



Illumio® ASP 18.1 VEN Deployment

Last Updated: 06/30/2018

Table of Contents

| | |
|---|-----------|
| Product Version | 5 |
| About Illumio | 5 |
| Illumio ASP Training | 5 |
| Search Knowledge Base and Documentation | 5 |
| Illumio Support | 5 |
| Recommended Skills | 5 |
| How To Use This Guide | 6 |
| Related Documentation | 6 |
| Notational Conventions | 6 |
| Illumio VEN Overview..... | 7 |
| VEN Software Architecture and Theory of Operations | 7 |
| Management Interfaces for the PCE and VEN | 7 |
| Cycle of Common VEN Tasks | 9 |
| VEN Deployment Design Choices for On-Premises PCE or Illumio Secure Cloud | 9 |
| Prerequisites and Planning before VEN Deployment | 10 |
| Upgrade paths and planning tool | 10 |
| VEN Deployment Planning Checklist | 10 |
| Upgrade Paths and Planning Tool | 11 |
| Required Communications between PCE and VEN | 11 |
| Operating System and Package Dependencies | 11 |
| Linux | 12 |
| Windows | 13 |
| Download the VEN Software | 13 |
| Determine VEN Package by Operating System and CPU Architecture | 13 |
| Decide to Activate VEN During or After Installation | 15 |
| Generate Unique VEN Activation Code | 15 |
| Optional – Preparing VEN-unactivated Golden Master Machine Images | 16 |

| | |
|---|-----------|
| Install Linux VEN | 16 |
| Default Installation Directories | 16 |
| Optional Disable Dependency Check for ca-certificates during Installation | 16 |
| RPM Only: Installing to a Non-Default Directory | 16 |
| Linux VEN Installation with Activation | 17 |
| Linux Installation and Activation with Environment Variables | 17 |
| Example of Linux Environment Variables | 18 |
| Change Default Name of User at Installation | 18 |
| Linux VEN Activation After Installation | 19 |
| Install Windows VEN..... | 19 |
| Run PowerShell as Administrator with Execution Policy | 19 |
| Windows Installation Directories | 19 |
| Windows VEN Installation with Activation | 20 |
| Windows Installation with Environment Variables | 20 |
| Set environment variables for custom installation path and data directory | 21 |
| Windows Install VEN without Activation | 21 |
| Windows VEN Activation after Installation | 21 |
| Optional – Windows VEN Installation with Disabled WFP Optimization | 22 |
| Uninstalling the VEN | 22 |
| Uninstalling the VEN on Linux | 22 |
| Uninstalling the VEN on Windows | 23 |
| Upgrade the VEN - See VEN Operations Guide | 23 |
| illumio-ven-ctl Syntax and Command-line Options | 23 |
| Linux illumio-ven-ctl Help | 24 |
| Windows illumio-ven-ctl.ps1 Help | 24 |
| illumio-ven-ctl Activation Options | 26 |
| illumio-ven-ctl Deactivation Options | 29 |
| Unpair options on Linux | 29 |
| Unpair Options on Windows | 29 |

| | |
|---|-----------|
| Support Report During Deactivation | 31 |
| Pairing via the VEN Repository ("VEN Repo")..... | 31 |
| Pairing Profiles and the Pairing Script | 31 |
| What the Pairing Script Does | 32 |
| Example Pairing Script for Linux..... | 32 |
| Pairing Script Command Line Overrides | 32 |
| Adding Pairing Options to the Pairing Script..... | 33 |
| Preparing Golden Master Images for Workload Deployment | 34 |
| Using prepare via the Pairing Profile | 34 |
| Using the prepare option on the command line or from a file | 35 |
| Revision History: Illumio ASP VEN Deployment 18.1 | 35 |

Product Version

Illumio ASP Version: 18.1.0 (Standard release)

About Illumio

Copyright © 2013 - 2018 Illumio, Inc., 160 San Gabriel Drive, Sunnyvale, CA 94086

Illumio's products and services are built on our patented technologies. For information on Illumio's patents and patent applications, see <https://www.illumio.com/patents>.

Illumio ASP Training

Illumio offers a wide yet focused training curriculum for Illumio Adaptive Security Platform (ASP), 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 ASP, log into your [Illumio Support account](#) and select the **Knowledge Base** or **Documentation** tabs.

Illumio 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
- Solid understanding of Illumio ASP

- 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
- Understanding TCP/IP networks, including protocols and well-known ports
- Familiarity with PKI certificates

How To Use This Guide

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

The guide includes details on the following:

- Activating the VEN on your systems' native operating system, either during installation or afterwards.
- Interactions with the Illumio ASP Policy Compute Engine (PCE).
- Upgrading the VEN.
- Other topics.

The *VEN Deployment Guide* has several main divisions:

- Illumio VEN overview, with interaction with the PCE.
- Command-line-oriented sections with syntax examples for installation.

Related Documentation

Illumio ASP documentation is available from the [Support portal](#).

- *PCE Web Console* guide: working with Illumination, designing policy, creating labels, and provisioning and administering VENs.
- *PCE Deployment* guide: requirements, planning, and installing the PCE.
- *PCE Operations* guide: *common* operational tasks on the PCE
- *PCE REST API* guide: Programming Illumio ASP
- *VEN Deployment* guide: installing and activating the VEN
- *VEN Operations* guide: administering the VEN after installation

Notational Conventions

- *New term*: Newly introduced terminology is indicated by italics. Example: *activation code*.
- Command-line examples are in monospace. Example: `illumio-ven-ctl --activate`
- *Arguments* on command lines are *monospace italics*. Example: `illumio-ven-ctl --activate activation_code`

Illumio VEN Overview

Central to Illumio Adaptive Security Platform (ASP) is the Virtual Enforcement Node (VEN), a lightweight software agent you install on systems to make them Illumio ASP managed workloads. Also central to Illumio ASP is the PCE. The VEN and the PCE are both essential to Illumio ASP. Interactions between the VEN and the PCE are detailed throughout this guide and in the [related documentation](#).

The VEN examines the workload with which it is paired, determining the exact operating system, IP address details, protocols, and processes listening on ports, and sends that context to the Policy Compute Engine (PCE).

The PCE determines the graph of dependencies between workloads or individual processes and computes accurate security policies to enforce on the VEN. The PCE and VENs work together to continuously monitor and adapt security to changes. VEN policy enforcement is done using iptables in Linux workloads and Windows Filtering Platform (WFP) on Windows workloads.

You can activate VEN either during installation or after installation.

When you activate a VEN, the workload where the VEN is installed is considered paired with the PCE. At activation, the VEN assumes control of the workload's networking system. The VEN reports the workload's information to the PCE, such as all services on the workload, all open ports, details about the operating system, and workload location.

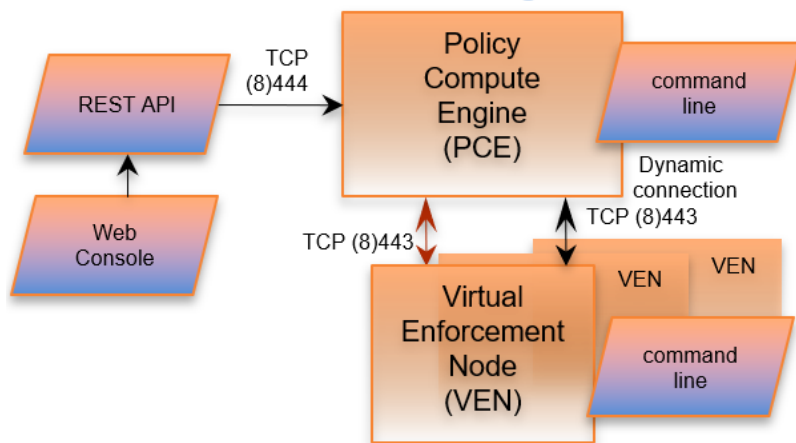
VEN Software Architecture and Theory of Operations

For details about the VEN software architecture, associated components, the basic theory of VEN operations, and other aspects of the VEN, see the [VEN Operations Guide](#).

Management Interfaces for the PCE and VEN

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

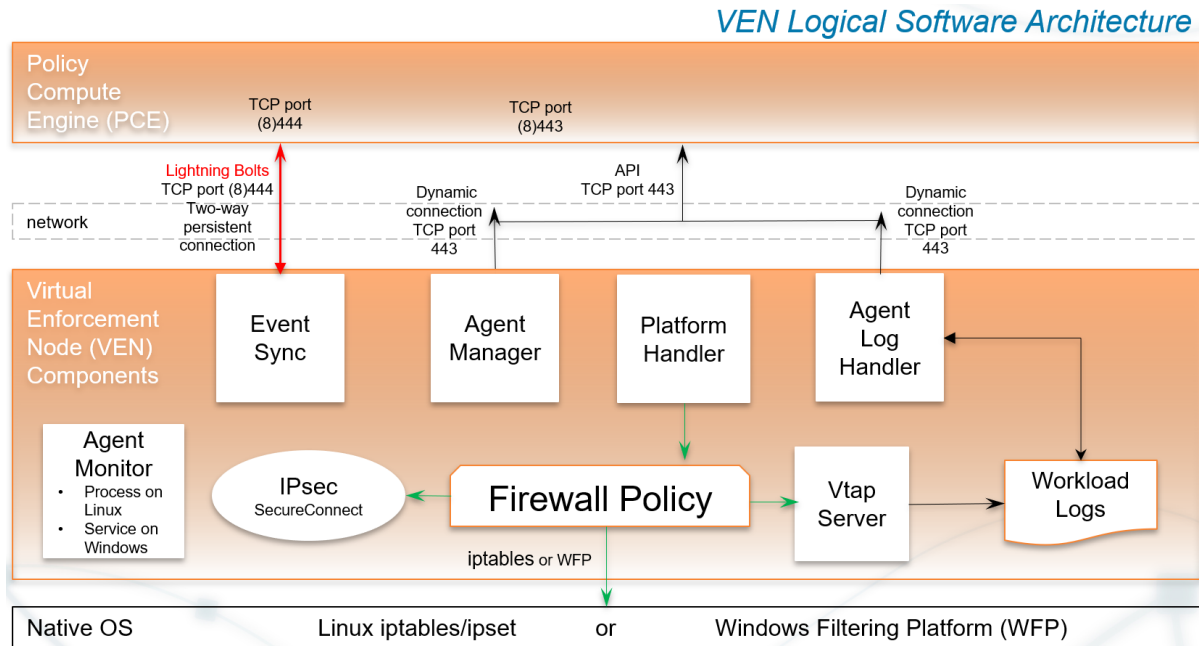
PCE and VEN Management Interfaces



| Interface | Notes | See... |
|------------------|---|---|
| PCE web console | With the PCE web console, you can perform many common tasks for managing Illumio ASP. | PCE Web Console guide at Documentation |
| PCE command line | Use of the command line directly on the PCE. A primary management tool on the PCE is the command line <code>illumio-pce-ctl</code> control program. You can perform many common tasks for managing Illumio ASP on the PCE command line, including the VEN. | <code>illumio-pce-ctl</code> in the PCE Operations guide at Documentation |
| REST API | With the Illumio ASP REST API, you can perform many common tasks for managing Illumio ASP. One use of the REST API is to automate the management of large groups of workloads, rather than each workload individually. The endpoint for REST API requests is the PCE itself, not the workload; the REST API does not communicate directly with the VEN. | REST API guide at Documentation |
| VEN command line | Use of the command-line directly on the VEN workload. A primary management tool on the VEN command line is the <code>illumio-ven-ctl</code> control program. | <code>illumio-ven-ctl</code> in the VEN Operations guide at Documentation |

This guide focuses on the VEN command-line interface.

Cycle of Common VEN Tasks



VEN Deployment Design Choices for On-Premises PCE or Illumio Secure Cloud

The VEN can be deployed both by organizations who have deployed the on-premises PCE and by organizations that rely on Illumio SecureCloud. The design choices for VEN deployment are nearly identical.

The following table summarizes the deployment choices.

| Option | Secure Cloud | On-premises PCE | Description |
|---------------------|--------------|-----------------|---|
| VEN single packages | No | Yes | This deployment model is also known as the <i>single package deployment model</i> . It is based on downloadable packages for installation directly on the workload. |

| Option | Secure Cloud | On-premises PCE | Description |
|-----------------------------|--------------|-----------------|---|
| VEN Repository ("VEN repo") | Yes | Yes | Via Illumio's VEN repo, customer-hosted repo or the PCE Virtual Appliance, which includes an embedded VEN repo. |

- i** Illumio recommends the on-premises deployment and the single package installation option on supported workload OSs, rather than the Illumio VEN repo.
- Using the single package installation, all installation takes place within your own computing environment.
 - The VEN repo is primarily for use by Illumio ASP Secure Cloud customers.

Prerequisites and Planning before VEN Deployment

Before you install the VEN on a workload, make sure you meet the requirements detailed in this section.

Upgrade paths and planning tool

For details on upgrade paths for versions of the PCE and VEN, see [Versions and Releases](#).

An [upgrade planning tool](#) is also available to help you plan your deployments.

VEN Deployment Planning Checklist

This checklist summarizes VEN planning considerations and requirements detailed in this guide.

| Step | See... |
|---|---|
| The PCE is installed with working VEN communications. | Required Communications between PCE and VEN |
| Supported operating system versions for VEN workloads | Operating System and Package Dependencies |

| Step | See... |
|--|--|
| If upgrading the VEN, determine your upgrade path. | Upgrade paths and planning tool |
| Download the VEN software | Download the VEN Software |
| Determine the installation packages you need for your workload OSs and CPUs | Determine VEN Package by Operating System and CPU Architecture |
| Decide to activate VEN either during installation or after installation | Decide to Activate the VEN During or After Installation |
| <ul style="list-style-type: none"> Plan unique activation code for each VEN Generate VEN pairing profiles and activation codes (pairing key) | <ul style="list-style-type: none"> Generate Unique VEN Activation Code illumio-ven-ctl Syntax and Command-line Options |
| Optionally prepare machine images with the VEN | Optional – Preparing VEN-unactivated Golden Master Machine Images |

Upgrade Paths and Planning Tool

For details on upgrade paths for versions of the PCE and VEN, see [Versions and Releases](#).

An [upgrade planning tool](#) is also available to help you plan your deployments.

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 following operating systems.

Linux




- On Linux, you must ensure all OS package dependencies are installed prior to installing the VEN software.
- If Illumio has not listed a specific version of a package dependency, use the version shipped with the OS distribution.

| Linux OS Version | Package Dependencies | Notes |
|---|---|---|
| Amazon Machine Image (AMI) 2016.03, 2016.09, 2017.03, 2018.03 | curl, net-tools, bind-utils, ipset, libnftnl, libcap, gmp, GNU sed | |
| <ul style="list-style-type: none"> • CentOS 5.5 - 5.11 • Red Hat 5.5 - 5.11 | curl, bind-utils, iptables, iptables-ipv6, libcap, gmp, GNU sed bind-utils package can be replaced by bind97-utils. | |
| <ul style="list-style-type: none"> • CentOS 6.2 - 6.9 • Red Hat 6.2 - 6.9 • Oracle Linux 6.2 - 6.9 with Red Hat kernel • Oracle Linux 6.2 - 6.9 with UEK 2 & 3 kernel | curl, net-tools, bind-utils, iptables (1.4.7-16 minimum or later), ipset (6.11-4 minimum or later), libnftnl, libmnl, gmp, GNU sed | |
| <ul style="list-style-type: none"> • CentOS 7.0 - 7.5 • Red Hat 7.0 - 7.5 • Oracle Linux 7.0 - 7.5 with Red Hat kernel • Oracle Linux 7.0 - 7.2 with UEK 2 & 3 kernel | curl, net-tools, bind-utils, iptables-ipv6 (1.4.7-16 minimum or later), iptables (1.4.7-16 minimum or later), ipset (6.11-4 minimum or later), libnftnl, libmnl, libcap, gmp, GNU sed | |
| <ul style="list-style-type: none"> • Debian 7.0 (Wheezy) • Debian 8 (Jessie) • Debian 9 (Stretch) | apt-transport-https, curl, net-tools, dnsutils, uuid-runtime, ipset, libnftnl0, libmnl0, libcap2, libgmp10, GNU sed | apt-transport-https package is required for pairing with Debian repo. |

| Linux OS Version | Package Dependencies | Notes |
|--|--|--|
| <ul style="list-style-type: none"> • SUSE SLES 11 SP3, 11 SP4 • SUSE SLES12 SP1 | openssl-certs, curl, net-tools, bind-utils, ipset, libnftnl, libmnl, libcap2, gmp, iptables, GNU sed | For SUSE 11, Illumio recommends Kernel version 3.0.101-0.47.71 |
| <ul style="list-style-type: none"> • Ubuntu 12.04 • Ubuntu 14.04 • Ubuntu 16.04 • Ubuntu 18.04 | curl, net-tools, dnsutils, uuid-runtime, ipset, libnftnl, libmnl, libcap2, libgmp10, GNU sed | Ubuntu 18.04 ("Bionic Beaver") also requires the Ubuntu 16.04 ("Xenial") distribution. Be sure to install the Xenial deps on Bionic. |

Windows

 Make sure you have installed all the latest Windows Service Packs before installing the VEN.

| Windows OS Versions | Package Dependencies | Notes |
|---|-----------------------------------|--|
| <ul style="list-style-type: none"> • Windows Server 2008 R2 SP1 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows 7 • Windows 10 | Latest SPs for desired OS version | <ul style="list-style-type: none"> • Policy enforcement on wireless/VPN interfaces is not supported. • Windows Server 2008 R2 SP1 and Windows 7 support Transport Layer Security (TLS)/1.1, which secures network connections. • Windows 7 and Windows 10 have limited configurations only; recommended for use in VDI or other similar environments that primarily use wired interfaces. |

Download the VEN Software

Download the VEN software package from the [Illumio Support site](#).

Determine VEN Package by Operating System and CPU Architecture

After you have downloaded and unpacked the software, determine the VEN appropriate for your OSs. These file naming conventions indicate OS and CPU architecture.

- For example, to install the VEN on 64-bit RedHat/CentOS 6.x (identifier i686), use this file:

`illumio-ven-18.1.0-20160705144421c6.x86_64.rpm`

- For example, to install the VEN on 64-bit Windows 2012, use this file:

`VENInstaller-18.1.0-20160705144421-x86.msi`

| Platform | OS Variant | Package Identifier (File Extension) |
|----------|--|---|
| Linux | Amazon Machine Image | <ul style="list-style-type: none"> • 32-bit: c6.i686 • 64-bit: c6.x86_64 |
| | Debian 7 Wheezy, Debian 8 Jessie, Debian 9 Stretch | <ul style="list-style-type: none"> • 32-bit: d7.i386 • 64-bit: d7.amd64 |
| | RedHat/CentOS 5.x | <ul style="list-style-type: none"> • 32-bit: c5.i686 • 64-bit: c5.x86_64 |
| | RedHat/CentOS/Oracle 6.x | <ul style="list-style-type: none"> • 32-bit: c6.i686 • 64-bit: c6.x86_64 |
| | RedHat/CentOS/Oracle 7.x | 64-bit: c7.x86_64 |
| | Ubuntu 12 Precise | <ul style="list-style-type: none"> • 32-bit: u12.i386 • 64-bit: u12.amd64 |
| | Ubuntu 14 Trusty | <ul style="list-style-type: none"> • 32-bit: u14.i386 • 64-bit: u14.amd64 |
| | Ubuntu 16 Xenial | <ul style="list-style-type: none"> • 32-bit: u16.i386 • 64-bit: u16.amd64 |
| Windows | Windows 2008 R2 SP1, 2012, 2012 R2 | <ul style="list-style-type: none"> • 32-bit: x86 • 64-bit: x64 |

Decide to Activate VEN During or After Installation

Regardless of the deployment option you decide on, you can choose to activate a VEN either during installation or after installation. Both options are discussed in this guide.

Your choice depends several considerations:

- How your organization usually deploys software on individual systems, that is, your standard operating procedures.
- Whether or not you want Illumio ASP security to take effect immediately after installation on individual workloads or you want to activate VEN en masse by organization, or some other rollout scheme.
- Whether or not your Illumio ASP policies have already been designed and created to secure the workloads.

The mechanisms for activation are nearly identical regardless of your choice:

In the PCE web console, you can generate a "pairing" script that will make the workload activate at boot.

Directly on the workload, you can use the `illumio-ven-ctl --activate` options.

For creating machine images with an unactivated VEN and unique activation code already installed, see [Optional – Preparing VEN-unactivated Golden Master Machine Images](#).

Generate Unique VEN Activation Code

You need a unique *activation code* for each VEN. (The activation code is also known as a *pairing key*.) You can get an activation code in the following ways:

- In the PCE web console, create a Pairing Profile.
- With the Illumio ASP REST API

See [Recommended Documentation](#) for details.

You can use the activation code either during installation or after installation, [depending on your choice](#).



Unique activation code for each workload

Do not use a single activation code for more than one workload. The activation code is the unique identifier for the VEN to establish secure communications with the PCE.

Optional -- Preparing VEN-unactivated Golden Master Machine Images

If you are using machine images for faster deployment of the VEN, consider preparing them to activate the VEN the first time the workload is booted. See the details in [Preparing Golden Master Images for Workload Deployment](#).

Install Linux VEN

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".

Default Installation Directories

The Linux VEN is installed into two directories:

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

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`

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 VEN Installation with Activation

You can activate during installation with environment variables. (The PCE web console uses the term "pairing" for activation.)

You need to know the PCE hostname and port and you must obtain an activation code ("pairing key").

Linux Installation and Activation with Environment Variables

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

Environment variables are not supported with the `illumio-ven-ctl` control script, only with the single package installation. For more details about `illumio-ven-ctl`, see the [VEN Operations guide](#).

| Variable | Description |
|--------------------|--|
| VEN_DATA_DIR | Directory where the <code>illumio_ven_data</code> directory is created. This option can also be used when you are upgrading a VEN with RPM or Debian. |
| VEN_INSTALL_ACTION | Activate or prepare the VEN during installation. Valid values: <ul style="list-style-type: none"> <code>activate</code>: Requires an activation code on the <code>illumio-ven-ctl</code> control script or set in the <code>VEN_ACTIVATION_CODE</code> environment variable. <code>prepare</code>: Used to defer activation until after installation. For example, see Preparing Golden Master Images for Workload Deployment. |
| VEN_NONPRIV_UID | If <code>VEN_NONPRIV_USER</code> is not set, create the <code>ilo-ven</code> user with the specified UID. |
| VEN_NONPRIV_GID | If <code>VEN_NONPRIV_USER</code> is not set, create the <code>ilo-ven</code> group with the specified GID. |
| VEN_NONPRIV_USER | Existing username to override the default username <code>ilo-ven</code> . The group name of the specified user is the primary existing group name of the specified user. <ul style="list-style-type: none"> If <code>VEN_NONPRIV_USER</code> is set, any values for <code>VEN_NONPRIV_UID</code> and <code>VEN_NONPRIV_GID</code> are ignored. Conversely, if <code>VEN_NONPRIV_USER</code> is <i>not</i> set, any values for <code>VEN_NONPRIV_UID</code> and <code>VEN_NONPRIV_GID</code> take effect. |

| Variable | Description |
|-----------------------|---|
| VEN_MANAGEMENT_SERVER | The FQDN of PCE server and its port. For example: pce.mycompany.com:8443 |
| VEN_ACTIVATION_CODE | The activation code described in Generate VEN Pairing Profiles and Activation Code (Pairing Key) in PCE Console |

Example of Linux Environment Variables

To activate the VEN during installation, set the following environment variables before invoking the installation command. For details on values for these environment variables, see [Linux VEN Installation with Activation](#).

- 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 single 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
```

For more details about using environment variables, see [Linux Installation and Activation with Environment Variables](#).

Linux VEN Activation After Installation

To activate the VEN after installation, use the `illumio-ven-ctl` control script with the `--activate` option 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 --management-server pce.mycompany.com:8443 --activation-code
activation_code --mode illuminated
```

For information on using the VEN control script for activation, see [illumio-ven-ctl Activation Options](#) and [illumio-ven-ctl Deactivation Options](#).

Install Windows VEN

With the Windows VEN MSI, you have the option of activating (pairing) the VEN either during installation or after installation. Both are described in this guide.

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 Environment Variables

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

Environment variables are not supported with the `illumio-ven-ctl` control script, only with the single 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 . |
| DATAFOLDER | Directory where the <code>illumio_ven_data</code> 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: <code>pce.mycompany.com:8443</code> |
| ACTIVATION_CODE | The activation code described in Generate VEN Pairing Profiles and Activation Code (Pairing Key) in PCE Console |

Set environment variables for custom installation path and data directory

The following installation command line for the VEN on Windows shows the optional use of environment 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
```

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`

For a list of options for activating the Windows VEN, see [Pairing Options](#).

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:> msixexec /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.

Uninstalling the VEN

To uninstall the VEN, Illumio recommends that you use the **Unpair workloads** feature in the PCE web console, which is documented in the [PCE web console user guide](#), rather than the control scripts shown here.

If the PCE is unavailable, you can deactivate/uninstall on the Workload itself with the control scripts described below.

At uninstallation, the VEN unpairs from the PCE.

For more information on pairing options, see [Pairing and Unpairing Command Line Options](#).

Uninstalling the VEN on Linux

The commands below uninstall the VEN:

- **RPM**

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

- **Debian**

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

SUSE Linux: If a SUSE workload is unpaired while 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](#).

Uninstalling the VEN on Windows

The commands below uninstall the VEN. 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.

Upgrade the VEN - See VEN Operations Guide

Because upgrading is often considered an operational task, details for upgrading are in the [VEN Operations Guide](#).

illumio-ven-ctl Syntax and Command-line Options

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

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

Linux illumio-ven-ctl Help

```
$ illumio-ven-ctl --help
```

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

Windows illumio-ven-ctl.ps1 Help


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

```

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

```


illumio-ven-ctl Activation Options

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

If you are activating with a PCE that has a Pairing Profile configured to block changes to policy state (the `illumio-ven-ctl` option `--mode`) or label assignment (the `illumio-ven-ctl` options `--env`, `--loc`, `--role`, `--app`), you must not use these options one 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 |
|---|------------------------------|----------|---|
| <code>--activation-code</code> <code>-a</code> | <code>activation_code</code> | Required | <p>Inputs the activation code of the VEN into the pairing script. This code is auto-generated by the Pairing Profile.</p> <div>  Unique activation code for each workload Do not use a single activation code for more than one workload. The activation code is the unique identifier for the VEN to establish secure communications with the PCE. </div> |
| <code>--management-server</code> <code>-m</code> | PCE hostname/IP | Required | Sets the hostname or IP address of the host where the VEN can retrieve master configuration information. |
| <code>--name</code> <code>-n</code> | server friendly name | Optional | <p>Sets a friendly name that will be used for this workload when it appears in the PCE web console.</p> <p>Example:</p> <pre>--name "Web Server 1"</pre> |
| <code>--env</code> | environment <label_name> | Optional | <p>Inputs an Environment Label for this workload. Example:</p> <pre>--env Production</pre> |
| <code>--loc</code> | location <label_name> | Optional | <p>Example:</p> <pre>--env "Production US"</pre> |
| <code>--role</code> | role <label_name> | Optional | <p>Assigns a Role Label for this workload. Example:</p> <pre>--role "Dev Group"</pre> |

| Option | Argument | Required | Notes |
|---|---|----------|---|
| <code>--app</code> | <code>application <label_name></code> | Optional | Assigns an Application Label for this workload. Example: <code>--app "Web Service"</code> |
| <code>--mode</code> | <code>illuminated enforced idle</code> | Optional | Sets the policy state for the workload. For explanation of the various states, see "Workload Policy States" in the VEN Operations guide. |
| <code>--log-traffic</code> | <code>true false</code> | Optional | Enables or disables traffic logging. If not specified, logging is set to <code>true</code> by default. |
| <code>--visibility-level</code> | <code>flow_summary flow_drops flow_off</code> | Optional | Defines the extent of the data the VEN collects and reports to the PCE from a Workload in the <code>enforced</code> 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. |
| <p>Default: <code>flow_summary</code>.</p> <ul style="list-style-type: none"> <code>flow_summary</code> ("High Detail" in the PCE web console): The VEN collects traffic connection details (source IP, destination IP, protocol, and source and destination port) for both allowed and blocked connections. This option creates traffic links in the Illumination map and is typically used during the building and testing phase of your security policy. <code>flow_drops</code> ("Less Detail" in the PCE web console): The VEN only collects traffic connection details (source IP, destination IP, protocol, and source and destination port) for blocked connections. This option provides less detail for Illumination but demands less system resources from a Workload and is typically used for policy enforcement. <code>flow_off</code> ("No Detail" in the PCE web console): The VEN does not collect any details about traffic connections. This option provides no Illumination detail and demands the least amount of resources from workloads. This mode is useful when you are satisfied with the rules that have been created and do not need additional overhead from observing workload communication. | | | |

| Option | Argument | Required | Notes |
|----------------------------|---------------------------------|----------|---|
| -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. |

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.

| Unpair Option | Description |
|---------------|-------------|
| Windows VEN | |
| recommended | |
| saved | . |
| open | |
| unmanaged | . |

| Linux VEN | |
|-------------|---|
| recommended | |
| saved | . |
| open | . |

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.

Pairing via the VEN Repository ("VEN Repo")

The pairing feature is based on the VEN repo deployment model, described in [VEN Packages vs. Illumio's Central VEN Repo](#). However, the preferred method for activating a VEN is to activate directly on a workload with the [illumio-ven-ctl Activation Options](#).

If you are subscribed to the Illumio Secure Cloud service, have deployed your own on-premises VEN repo, or are using the PCE Virtual Appliance (which embeds a VEN repo), you can deploy the VEN software using the Illumio `pair` script, which is created when you configure a Pairing Profile in the PCE web console.

Pairing Profiles and the Pairing Script

You create a Pairing Profile in the PCE web console. The Pairing Profile allows you to configure the VEN pairing script by setting Label assignments, policy state (idle, illuminated, enforced), as well as creating a pairing key (called an `activation-code` in the pairing script). You can also use the Pairing Profile to configure the lifespan of the pairing key - how long it can be used, or a limit on its uses - as well as the ability to disable the pairing key. For example, you can "stop" the Pairing Profile to prevent the pairing key from that profile from being used to pair any other workloads.

To pair a workload, copy the pairing script of a configured Pairing Profile, open an SSH session to the workload to pair and then paste the pairing script into the shell window. When the script ends, the workload is successfully paired.


What the Pairing Script Does

The script pair script does the following:

- Prepares the target workload for the VEN software package (cleanup existing temp files, create necessary directories).
- Downloads the VEN software package from the repo (using the curl program).
- Installs the VEN Software package on the target workload.
- Activates the VEN with the PCE.

Example Pairing Script for Linux

This is what the pairing script generated from the PCE web console looks like for a Linux-based VEN. The pairing script for Windows is identical except for the OS-related commands.

 If you are using your own repo, the `--management-server` option must match the repo configured for your PCE deployment.

```
$rm -fr /opt/illumio/scripts && umask 027 && mkdir -p /opt/illumio/scripts && curl https://
repo.illum.io/sPl1t0Exo0FIEphoewIujIucrLaT0AS3/pair -o /opt/illumio/scripts/pair && chmod
+x /opt/illumio/scripts/pair && /opt/illumio/scripts/pair --repo-host repo.illum.io --repo-
dir sPl1t0Exo0FIEphoewIujIucrLaT0AS3 --repo-https-port 443 --management-server
pce.mycompany.com:8443 --activation-code activation_code --mode enforced
```

Pairing Script Command Line Overrides

When you configure the Pairing Script in the PCE web console, you can set command line overrides that prevent a user from setting the workload's policy state or Labels.

If you configure a Pairing Script with command `-i` overrides, the person running the pairing script cannot append any other parameters while running the pairing script Curl command on the workload. If a user attempts to add additional "locked" pairing options when running the pairing script, the pairing process fails. The script exits with this final message:

```
"Workload has FAILED pairing with Illumio"
```

When the VEN deployment fails for this reason, an audit event is generated named "Workload pairing failed" with a severity of "Error" in the web console, or listed in syslog (JSON) as 'server_pairing_failed'.

Adding Pairing Options to the Pairing Script

You can add additional pairing options when you run the pairing script, such as assign Labels to the workload, set the workload policy state, and set logging levels for VEN traffic. For a list of pairing options, refer to [Pairing Options](#).

Linux

For example, if you are using a pairing script with no command line overrides, and you wanted to add an Environment Label to the workload (`--env Production`), add the two options at the end of the Linux pairing script as shown here. For ease of reading, the example below uses the Linux line continuation character, which `\`. The actual pairing script is a single line.

```
rm -fr /opt/illumio/scripts && \
umask 027 && \
mkdir -p /opt/illumio/scripts && \
curl https://repo.illum.io/sPl1t0Exo0FIEphoewIujIucrLaT0AS3/pair -o /opt/illumio/scripts/pair && \
chmod +x /opt/illumio/scripts/pair && \
/opt/illumio/scripts/pair \
--repo-host repo.illum.io \
--repo-dir sPl1t0Exo0FIEphoewIujIucrLaT0AS3 \
--repo-https-port 443 \
--management-server pce.mycompany.com:8443 \
--activation-code some_activation_code \
--env Production
```

Windows

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

```
Set-ExecutionPolicy -Scope process remotesigned -Force; `
Start-Sleep -s 3; `
(New-Object System.Net.WebClient).DownloadFile("https://repo.illum.io/Z3JldGVsbHVuZl0aGF0Y2hlcjg1dGgK/`
pair.ps1", "$pwd\Pair.ps1"); `
.\Pair.ps1 `
--repo-host repo.illum.io `
--repo-dir Z3JldGVsbHVuZl0aGF0Y2hlcjg1dGgK/ `
--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 large enterprises use "Golden Master" machine images for faster deployment.

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.
- Do not reuse a single activation code for more than one workload. The activation code is the unique identifier that allows the VEN to establish a secure communication with the PCE.

Using prepare via the Pairing Profile

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

- In the PCE web console, create a Pairing Profile, or you can select an existing Pairing Profile.
- Make a copy your 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 first time the workload is booted.

- Stop the VEN after installation with `prepare`:

```
illumio-ven-ctl stop
```

Using the prepare option on the command line or from a file

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:
 - 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_code: 11bbbe89962159ffe7f0b7e71a532910aa47171f97bc0ad3a0219a780f559006a320587bba966a854
masterconfig_server: pce.mycompany.com:8443
```

The configuration file is read the next time the VEN is started.

Revision History: Illumio ASP VEN Deployment 18.1

| Date | Description |
|------------|--|
| 2018-06-30 | Corrected package dependencies for Red Hat 6 and 7: remove duplicate requirements. |
| 2018-06-27 | <ul style="list-style-type: none"> • Root access is required on the Linux workload to install the Linux VEN. • Cosmetic overhaul |
| 2018-06-18 | Added details about the <code>agent_activation.cfg</code> file in Preparing Golden Master Images for Workload Deployment . |
| 2018-06-15 | <ul style="list-style-type: none"> • Emphasis on Unique Activation Code for Each VEN. • Corrected example of <code>illumio-ven-ctl --mode</code> option. • Corrected broken hyperlinks for Linux environment variables. |

| Date | Description |
|------------|---|
| 2018-06-08 | PKI certificate to download VEN software is no longer required. |
| 2018-06-01 | Included details on Upgrade paths and planning tool . |
| 2018-05-11 | <ul style="list-style-type: none">• Updated for Illumio ASP version 18.1.• Reorganization and miscellaneous corrections throughout; removal of section numbering.• Start of revision history. |