illumio

Illumio In Production

A Framework for Maintenance in Production

Table of Contents

Section 1: Introduction

Purpose

To provide a guide with recommendations and best practices on how to operationalize Illumio in your production environment. We are sharing best practices learned to assist with the maintenance and health of your environment, and to administer and manage Illumio once in production. This document is provided to Illumio customers upon request.

Scope

This document offers a framework of best practices, focusing on the operationalization of your Illumio environment in production. These practices are specifically tailored to the Illumio product and leverage the wealth of up-to-date information available on Illumio.com through direct links.

Section 2: Illumio Technical Support

Illumio Support

Within the Illumio Support portal, we provide our customers with information and support to ensure they are always informed through the ability to search, including:

Resources	Description	Link
Support	Cases, knowledge base, software, tools, etc.	support.illumio.com
Requesting support portal access	Process of support portal access for new users and those who require additional access	Self-registration: portal.illumio.com Additional access: support.illumio.com/knowledge-base/articles/requesting-support-portal-access.html
Community	Ask questions, onboarding, deployment, best practices	community.illumio.com
Documentation	Documentation portal	docs.illumio.com
Knowledge base	Centralized repository of troubleshooting, how to, and informational articles.	support.illumio.com/knowledge-base/index.html
OS support and dependencies	To check OS support and dependencies for both PCE, VEN, and other Illumio products	support.illumio.com/software/os-support-package-dependencies/ven.html
Tools	Downloadable tools	support.illumio.com/tools/index.html
Workloader	Workloader CLI tool on GitHub	github.com/brian1917/workloader/releases
Training	Training courses	support.illumio.com/training/course-catalog.html
Supported apps and integration tools	Third-party applications and tools to use with PCE	docs.illumio.com/guides/integrations/supported-apps-and-integration-tools.html
Email notifications for new posts in the Community	How to subscribe and receive email notifications for new posts in the Community	support.illumio.com/knowledge-base/articles/how-to-receive-email-notifications-for-topic-discussions-in-the-community.html

Section 3: Illumio Training

We offer customers self-paced training.

Recommended self-paced training courses to complete for Illumio Core SaaS deployment: support.illumio.com/training/certifications/illumio_core_associate:_saas.html

Recommended self-paced training courses to complete for Illumio Core on-premises deployment: support.illumio.com/training/certifications/illumio_core_associate:_on-premises.html

Complete course catalog: support.illumio.com/training/course-catalog.html

Additional recommended courses:

- 410 VEN Deployment Quick Start (self-paced)
- 520 Illumio Endpoint (self-paced)
- 460 Illumio Tools (self-paced) – workloader

Section 4: Accessing Illumio PCE in Production

Who has access to Illumio UI?

Illumio is managed and operated by your security team. Only members who are part of your security team should get read/write access to the application.

- On-premises customers logon referencing port 8443 by default but can be configured to use a custom port.
- SaaS customers logon referencing port 443 by default and is not customizable.

Illumio Support

Illumio Core includes several roles that grant users access to perform operations. Each role is matched with a scope. You can add users (local and external) and groups to all the roles.

Roles with global scopes

These global roles use the scope All Applications, All Environments, and All Locations. You cannot change the scope for these roles. The roles have the following capabilities in Illumio Core.

Role	Granted access
Global Organization Owner	Perform all actions: add, edit, or delete any resource, security settings, or user account
Global Administrator	Perform all actions except user management: add, edit, or delete any resource or organization setting
Global Viewer	View any resource or organization setting. They cannot perform any operations. This role was previously called Global Read Only.
Global Policy Object Provisioner	Provision rules containing IP lists, services, and label groups. They cannot provision rulesets, virtual services, or virtual services, or add, modify, or delete existing policy items.

Roles with specific scopes

You can apply the following roles to specific scopes. These roles are called Scoped Roles.

Role	Granted access
Full ruleset manager	Add, edit, and delete all rulesets within the specified scope.
Limited Ruleset Manager	Add, edit, and delete all rulesets within the specified scope. Add, edit, and delete rules when the provider and consumer match the specified scope. Ruleset Managers with limited privileges cannot manage rules that use IP lists, custom iptables rules, user groups, label groups, iptables rules as consumers, or have internet connectivity.
Ruleset Viewer	Read-only access to rules that match the specified scope. Ruleset Viewers cannot edit rules or rulesets.
Ruleset Provisioner	Provision rulesets within specified scope.
Workload Manager	Manage workloads and pairing profiles within the specified scope. Read-only access provided to all other resources.

Please see our guide on access control for additional information: docs.illumio.com/core/23.5/content/guides/pce-administration/access-configuration/role-based-access-control.html

Section 5: Illumio Product Integration

Technology alliance partners

Our Illumio product has integrations available with multiple technology partners.

For additional information refer to illumio.com/partners

Supported apps and integration tools

We develop and maintain third-party applications and tools to help our customers streamline security workflows that involve the Illumio PCE apps and integration tools.

Integration	Type	Description
Ansible	Automation	Ansible modules for VEN and C-VEN pairing and label creation/update/removal
IBM QRadar	SIEM	Connector and dashboards to view Illumio flow and event data
IBM QRadar	SOAR	Provides a selective port-blocking playbook
Palo Alto Cortex	SOAR	Provides a selective port-blocking playbook
Python	SDK	Python REST client for Illumio PCE APIs
ServiceNow	CMDB	Uses ServiceNow CMDB as the source of truth for labeling PCE workloads with R/A/E/L labels
Splunk	SIEM	Connector and dashboards to view Illumio flow and event data
Terraform	Automation	Terraform HCL scripts to manage PCE policy and policy objects

For additional information refer to docs.illumio.com/guides/integrations/supported-apps-and-integration-tools.html

Section 6: Illumio Best Practices

PCE administration guide

This guide describes how to maintain and operate the PCE and Ven.

For additional information, refer to: docs.illumio.com/core/23.2/content/landingpages/guides/pce-administration.htm

PCE health

With this API, you can see the following health information:

- How long the PCE has been running, its runlevel, and overall health (normal, warning, or error)
- Each node hostname, IP address, uptime, runlevel, and whether the PCE software is running properly.
- Each node type (core or data), and which data node is the primary database and which is the database replica.
- The replication delay for the database replica.
- Information about PCE service alerts, such as the number of degraded or failed services in the cluster, so you can see where service failures have occurred.

NOTE: This API is only available for Illumio Core PCE installed on-premises and is not available for Illumio Cloud (SaaS) customers.

For additional information, refer to: docs.illumio.com/core/23.5/content/guides/rest-api/pce-management/pce-health.htm

Install and upgrade

The information in this category provides all you need to deploy Illumio Core and the VEN on hosts to create managed workloads in your environment. Illumio Core consists of these main components:

- PCE enables centralized visibility and policy management for globally distributed environments at a massive enterprise scale.
- VENs are installed in discrete operating system instances and provide complete visibility and enforcement.

For additional information, refer to:

- **Illumio Core Upgrade Why and How:** docs.illumio.com/core/23.2/content/landingpages/guides/upgrade-summary.htm
- **PCE Installation and Upgrade Guide:** docs.illumio.com/core/23.2/content/landingpages/guides/pce-install-upgrade.htm
- **VEN Installation and Upgrade Guide:** docs.illumio.com/core/23.2/content/landingpages/guides/ven-install-upgrade.htm
- **Endpoint Installation and Usage Guide:** docs.illumio.com/core/23.2/content/landingpages/guides/illumio-endpoint-segmentation.htm

Versions and compatibility

Below are descriptions of our PCE and VEN versioning. Use the Upgrade Path Tool to check PCE/VEN compatibility BEFORE upgrading the PCE or the VEN.

Release type	Description	Recommended for
Endpoint	Endpoint releases of the Endpoint VEN receive limited maintenance for 1 year.	This track is the best fit for the SaaS customers with Endpoint deployments that always want to take advantage of the latest new features and capabilities from Illumio as soon as they are available and can commit to upgrading to the next Endpoint feature release for bug fixes and security updates.
Long Term Support (LTS)	Long Term Support releases of the PCE And VEN receive active maintenance for 1 year and then limited maintenance for another 2 years.	This track is the best fit for customers that wish to upgrade less frequently and stay on a version of the PCE or VEN with active maintenance support.
Standard	Standard releases of the PCE and VEN receive limited maintenance for 1 year.	This track is the best fit for customers that always want to take advantage of the latest new features and capabilities from Illumio as soon as they are available, and can commit to upgrading to the next standard or LTS release for bug fixes and security updates.

Software releases

Support status	Description
Active maintenance	Illumio will provide regular maintenance updates for reported bugs and security issues and add support for new minor operating system versions in the latest Illumio release.
Limited maintenance	Illumio will provide hotfixes for verified P1 issues and critical security issues and add support for new minor operating system versions in the latest Illumio release. For all other bug fixes and security updates, customers will need to upgrade to a newer release.
PCE dependent	Support for releases of NEN, Kubelink, Flowlink, and CLI will be in effect as long as the PCE they are compatible with is in support. Hotfixes and updates will be made available on the latest release. Customers using older releases may be required to upgrade to the latest release.
End of support	A release that is no longer supported.

For additional information, refer to:

- **Long Term Support (LTS) releases:** support.illumio.com/knowledge-base/articles/FAQ-LTS-releases.html
- **Upgrade Path Tool:** support.illumio.com/software/download.html#pce_software/upgrade
- **Versions, compatibility, and support status:** support.illumio.com/software/versions-and-compatibility.html

Software support

The amount of data collected and stored by the PCE can be large. Events, Explorer, and the internal syslog all generate data that is stored in PCE databases and log files. When the amount of stored data is not managed carefully, disks can become overfull.

This occurrence can cause a variety of symptoms:

- Inability to take backups
- Failing API calls
- General PCE functionality issues

Even when these issues do not occur, a large amount of stored data creates larger database backups, and it takes longer to backup and restore the database. To successfully manage these issues, consider the following recommendations:

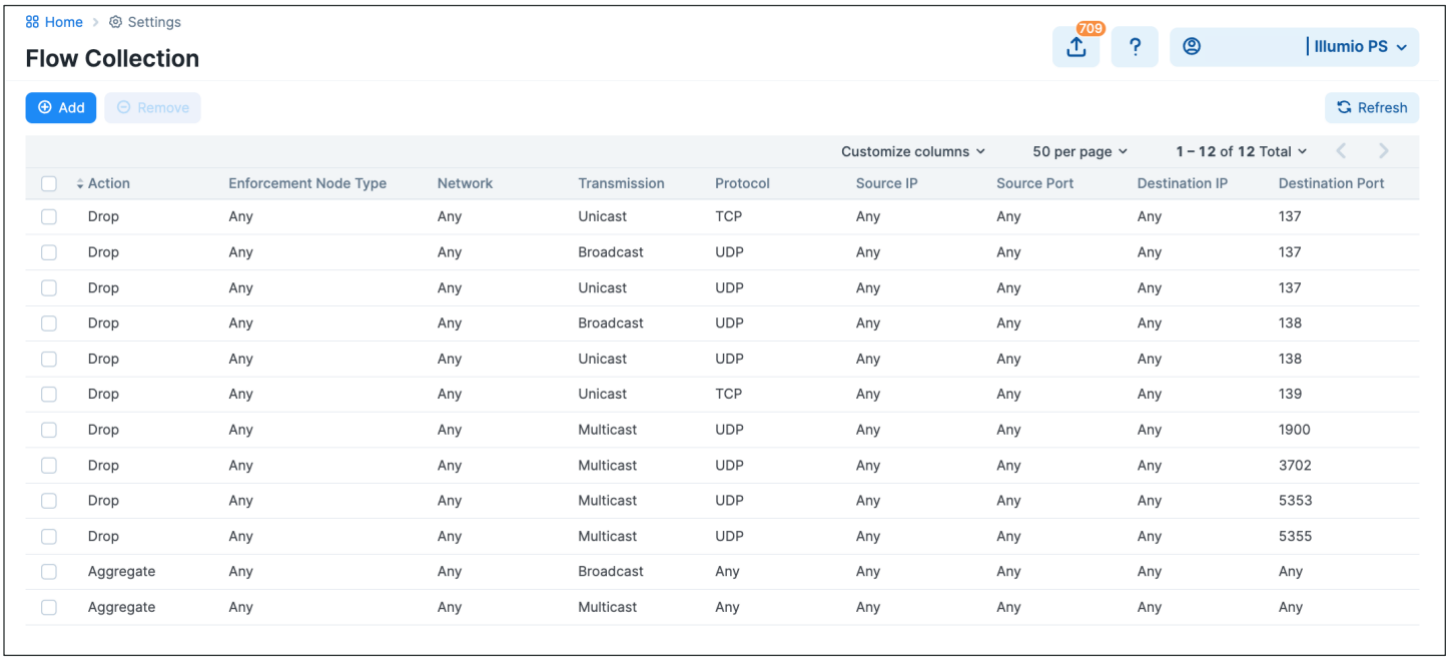
- **Identify:** Know your organization's policies, backup strategies, and monitoring strategies
- **Detect:** Monitor ongoing disk usage
- **Respond:** Know how to troubleshoot and fix issues related to data storage
- **Recover:** Set up your PCE deployment to reduce disk usage

For more information, refer to: docs.illumio.com/core/23.2/content/guides/pce-administration/manage-pce-nodes-and-clusters/manage-data-and-disk-capacity.htm

FEATURE: Configure Flow Collection Settings

This guide describes how to configure Flow Collection settings to help when flow log storage is consuming too much space and to drop noisy traffic such as scanners, DNS exposed to Internet-specific servers, etc.

For more information, refer to: support.illumio.com/knowledge-base-/articles-how-to-reduce-the-amount-of-traffic-which-is-stored-in-the-flow-logs.html



Action	Enforcement Node Type	Network	Transmission	Protocol	Source IP	Source Port	Destination IP	Destination Port
Drop	Any	Any	Unicast	TCP	Any	Any	Any	137
Drop	Any	Any	Broadcast	UDP	Any	Any	Any	137
Drop	Any	Any	Unicast	UDP	Any	Any	Any	137
Drop	Any	Any	Broadcast	UDP	Any	Any	Any	138
Drop	Any	Any	Unicast	UDP	Any	Any	Any	138
Drop	Any	Any	Unicast	TCP	Any	Any	Any	139
Drop	Any	Any	Multicast	UDP	Any	Any	Any	1900
Drop	Any	Any	Multicast	UDP	Any	Any	Any	3702
Drop	Any	Any	Multicast	UDP	Any	Any	Any	5353
Drop	Any	Any	Multicast	UDP	Any	Any	Any	5355
Aggregate	Any	Any	Broadcast	Any	Any	Any	Any	Any
Aggregate	Any	Any	Multicast	Any	Any	Any	Any	Any

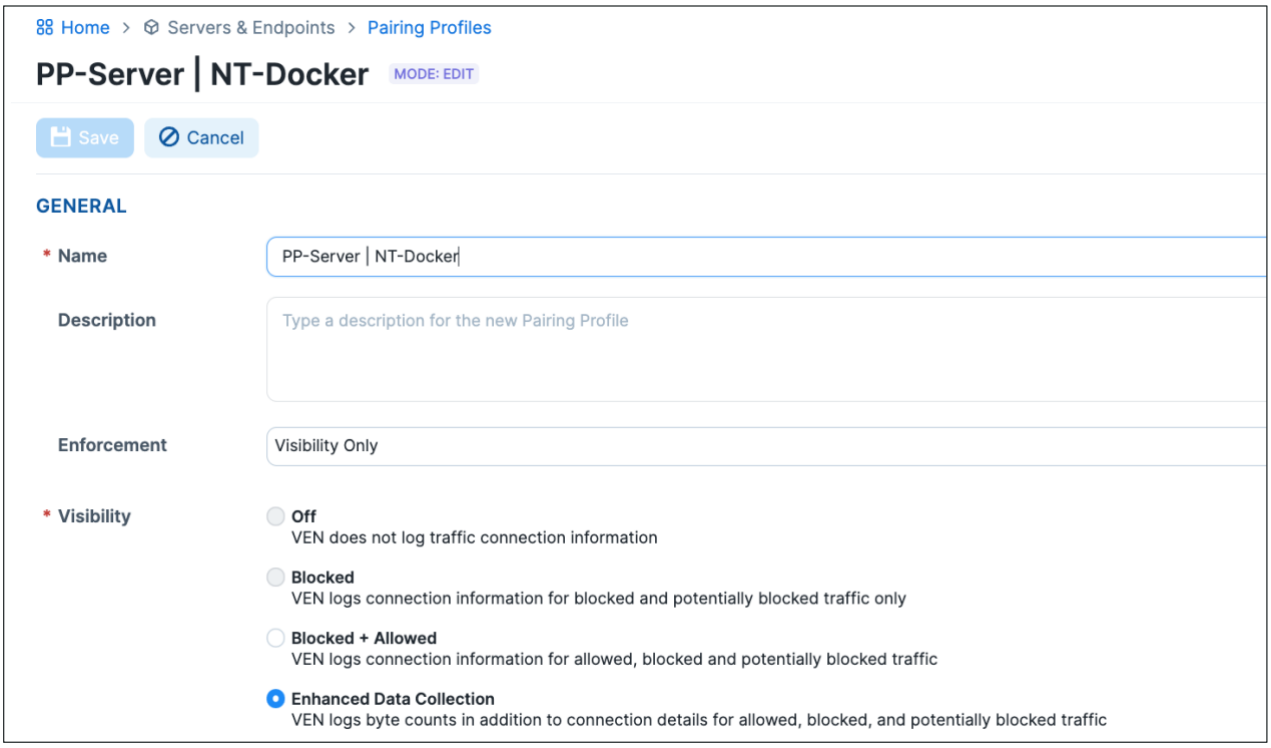
FEATURE: EDC (Enhanced Data Collection – VEN Byte Count)

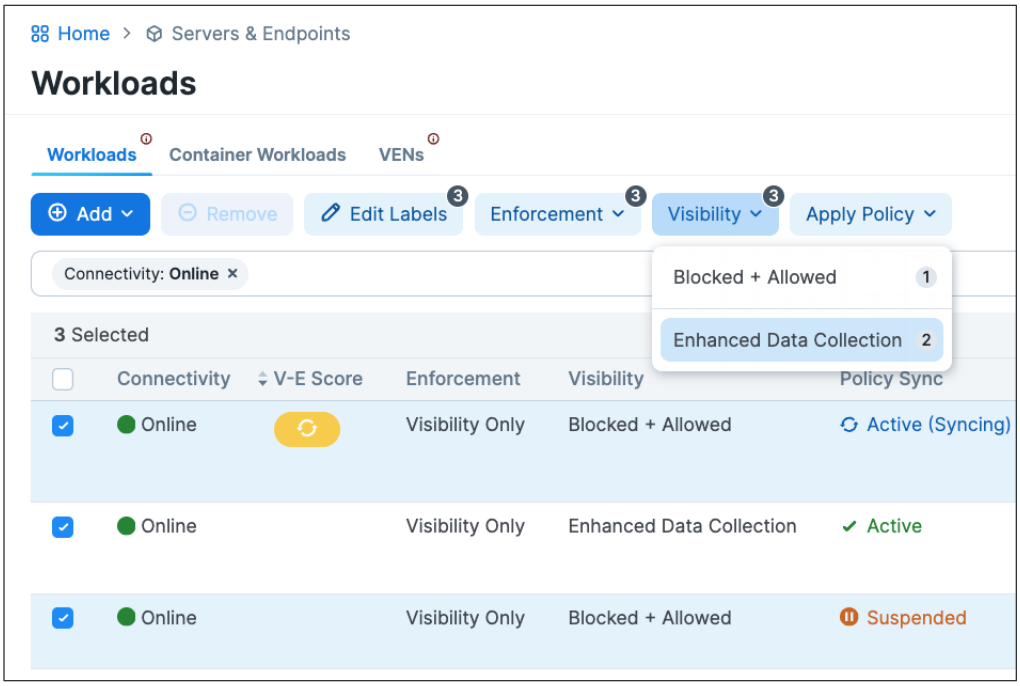
This topic explains the feature Enhanced Data Collection – VEN Bye Count to show the amount of data transfer on a workload.

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

For more information, refer to:

- docs.illumio.com/core/23.2/content/guides/ven-administration/monitor-and-diagnose-ven-status/ven-to-pce-communication.htm
- support.illumio.com/knowledge-base/articles/how-to-enable-enhanced-data-collection
- docs.illumio.com/core/23.2/content/guides/security-policy/workloads/workloads-vens.htm


Home > Servers & Endpoints > Pairing Profiles
PP-Server | NT-Docker
MODE: EDIT
Save
Cancel
GENERAL
* Name
PP-Server | NT-Docker
Description
Type a description for the new Pairing Profile
Enforcement
Visibility Only
* Visibility
Off
VEN does not log traffic connection information
Blocked
VEN logs connection information for blocked and potentially blocked traffic only
Blocked + Allowed
VEN logs connection information for allowed, blocked and potentially blocked traffic
Enhanced Data Collection
VEN logs byte counts in addition to connection details for allowed, blocked, and potentially blocked traffic


Home > Servers & Endpoints
Workloads
Workloads
Container Workloads
VENs
Add
Remove
Edit Labels
Enforcement
Visibility
Apply Policy
Connectivity: Online
Blocked + Allowed 1
Enhanced Data Collection 2
3 Selected
Connectivity
V-E Score
Enforcement
Visibility
Policy Sync
Online
Visibility Only
Blocked + Allowed
Active (Syncing)
Online
Visibility Only
Enhanced Data Collection
Active
Online
Visibility Only
Blocked + Allowed
Suspended

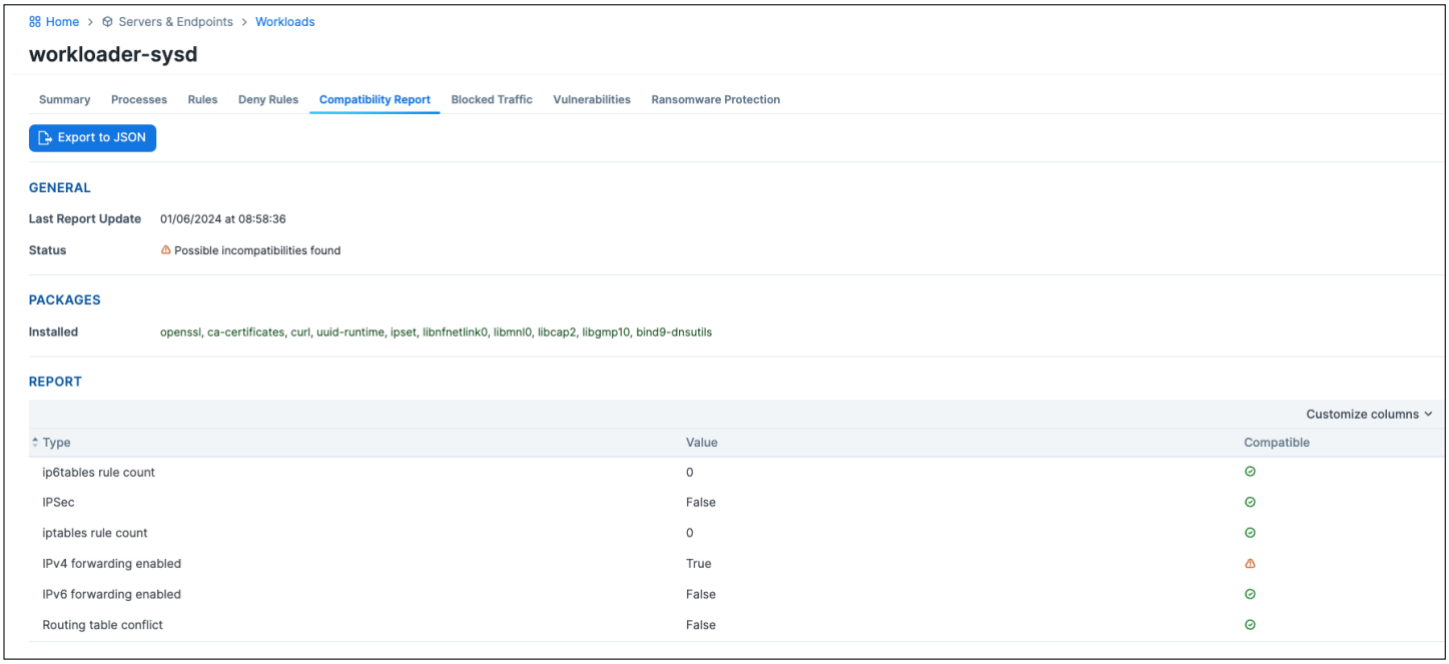
FEATURE: VEN Compatibility Check (Compatibility Report)

This topic explains how to use the VEN Compatibility Check feature after installing VENs on workloads.

When you pair VEN in the Idle state or change the VEN state to Idle, the VEN performs several compatibility checks and sends the results to the PCE.

This process occurs every 24 hours and checks whether the preexisting workload state will have issues when the VEN is moved out of the Idle state.

For more information, refer to: docs.illumio.com/core/23.5/Content/Guides/ven-install-upgrade/reference/ven-compatibility-check.htm



What is a workload?

Workloads that have a VEN installed and paired with the PCE, workloads have the following attributes:

- Workload enforcement and visibility state
- Connectivity and policy sync state
- Workload labels
- Attributes

Information pages available on a workload:

- Summary
- Processes
- Rules
- Deny rules

For more information, refer to: docs.illumio.com/core/23.2/Content/Guides/security-policy/workloads/workloads-in-the-pce.htm

What is an unmanaged workload?

An Unmanaged Workload is a Workload (a discrete operating system instance running on a physical device, a virtual machine, or as a cloud instance) that doesn't have a VEN.

Unmanaged workloads extend rule-writing capabilities to network entities that are not paired with the PCE and do not have an installed VEN. Adding unmanaged workloads to the PCE allows you to write rules so that workloads that are paired with the PCE can communicate with those other entities. The policy between workloads with a VEN and unmanaged workloads is enforced using the outbound rules on the workloads where the VEN is running. For Unmanaged workloads, enforcement is displayed blank.

Add an unmanaged workload

An Unmanaged Workload does not have the VEN installed on it but can be used in a Rule to allow communication between it and other Workloads or Bound Services.

The unmanaged workload IP address is compared to managed workload's NIC with the default gateway. If an unmanaged workload has multiple IP addresses, the managed workload must contain all of them.

You can add unmanaged workloads from two different ways:

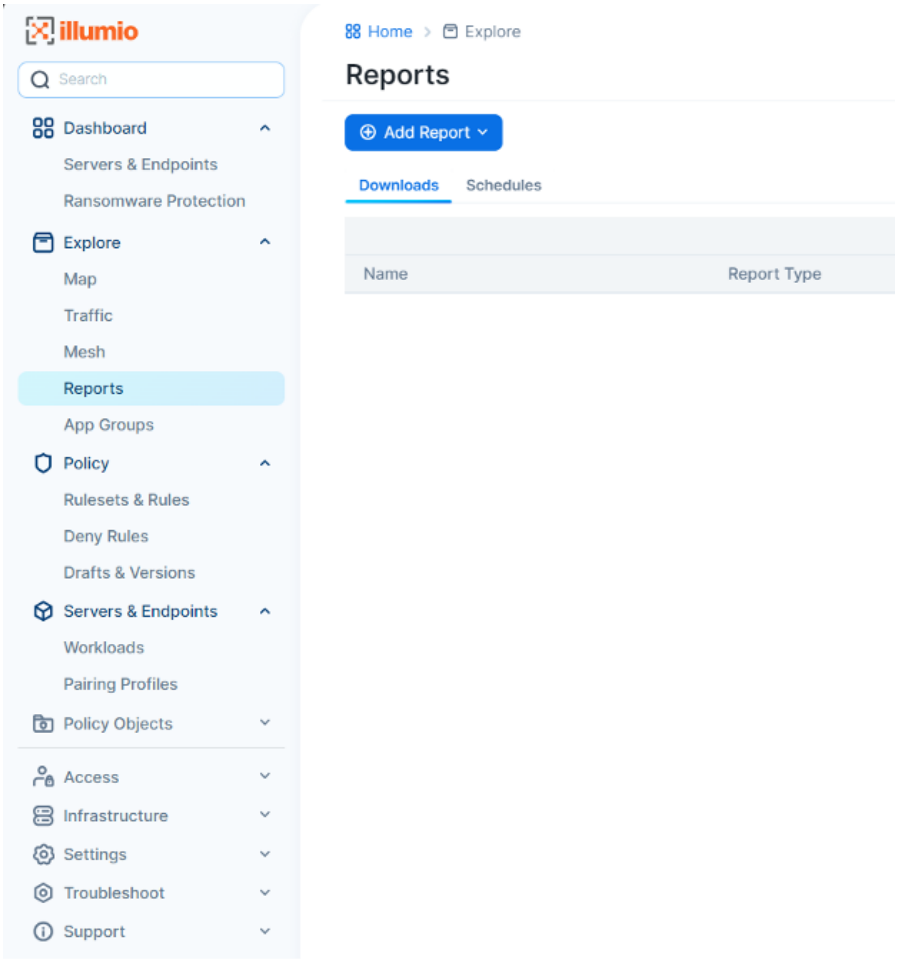
1. You can add unmanaged workloads from the Workloads list. After assigning labels, write label-based Rules that apply to unmanaged workloads.
2. You can also create an unmanaged Workload from a blocked traffic IP address. See Create Unmanaged Workload from Blocked Traffic for information.

For more information, refer to:

- docs.illumio.com/core/23.2/Content/Guides/security-policy/workloads/workload-setup-using-pce-web-console.htm
- docs.illumio.com/core/23.2/Content/Guides/security-policy/workloads/blocked-traffic.htm#create-unmanaged-workload-from-blocked-traffic

Section 7: Illumio Reporting

Pre-requisites: Global Organization Owner role



There are three kinds of reports that can be auto-generated by the PCE based on a said cadence:

Executive Summary

Provides information to decision makers about the overall deployment of Illumio within the organization's computing environment. These reports are intended to provide more business-oriented information than tactical data.

App Group Summary Report

App Group Summary reports are designed for application owners or other people in your organization who need to understand the security of your applications, such as IT security auditors.

Illumination Plus Report

This report is tailored to a specific scope created by a user. It will provide all traffic shown that matches the scope of the report over the specified time period.

For reference on Illumination Plus, see Visualization Tools (illumio.com).

For more information on reporting, refer to: docs.illumio.com/core/23.4/Content/Guides/visualization/reports/about-reports.htm

Section 8: Illumio Log Collection

PCE logs

Most PCE logs are written to syslog, but some logs are written directly to a file in the directory you specify with the log_dir parameter in the PCE runtime_env.yml file.

This table lists the main PCE services and the log file name or the syslog filter for the service.

PCE service	Syslog filter rule or log file name
agent_service **agent_background_worker_service**	program("illumio_pce/agent")
agent_traffic_redis_cache **agent_traffic_redis_server** **agent_traffic_service**	program("illumio_pce/agent_traffic")
auditable_events_service	message('"category":"auditable"');
collector_service	program("illumio_pce/collector");
database_monitor	program("illumio_pce/database_monitor");
database_servicedatabase_slave_service	program("illumio_pce/postgresql");
ev_service	program("EventService");
executor_service	program("illumio_pce/executor");
fileserver_service	program("illumio_pce/fileserver");
fluentd_source_service	program("illumio_pce/fluentd");
ilocron	program("illumio_pce/ilocron");
login_service	program("illumio_pce/login");
memcached	program("illumio_pce/memcached");
node_monitor	program("illumio_pce/system_health");
redis	program("redis");
search_index_service	program("illumio_pce/search_index");
server_load_balancer	program("haxproxy");
service_discovery_service	program("illumio_pce/service_discovery"); program("consul");
web_server	match("nginx;" value("MESSAGE"));

Please see our guide on PCE Logs for additional information: docs.illumio.com/core/23.2/Content/Guides/pce-administration/monitor-and-diagnose-pce-health/pce-logs.htm

VEN logging

The VEN captures logs of its operation and traffic flow summaries locally on the workload. There are several different application log files, each with one backup. Application logs are rotated from primary to backup when their size reaches 15 MB. Application log files are preserved at reboot because application logs are stored in files on a workload.

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

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

Support status	Description	Notes
Traffic flow log	Every 10 minutes	• The VEN checks if there are logs, and if so, sends them to the PCE. • If the PCE is inaccessible, the VEN retains flow summaries for the previous 24 hours but purges logs that are older than 24 hours, with the oldest log at every 24-hour mark. • When logs are purged, the VEN locally logs an alert, which is posted to the PCE as an event when connectivity is restored.

The SQLite command-line tool comes with the VEN, which you can use to query the flow log databases. For details on VEN logging and multiple query examples please see the VEN Logging guide below.

Section 9: Event Monitoring and Alerting

This section describes how to do typical administration tasks related to PCE events. Illumio Core generates a rich stream of structured messages that provide the following information:

- Illumio PCE system health
- Illumio PCE notable activity
- Illumio VEN notable activity

Illumio Core events are structured and actionable. Using the event data, you can identify the severity, affected systems, and what triggered the event. Illumio Core sends structured messages using the syslog protocol to remote systems, such as Splunk and QRadar. You can set up your remote systems to automatically process the messages and alert you.

Please see our guide on Events Monitoring Best Practices for additional information.

Here is a brief outline highlighting the importance of event monitoring and alerting in Illumio.

Overview of event administration

- An overview of events and SIEM integration
- Events setup considerations
- Event record formats, types, and common fields
- Event types by resource
- SIEM integration considerations and recommendations

See also the following related documentation:

- U.S. National Institute for Standards and Technology's NIST 800-92 Guide to Computer Security Log Management
- U.S. Department of Homeland Security National Cybersecurity Center

Illumio strongly recommends that you be familiar with the following technology:

- Solid understanding of Illumio Core
- Familiarity with syslog
- Familiarity with your organizations' Security Information and Event Management (SIEM) systems

Events described

- Detailed description of PCE events, their types, syntax, and record formats.
- List and description of event types, including common criteria only events.
- Best practices for event monitoring, emphasizing the need for comprehensive surveillance and analysis.

Events setup

- Configuration guidelines for setting up the events framework, including requirements, settings, SIEM integration, and syslog forwarding.
- Events are enabled by default in the PCE and cannot be disabled, in accordance with Common Criteria Compliance
- Use the PCE web console to change event-related settings and the PCE runtime_env.yml for traffic flow summaries.

Event monitoring best practices

- A comprehensive list of operational practices to enhance event monitoring, including trend analysis, troubleshooting, and recovery from events.
- Emphasis on integrating event monitoring into broader security operations for a holistic approach.

List of event types

- An expanded table of JSON event types, descriptions, and the corresponding CEF/LEEF success or failure events.
- Instructions for viewing, exporting, and analyzing event data, including use of the PCE web console and command line.

JSON Event Type	Description
access_restriction.create	Access restriction created
access_restriction.delete	Access restriction deleted
access_restriction.update	Access restriction updated
agent.activate	Agent paired
agent.activate_clone	Agent clone activated
agent.clone_detected	Agent clone detected

For a comprehensive list of events see: https://docs.illumio.com/core/23.5/Content/Guides/events-administration/events-described/list-of-event-types.htm

For more information on Events Administration: https://docs.illumio.com/core/23.2/Content/Guides/events-administration/overview/about-this-guide.htm

How to get PCE support and inventory reports

Generate PCE Support Bundle in Web Console (on-premises only for 21.5 and above)

The PCE web console has a Support Bundles page where you can generate PCE support reports. PCE support bundles can also be generated at the command line, but the web console provides a more convenient method which is accessible to more types of users.

To generate a support bundle:

1. Choose **Troubleshooting** > **PCE Support Bundles** from the main dropdown menu.
2. Click **Generate**. The support bundle generation dialog box appears.
3. (Optional) Click **Log Collection** and specify the time range.
4. Click **Generate** again in the dialog box. The dialog disappears. The PCE Support Bundles tab displays the report generation status for each node. When the reports for all nodes are complete, an aggregate support bundle is made available for download.
5. Click **Download**.

Up to five previously generated PCE support bundles remain available for download in a list on the PCE Support Bundles tab.

If needed, the Support and Inventory reports can be generated from the PCE command line.

Please see our guide on Support and Inventory reports for additional information:
docs.illumio.com/core/23.2/content/guides/pce-administration/monitor-and-diagnose-pce-health/support-reports-for-pce.htm

The following knowledge base article provides additional details on how to provide Policy Compute Engine (PCE) support and inventory reports to Illumio Technical Support for analysis.

SIEM integration for monitoring and alerting

Forward Events to External Syslog Server (On-Prem only)

The PCE has an internal syslog repository, “Local” where all the events get stored. You can control and configure the relaying of syslog messages from the PCE to multiple external syslog servers.

To configure forwarding to an external syslog server:

1. From the PCE web console menu, choose **Settings** > **Event Settings**.
2. Click **Add**.

The Event Settings - Add Event Forwarding page opens.

3. Click **Add Repository**.
4. In the Add Repository dialog:

- *Description*: Enter name of the syslog server.
- *Address*: Enter the IP address for the syslog server.
- *Protocol*: Select TCP or UDP. If you select UDP, you only need to enter the port number and click **OK** to save the configuration.
- *Port*: Enter port number for the syslog server.
- *TLS*: Select Disabled or Enabled. If you select Enabled, click "Choose File" and upload your organization's "Trusted CA Bundle" file from the location it is stored on.

The Trusted CA Bundle contains all the certificates that the PCE (internal syslog service) needs to trust the external syslog server. If you are using a self-signed certificate, that certificate is uploaded. If you are using an internal CA, the certificate of the internal CA must be uploaded as the "Trusted CA Bundle".

- *Verify TLS*: Select the checkbox to ensure that the TLS peer's server certificate is valid.

5. Click **OK** to save the event forwarding configuration.

Please see our guide on syslog forwarding for additional information.
docs.illumio.com/core/23.5/Content/Guides/events-administration/events-setup/syslog-forwarding.htm

Forward flow data and events to SIEM from SaaS PCE

To receive flow data and events from the SaaS PCE an S3 bucket must be created. The S3 bucket can either be customer provided or an Illumio Managed S3 Bucket Subscription.

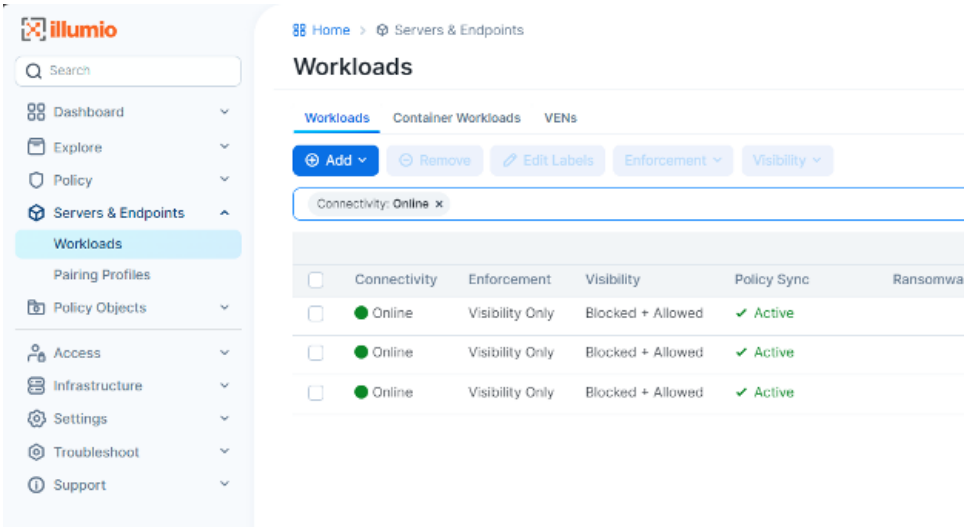
The following information will need to be provided to Illumio, to start sending flow data and events:

S3 bucket type	Information required
Customer-provided S3 bucket	• The AWS S3 Bucket Name • Your AWS Account ID • The External ID • The Role Name (default: illumio-flow-logs) • The AWS Region where the bucket exists
Illumio-managed S3 bucket subscription	• Domain Name • What data region to create the bucket in (EU, US, UK, etc.)

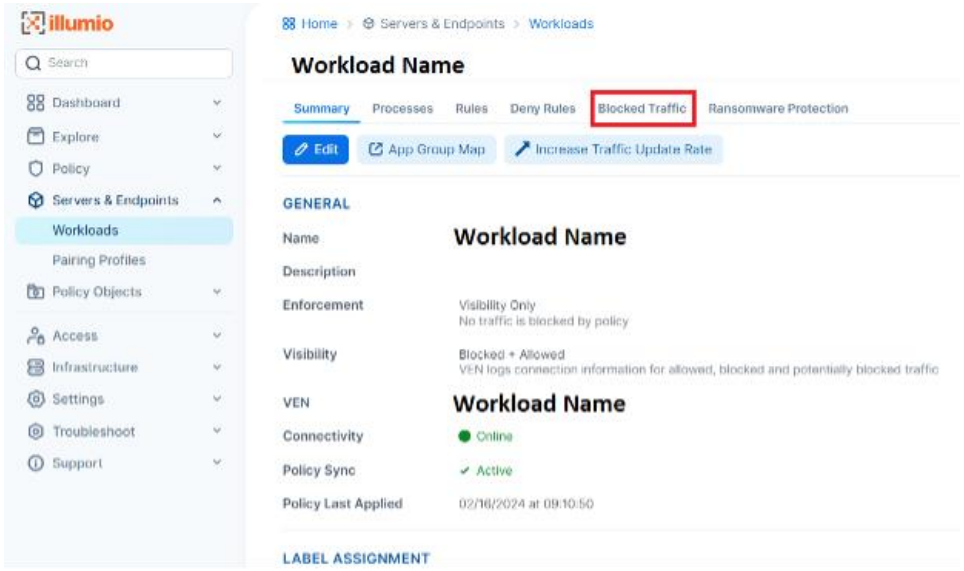
The following knowledge base article provides additional information on sending flow data and events from the SaaS PCE: support.illumio.com/knowledge-base/articles/Flow-logs-for-Illumio-Secure-Cloud-PCE.html

Section 10: Blocked Traffic

Blocked traffic is a tab that can be viewed from each workload's page in the PCE GUI which can assist in the rule-building process. To access blocked traffic, simply go to Servers & Endpoints > Workloads and select the appropriate workload.



Once in the workload page, you will see the "Blocked Traffic" tab.



This tab can be viewed to see any potentially blocked traffic, if workload is in a non-enforced mode. The user will see blocked traffic if the workload is in Selective Enforcement and the flow was blocked by a boundary, or Full enforcement mode and no rule exists to allow traffic.

Potentially blocked traffic means that there is a potential for the traffic to be blocked if the workload is moved into enforcement mode, as no rule exists to allow the traffic.

Blocked traffic means the traffic was blocked due to no rule existing to allow the traffic in the mode.

Blocked traffic may also be viewed within Illumination Plus with the appropriate scopes entered.

There are two modes to view traffic in Illumination Plus:

Reported view, which shows traffic based on the provisioned policy of the VEN at the time the traffic occurred. This reporting is immutable as it reports what happened.

Draft view, which shows how traffic will behave based on draft rules which exist in the PCE. This reporting will show what potentially will happen to traffic once rules are provisioned

About Illumio

Illumio, the Zero Trust Segmentation company, stops breaches and ransomware from spreading across the hybrid attack surface. The Illumio ZTS Platform visualizes all traffic flows between workloads, devices, and the internet, automatically sets granular segmentation policies to control communications, and isolates high-value assets and compromised systems proactively or in response to active attacks. Illumio protects organizations of all sizes, from Fortune 100 to small business, by stopping breaches and ransomware in minutes, saving millions of dollars in application downtime, and accelerating cloud and digital transformation projects.