Illumio® Adaptive Security Platform® 18.2 PCE Deployment Guide

09/06/2018

Table of Contents

Product Version

- Illumio Adaptive Security Platform Current PCE Version: 18.2.0 (Standard release)
- Illumio Adaptive Security Platform Current VEN Version: 18.2.0 (Standard 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:

- Your organization's security goals.
- General knowledge of Illumio Adaptive Security Platform.
- General computer system administration of Linux and Windows operating systems, including startup/shutdown, common processes or services.
- Linux shell (bash), Windows PowerShell, or both.
- TCP/IP networks, including protocols, well-known ports, and the Domain Name System (DNS).
- Familiarity with TLS/SSL certificates.

Related Documentation

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

- *Policy Compute Engine (PCE) Web Console Guide*: working with Illumination®, designing security policy, and provisioning and administering VENs.
- *Policy Compute Engine (PCE) Deployment Guide*: planning and installing the PCE.
- *Policy Compute Engine (PCE) Operations Guide:* common management tasks of the PCE.
- *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) Supercluster Reference Implementation*: comparing designs of network architectures for the PCE Supercluster with the F5 Global Traffic Manager (GTM).
- *Policy Compute Engine (PCE) REST API Guide*: web-programming Illumio® Adaptive Security Platform®.

- *Policy Compute Engine (PCE) Advanced Command-line Tool Guide*: using the CLI tool on your own local computer for management of PCE resource objects, including importing vulnerability data for analysis in Illumination®.
- *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 has several high-level divisions:

- Conceptual overview.
- Sections on deployment planning and prerequisites.
- Downloading and installing the PCE.
- Additional deployment tasks.

Overview to PCE Deployment

This document describes the general process and tasks for deploying the on-premises Policy Compute Engine (PCE).

Illumio provides the PCE software, while you provide the hardware, operating system, and associated system services on which the PCE runs.

PCE Multiple Node Clusters

A *PCE node* is a single host (server or VM) that runs the PCE. Each node in the cluster is configured by its node type, which defines its services:

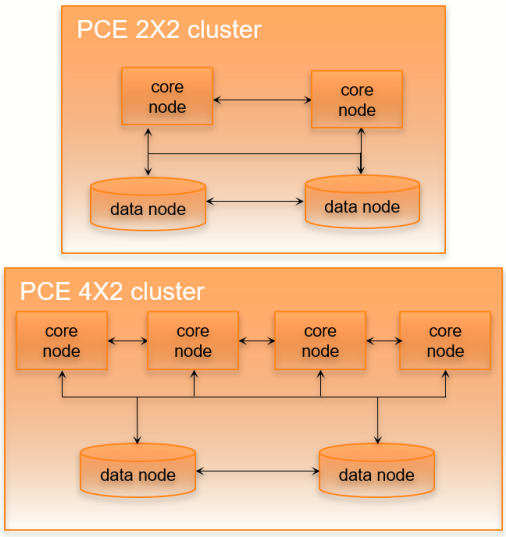
- Core node, known as Core1, Core2, Core 3, and Core 4.
- Data node, known as Data 1 and Data 2.

The total collection of nodes is a *PCE cluster*. In production it is typically deployed as a *multiple node cluster* (MNC).

Multi-node Cluster Configurations - 2X2 and 4X2

- In a typical PCE deployment, for redundancy, you deploy two instances of each node type in a *PCE 2X2 cluster*.
- For larger deployments, you can expand the PCE cluster to four Core nodes and two Data nodes in a *PCE 4X4 cluster*.

PCE Multi-node Cluster Types



PCE Deployment Planning and Prerequisites

Planning Checklist

Below is a checklist planning your deployment. These details are described in later sections.

Prerequisite	See section...
Capacity sizing	PCE Capacity Planning
Verify PCE reserved port ranges	Reserved Port Ranges for PCE Cluster Communications
Load balancer setup	Load Balancer Requirements
DNS domain name setup	DNS Requirements
Mail software	SMTP Requirements
TLS setup, including SSL certificate types and settings	• TLS (SSL) Requirements • Negotiation of TLS versions • Optional -- validate your TLS/SSL certificate
OS package dependencies, libraries, NTP, IPTables, UTF-8, Trusted CA, syslog, process and file limits, and kernel parameters	Operating System Setup and Package Dependencies
Download the software	Download the PCE software
Optionally verify the signature of downloaded package	Optional -- Verify signature of downloaded packages against Illumio's public key
VEN deployment planning	VEN Deployment Models

Upgrade paths and planning tool

For details on upgrade paths for versions of the PCE and VEN, see Versions and Releases on the Illumio support site.

An upgrade planning tool is also available to help you plan your deployments.

PCE Capacity Planning

PCE Cluster Capacity Requirements

Use the guidelines and requirements to estimate host system capacity based on typical usage patterns. Exact requirements vary on a large number of factors, including, but not limited to:

- Number of managed workloads.
- Number of unmanaged workloads and other labeled objects, such as Bound Services.
- Policy complexity, which includes the following:
  - Number of rules in your rulesets.
  - Number of labels, IP lists, and other objects in your rules.
  - Number of IP ranges in your IP lists.
  - Number of workloads affected by your rules.
- Frequency at which your policy changes.
- Frequency at which workload are added or deleted, or workload context changes, such as change of IP address.
- Volume of traffic flows per second reported to the PCE from all VENs.
- Total number of unique flows reported to the PCE from all VENs.

Plan with the recommended sizes
The capacity planning table below shows the **minimal** sizes.
Illumio encourages you to plan for the recommended sizes.
In addition, based on your actual usage and the various specific factors listed above, your capacity needs might be even greater than the recommended sizes.

Type	VENs/ Workloads[1]	Minimum Cores/Clock Speed [2]	Minimum RAM per Node[3]	Minimum Disk Size[4]	Minimum Disk IOPS[5]
2X2	• 2,500 VEN • 12,500 workloads	4 cores per node • 2.4 GHz • Recommended: 3.2 GHz	32 GB	• Core nodes: 100 GB • Data nodes: 250 GB	• Core nodes: 100 IOPS • Data nodes: 600 IOPS

Type	VENs/ Workloads[1]	Minimum Cores/Clock Speed [2]	Minimum RAM per Node[3]	Minimum Disk Size[4]	Minimum Disk IOPS[5]
2X2	• 10,000 VENs • 50,000 workloads	16 cores per node • 2.4 GHz • Recommended: 3.2 GHz	• 64 GB • Recommended: 128 GB	• Core node: 200 GB • Data nodes: 1 TB	• Core nodes: 100 IOPS • Data nodes: 1,800 IOPS
4X2	• 25,000 VENs • 125,000 workloads	16 cores per node • 2.4 GHz • Recommended: 3.2 GHz	• 64 GB • Recommended: 128 GB	• Core nodes: 200 GB • Data nodes: 1 TB	• Core nodes: 100 IOPS • Data nodes: 5,000 IOPS

Footnotes

[1] Estimated, anticipated number of VENs/workloads is the sum of both the estimated number of managed VENs and estimated number of unmanaged workloads.
[2] CPUs:

- The recommendations for number of cores is based only on the *physical* cores from allocated CPUs, irrespective of hyper-threading or virtual cores.
- Full reservations for vCPU. No overcommit.

[3] Full reservations for vRAM. No overcommit.
[4] Additional disk requirements:

- Network File Systems (NFS) is not supported.
- Minimum of 85% of disk size must be allocated to PCE persistent data and logs.

[5] Input/output operations per second (IOPS) are based on 8K random write operations. IOPS specified for an average of 300 flow summaries (80% unique src_ip, dest_ip, dest_port, proto) per workload every 10 minutes. Different traffic profiles may require higher IOPS. For more than 100 IOPS, either Solid-State Disk (SSD) or Storage Area Network (SAN) is required. Locally attached, spinning hard disk drives (HDD) are not sufficient.

Reserved Port Ranges for PCE Cluster Communications

The following port ranges are needed for communications among the nodes of the PCE cluster.

Protocols	Port Range
TCP	3100 to 3600
TCP	5100 to 6300
TCP and UDP	8000 to 8400
TCP	11200 to 11300

Load Balancer Requirements

A server load balancer or DNS-level load balancer is required to distribute traffic to the PCE Core nodes.

Configure the load balancer with the Illumio REST API to monitor the PCE's health check and determine if the cluster core nodes are available. See the *REST API Guide* for exact usage.

```
GET [api_version]/node_available
```

No authentication is required to call this API. An HTTP status code of 200 means the node is healthy and connected to the rest of the cluster. Any other status code or no response means the node is unhealthy and cannot accept requests. Unhealthy or unresponsive nodes should be removed from the load balancing pool.

- There can be up to a 30 second delay for the health check API to return the actual status of the node.
- In the 4x2 configuration, a maximum of two Core nodes are available (return a status code of 200) at any time.
- If you are using a DNS load balancer to handle traffic to the PCE, the DNS must be able to run health checks against the `/node_available` API, and the DNS load balancer should only serve IP addresses for the cluster FQDN of those nodes that respond to the `/node_available` API.

IP Address

A statically-assigned IP address is highly recommended. By default, the PCE uses the first available private IP address you define.

> If you are using a public IP address or if the node has multiple interfaces, you need to configure the PCE to use a different private IP address. For assistance, contact Illumio Customer Support.

To configure networking, see your OS vendor's documentation on the `ifcfg-eth`*`N`* `script`.

DNS Requirements

Your Domain Name System (DNS) must resolve the PCE's Fully Qualified Domain Name (FQDN). The FQDN must be resolvable on all managed workloads, on all nodes in the PCE cluster, and for all users of the PCE web console and REST API.

If you are using DNS-level load balancing the PCE FQDN should resolve to the IP addresses of the Core nodes. If you are using a server load balancer, the PCE FQDN should resolve to the VIP(s) of the server load balancer.

SMTP Requirements

An SMTP relay is required to send user invitations and "forgot password" email replies from the PCE.

The SMTP configuration parameter during PCE installation is `smtp_relay_address`. Allowable values are either an IP address with its SMTP port (default 587) or a resolvable FQDN with the SMTP port.

TLS (SSL) Requirements

PCE communication is secured using the Transport Layer Security (TLS) protocol, the successor to the deprecated Secure Sockets Layer (SSL) protocol. TLS is used for securing the following communication sessions:

- User access to the PCE web console and REST API over the HTTPS protocol.
- Communication between the PCE and VENs.
  VEN-to-PCE communications for the EventService (default is port 8444) are secured by the ECDHE suite of cryptographic ciphers, which use an elliptic curve Diffie-Hellman key exchange. This exchange is signed with RSA signature algorithms.
- Communication between PCE nodes in a multi-node cluster.

If you want to generate a temporary, self-signed certificate, see this Illumio Support KB article for instructions.

For an in-depth discussion of deploying the PCE with TLS, see this this KB titled Preparing Certificates for a PCE deployment.

X.509 Certificate

An X.509 server certificate must be installed on each PCE node during installation. When any client (the VEN) opens a TLS session to the PCE (for example, pairing a workload, accessing the PCE web console, retrieving updated policy), the PCE presents the server certificate to secure the communication. The server certificate is

uploaded as part of a certificate bundle that contains the server certificate and the chain of CA certificates (Intermediate or Root) to establish the chain of trust back to a Root CA. T

> ⚠ The client must be able to validate the chain of trust back to the Root CA for this certificate; otherwise, the TLS handshake fails. You might need to add all the certificates in the chain of trust to the keychain of the client.

The certificate package for the Illumio PCE must meet the following basic criteria:

1. The file must contain PEM-encoded certificates.
2. The certificate's signature algorithm must be SHA256WithRSAEncryption.
3. The certificate's signature algorithm must ***not*** be RSASSA-PSS.
4. The file must contain the server certificate and the entire certificate chain necessary to establish the chain of trust back to a Root CA.
    a. The package must include all of the CA certificates (Intermediate and/or Root) needed to establish the chain of trust back to a Root CA.
        i. If the certificate is generated by a Private CA, all certificates in the chain of trust back to the Root CA must be included. This includes the Root CA Certificate and any applicable Intermediate CA certificates.
        ii. If the certificate is generated by a major Public CA (e.g., VeriSign, GeoTrust, Entrust, Thawte), any Intermediate CA certificates needed to establish the chain of trust back to the Public Root CA must be included.
    b. Pay careful attention to the order of the certificates in the bundle. The server certificate MUST be first. If you have an Apache-style bundle generated by a standard cert request process, you'll need to open the file up in a text editor and reverse the order of the certs. Apache always expects the root cert to come first, then any intermediates in order (from the root down), and the server certificate is last. The PCE uses nginx, which expects the opposite order. For additional details, see the Nginx documentation.
    The certificate bundle should look something like this:

```
-----BEGIN CERTIFICATE-----
<server cert goes here>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<intermediate CA cert goes here>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<root CA cert goes here>
-----END CERTIFICATE-----
```

5. All certificates in the bundle must be valid for the current date. Note that this depends on the system time being set correctly.
6. A trusted root store must be available for OpenSSL to validate certificates.
7. The certificate must match the PCE FQDN. This can be an exact match (e.g., pce.mycompany.com) or a wildcard match (e.g., *. mycompany.com).

The certificate must support both Server and Client authentication. Client authentication is used between nodes in a multi-node cluster. Run the following command and verify `'TLS Web Server Authentication, TLS Web Client Authentication'` appears within the `'X509v3 Extended Key Usage'` section.

```
$ openssl x509 -text -noout -in pce.mycompany.com.bundle.crt

...
 X509v3 Extended Key Usage:
         TLS Web Server Authentication, TLS Web Client Authentication
...
```

RSASSA-PSS Signature Algorithm Not Supported, Use SHA256WithRSEencryption

The certificate signature algorithm RSASSA-PSS, which is based on PKCS 1 version 2.1, is not supported because it cannot be validated. This is a widely known problem with this signature algorithm.

The PCE certificate requires the SHA256WithRSEencryption signature.

> ⚠ If you use Microsoft Certificate Authority (CA) to sign PCE certificates, make sure to use the SHA256WithRSEencryption. PKCS#1 version 2.1 is enabled by default on Microsoft CAs and thus produces the unsupported RSASSA-PSS signature algorithm.

Private Keys

The private key that matches the X.509 certificate must be installed on each PCE node during installation:

- The private key must be PEM-encoded.
- The file must not be encoded.
- The file must not be password protected.

Negotiation of TLS Versions for Communications

The PCE negotiates the use of Transport Layer Security (TLS) versions 1.0, 1.1 or 1.2 for VEN-to-PCE communications, the PCE's web server for the PCE web console, and the REST API. The PCE selects the highest version that the your workloads support.

- The PCE default minimum version is TLS 1.0.
- For VEN versions 18.1 and later, all VENs are use TLS 1.2.
- SUSE VEN version 17.1.x requires minimum version TLS 1.0.

- Windows Server 2008 R2 SP1: The HTTP Client library, WinHttp, does not have the necessary API to limit SSL negotiation only to TLS 1.2. This must be configured via the Registry.

Changing Default TLS version

You can use TLS 1.0, 1.1 or 1.2 with any version of the VEN, except version 17.1, which requires TLS 1.0. In addition, you should verify that any browser you use is capable of negotiating the minimum version you set.

If you want to change the minimum TLS version, edit the following parameter in `runtime_env.yml`:

```
min_tls_version
```

The value of `min_tls_version` configures the PCE front end ports in `runtime_env.yml`:

- `front_end_https_port` (default 8443)
- `front_end_https_management_port` (defaults to front_end_https_port)
- `front_end_event_service_port` (default 8444)

Allowable values:

- `tls1_0` allows TLS 1.0, 1.1, and 1.2.
- `tls1_1` allows TLS 1.1 and 1.2.
- `tls1_2` allows only TLS 1.2.

Operating System Setup and Package Dependencies

The PCE is supported on Red Hat Enterprise Linux (RHEL) or CentOS 6 or 7 and minor release versions.

NTP

Set up a Network Time Protocol (NTP) client for time synchronization.

To install and configure NTP, run the following commands:

```
# yum install ntp # Install ntp module
# date # Verify that the timezone is set correctly. If wrong, fix the timezone with timedatectl set-timezone
# systemctl enable ntpd # Set NTP to start at boot
# service start ntpd # Start the ntpd daemon
# chkconfig ntpd on # Verify the ntpd daemon configuration
```

IPTables

For the initial installation, you might want to disable iptables.

If iptables is enabled, you must configure it to allow inbound HTTPS connections to the PCE core nodes and service ports.

```
# service iptables stop
# chkconfig iptables off
```

Language: UTF-8

Set the system language to a UTF-8 variant of English either `en_US.UTF-8` or `en_GB.UTF-8`.

Set the variable `LANG="en_US.UTF-8"` or `LANG="en_GB.UTF-8" in the following files:`

- RHEL 6: `/etc/sysconfig/i18n`
- RHEL 7: `/etc/locale.conf`

Trusted Public Certificate Authority (CA) Store

A trusted root public CA store must be available for OpenSSL to validate certificates.

If you rely on a certificate signed by a public CA, be sure to install the latest public root CA certificates `ca-certificates` package.

```
# yum install ca-certificates
```

If your certificate is signed by a private CA or if the signing CAs are already included in each node's trusted root CA store, the `ca-certificates` package is not required.

syslog

A syslog daemon such as rsyslog, syslog-ng must be configured and running on the core node.

On RHEL/CentOS, rsyslog is installed by default. Run the following command to verify it is running:

```
# service rsyslog status
```

Preview – PCE-internal syslog. This release of Illumio Advanced Security Platform includes a preview feature: PCE-internal syslog. The purpose of the PCE-internal syslog is to help organizations use syslog without installing it themselves. For documentation, contact Illumio Customer Support.

Process and File Limits

For best performance, modify the parameters detailed here in the `/etc/security/limits.conf` file for each node.

Core Nodes values in limits.conf

Failure to set these values correctly can severely impact system performance.

- If your settings are already greater than these, you do not need to reduce them to these values.
- If you have automated processes that change these values, adjust those processes to not change them.
- To restrict this change to only the PCE runtime user, then replace the asterisk shown below with the Unix user-id of the defined PCE runtime user.
- If you run additional processes on the PCE, such as monitoring or other operations processes, you might need to increase the value of `nofile`.

```
* soft    core            unlimited
* hard    core            unlimited

* hard    nproc           65535
* soft    nproc           65535

* hard    nofile          65535
* soft    nofile          65535
```

Data Nodes values in limits.conf

```
* soft    core            unlimited
* hard    core            unlimited
```

Core Nodes values in 90-nproc.conf

If the `/etc/security/limits.d/90-nproc.conf` file is configured on your system, you must also change its `nproc` values.

Be sure there are no additional configuration files in `/etc/security/limits.d` that might override the recommended limits.

```
* hard    nproc           65535
* soft    nproc           65535
```

Kernel Parameters in sysctl.conf

For optimal performance of the PCE, set the following kernel parameters for each node.

If your settings are greater than these, you do not need to lower them.

Parameters are configured in the `/etc/sysctl.conf` file. After the settings are configured, apply them to the kernel with the following command. Otherwise, the changes take effect at the next boot.

```
# sysctl -p
```

Core Nodes in sysctl.conf

```
fs.file-max        = 2000000
net.core.somaxconn = 16384
```

Data Nodes in sysctl.conf

```
 fs.file-max          = 2000000
kernel.shmmax        = 60000000
vm.overcommit_memory = 1
```

About Your Organization Name

Have ready your full organization name, which you specify at installation.

For on-premise PCE deployments, installation creates an organization identifier (org-ID) and assigns the value of `1` to org ID. The value `1` distinguishes your on-premises PCE from the Illumio Adaptive Security Platform Cloud (SaaS) service. The org-ID is needed with the REST API and other purposes.

Download the PCE Software

Download the software from the Illumio Support site.

Install the PCE Software

The PCE RPM is the easiest way to install the software if you can use the default directory locations and runtime user account (`ilo-pce`).

As root, run this command to install the PCE on each of the nodes in your deployment:

```
# rpm -ivh /path_to/pce_rpm_file
```

After the installation and and configuration of the PCE, you do not need to run the PCE as root.

After you have installed the RPM, run the PCE setup wizard to configure the software.

RPM Installation Directories

The PCE software RPM installs to the following directories:

Location	Contents at Installation	Permissions / Ownership
`/opt/illumio-pce/`	PCE software	`dr-xr-x---. root ilo-pce`
`/etc/illumio-pce`	Empty	`drwxr-xr-x. root root`
`/etc/init.d/illumio-pce`	Service script	`-rwxr-xr-x. root root`

`/var/lib/illumio-pce/`
`tmp/`
`runtime/`
`data/`
`keys/`
`cert/`
	Empty	`drwxr-x---. root ilo-pce`
		`drwx------. ilo-pce ilo-pce`
		`drwx------. ilo-pce ilo-pce`
		`drwx------. ilo-pce ilo-pce`
		`drwx------. ilo-pce ilo-pce`
		`drwx------. ilo-pce ilo-pce`

`/var/log/illumio-pce`	Log files	`drwx------. ilo-pce ilo-pce`

RPM Runtime User and Group

The PCE installation creates a runtime user and group named `ilo-pce` to run the PCE software. For security, the `ilo-pce` user is configured without a login shell or home directory.

> **No login shell or home directory**
> For better security, do not give the `ilo-pce` user a login shell or home directory.

PCE comands should be run as root or as a user belonging to the `ilo-pce` group. You run the PCE software with `sudo`, as shown throughout this guide:

```
# sudo -u ilo-pce somePCEcommand
```

You might have have a need to put several users into the `ilo-pce` group for shared maintenance or other needs. However, only the `ilo-pce` user is actually used to run the software.

Used in

- 18.1 PCE Ops guide
- 18.1.deployment guide
- 18.2 PCE Deployment guide
- 18.2 Ops guide

PCE Control Interface

The Illumio PCE control interface `illumio-pce-ctl` is a command-line tool for performing key tasks for operating your PCE cluster such as starting and stopping nodes, setting cluster runlevels, and checking the cluster status.

The PCE also includes two other command-line utilities used to setup and operate your PCE:

- `illumio-pce-env`. Used for verifying and collecting information about the PCE runtime environment.
- `illumio-pce-db-management`. Used for PCE database management.
- `supercluster-sub-command`. Used for Supercluster specific operations.

The PCE control interface can only be executed by the PCE runtime user (`ilo-pce`), which is created during the PCE RPM installation.

In this document, all command-line examples assume a RPM installation. If you installed the PCE tarball, you will need to modify the commands based on your PCE user account and the directory where you installed the software.

Control command access via /usr/bin. By default, for easier command execution, the installation of the PCE creates softlinks in `/usr/bin` for the Illumio PCE control commands. The `/usr/bin` directory is usually included by default in the PATH environment variable in most Linux systems. If for some reason your PATH does not include `/usr/bin`, add it to your PATH with the following command. You might want to add this command to your login files (`$HOME/.bashrc` or `$HOME/.cshrc`).

```
export PATH=$PATH:/usr/bin
```

Syntax

In this document, all command-line examples assume a RPM installation. If you installed the PCE tarball, you will need to modify the commands based on your PCE user account and the directory where you installed the software.

to make it simpler to run the PCE command-line tools. you can either run the following Linux softlink commands or add them to your PTH environment variable as described above.

```
$ cd /usr/bin $ sudo ln -s /opt/illumio-pce/illumio-pce-ctl ./illumio-pce-ctl $ sudo ln -s /opt/illumio-pce/illumio-pce-db-management ./illumio-pce-db-management $ sudo ln -s /opt/illumio-pce/illumio-pce-env ./illumio-pce-env
```

After these commands are executed, you can run the PCE command-line tools using the following syntax:

```
$ sudo -u ilo-pce illumio-pce-ctl sub-command -option
```

where:

- *sub-command* is an argument displayed by `illumio-pce-ctl --help`.

Validate and Install the TLS Certificate and Private Key

For information on the contents and formats of your certificates see "TLS Requirements".

Optionally validate your certificate

Your TLS certificates are validated at start-up. An error message is displayed if the certificate or its chain of trust is not valid.

You can validate your TLS certificate yourself, including the chain of trust and other aspects, with the `illumio-pce-env setup --list` command. The `--list` option does not create a new `runtime_env.yml` configuration file, discussed in "Configure the PCE with the Setup Script", but instead performs a series of checks on your configuration, including certificates, and gives a more complete indication of possible problems.

Validate after installing certificates

If you have already installed your certificates in the locations configured in the `runtime_env.yml` file, you can validate with the following command. The `--test` option takes a verbosity level argument, which is from 1 (least verbose) to 5 (most verbose). With verbosity level 5, the command displays the results of its validation of your certificates.

```
illumio-pce-env setup --list --test 5
```

Alternative syntax for certificate validation after installing

Additional mechanisms for certificate validation include:

- `illumio-pce-env setup --list --test 5:`*`some.alternative.hostname`*

  This syntax checks the certificate and chain against the specified *`some.alternative.hostname`*, such as the FQDN you plan to use for the PCE in production.

- `illumio-pce-env setup --list --test 5+`

  The `+` syntax creates a loopback OpenSSL server running on port 4433 and attempts to curl to it.

Validate before installing certificates without runtime_env.yml file

If you have not yet configured your `runtime_env.yml` file, discussed in Configure the PCE with the Setup Script, and want to validate your certificates before copying them to your planned production location, use the following command.

```
# illumio-pce-env setup --batch --list email=required@emailaddress node=snc0 \
cert=/path/to/cert pkey=/path/to/private_key trust=/path/to/certificate_chain --test 5
```

Option	Description
`email=`	A value is required
`node=snc0`	Topology to check.
`cert=`	The absolute path to your certificate
`pkey=`	The absolute path to your certificate's private key
`trust=`	The absolute path to your certificate's CA chain of trust

Messages for valid certificates, errors, and warnings

Correctly configured certificates are indicated by these messages:

- `Valid: Certificate chain is verified`
- `Valid: web_service_certificate tests passed.`

Possible problems with the certificates are indicated by error messages such as the following:

- `Warning: group xxx can write to web_service_certificate`
- `Error: unable to find trusted_ca_bundle yyy`
- `Warning: trusted_ca_bundle missing or inaccessible.`
- `Missing CA`
- `Error: unable to verify certificate chain`
- `Error: unable to validate web_service_certificate`

Install certificate

Copy the TLS certificate and private key to each of the nodes in your deployment.

You can store the files in any readable location on the node. The PCE RPM installation creates the `/var/lib/illumio-pce/cert` directory where you can store these files.

The certificate and private key must be readable by the PCE runtime user.

Configure the PCE with the Setup Wizard

After the basic installation, configure the PCE.

Prior to running the software, you need to be sure it is properly configured with a runtime configuration.

The PCE Runtime Environment File (`runtime_env.yml`) is used to configure the PCE software. The default location of this file is `/etc/illumio-pce/runtime_env.yml`. You can override this location by setting the `ILLUMIO_RUNTIME_ENV` environment variable. You can create the `runtime_env.yml` file manually or use the PCE software setup script to create and modify the file.

Before you run the PCE software setup script, make sure you review the required parameters in the PCE `runtime_env.yml` file. For a list of all required and optional PCE software configuration parameters, see Runtime Environment File Parameters.

You will be prompted to provide these parameters during the setup.

Launch the PCE Setup Wizard

From the host command line, **as root**, run the following command to launch the setup wizard:

```
[root]# illumio-pce-env setup
```

Using the PCE Setup Wizard

When you first launch the setup wizard from the command prompt, the script will indicate if the `$ILLUMIO_RUNTIME_ENV` environment variable is set:

These first two screens will only appear if you launch the setup wizard from the command line (i.e., you installed directly from RPM and did not use the ISO).

```
$ Illumio PCE Runtime Setup (new configuration -> ENV=my_pce.yml):
```

The `ENV= text` indicates that the new configuration will be written to the file defines for `ILLUMIO_RUNTIME_ENV`. If the `ILLUMIO_RUNTIME_ENV` environment variable is not set, the setup will display that this is a new configuration and write the `runtime_env.yml` file to the default location (`/etc/illumio-pce/runtime_env.yml`).

```
$ Illumio PCE Runtime Setup (new configuration)
```

General Configuration

The setup wizard displays any descriptive help text followed by a prompt where you can either accept the previous or default value, or enter a new value. If the field is optional, pressing Enter on your keyboard will clear the field from view if the resulting value is empty. If instead there is a corresponding default value it displays `# default` next to that value.

The prompt itself encapsulates the previous value in brackets:

```
node_type [core]:
```

Pressing Enter will keep the value in brackets. Any previously-set value always takes precedence at the prompt; e.g., if there's a previous value, it will be displayed instead of any default one.

If you are unsure whether the value displayed by the prompt is a previously set or default or recommended value, you can enter a question mark (`?`). This will display the default or recommended value, if available:

```
opts =>  core [ data0 data1 ]
node_type [core]: ?
```

If there are multiple options, you may use the auto-complete functionality by typing the first few characters and pressing Tab on your keyboard to auto-complete or suggest any remaining choices. When the prompt is for a directory or filename, you may use the autocomplete function to more quickly populate the field

When using the prompted wizard, you can press CTRL+C to escape to a control menu which provides the following options:

- Quit without saving
- Restart the wizard (with an optional field value)
- Skip to a future field (with a field value)
- Save (with an optional target file)
- Exit

For example, entering this command will save the configuration to a different file and quit the setup.

```
 $ Type (q)uit, (r)estart, (f)ield, (s)ave to file or default resume: save /tmp/
sample.cfg
```

Command-line, Batch or List Mode (--batch, --list)

The batch option is used to operate the setup script from the command-line. Instead of prompting for each value, it automatically accepts any previous/default value automatically. If there are missing (non-optional) fields, it displays an error and returns a non-zero exit code. To set a value on the command-line, use:

```
[root]# illumio-pce-env setup front_end_https_port=7443 pce_fqdn="sample.illumio.com" -b
```

This will set these values instead of prompting for them. You can also pre-set these values in non-batch mode by using key=value arguments.

> **Batch mode creates new configuration file**
> Batch mode automatically saves the new configuration unless there is an error.

The `--list` option also does not prompt for values. It displays the currently configured values, replacing them with any specified command-line values. The `--list` option does not save the configuration to the `runtime_env.yml` file. The `--list` option is useful to validate your TLS/SSL certificate.

Advanced Runtime Environment Parameters

Your Illumio support representative may provide you with certain advanced parameters to add to your `runtime_env.yml` file. If you include the name of these parameters on the command line, the setup script will prompt for them.

```
[root]# illumio-pce-env setup <advanced_parameter_name_1> <advanced_parameter_name_2> ...
```

Additional Options

When using the setup script, several additional options are available. You can use `-h` to display these options:

Usage

```
[root]# illumio-pce-env setup [options...] [field[:field...]=[value[,value...]]...
```

Display Options

Option	Descriptions
`-b, --batch`	Don't prompt for field values.
`-d, --default`	Show default values.
`-e, --empty`	Display empty fields (implies `-d`).
`-f, --field  *[:*][,...]`	Specify a field pattern list; only process these items.
`-g, --[no-]guide`	Show descriptive information for each field where available (default).
`-h, --help`	Provide usage statement.
`-m, --macros`	Show list of available shortcut keys.
`-o, --[no-]optional`	Process optional fields (default).
`-q, --quiet`	Don't display help text for each field (same as `--no-guide`)
`-r, --reveal`	Don't mask secret key(s) in field output.
`-t, --text`	Use regular text instead of colors.

File Options

Option	Description
`-c, --config <file>`	Process a different environment file (`new=-`).
`-s, --save <file>`	Save results to a different file (`stdout=-, system default=!`).
`-z, --zap`	Remove pre-existing default fields.

Verify the PCE Runtime Environment

After configuring the `runtime_env.yml` file, run the environment check command to ensure the node is properly set up.

As the PCE runtime user, run the following command:

```
# sudo -u ilo-pce illumio-pce-env check
Checking PCE runtime environment.
OK
```

Correct any errors before proceeding.

Used in

- 18.1 PCE Ops guide
- 18.1.deployment guide
- 18.2 PCE Deployment guide
- 18.2 Ops guide

PCE Control Interface

The Illumio PCE control interface `illumio-pce-ctl` is a command-line tool for performing key tasks for operating your PCE cluster such as starting and stopping nodes, setting cluster runlevels, and checking the cluster status.

The PCE also includes two other command-line utilities used to setup and operate your PCE:

- `illumio-pce-env`. Used for verifying and collecting information about the PCE runtime environment.
- `illumio-pce-db-management`. Used for PCE database management.
- `supercluster-sub-command`. Used for Supercluster specific operations.

The PCE control interface can only be executed by the PCE runtime user (`ilo-pce`), which is created during the PCE RPM installation.

In this document, all command-line examples assume a RPM installation. If you installed the PCE tarball, you will need to modify the commands based on your PCE user account and the directory where you installed the software.

Control command access via /usr/bin. By default, for easier command execution, the installation of the PCE creates softlinks in `/usr/bin` for the Illumio PCE control commands. The `/usr/bin` directory is usually included by default in the PATH environment variable in most Linux systems. If for some reason your PATH does not include `/usr/bin`, add it to your PATH with the following command. You might want to add this command to your login files (`$HOME/.bashrc` or `$HOME/.cshrc`).

```
export PATH=$PATH:/usr/bin
```

Syntax

In this document, all command-line examples assume a RPM installation. If you installed the PCE tarball, you will need to modify the commands based on your PCE user account and the directory where you installed the software.

to make it simpler to run the PCE command-line tools. you can either run the following Linux softlink commands or add them to your PTH environment variable as described above.

```
$ cd /usr/bin $ sudo ln -s /opt/illumio-pce/illumio-pce-ctl ./illumio-pce-ctl $ sudo ln
-s /opt/illumio-pce/illumio-pce-db-management ./illumio-pce-db-management $ sudo ln -s /
opt/illumio-pce/illumio-pce-env ./illumio-pce-env
```

After these commands are executed, you can run the PCE command-line tools using the following syntax:

```
$ sudo -u ilo-pce illumio-pce-ctl sub-command -option
```

where:

- *sub-command* is an argument displayed by `illumio-pce-ctl --help`.

PCE Service Script illumio-pce for Boot

The `illumio-pce service` script in `/etc/init.d/illumio-pce` is switches to the runtime user (`ilo-pce`) prior to running other PCE program. The primary purpose of the `init.d` service script is to start the product on boot. The service script can also be run with the `/sbin/service` command.

```
$ service illumio-pce
Usage: illumio-pce {start|stop|restart|[cluster-]status|{set|get}-runlevel|control|database|
environment|setup}
```

Runlevels

PCE runlevels define the system services started for common operations, such as upgrade, downgrade, and restore.

The runlevel is set with the following command:

```
illumio-pce-ctl set-runlevel numeric_runlevel
```

The *numeric_runlevel* varies by type of operation.

Setting runlevel might take some time to complete, depending on the cluster configuration. Check the progress with the following command:

```
illumio-pce-ctl cluster-status -w
```

PCE Start

As the PCE runtime user, perform the following steps:

1. **On each node**, start the PCE at runlevel 1.

   ```
   # sudo -u ilo-pce illumio-pce-ctl start --runlevel 1
   ```

2. **On each node**, check the status of the software. Make sure the node status is RUNNING before proceeding to the next step. It can take up to 10 minutes for the various services to start.

   ```
   # sudo -u ilo-pce illumio-pce-ctl status
   Checking Illumio Runtime            RUNNING 0.38s
   ```

   If the node does not come up properly after 10 minutes, check the following:
   a. Runtime environment file
   b. Network connectivity between nodes/iptables
   c. Certificates
   d. System locale (must be UTF-8)

Initialize the PCE

As the PCE runtime user, perform the following steps:

1. **On any node**, run the following command to initialize the PCE database:

   ```
   # sudo -u ilo-pce illumio-pce-db-management setup
   ```

2. **On the data0 node**, bring the system up to run level 5.

   ```
   # sudo -u ilo-pce illumio-pce-ctl set-runlevel 5
   ```

3. **On any Core node**, check the status of the cluster.

```
# sudo -u ilo-pce illumio-pce-ctl cluster-status
```

Important: Make sure the cluster status is `Running` before proceeding to the next step.

4. **On any Core node**, create the initial PCE user and organization name. You are prompted for a password. The password must conform to these restrictions: at least 8 characters, no more than 128 characters, at least 1 upper case character, 1 lower case character and 1 number.

```
# sudo -u ilo-pce illumio-pce-db-management  create-domain --user-name <user-email-address>
--full-name  '<user-full-name>'  --org-name  '<organization-name>'
```

For example:

```
# sudo -u ilo-pce illumio-pce-db-management  create-domain --user-name myuser@mycompany.com --full-name
'Joe User' --org-name  'ACME Inc.'

Reading /var/illumio-pce-data/runtime_env.yml.
INSTALL_ROOT=/var/illumio-pce
RENV=production (defaulted because not set in runtime_env.yml)

Please enter a password with at least 8 characters with one uppercase, one lowercase and
one number.

Enter Password:
Re-enter Password:
------------------------------------------------------------
Running cd /var/illumio-pce/illumio/webservices/people && RAILS_ENV=production bundle exec rails
runner script/create_org_owner
--output-file /tmp/illumio/org.yml --user-name myuser@mycompany.com --create-org
--org-name 'ACME Inc.'
Completed in 5.471846432 sec. Exit Code = 0
------------------------------------------------------------
Running cd /var/illumio-pce/illumio/webservices/agent && RAILS_ENV=production bundle
exec rails runner script/create_org_defaults
--input-file /tmp/Illumio/org.yml
Completed in 5.609754678 sec. Exit Code = 0
------------------------------------------------------------
Running cd /var/illumio-pce/illumio/webservices/login && RAILS_ENV=production
ILO_**********bundle exec rails runner
script/setup_initial_config --org-data /tmp/Illumio/org.yml
--user-name myuser@mycompany.com
--full-name 'Joe User'
domain_name=mycompany.com
  Completed in 5.303522871 sec. Exit Code = 0
Done.
```

5. Point a web browser to the PCE FQDN and log in using the account you just created.
6. The PCE is now up and running.

Additional Deployment Tasks

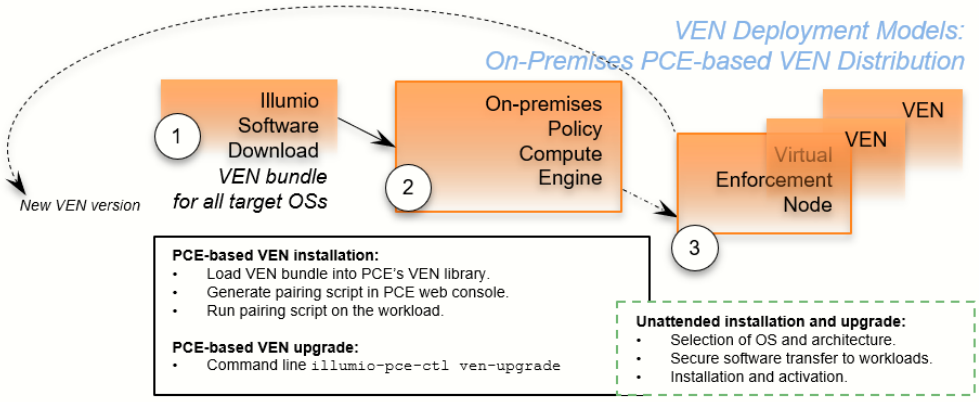
VEN Deployment Models

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.

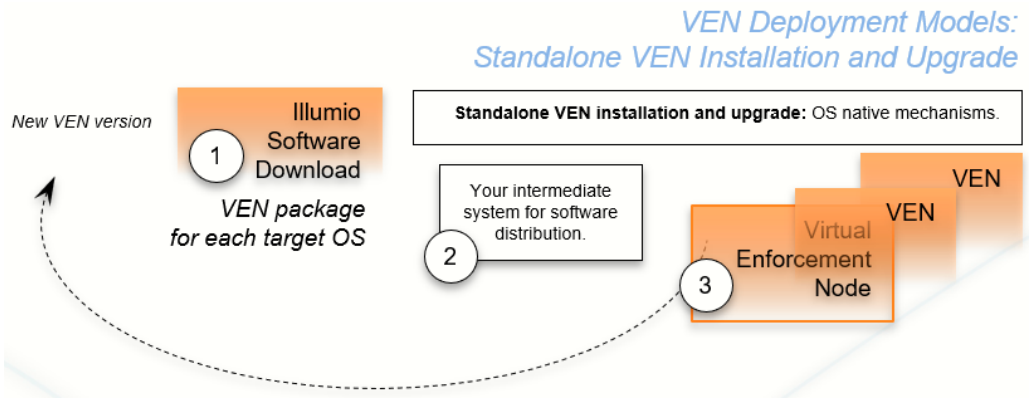
    - Installs the VEN software.
    - Activates/pairs the VEN with its PCE.
- For VEN upgrade, on the on-premises PCE command-line, you run `illumio-pce-ctl ven-upgrade` for either all workloads or selective workloads.
- Some features are not available with PCE-based deployment, such as Kerberos support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

For more information, see the *VEN Deployment Guide*.

Configure PCE backups

You should maintain and perform regular backups of the PCE database based on your company's backup policy. Additionally, always backup your PCE database before upgrading to a new version of the PCE.

As the PCE runtime user, run this command to back up the PCE database to a file:

```
# sudo -u ilo-pce illumio-pce-db-management dump –-file <location-of-db-dump-file>
```

Configure syslog

Most PCE logs are written to syslog. Without additional configuration, syslog sends the PCE log message to the default destination on your Linux host, `/var/log/messages`. To change this default, configure the syslog service on each node. See the *Auditable Events and SIEM Integration Guide*.

Configure Log Rotation

To manage the size of log files, configure logrotate or your own custom equivalent.

The PCE includes a configuration template for logrotate in `install_root/templates`.

Files	Contents	Recommended Rotation and Pruning Schedule
`/var/log/messages` (or syslog configuration location)	PCE logs written to syslog	• Rotate at 100MB • Compress archived files • Keep 9 archived files before deleting
`log_dir/*`	PCE logs written to file	• Rotate at 10MB • Compress archived files • Keep 4 archived files before deleting

Files	Contents	Recommended Rotation and Pruning Schedule
`log_dir/systats`	PCE system statistics written to file, such as top 10 processes by memory and CPU and disk usage	**No action required.** These files are automatically rotated daily.

Runtime Environment File Parameters

This section lists important PCE runtime configuration parameters, their meaning, their purpose, and their exposure levels.

Runtime File Exposure Levels

The Illumio PCE `runtime_env.yml` file provides the following exposure levels for PCE configuration:

- **Public Stable** (`public_stable`). These `runtime_env.yml` parameters can be used by all customers. All changes backward compatible.
- **Public Experimental** (`public_experimental`). These `runtime_env.yml` parameters can be used by all customers but might change from release to release with no guarantee of backwards compatibility.

Required Runtime Parameters

The following table lists required `runtime_env.yml` file parameters for each PCE software node you deploy. All required parameters have no default values. All paths configured in this file must be absolute.

Runtime Environment File Parameter	Description	Exposure Level
`enabled_preview_features`	Includes sub-parameters to enable identified preview features	
`install_root`	The full path to the location of the PCE binaries and scripts. The software does not write to any files in this directory, so it can be read-only. For example: `install_root: /opt/illumio-pce`	Public Stable

Runtime Environment File Parameter	Description	Exposure Level
`runtime_data_root`	The full path to the location where the PCE writes runtime data. This data can be deleted on reboot, if necessary. This directory should have 700 permissions, but all of its files will have 600 permissions. This directory must be owned by the user that runs the PCE software. For example: `runtime_data_root: /var/lib/illumio-pce/runtime`	Public Stable
`persistent_data_root`	The full path to the location where the PCE writes persistent data. This data must persist across reboots for the software to work properly. This directory should have 700 permissions, but all of its files will have 600 permissions. This directory must be owned by the user that runs the PCE software. For example: `persistent_data_root: /var/lib/illumio-pce/data`	Public Stable

Runtime Environment File Parameter	Description	Exposure Level
`ephemeral_data_root`	The full path to the location where the PCE writes temporary files. These files must not be deleted while the software is running, but they should be deleted on reboot. This directory should have 700 permissions, but all of its files will have 600 permissions. **Note**: Illumio does not recommend using '`/tmp`' due to the '`tmpwatch`' utility on RHEL/CentOS 6. For example: `ephemeral_data_root: /var/lib/illumio-pce/tmp`	Public Stable
`log_dir`	The PCE software writes some text file logs to this directory (although most PCE services log to syslog). `logrotate` (or similar) should be used to manage these files. For example: `log_dir: /var/log/illumio-pce`	Public Stable
`pce_fqdn`	The Fully Qualified Domain Name (FQDN) of the PCE cluster. For example: `pce_fqdn: pce.mycompany.com`	Public Stable
`cluster_public_ips: cluster_fqdn`	The FQDN of your entire cluster. **Note:** If you change the value of `cluster_public_ips`, wait for the paired VENs to receive the new IP addresses and begin heartbeating to them.	Public Stable

Runtime Environment File Parameter	Description	Exposure Level
`web_service_certificate`	Full path to the X.509 public certificate used by this node for Transport Layer Security (TLS). See the 'Certificate Requirements' section above for more information on the contents of the certificate files. For example: `web_service_certificate: /etc/pki/tls/certs/my_cert.crt`	Public Stable

`web_service_private_key`	Specify the RSA Private Key for TLS that matches the public certificate.
	
	The Private Key must be PEM encoded in PKCS#12 format, without a password.
	
	For example:
	
	`web_service_private_key: /var/lib/illumio-pce/cert/rsa_private_key.key`
	
	Altneratively, you may specify a script (using $ notation) that outputs the private key. This is useful if you need to store the key in a Hardware Security Module (HSM) or other key store.
	
	For example:
	
	`web_service_private_key: $ /var/lib/illumio-pce/cert/get_rsa_private_key.sh`
	
	Note that this script can be located anywhere on the file system, as long as it is executable by the `ilo-pce user`.
	
	Example script output:
	
	`$ /local/scripts/get_rsa_private_key.sh`
	`-----BEGIN RSA PRIVATE KEY-----`
	`MIIE...`
	`many lines trimmed here`
	`-----END RSA PRIVATE KEY-----`
		Public Stable

Runtime Environment File Parameter	Description	Exposure Level
`email_address`	Email sender address to be used by the PCE when sending emails from the system. For example, to send invitations and notifications. For example: `email_address: noreply @exampleblocked_traffic.com`	Public Stable
`service_discovery_fqdn`	The FQDN or IP address of the first core node.	Public Experimental
`service_discovery_encryption_key`	Key used to encrypt Service Discovery node traffic. This value must be the same for all PCE nodes. This key also must be 16 bytes that are base64 encoded. For example: `service_discovery_encryption_key: 6h09ACGeLksZXkG5OtkcDw==`	Public Stable
`node_type`	The type of the PCE software node. Possible values: • `snc0 (Not supported for production)` • `core` • `data0` • `data1` For example: `node_type: core`	Public Stable
`login_banner`	Allows on premise customers customize the messaging on the PCE log in screen, typically used for legal copy when a user logs in according to company policy.	Public Stable

Optional Runtime Parameters

The following table lists common optional `runtime_env.yml` file parameters for each PCE software node you deploy. Your Illumio Professional Services representative may provide additional parameters to configure certain advanced functions.

Runtime Environment File Parameter	Description	Exposure Level
`ven_repo_url`	The base URL used to fetch the VENs and to enable Workload pairing with the PCE. This value must be in the form `https://host[:port]/repo_dir` Alternate ports can be used by specifying the port at the end of hostname and `repo_dir` cannot be empty. For example: `https://repo.example.com:8443/onpremgCBURz8Y4zkGk1u7N9ialjPGlZ` **Default Value**: None.	Public Stable

Runtime Environment File Parameter	Description	Exposure Level

`ven_repo_ips`	IP addresses of the VEN repository.
	
	These IP addresses are injected into iptables to allow outbound access to the `yum/apt get` repos without having to write an explicit PCE policy.
	
	Setting this parameter also allows outbound access on 80 and 443 to these IP addresses. You can specify both single IP addresses or IP addresses with CIDR notation.
	
	If this parameter is not specified, the VEN will not be allowed to access the repository containing VEN software packages.
	
	For example:
	
	`ven_repo_ips:`
	`- 1.2.3.4`
	`- 5.6.7.8/8`
	
	Default Value: None.
		Public Stable

`cluster_type`	PCE cluster type. One of these two types: • `4node_v0`: 2x2 PCE Cluster • `6node_v0`: 4x2 PCE Cluster **Default Value**: `4node_v0`.	Public Stable

Runtime Environment File Parameter	Description	Exposure Level
`front_end_https_port`	The front end HTTPS port. If the cluster is front-ended by a SLB such as F5, then the SLB must be configured to forward this port. For example: `front_end_https_port: 8443` **Default Value**: See also `front_end_management_https_port`. If neither `front_end_management_https_port` nor `front_end_https_port` have been set, the default is TCP 8443.	Public Stable
`front_end_event_service_port`	The front end Event Service port. If not specified, then port 8444 is used. If the cluster is front-ended by a SLB such as F5, then the SLB must be configured to forward this port. The idle connection timeout on the SLB may also need to be configured to maintain the connections on this port. Please consult with your Illumio Professional Services representative for additional information on configuring your load balancer. For example: `front_end_event_service_port: 8444` **Default Value**: `8444`	Public Stable

Runtime Environment File Parameter	Description	Exposure Level
`front_end_management_https_port`	The port for PCE Web Console and REST API. The purpose of this key is to separate different kinds of communication. See also `front_end_https_port`. If neither `front_end_management_https_port` nor `front_end_https_port` have been set, the default is TCP 8443.	Public Stable
`syslog_event_export_format`	Allows you to specify VEN flow summaries and Organization events to the following event formats for export: CEF, LEEF, or JSON. **Note**: If you specify CEF or LEEF, you will continue getting traffic flows and Organization events in JSON.	Public Stable

`trusted_ca_bundle`	Path to the Trusted Root Certificate bundle.
	
	This parameter is used by the PCE to validate that the certificates are trusted and indicates the path to the trusted root certificate bundle file.
	
	For example:
	
	`trusted_ca_bundle: /etc/ssl/certs/ca-bundle.crt`
	
	Default Value:
	`/etc/ssl/certs/ca-bundle.crt`
		Public
		Stable

`email_display_name`	Email display name to be used when sending email from the system. For example, to send invitations and notifications from the PCE. For example: `email_display_name:'noreply'` **Default Value**: `noreply`	Public Stable

Runtime Environment File Parameter	Description	Exposure Level

`smtp_relay_address`	SMTP relay information used by the PCE to send email; for example, to send invitations and notifications.
	
	It is assumed that an SMTP Relay runs on localhost and listens on `127.0.0.1/587`.
	
	If that is not true then the configuration needs to be specified. This value only needs to be specified on the Core nodes.
	
	The form used is either:
	
	`ip_address (e.g. 127.0.0.1)`
	
	Or
	
	`ip_address:port (e.g. 127.0.0.1:587)`
	
	Note: If no port is specified, then port 587 is used.
	
	For example:
	
	`smtp_relay_address: 127.0.0.1:587`
	
	Default Value: `127.0.0.1:587`
		Public Stable

`export_flow_summaries_to_fluentd`	Used to specify which types of traffic flow summaries you want to export to Fluentd: allowed ('`accepted`'), potentially blocked, and blocked.
	
	For example:
	
	`export_flow_summaries_to_fluentd: - accepted`
	`- potentially_blocked`
	`- blocked`
		Public Experimental

Runtime Environment File Parameter	Description	Exposure Level

`export_flow_summaries_to_syslog`	Used to enable traffic flow summaries to syslog. You can export blocked,
	potentially blocked, and/or allowed ('`accepted`')
	
	For example:
	
	`export_flow_summaries_to_syslog:`
	`- accepted`
	`- potentially_blocked`
	`- blocked`
	If you only wanted to export blocked traffic summaries, then you
	would only include the flow summary type when defining the parameter.
	
	For example:
	`export_flow_summaries_to_syslog:`
	`- blocked`
		Public
		Experimental

`syslog_event_export_format`	Used to indicate the output format for both audit events and traffic summaries to syslog, either JSON, CEF, or LEEF. For example, if you only wanted to export events to the CEF format, you would configure this parameter as follows: `syslog_event_export_format: cef` If you leave this parameter undefined, the PCE will only export events to JSON.	Public Stable

PCE Upgrade/Downgrade

This section provides information on how to upgrade or downgrade the PCE software. Important considerations before you begin:

- For upgrade, you should directly invoke the `illumio-pce-ctl` control script. For example:

  `$` **`sudo -u ilo-pce illumio-pce-ctl`** ***`command`***
  Do not use the `service illumio-pce start` or any service commands when upgrading. The service command is designed to be run without prompting, which is required for certain upgrades, so do not use any the PCE service commands during this upgrade process.

- After upgrading the PCE software version, the `illumio-pce-db-management migrate`' command must be run on any node before bringing the cluster to run level 5.
- Make sure you upgrade all nodes in the cluster to the same version before restarting the nodes; otherwise, none of the nodes in your cluster will start.
- Do not upgrade your VENs until the PCE version upgrade is successful. After Illumio VENs are upgraded, rolling back the PCE upgrade is not supported.
- Check to ensure that any asynchronous jobs have not been submitted right before you plan to do the software upgrade. As a general best practice, you should wait until all asynchronous jobs have finished before upgrading the PCE software.
- For a multi-version upgrade, in the following "Prepare for Upgrade" section, the 'Backup PCE Database and Current Software' tasks below should only be done a single time at the beginning of the first upgrade sequence. This allows you to rollback to the starting version if there is an issue with the upgrade.

Upgrade paths and planning tool

For details on upgrade paths for versions of the PCE and VEN, see Versions and Releases on the Illumio support site.

An upgrade planning tool is also available to help you plan your deployments.

Backup the PCE

1. Before you begin the backup, you need to determine the Data node that requires a backup. To find out which node runs this service, use the `illumio-pce-ctl cluster-status` command:

```
$ sudo -u ilo-pce illumio-pce-ctl cluster-status

SERVICES (runlevel: 5) NODES (Reachable: 1 of 1)
====================== ============================
agent_background_worker_service 192.168.33.90
agent_service NOT RUNNING
agent_slony_service 192.168.33.90
agent_traffic_redis_cache 192.168.33.90
agent_traffic_redis_server 192.168.33.90          <=== dump command should run from this node
agent_traffic_service NOT RUNNING
...
```

2. Run these commands on the Data node that is running the `agent_traffic_redis_server` service to back up the databases to a file.

   Both Policy and Traffic Databases

```
$ sudo -u ilo-pce /<new_path>/illumio-pce-db-management dump --file <location of policy backup file>
```

Only Traffic Database

```
$ sudo -u ilo-pce /<new_path>/illumio-pce-db-management traffic dump --file <location of traffic backup file>
```

3. After the commands complete, copy the backup files to a fault-tolerant storage location.

Back up the PCE Runtime Environment File

Store a copy of each node's `runtime_env.yml` file on a system that is not part of the Supercluster. The default location of the PCE Runtime Environment File is `/etc/illumio-pce/ runtime_env.yml`.

Upgrade the PCE

The upgrade process includes these general steps:

- Upgrade the PCE software with RPM or Tarball
- Remove older events version 1 records from the database
- Migrate the PCE database

Stop the PCE Software

On **each** node in the cluster, stop the PCE software.

```
$ sudo -u ilo-pce illumio-pce-ctl stop
```

Upgrade RPM Installation

On **each** node in the cluster, upgrade to the new PCE RPM version:

```
$ rpm -Uvh <illumio_pce_rpm>
```

Update PCE Runtime Environment File

Consult the Release Notes to determine if any changes to the PCE Runtime Environment File (`runtime_env.yml`) are required to upgrade. If changes are required:

1. On **each** node in the cluster, update the `runtime_env.yml` file.
2. On **each** node in the cluster, check the validity of the `runtime_env.yml` file by running this command:

```
$ sudo -u ilo-pce illumio-pce-ctl check-env
```

Migrate the PCE Database

Start the PCE Software at Runlevel 1 (Database Operations Only)

1. On **each** node in the cluster, start the software at run level 1:

   ```
   $ sudo -u ilo-pce illumio-pce-ctl start --runlevel 1
   ```

2. For some upgrades, you might be prompted to upgrade the database PostgreSQL software on **one** of the Data nodes. If you do not see this prompt, go to the next step. At the prompt, when asked if you want to continue the upgrade, type `yes` and then Enter on your keyboard.

   ```
   The PCE software is running a newer version(9.6.1) of the postgres software than the database
   version(9.3.)
   The PCE software will upgrade the database to the newer release.
   Prior to this upgrade, Illumio recommends that you make a backup/copy of your /var/lib/illumio-pce/data
   directory


   Do you wish to continue with the database upgrade. [yes/no]: yes
   Proceeding with database upgrade
   ```

3. On **each** node in the cluster, verify the PCE software status by running these commands:

   ```
   $ sudo -u ilo-pce illumio-pce-ctl status -sv --wait
   ```

4. On any node, run this command to migrate the database to the latest schema version:

   ```
   $ sudo -u ilo-pce illumio-pce-db-management migrate
   ```

Bring the PCE Software to Runlevel 5 (Fully Operational)

1. Set the software to run level 5 to bring the cluster to a running state:

```
$ sudo -u ilo-pce illumio-pce-ctl set-runlevel 5
```

Note: If you did not run the '`illumio-pce-db-management migrate`' command on the database master node in the first step of this task, you will not be able to bring the node up to level 5 and you will not be able to start the other nodes in the cluster. If some of the nodes in the cluster are already running, then they will be shutdown until you successfully migrate the database. If you attempt to start the upgraded PCE cluster without migrating the database, this error is displayed:

```
$ sudo -u ilo-pce illumio-pce-ctl start
Starting Illumio Runtime STARTING 20.96s
$
$ Stopping PCE software: DB migrations mismatch for DB: avenger_executor_dev: Missing migrations.
```

2. On each node in the cluster, verify the PCE software status by running these commands:

```
$ sudo -u ilo-pce illumio-pce-ctl status -s -v -w
$ sudo -u ilo-pce illumio-pce-ctl cluster-status -w
```

3. If you are using a front end load balancer (F5 or DNS), make sure that the load balancer is sending requests to the two Core nodes in the cluster.
4. From PCE web console, log in and verify VEN synch status is showing as "Verified" for a few randomly selected Workloads.
5. You can view a Workload's VEN policy status by selecting a Workload's details page.
6. Under the section VEN, make sure that Policy Sync shows "Verified." Illumio recommends checking a few randomly selected Workloads to verify policy sync for the VEN.

Downgrade/Rollback to a Previous Version

This section describes the tasks necessary to roll back the PCE software to a previous version in the event of a PCE software upgrade failure or defect. To roll back the PCE software to a previous version, follow these instructions:

Stop the PCE Software

On **each** node in the cluster, stop the PCE software.

```
$ sudo -u ilo-pce illumio-pce-ctl stop
```

Downgrade RPM Installation

On **each** node in the cluster, run this command:

```
$ rpm -Uh <illumio_pce_rpm> --oldpackage
```

Downgrade Tarball Installation

On **each** node in the cluster, run this command:

```
$ mv <install_root_previous_release> <install_root>
```

For example:

```
$ mv /opt/illumio-pce-previous-release /opt/illumio-pce
```

Revert PCE Runtime Environment File

If you made changes to the `runtime_env.yml` file, restore the previous version of the file:

For example:

```
$ cp /etc/illumio-pce/runtime_env.yml-backup /etc/illumio-pce/runtime_env.yml
```

Remove PCE Data

On **each** node in the cluster, run this command:

```
$ rm -rf /var/lib/illumio-pce/data/*
```

Start the PCE Software at Runlevel 1 (Database Operations Only)

1. On **each** node in the cluster, start the software at run level 1:

```
$ sudo -u ilo-pce illumio-pce-ctl start --runlevel 1
```

2. On **each** node in the cluster, verify the PCE software status by running these commands:

```
$ sudo -u ilo-pce illumio-pce-ctl status -s -v -w
$ sudo -u ilo-pce illumio-pce-ctl cluster-status -w
```

Revert the PCE Data

On **one** of the Data nodes of the cluster, run this command to restore the backup you took at the beginning of the upgrade:

```
$ sudo -u ilo-pce illumio-pce-db-management restore --file <location of prior db dump file>
```

Copy the restored Illumination® data file to the **other** Data node. The file is located in the following directory:

```
/var/lib/illumio-pce/data/redis/redis_traffic_0_master.rdb
```

Migrate the PCE Database

On **one** of the Data nodes of the cluster, run this command to migrate the database to the latest schema version:

```
$ sudo -u ilo-pce illumio-pce-db-management migrate
```

Bring the PCE Software to Runlevel 5 (Fully Operational)

1. Set the software to run level 5 to bring the cluster to a running state:

```
$ sudo -u ilo-pce illumio-pce-ctl set-runlevel 5
```

Note: If you did not run the '`illumio-pce-db-management migrate`' command on the database master node in the first step of this task, you will not be able to bring the node up to level 5 and you will not be able to start the other nodes in the cluster. If some of the nodes in the cluster are already running, then they will be shutdown until you successfully migrate the database. If you attempt to start the upgraded PCE cluster without migrating the database, you will see this error:

```
$ sudo -u ilo-pce illumio-pce-ctl start
Starting Illumio Runtime STARTING 20.96s
$
$ Stopping PCE software: DB migrations mismatch for DB: avenger_executor_dev: Missing migrations.
```

2. On each node in the cluster, verify the PCE software status by running these commands:

```
$ sudo -u ilo-pce illumio-pce-ctl status -s -v -w
$ sudo -u ilo-pce illumio-pce-ctl cluster-status -w
```

3. If you are using a front end load balancer (F5 or DNS), make sure that the load balancer is sending requests to the two Core nodes in the cluster.
4. From PCE web console, log in and verify VEN synch status is showing as "Verified" for a few randomly selected Workloads.
5. You can view a Workload's VEN policy status by selecting a Workload's details page.
6. Under the section VEN, make sure that Policy Sync shows "Verified." Illumio recommends checking a few randomly selected Workloads to verify policy sync for the VEN.

FIPS Compliance for PCE and VEN

This section details the operational requirements for compliance with Federal Information Processing Standard (FIPS) 140-2 for both the Illumio Adaptive Security Platform Policy Computer Engine (PCE) and the Linux and Windows Virtual Enforcement Node (VEN).

This release of the Illumio Adaptive Security Platform supports FIPS compliance for the Policy Compute Engine (PCE) and Virtual Enforcement Node (VEN) on Linux and Windows.

FIPS compliance is not supported for the PCE Virtual Appliance, the VEN for AIX, and the VEN for Solaris.

FIPS-related U.S. Goverment and Third-Party Vendor Documentation

- Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules
- Red Hat Enterprise Linux OpenSSL Cryptographic Module NIST Security Policy
- RHEL v7.1 Red Hat Enterprise Linux Kernel Crypto API Cryptographic Module v4.0
- RHEL v7.4 Red Hat Enterprise Linux Kernel Crypto API Cryptographic Module v5.0
- Windows Server 2012 NIST Security Policy
- Windows Server 2016 NIST Security Policy

Non-Government Customers with No FIPS Requirement

Compliance to FIPS 140-2 requires additional operational restrictions, such as specific operating system versions and server hardware.

Illumio recommends that non-government customers who do not have requirement for FIPS 140-2 *not* configure and deploy the Illumio Adaptive Security Platform to support FIPS compliance.

Compliance Affirmation Letters

Third-party FIPS-compliance affirmation letters for Illumio Adaptive Security Platform are available on Illumio's Federal Solutions page.

Prerequisites for PCE FIPS Compliance

1. PCE server hardware requires the Intel Ivy Bridge CPU (2012) or later.
2. RedHat v7.4 required.
3. Customer-provided SSL certificates from a public CA or a customer CA. The certificates must have a minimum key size of 2048 to secure PCE communications.

Prerequisites for Linux VEN FIPS Compliance

For SecureConnect (IPSec encryption among workloads), to claim FIPS compliance, the VEN must be installed on either RHEL v7.1 or RHEL v7.4 and configured to operate in FIPS mode as detailed in either of the following vendor documents:

- For RedHat 7.1, Section 9.1 ("Cryptographic Officer Guidance") of the RHEL v7.1 Red Hat Enterprise Linux Kernel Crypto API Cryptographic Module v4.0.
- For RedHat 7.4, Section 9.1 ("Cryptographic Officer Guidance") of the RHEL v7.4 Red Hat Enterprise Linux Kernel Crypto API Cryptographic Module v5.0.

For all Linux versions of the VEN, there are no other special OS requirements or additional configurations required to enable FIPS-compliant OpenSSL communications. The Linux VEN's FIPS OpenSSL module is built directly into the VEN and is not supplied by the underlying OS; the LINUX VEN operates by default in FIPS mode.

Prerequisites for Windows VEN FIPS Compliance

For FIPS compliance on Windows, either Windows Server 2012 or Windows Server 2016 must be configured according to the following vendor documents:

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

Steps to Enable FIPS Compliance for the PCE

To enable FIPS compliance on the PCE:

1. After installing RHEL7.4, follow the required steps in Section 9.1, Crypto Officer Guidance, Red Hat Enterprise Linux OpenSSL Cryptographic Module NIST Security Policy.
2. Reboot the system.
3. After reboot, verify that the setting `/proc/sys/crypto/fips_enabled` is equal to 1.
4. Install the Illumio ASP RPM as detailed in this guide.
5. During PCE installation, provide the PCE with SSL certificates that have a minimum RSA key size of 2048.

After completing the remainder of the PCE set up, the PCE is FIPS compliant.

FIPS Compliance for Linux Workloads

For all Illumio supported Linux Workloads, the standard 18.1 GA VEN release (and all later releases) support VEN Linux FIPS compliance. Starting with the VEN Linux 18.1 release, all VEN OpenSSL communications by default operate in a FIPS compliant mode.

To claim FIPS compliance for the VEN SecureConnect feature (IPSec encryption between workloads), the VEN must be installed on either RHEL v7.1 or RHEL v7.4 and configured to operate in FIPS mode as documented in Section 9.1 ("Cryptographic Officer Guidance") of the RHEL v7.1 Red Hat Enterprise Linux Kernel Crypto API Cryptographic Module v4.0 or in Section 9.1 ("Cryptographic Officer Guidance") of the RHEL v7.4 Red Hat Enterprise Linux Kernel Crypto API Cryptographic Module v5.0.

FIPS Compliance for Windows Workloads

For Windows Workloads, the standard 18.1 GA VEN release (and all later releases) support VEN Windows FIPS compliance. The Windows VEN is FIPS-compliant when installed on either Windows Server 2012 or Windows Server 2016. To operate the FIPS-compliant Windows VEN, the Windows system must be configured to operate in FIPS mode as documented in Section 2 of the Windows Server 2012 NIST Security Policy or Section 2 of the Windows Server 2016 NIST Security Policy.

Alternative to PCE RPM Installation – Install the PCE Tarball

Install the PCE RPM distribution
The preferred installation mechanism is the RPM distribution, which is easier than the tarball installation.

If you are installing the PCE tarball distribution, do the following tasks on each of the nodes in your deployment:

1. Create the PCE user account to run the software.
2. Resolve OS dependencies.
3. Create the directory structure for the PCE. The PCE tarball supports a configurable directory structure. This enables you to choose the directory structure that best meets your needs.

Directory	Use	Permissions	Example
`install_root`	PCE binaries and scripts.	Read / Execute	`/opt/illumio-pce`
`persistent_data_root`	A writable location where the PCE writes its persistent data. Must be owned by the user that runs the PCE.	Read / Write	`/var/lib/illumio-pce/data`
`runtime_data_root`	A writable location where the PCE writes runtime data. Must be owned by the user that runs the PCE.	Read / Write	`/var/lib/illumio-pce/runtime`
`ephemeral_data_root`	A writable location where the PCE writes temporary files.	Read / Write	`/var/lib/illumio-pce/tmp`
`log_dir`	The PCE writes text file logs to this directory. You must configure logrotate (or similar) to ensure log files do not grow too large.	Read / Write	`/var/log/illumio-pce`

   The table below lists the directories used by the PCE. You need to create these directories and update the listed PCE Runtime Environment File with the proper values. The default location of the PCE Runtime Environment File is `/etc/illumio-pce/ runtime_env.yml`, but for the exact location on your systems, check the value of the `log_dir` parameter
4. Copy the PCE tarball into the `install_root` directory and untar it.
5. Create an init script to run `install_root/illumio-pce-ctlstart` at boot.

Upgrade Tarball Installation

- The `$ILLUMIO_RUNTIME_ENV` shell environment variable defines the location of the `runtime_env.yml` file.
- The following variables used in this section refer to entries in the `runtime_env.yml` file for each node in the cluster:
  - `<install_root>`
  - `<persistent_data_root>`
  - `<log_dir>`

On **each** node in the cluster, do the following steps:

1. Move the old software version to a backup directory:

   ```
   $ mv <install_root> <install_root_previous_release>
   ```

   For example:

   ```
   $ mv /opt/illumio-pce /opt/illumio-pce-previous-release
   ```

2. Install the new PCE TGZ version:

   ```
   $ mkdir <install_root>
   $ cd <install_root>
   $ tar -xzf <illumio_pce_tar_gz>
   ```

Change Tarball Installation to RPM Installation

Perform these steps to install a first-time RPM to replace previous tarball installation.

1. **As the previous PCE runtime user**, stop the PCE on each node

   ```
   # illumio-pce-ctl stop set-runlevel 1
   ```

2. Remove the software installed by the tarball by removing all files under the `<install_root>` directory.

   ```
   # mv install-root install-root.prev
   ```

3. Change the previous PCE runtime user and group to `ilo-pce:ilo-pce`.

```
# usermod --login ilo-pce <previous-user>
# groupmod --new-name ilo-pce <previous-group>
```

4. Install the the PCE using the RPM.

```
 # rpm -ivh --nopre illumio-pce-16.6-0.x86_64
```

   Note: The `--nopre` option prevents the RPM from creating these two empty directories: `/var/lib/illumio-pce` and `/var/log/illumio-pce`.
5. Move the existing `runtime_env.yml` file to `/etc/illumio-pce`
6. Update the `ILLUMIO_RUNTIME_ENV` environment variable to `/etc/illumio-pce/runtime_env.yml` or you can delete this environment variable. The PCE automatically looks for the runtime environment file in this location.
7. If necessary, change the `install_root` parameter in the `runtime_env.yml` file to `/opt/illumio-pce`.
8. As the new PCE runtime user, start the PCE on each node

```
# sudo -u ilo-pce illumio-pce-ctl start
```

9. **As the new PCE runtime user**, migrate the database on the data0 node.

```
# sudo -u ilo-pce illumio-pce-db-management migrate
```

10. **As the new PCE runtime user**, bring the PCE to run level 5.

```
# sudo -u ilo-pce illumio-pce-ctl set-runlevel 5Revision History
```

Revision History

Illumio Adaptive Security Platform PCE Deployment Guide

Date	Description
2018-09-06	• Updated for Illumio Adaptive Security Platform version 18.2. • Added "Optionally validate your certificate". • "Upgrade the PCE" moved from *PCE Operations Guide* to *PCE Deployment Guide* (this guide).
2018-06-11	PKI certificates are no longer required to download the PCE Software.
2018-06-08	Include details on how to optionally validate your TLS/SSL certificate.

Date	Description
2018-06-01	• Include details on upgrade paths and planning tool • Miscellaneous minor corrections/clarifications
2018-05-10	Updated for Illumio Adaptive Security Platform version 18.1: • Removal of section numbering. • Addition of glossary of common terminology • Start of revision history