activate or prepare the VEN during installation. Valid values: • `activate`: Requires an activation code on the `illumio-ven-ctl` control script or set in the `VEN_ACTIVATION_CODE` environment variable. • `prepare`: Used to defer activation until after installation. For example, see "Preparing Golden Master Images for Workload Deployment".
`VEN_MANAGEMENT_SERVER`	The FQDN of the PCE server and its port.
`VEN_NONPRIV_UID`	If `VEN_NONPRIV_USER` is not set, create the `ilo-ven` user with the specified UID.
`VEN_NONPRIV_GID`	If `VEN_NONPRIV_USER` is not set, create the `ilo-ven` group with the specified GID.

Variable	Description
VEN_NONPRIV_USER	Existing username to override the default username ilo-ven. The group name of the specified user is the primary existing group name of the specified user. • If VEN_NONPRIV_USER is set, any values for VEN_NONPRIV_UID and VEN_NONPRIV_GID are ignored. • Conversely, if VEN_NONPRIV_USER is *not* set, any values for VEN_NONPRIV_UID and VEN_NONPRIV_GID take effect.

Example of Linux Environment Variables

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

- VEN_MANAGEMENT_SERVER
- VEN_ACTIVATION_CODE
- VEN_INSTALL_ACTION

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

```
$ VEN_MANAGEMENT_SERVER=pce.mycompany.com:8443
$ VEN_ACTIVATION_CODE=  activation_code
 $ VEN_INSTALL_ACTION=activate
$ rpm -ivh illumio-ven*.rpm
```

or

```
 $ dpkg -i illumio-ven*.dpkg
```

Change Default Name of User at Installation

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

```
$ VEN_NONPRIV_USER=desired_existing_username
$ rpm -ivh illumio-ven*.rpm
or
$ dpkg -i illumio-ven*.dpkg
```

Disable Agent Monitor cronjob Before or After Installation

Linux VEN installation creates a cronjob to check the VEN Agent Monitor process and restart it if necessary. This cronjob runs every 10 minutes.

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

To disable the Linux VEN monitoring cronjob before installation:

Set the following environment variable:

```
export VEN_DISABLE_MONITOR_RESTART=true
```

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

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

You have several options:

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

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

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

      ```
      illumio-ven-ctl restart
      ```
    - Be sure that your monitoring process has sufficient permissions to restart the VEN.

Linux VEN Upgrade

Preserve Custom Environment Variable Settings

If you installed the VEN with custom environment variable settings, for upgrade you need to specify those same environment variables. See "Linux Installation with Environment Variables".

Running the Standalone Upgrade

To start the upgrade:

```
$ /opt/illumio/admin/upgrade
or
$ /opt/illumio/admin/upgrade -y # The -y option suppresses the confirmation prompt.
```

A record of the upgrade is stored in `/opt/illumio/log/upgrade.log`.

Linux VEN Activation After Installation

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

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

```
$ illumio-ven-ctl activate --activation-code activation_code --management-
server pce.mycompany.com:8443  --mode illuminated
```

Standalone Linux VEN Upgrade

Preserve Custom User Name

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

Set Non-default Data Directory before Upgrade

If you previously installed the VEN to non-default installation and data directories with the `VEN_DATA_DIR` environment variable, you need to specify the same value for `VEN_DATA_DIR` before upgrade. See the "VEN Deployment" guide.

Running the Upgrade

To start the upgrade:

```
$ /opt/illumio_ven/admin/upgrade
or
$ /opt/illumio_ven/admin/upgrade -y # The -y option suppresses the confirmation prompt.
```

A record of the upgrade is stored in `/opt/illumio/log/upgrade.log`.

Standalone Uninstall Linux VEN

The commands below uninstall the VEN:

RPM

```
$ rpm -e illumio-ven
```

- **Debian**

```
$ dpkg -e illumio-ven
```

SUSE Linux: If a SUSE workload is unpaired in the enforced policy state, the uninstallation might not complete if the workload does not have rules that allow it to connect to SUSE repos. To avoid this issue, change the policy state to Build or Test before unpairing. See policy states in the *VEN Operations Guide*.

Standalone Install Solaris VEN

This section discuss the standalone model for installing and upgrading the VEN for Solaris.

The VEN for Solaris supports two different Solaris machine architectures: SPARC and x86_64.

The Solaris VEN software download is a compressed tar archive file that contains one file for each of the supported machine architectures. The installation steps for both machine architectures are identical. In the steps below, be sure you enter the correct identifier for your machine architecture.

Solaris VEN Known Limitations and Considerations

- For installation on a Solaris minimal server, `bash` and `xpg4` POSIX-compliant tools are the key software. Be sure to install `xpg4` on your system.
- Installing or activating the Solaris VEN on a workload running an LDAP client can take longer than on other workloads with out an LDAP client.
- IPFilter
    - Before installing the Solaris VEN, install IPFilter.
    - Do not uninstall the IPFilter package from the workload running a VEN that is paired with PCE.
- The system's state table limit is 65,536 entries. If that limit is reached, IPFilter drops packets. Correct the issue by increasing the state table limit.
- Illumio recommends not to run Solaris zones on the workload.
- The Solaris VEN does not support Kerberos authentication.

Default Installation Directories

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

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

Write-Protected Home Directory – Pre-Create Username

At installation, the VEN attempts to create the home directory for its default username `ilo-ven` or for any custom username you specify at installation. If the VEN user's home directory is write-protected or its parent directory does not exist, the installation fails.

Some examples of this problem:

- If users' home directories are on a write-protected automounted file system, the installation fails.
- If `/home` does not exist, the installation fails because the VEN's home directory cannot be created.

Workaround:

- Before installation, create the desired username, group, and home directory.

- Make sure this user has write permission on the `/home` directory so that its own subdirectory can be created.

Change Default Username for Solaris VEN Installation

You can change the username who owns and runs the VEN software. There are two methods:

- Via the prompts during interactive installation.
- Via a non-interactive response file for batch or automated installation.

Before Installing the Solaris VEN...
Regardless of the method, before installing the Solaris VEN:

- Create the desired username and home directory.
- Assign the username to the desired group.
- Make sure that the desired username has sufficient read/write privileges to create the default VEN installation directory `/opt/illumio_ven`.

Change Username in Interactive VEN Installation

When you install the Solaris VEN interactively, you are prompted for the username. In this example, the desired username is `illumio-solaris-ven`:

```
... Untar and unzip the downloaded Solaris VEN package
# pkgadd -d  dir_of_extracted_package  illumio-ven
 Processing package instance < illumio-ven> from dir_of_extracted_package
...
Would you like to use the standard VEN user, ilo-ven, for this installation? [y,n] n
Enter the username of an existing user to use instead of ilo-ven: illumio-solaris-ven
...
## Executing postinstall script.
Installation of <illumio-ven> was successful.
```

Response File to Change Username in Batch VEN Installation

Supplied with the VEN software, a *response file* includes the default settings for the installation program. You can override the default username, `ilo-ven`, by creating a custom response file in your own custom directory. In the following example, the custom username is `illumio-solaris-ven`:

To change the username, install the VEN, and activate it:

1. Create your own custom response file with `pkgask`:

   `# #` The value of environment variable `MY_RESPONSE_FILE` below is *only* the path to where you want to create the response file.
   `# #` The name of the response file in that *`path_to_my_custom_response_file`* is always `response`.

```
   # MY_RESPONSE_FILE=path_to_my_custom_response_file
# pkgask -d dir_of_extracted_package -r $MY_RESPONSE_FILE illumio-ven
Processing package instance < illumio-ven> from path_to_my_custom_response_file
Would you like to use the standard VEN user, ilo-ven, for this installation? [y,n] n
Enter the username of an existing user to use instead of ilo-ven: illumio-solaris-user

... Omitted lines
Response file path_to_my_custom_response_file/response was created.
Processing of request script was successful.
```

2. Create a script the includes the following command. This script can then be run in batch or for automated installation.

   In this example, take note of the following points:

   - The creation of your script is not shown.
   - The first line is what you should put in your script.
   - On the first line:
     - The required `pkgadd` options `-r` and `-a`.
     - The path to the exact required filename *`dir_of_extracted_package`* / **`admin`**.
     - The path to the filename *`path_to_my_custom_response_file`*/**`response`**.
   - The remainder of the lines are the standard output of running the command.

```
# pkgadd -d dir_of_extracted_package -a dir_of_extracted_package/illumio-ven/
root/opt/illumio_ven/etc/templates/admin \
 -r path_to_my_custom_response_file/response illumio-ven
 Processing package instance <illumio-ven> from dir_of_extracted_package
## Executing checkinstall script.
## Executing preinstall script.
## Installing part 1 of 1.
... Omitted lines
Installation of <illumio-ven> was successful.
```

Steps to install Solaris VEN

1. Optionally, you can change the username of the owner of the installed Solaris VEN. see "Solaris VEN Installation -- Change Default Username".

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

   ```
   /etc/certs/ca-certificates.crt
   ```
3. Extract the software.
   a. Solaris 10 Update 11:
      ```
      # gunzip illumio-ven-ven_version.pkg.tgz
      # tar -xvf illumio-ven.ven_version.pkg.tgz
      ```
   b. Solaris 11.x:
      ```
      # tar -xvzf illumio-ven.ven_version.pkg.tgz
      ```
4. To install, enter the following command:

   ```
   # pkgadd -d -a illumio-ven/root/opt/illumio_ven/etc/templates/admin
   ```
5. The package installation script prompts you for configuration information. Press the **Enter** key or enter `y` to accept the default value, or enter the desired values.

Activate a Solaris VEN After Installation

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

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

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

The following example shows how to activate the VEN and set its mode to `illuminated`:

```
$ illumio-ven-ctl activate --activation-code activationCode --management-server
fqdn:port  --mode illuminated
```

Standalone Install Windows VEN

This section discuss the standalone model for installing and upgrading the VEN for Microsoft Windows.

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

Run PowerShell as Administrator with Execution Policy

Use Windows PowerShell to run the VEN installation program.

Run PowerShell as Administrator, because the installation affects the operating system. Right-click the PowerShell icon and select "Run as Administrator".

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

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

Windows Installation Directories

By default, the Windows VEN installation directories are as follows:

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

Windows VEN Installation with Activation

The VEN MSI installer supports these environment variables:

- `MANAGEMENT_SERVER`
- `ACTIVATION_CODE`

To activate the Windows VEN during installation, execute the following command:

```
msiexec /i ven_installation_filename.msi MANAGEMENT_SERVER=pce_fqdn:pce_portnumber
 ACTIVATION_CODE=activation_code
```

Windows Installation with Command-line Variables

The following table lists VEN command-line variables that you can set for the package installation on Windows.

> Command-line variables are not supported with the `illumio-ven-ctl` control script, only with the package installation. For more details about `illumio-ven-ctl`, see the *VEN Operations Guide*.

Variable Name	Description
`INSTALLFOLDER`	Directory where the VEN is to be installed. For command-line usage, see "Set environment variables for custom installation path and data directory".

Variable Name	Description
DATAFOLDER	Directory where the illumio_ven_data directory is created. For command-line usage, see "Set environment variables for custom installation path and data directory".
MANAGEMENT_SERVER	The FQDN of PCE server and its port. For example: pce.BigCo.com:8443
ACTIVATION_CODE	The activation code.

Set command-line variables for custom installation path and data directory

The following installation command line for the VEN on Windows shows the optional use of of command-line variables to override the default directories.

Be sure you use the standard Windows environment variables so that the directories are created with the proper paths. The example below relies on the %PROGRAMFILES% environment variable. Your own usage depends on the custom path you want to create. The syntax below uses the Windows PowerShell line-continuation character, which is `, but the command can be on only a single line.

```
msiexec /i nameOfVenstaller.msi `
 INSTALLFOLDER=%PROGRAMFILES%_someDirectoryPathForVENBinaries_ `
DATAFOLDER=%PROGRAMFILES%_someDirectoryPathForData_ `
/qb
```

Standalone Windows Install VEN without Activation

You can install the Windows VEN without activation by either double-clicking the Windows MSI file or by executing the following command in PowerShell:

```
c:> msiexec /i ven_installation_filename.msi /qn /l*vx VENInstaller.log
```

Windows VEN Activation after Installation

Be sure that you have proper administrative permissions. See "Run PowerShell as Administrator with Execution Policy".

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

```
B:> "C:\Program Files\Illumio\illumio-ven-ctl.ps1" `
  activate -activation-code activation_code `
-management-server pce_fqdn:pce_portnumber `
-activation_option
```

Windows VEN Activation Options

You have several activation options you can set while pairing. You can set the workload policy state and apply Labels at the time of activation. This example shows how to activate a Windows workload with the following options:

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

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

Standalone Windows VEN Upgrade

1. Change directories to the following path:
   PS> **cd %ProgramFiles(x86)%\Illumio\admin**
2. Start the upgrade:
   PS> **illumio-ven-ctl.ps1 upgrade**
3. When asked if you want to upgrade the VEN, type `yes` and then press **Enter**. You can also suppress this prompt. See the `-y` option above.

A record of the upgrade is stored in `C:\ProgramData\Illumio\log\install.log`

Optional -- Windows VEN Installation with Disabled WFP Optimization

When you install the Windows VEN, by default, Windows Filtering Platform (WFP) Optimization is enabled for performance and support for IPSets.

To install the VEN *without* WFP Optimization, execute this command:

```
C:> msiexec /i ven_installation_filename .msi WFP_OPTIMIZATIONS_ENABLED=FALSE
```

If WFP Optimization has been disabled , Illumio sets an upper limit on the number of filters that the VEN can create: 32,767 (32K -1) filters.

Standalone Windows VEN Uninstall

The commands below uninstall the VEN on Windows. To unpair a Windows VEN, you must provide one of the unpair options: `saved` or `open` .

```
C:> {Env:ProgramFiles(x86)}\Illumio\admin\unpair.ps1  saved
```

Make sure that your execute policy for the Windows PowerShell is set to allow you to run the command. See "Run PowerShell as Administrator with Execution Policy".

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

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

Pairing Profiles, Pairing Scripts, and Prepare Scripts

In the PCE web console, you create a pairing profile with desired characteristics to create a script called a *pairing script* to run on a workload. The pairing script installs the VEN software, activates it, and gets the workload ready to accept security policy from the PCE. "Pairing" is also know as "activation".

Pairing script is an option

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

General Steps

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

Which VEN Version Is Activated

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

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

Creating a Pairing Profile and Pairing Script

See the *PCE Web Console User Guide*.

Types of Pairing Scripts and the Prepare Script

Regardless of the VEN deployment model, either PCE-based or standalone, you create the pairing script in the PCE web console and run the pairing script on the workload.

For creating a pairing script, see the PCE Web Console User Guide.

The difference between the two types of pairing scripts is shown below

Without the PCE-based Deployment Model	With the PCE-based Deployment Model
The pairing script contains options to obtain the software fromthe central Illumio VEN repo: • `--repo-host repo.illum.io` • `--repo-dir someDirectory` • `--repo-https-port 443`	The pairing script does not contain these options, because the software is obtained from your PCE.

The prepare script is for creating Golden Master machine images to activate the VEN the first time the image is booted. See "Preparing Golden Master Images for Workload Deployment".

Adding Options to the Pairing Script

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

Linux pairing script for PCE-Based deployment model

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

Example PCE-based pairing script with extra options

```
rm -fr /opt/illumio/scripts && umask 027 && mkdir -p /opt/illumio/scripts && curl https://pce.bigco.com/
sPl1tOExo0FIEphoewIujIucrLaTOAS3/pair -o /opt/illumio/scripts/pair && chmod +x /opt/illumio/scripts/pair && /
opt/illumio/scripts/pair  --management-server pce.bigco.com:8443 --activation-code some_activation_code --env
Production
```

Windows without the PCE-based Deployment model

For ease of reading, the example below uses the Windows PowerShell line continuation character, which `` ` ``. The actual pairing script is a single line.

Example Non-PCE-Based pairing script

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

Preparing Golden Master Images for Workload Deployment

Many organizations use "Golden Master" machine images for faster deployment.

With the standalone deployment model, you have two options for pairing:

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

Important considerations

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

Prepare via the Pairing Profile/Pairing Script

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

- In the PCE web console, create a Pairing Profile or select an existing Pairing Profile.
- Make a copy the pairing script.
- In the copy of the script, change all occurrences of `pair` to `prepare`.
- Execute the modified script on the image.
  The `prepare` script installs the VEN on the image and configures it to start the next time the workload is booted.
- Stop the VEN after installation with `prepare`:
  `illumio-ven-ctl stop`

Prepare on the workload with illumio-ven-ctl

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

- Use `illumio-ven-ctl` to set the image into "prepare" mode:
  `illumio-ven-ctl` **`prepare`** `-management-server` *`pce_fqdn:port`* `--activation-code` *`activation_key`*

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

  Contents of `agent_activation.cfg`:
  `activation_code:` *`your_activation_code`*
  `masterconfig_server:` *`your_pce_fqdn:your_port`*

Example activation configuration file

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

illumio-ven-ctl Syntax and Command-line Options

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

- Linux: default location is `/opt/illumio/bin`

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

illumio-ven-ctl Activation Options

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

If you are activating with a PCE that has a Pairing Profile configured to block changes to policy state (the `illumio-ven-ctl` option `--mode`) or label assignment (the `illumio-ven-ctl` options `--env`, `--loc`, `--role`, `--app`), you must not use these options on of these blocked configurations or the activation will fail.

Syntax note:

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

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

Option	Argument	Required	Notes
`--name | -n`	`server friendly name`	Optional	Sets a friendly name that will be used for this workload when it appears in the PCE web console. Example: `--name "Web Server 1"`
`--env`	`environment <label_name>`	Optional	Inputs an Environment Label for this workload. Example: `--env Production`
`--loc`	`location <label_name>`	Optional	Example: `--env "Production US"`
`--role`	`role <label_name>`	Optional	Assigns a Role Label for this workload. Example: `--role "Dev Group"`
`--app`	`application <label_name>`	Optional	Assigns an Application Label for this workload. Example: --app "Web Service"
`--mode`	`illuminated | enforced | idle`	Optional	Sets the policy state for the workload. For explanation of the various states, see "Workload Policy States" in the VEN Operations guide.

Option	Argument	Required	Notes
`--log-traffic`	`true` | `false`	Optional	Enables or disables traffic logging. If not specified, logging is set to `true` by default. Interacts with the `--visibility-level` option. See --visibility-level Arguments Correlated with --log-traffic Arguments.
`--visbility-level`	`flow_summary` | `flow_drops` | `flow_off`	Optional	Default: `flow_summary`. Defines the extent of the data the VEN collects and reports to the PCE from a Workload in the `enforced` mode (policy state), so you can control resource demands on Workloads. The higher levels of detail are useful for visualizing traffic flows in the Illumination map inside the PCE web console. Interacts with the `--log-traffic` option. See --visibility-level Arguments Correlated with --log-traffic Arguments.
`-wfp-optimizations-enabled`	`-wfp-optimizations-enabled true`	Optional	Use this option if you want to pair the Windows workload with the WFP_Optimization feature, which enables support for IPSets.

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

--log-traffic Argument	Effect by VEN Policy State	Description
`flow_summary`	Included in all policy states.	Default. Called **High Detail** in the PCE web console. The VEN collects traffic connection details for both *allowed* and *blocked* connections: source and destination IP address and port and protocol. This argument creates traffic links in the Illumination® map and is typically used during the **build** and **test** states.
`flow_drops`	Valid only in **enforced state.**	Called **Less Detail** in the PCE web console. The VEN collects connection details only for *blocked* traffic: source and destination IP address and port and protocol. This argument produces less detail for Illumination® but demands fewer workload system resources than `flow_summary`.
`flow_off`	No flow logging.	Called **No Detail** in the PCE web console. The VEN does not collect any details about traffic connections. This option produces no details for the Illumination® map but requires the fewest number of workload resources. Useful when you are satisfied with policy rules and do not need additional detail.

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

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

VEN mode/ state	--log-traffic Argument	--visibility-level Argument	Notes
illuminated	false	flow_summary	This is a combination of settings called **Build and Test** in the PCE web console
	~~false~~	~~flow_drops~~	Not a valid combination
	false	flow_off	
	true	flow_summary	In the PCE web console, this combination is called "Build and Test".
	~~true~~	~~flow_drops~~	Not a valid combination
	true	flow_off	
enforced	false	flow_summary	
	false	flow_drops	
	false	flow_off	No detail in enforced mode
	true	flow_summary	High detail in enforced mode.
	true	flow_drops	Low detail in enforced mode. - LOW DETAIL
	~~true~~	~~flow_off~~	Not a valid combination

illumio-ven-ctl Deactivation Options

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

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

Unpair options on Linux

- `recommended`:
  Temporarily allow only SSH/22 until reboot.

Security implications: If this workload is running a production application, it could break because this workload will no longer allow any connections to it other than SSH on port 22.

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

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

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

Unpair Options on Windows

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

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

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

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

- `unmanaged`:

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

Support Report During Deactivation

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

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

Revision History

Illumio Adaptive Security Platform VEN Deployment Guide

Date	Description
2018-09-19	Cosmetic update.
2018-09-06	Updated for Illumio Adaptive Security Platform version 18.2: • PCE-based deployment of the VEN. • Included details on AIX and Solaris VEN for standalone VEN installation.
2018-07	Added `illumio-ven-ctl` activation/deactivation options
2018-06-30	Corrected package dependencies for Red Hat 6 and 7: remove duplicate requirements.
2018-06-27	Root access is required on the "Linux workload to install the Linux VEN".
2018-06-18	Added details about the `agent_activation.cfg` file in "Preparing Golden Master Images for Workload Deployment".

Date	Description
2018-06-15	• Corrected example of `illumio-ven-ctl --mode` option. • Corrected broken hyperlinks for Linux environment variables.
2018-06-08	PKI certificate to download VEN software is no longer required.
2018-05-11	• Updated for Illumio Adaptive Security Platform version 18.1. • Reorganization and miscellaneous corrections throughout; removal of section numbering. • Start of revision history.