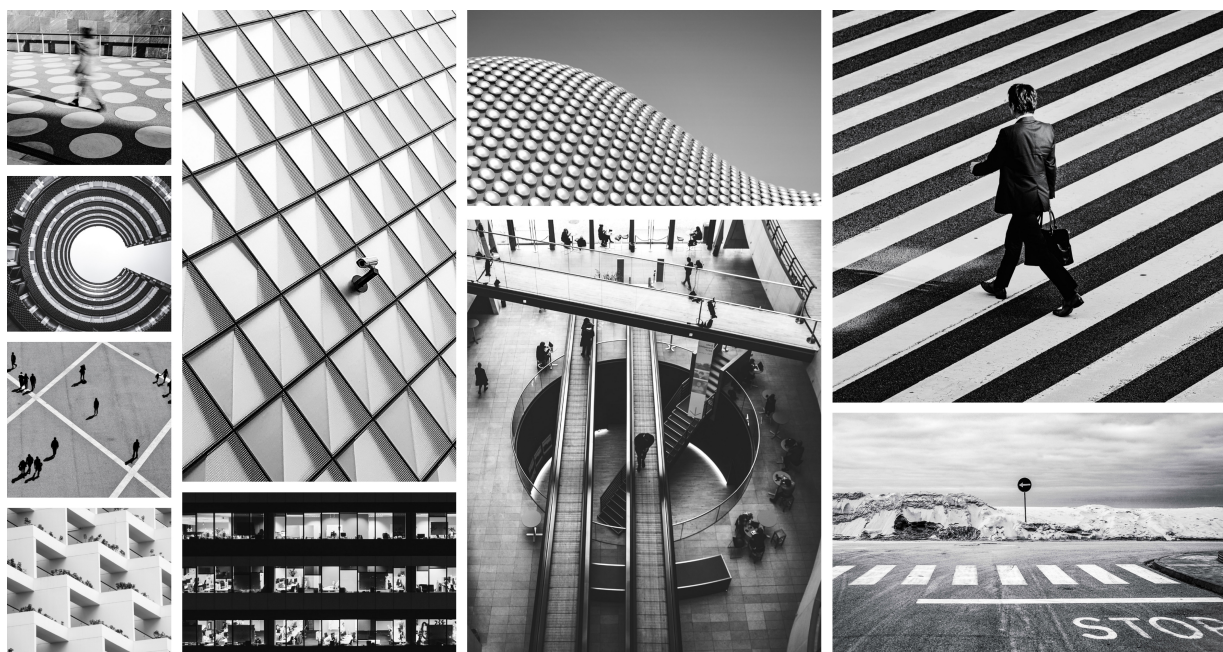




Illumio Core 24.4 Administration Guide

Published: 2024



The guides in this category explain how to operate, manage, maintain, and troubleshoot your Policy Compute Engine (PCE) and Virtual Enforcement Node (VEN) deployments. It also describes how to control the behavior of the PCE as it records events. You can change event-related settings in the PCE Web Console.

Table of Contents

Security Advisories	6
September 2024 Security Advisories	6
Ruby SAML gem component authentication bypass vulnerability	6
Severity	6
Affected Products and Patch Information	6
Resolution	6
References	7
Skipped Critical Patch Updates	7
Discovered By	7
Frequently Asked Questions	7
Modification History	8
September 2023 Security Advisories	8
Authenticated RCE due to unsafe JSON deserialization	8
Severity	8
Affected Products and Patch Information	8
Resolution	9
References	9
Skipped Critical Patch Updates	9
Discovered By	9
Frequently Asked Questions	9
PCE Administration	11
Overview of PCE Administration	11
Before You Begin	11
Notational Conventions	11
PCE Architecture and Components	11
PCE Control Interface and Commands	15
PCE Organization and Users	16
Connectivity Configuration for PCE	17
Connectivity Settings	17
SecureConnect Setup	23
AdminConnect Setup	28
Access Configuration for PCE	31
Role-based Access Control	31
Setup for Role-based Access Control	39
Role-based Access for Application Owners	44
Configure Access Restrictions and Trusted Proxy IPs	54
Password Policy Configuration	56
Authentication	60
Active Directory Single Sign-on	63
Azure AD Single Sign-on	91
Okta Single Sign-on	101
OneLogin Single Sign-on	103
Ping Identity Single Sign-on	104
VEN Administration Guide	108
Overview of VEN Administration	108
About This Administration Guide	108
VEN Architecture and Components	109
About VEN Administration on Workloads	114
illumio-ven-ctl General Syntax	125
Useful VEN and OS Commands	126
VEN State	129
VEN Startup and Shutdown	129
Disable and Enable VENs (Windows only)	130

VEN Suspension	131
Deactivate and Unpair VENs	135
VEN Deactivation and Unpairing	135
Deactivate and Unpair VENs	135
VEN Unpairing Details	138
Monitor and Diagnose VEN Status	139
VEN-to-PCE Communication	139
VEN Status Command and Options	144
VEN Logging	148
Tuning the IPFilter State Table (AIX/Solaris)	150
Manage Conntrack Table Size (Linux)	151
VEN Firewall Tampering Detection	153
VEN Tampering Protection	156
VEN Support Reports	160
VEN Troubleshooting	162
Events Administration and REST APIs	165
Overview of Events Administration	165
Before You Begin	165
About This Guide	165
Events Framework	166
Events Lifecycle for Resources	167
Events Described	168
Event Types, Syntax, and Record Format	168
List of Event Types	171
Common Criteria Only Events	182
View and Export Events	183
Examples of Events	186
Differences from Previous Releases	196
Events Monitoring Best Practices	196
Events Setup	199
Requirements for Events Framework	199
Events Settings	200
SIEM Integration for Events	203
Syslog Forwarding	204
Traffic Flow Summaries	207
Traffic Flow Types and Properties	208
Manage Traffic Flows Using REST API	210
Export Traffic Flow Summaries	215
Traffic Flow Summary Examples	216
Illumio Core PCE CLI Tool Guide 1.4.2	221
Overview of the CLI Tool	221
About This Guide	221
CLI Tool and PCE Resource Management	222
The <code>ilo</code> Command	223
HTTP Response Codes and Error Messages	224
Environment Variables	224
Installation and Authentication	225
Installation Prerequisites	226
Install, Upgrade, and Uninstall the CLI Tool	227
Authenticate with the PCE	229
CLI Tool Commands for Resources	231
View Workload Rules	231
View Report of Workload Services or Processes	232
View Host and System Inventory	233
Use the <code>list</code> Option for Resources	233

List Draft or Active Version of Rulesets	238
Import and Export Security Policy	238
Upload Vulnerability Data	240
CLI Tool Tutorials	249
How to Import Traffic Flow Summaries	249
How to Create Kerberos-Authenticated Workloads	250
How to Work with Large Datasets	252
How to Upload Vulnerability Data	253
New Document Locations	254
Core	255
Cloud	257
Other Products: Edge, Xpress, MSP	258
Integrations	258
PDF Library	260
Legal Notice	264

Security Advisories

This category includes announcements of security fixes and updates made in critical patch update advisories, security alerts and bulletins.

September 2024 Security Advisories

Here's a list of the security advisories for 2024.

Ruby SAML gem component authentication bypass vulnerability

The Ruby SAML gem is affected by an authentication bypass vulnerability, which impacts the Illumio PCE in both SaaS and on-premises deployments. An authenticated attacker could potentially leverage this vulnerability to authenticate as another SAML user. For SaaS customers, the target user can be in a different org and on a different cluster.

Severity

Critical: CVSS score is 9.9

CVSS: AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Affected Products and Patch Information

Security vulnerabilities addressed by this Security Alert affect the products listed below.

Table 1. Products Affected by the Security Vulnerability

Affected Products	Affected Versions	Fixed Version
Illumio Core PCE	<= 21.5.36	>= 21.5.37
	<= 22.2.42	>= 22.2.43
	<= 22.5.32	>= 22.5.34
	<= 23.2.30	>= 23.2.31
	<= 23.5.21	>= 23.5.22
	<= 24.2.0	>= 24.2.10

Resolution

Upgrade to the latest release for a given major version.

References

- <https://nvd.nist.gov/vuln/detail/CVE-2024-45409>
- <https://github.com/advisories/GHSA-jw9c-mfg7-9rx2>

Skipped Critical Patch Updates

Illumio strongly recommends that customers apply security patches as soon as possible. For customers that have skipped one or more Critical Patch Updates and are concerned about products that do not have security patches announced in this Critical Patch Update, please review previous Critical Patch Update advisories to determine appropriate actions.

Discovered By

External Security Firm

Frequently Asked Questions

- What software components are affected?
Only the Illumio PCE is impacted by this vulnerability.
- What products did this affect?
This vulnerability impacts the PCE, including Core on-premises deployments, Core SaaS, Endpoint, MSP, and Edge.
- Is Core SaaS affected?
SaaS PCE clusters were impacted. Those environments have been patched.
- I'm using Cloud. Am I impacted?
The Cloud platform is not affected.
- Will the patch affect performance?
The update is not expected to affect performance.
- How can I tell if this vulnerability was used against my on-premises PCE?
Illumio is creating queries that can be used by customers to detect known vectors for exploitation of this vulnerability. Please contact Illumio Support or your account team for assistance. If you suspect this vulnerability was used within your environment, please reach out to Illumio Support.
- Has Illumio investigated if this vulnerability was used on any SaaS PCEs?
Illumio is currently investigating all available data from the production SaaS environment and has so far found no indications that the issue has been exploited.
- I can't apply the patch immediately. How can I mitigate the issue in the meantime?
This vulnerability requires SAML to be enabled on the customer's PCE in order to be exploited. Customers who cannot patch their PCEs immediately, and who wish to mitigate this issue, can choose to disable SAML authentication on the PCE. For details, see the "Authentication" topic in the PCE Administration Guide. Additionally, customers can enable IP restrictions to limit access to only trusted source IPs (for example, for privileged accounts). For details, see the "Configure Access Restrictions and Trusted Proxy IPs" topic in the PCE Administration Guide.
- How long will the upgrade take?
The fix will be provided in a normal code release so this will take the same amount of time as any PCE upgrade.
- Were any Illumio customers impacted by this vulnerability?

Illumio is not aware of any exploitation of this vulnerability within any customer environments.

Modification History

- September, 2024: Initial Publication of CVE

September 2023 Security Advisories

Here's a list of the security advisories for 2023.

Authenticated RCE due to unsafe JSON deserialization

Unsafe deserialization of untrusted JSON allows execution of arbitrary code on affected releases of the Illumio PCE. Authentication to the API is required to exploit this vulnerability. The flaw exists within the `network_traffic` API endpoint. An attacker can leverage this vulnerability to execute code in the context of the PCE's operating system user.

Severity

Critical: CVSS score is 9.9

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Affected Products and Patch Information

Security vulnerabilities addressed by this Security Alert affect the products listed below.

Table 2. Products Affected by the Security Vulnerability

Affected Products	Affected Versions	Fixed Version
Illumio Core PCE	<= 19.3.6	>= 19.3.7
	<= 21.2.7	>= 21.2.8
	<= 21.5.35	>= 21.5.36
	<= 22.2.41	>= 22.2.42
	<= 22.5.30	>= 22.5.31
	<= 23.2.10	>= 23.2.11

Resolution

Upgrade to the latest release for a given major version.

References

<https://www.cve.org/CVERecord?id=CVE-2023-5183>

Skipped Critical Patch Updates

Illumio strongly recommends that customers apply security patches as soon as possible. For customers that have skipped one or more Critical Patch Updates and are concerned about products that do not have security patches announced in this Critical Patch Update, please review previous Critical Patch Update advisories to determine appropriate actions.

Discovered By

External Security Firm

Frequently Asked Questions

- What software components are affected?
Only the Illumio PCE is impacted by this vulnerability.
- What products did this affect?
This vulnerability impacts the PCE, including Core on-premises deployments, Core SaaS, Endpoint, MSP, and Edge.
- Is Core SaaS affected?
SaaS PCE clusters were impacted. Those environments have been patched.
- I'm using Cloud. Am I impacted?
The Cloud platform is not affected.
- How can I tell if this vulnerability was used against my on-premises PCE?
Illumio is creating queries that can be used by customers to detect known vectors for exploitation of this vulnerability. Please contact Illumio Support or your account team for assistance. If you suspect this vulnerability was used within your environment, please reach out to Illumio Support.
- Has Illumio investigated if this vulnerability was used on any SaaS PCEs?
Illumio is currently investigating all available data from the production SaaS environment and has so far found no indications that the issue has been exploited.
- I can't apply the patch immediately. How can I mitigate the issue in the meantime?
This vulnerability requires SAML to be enabled on the customer's PCE in order to be exploited. Customers who cannot patch their PCEs immediately, and who wish to mitigate this issue, can choose to disable SAML authentication on the PCE.
- Reference
For details, see the topic Authentication in the PCE Administration Guide.
Additionally, customers can: Enable IP restrictions to limit access to only trusted source IPs (for example, for privileged accounts). For details, see the topic Configure Access Restrictions and Trusted Proxy IPs in the PCE Administration Guide.

- How long will the upgrade take?
The fix will be provided in a normal code release so this will take the same amount of time as any PCE upgrade.
- Were any Illumio customers impacted by this vulnerability?
Illumio is not aware of any exploitation of this vulnerability on any customer environments.

PCE Administration

Overview of PCE Administration

This section describes how to maintain and operate the Policy Compute Engine (PCE). It also includes other tasks required to manage your PCE deployment and help you with ongoing PCE operations and administration.

Before You Begin

Before you begin, become familiar with the following technology:

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

Notational Conventions

This section gives information about the notational conventions used here.

Review these 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. Example:

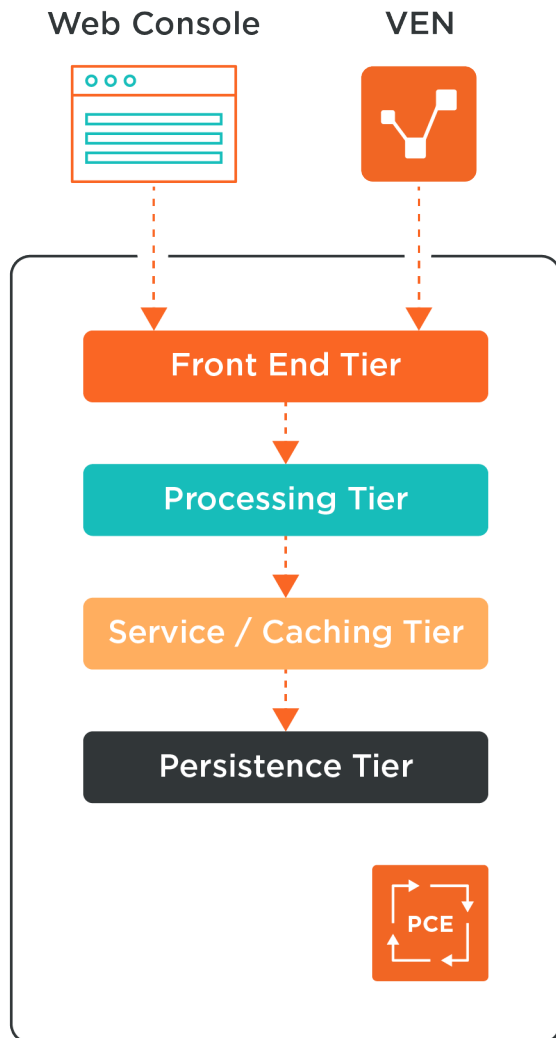
```
...  
some command or command output  
...
```

PCE Architecture and Components

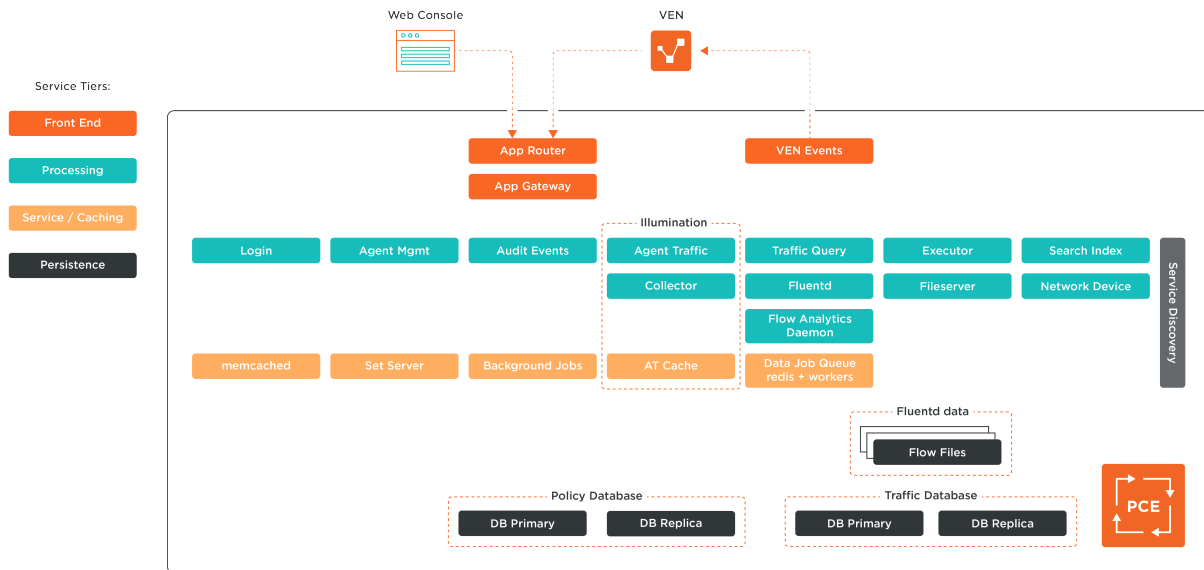
This section describes how the PCE functions, and provides an overview of its components and how they function together.

About the PCE Architecture

The PCE has four main service tiers that are used by both the PCE Web Console UI and the VEN:



Each of these service tiers are responsible for various functions, as shown below and described further in the following table.



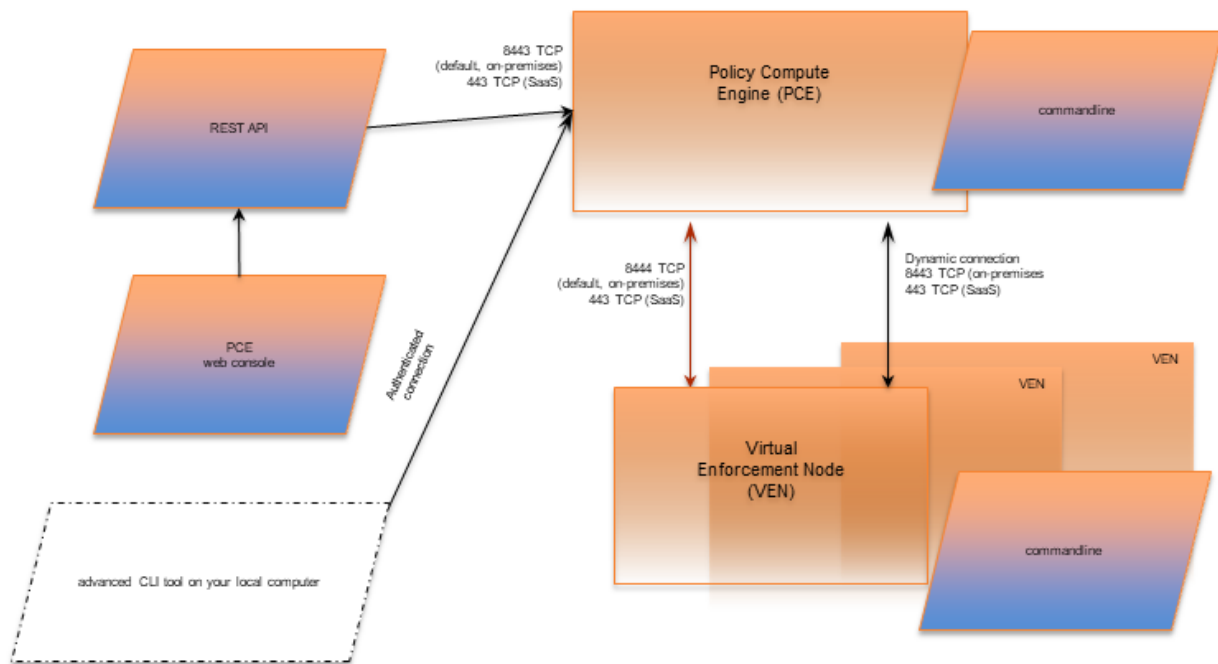
Description of PCE Components

Tier	PCE component	Description
Front-end	Management	Management interfaces include:
	interfaces: PCE web console and VEN	<ul style="list-style-type: none"> • PCE web console • REST API • PCE command line • VEN command line
	VEN events	For information, see VEN Administration Guide.
	App Router	Directs requests to the proper service.
	App Gateway	Ensures that all communication between cluster nodes is encrypted and that only cluster nodes can connect to internal services. Most services connect via the application gateway.
Processing	Login	Central server for authentication.
	Agent Manager	Manages data in the policy domain, such as workload context and policy definitions. Also, manages data for all user and organization authentication and authorization, such as users, organizations, API keys, and roles.
	Agent Traffic	Provides information about traffic to and from VENs. Serves as the service underlying Illumination.
	Collector	Aggregates packet and traffic flow information sent from the VEN. Serves as the service underlying Illumination.
	Audit Events	Creates an overview of auditable system events across the PCE and VENs.
	Fluentd	Log forwarder service that forwards the flow log files received from VENs.
	Executor	Backbone for asynchronous job execution, such as report generation and background jobs.
	Fileserver	Central storage and retrieval for large data files.

Tier	PCE component	Description
Service	Search Index	Supports auto-completion in the PCE web console.
	Traffic Query	API for traffic explorer
	Flow Analytics Daemon	Flow analytics daemon
	Network Device	Manages network devices such as switches and server load balancers that are managed by the PCE.
	memcached	Open source component: in-memory cache.
	Background Jobs	The backbone for asynchronous job execution, such as report generation and background jobs.
	Set Server	In-memory cache to aid in policy calculations.
	Agent Traffic cache	Stores the traffic flow data and graphs for Illumination. See Agent Traffic. In the PCE architecture diagram, labeled "AT Cache."
Persistence	Data Job Queue (Redis + workers)	Data job queue
	Fluentd data	Flow files
	Policy primary database and replica	Postgres database that contains all the policy and agent related data. The primary and replica databases run on separate data nodes.
	Traffic database primary and replica	Postgres database that contains all the historical traffic flow data. Traffic Explorer is backed by this data store. The primary and replica databases run on separate data nodes.

Management Interfaces for PCE and VEN

The following diagram illustrates the logical view of the management interfaces to the PCE and VEN.

PCE and VEN Management Interfaces

This guide focuses on the use of the `illumio-pce-ctl` control script and related administrative programs on the PCE itself.

Interface	Notes
PCE web console	With the PCE web console, you can perform many common tasks for managing the Illumio Core.
PCE command line	Use of the command line directly on the PCE. The <code>illumio-pce-ctl</code> command-line tool is the primary management tool on the PCE. You can perform many common tasks for managing the Illumio Core, including installing and updating the VEN.
REST API	With the Illumio Core REST API, you can perform many common management tasks, such as automating the management of large groups of workloads rather than each workload individually. The endpoint for REST API requests is the PCE itself, not the workload. The REST API does not communicate directly with the VEN.
VEN command line	The <code>illumio-ven-ctl</code> command-line tool is the primary management tool for the VEN.

PCE Control Interface and Commands

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.

**IMPORTANT**

In this guide, all command-line examples are based on an RPM installation. When you install the PCE using the tarball, you must modify the commands based on your PCE user account and the directory where you installed the software.

The PCE includes other command-line utilities used to set up and operate your PCE:

- `illumio-pce-env`: Verify and collect information about the PCE runtime environment.
- `illumio-pce-db-management`: Manage the PCE database.
- `supercluster-sub-command`: Manage specific Supercluster operations.

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

Control Command Access with `/usr/bin`

For easier command execution, PCE installation creates softlinks in `/usr/bin` by default for the Illumio PCE control commands. The `/usr/bin` directory is usually included by default in the `PATH` environment variable in most Linux systems. When 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 of `illumio-pce-ctl`

To make it simpler to run the PCE command-line tools, you can run the following Linux softlink commands or add them to your `PATH` environment variable.

```
$ 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 Organization and Users

A PCE organization is a group of policies and users targeted toward a specific business group or unit, including all the networking security rules and people who are associated

with the policy. An organization can contain any number of users, workloads, policy objects (policies, IP lists, services, and security settings), and labels.

Organizations are initially set up by your Illumio administrator. When an organization is created, an email is sent that contains a user login for the organization. When this user logs in, the organization is created, and users can now be invited to join.

Invite Users to Your Organization

When you are an organization owner, you can invite other users to your organization and grant roles to specify permissions for those users.

When you invite a user to your organization, the user receives an email at the specified address that contains a link for their account setup. The link in invitation email is valid only for 7 days, after which it expires. If you invited a user who did not receive their email or did not sign up using that email, you can re-invite them.

External Users and Non-Email Usernames

When you use an external corporate Identity Provider (IdP) to authenticate users with the PCE, but your IdP usernames do not use email addresses, the PCE cannot send email invitations to those users when you add them to the PCE. When you add this type of user, send them a login URL that they can use to set up their Illumio Core accounts and log in to the PCE web console.

Invitation Emails Are Not Sent

When users you invite do not receive their invitation emails, the SMTP server might not be configured correctly with the PCE.

- Make sure that your PCE's IP address is allowed to relay messages and that its emails are not blocked by any anti-spam protection.
- Check your PCE's `runtime_env.yml` file to make sure that the `smtp_relay_address` value is correct.

Connectivity Configuration for PCE

This section describes how to configure connectivity to control access to network resources and communication between workloads.

Connectivity Settings

This section describes how to modify PCE settings that affect connectivity.



NOTE

Permission to edit these settings depends on your role.

Private Data Centers

The PCE uses connectivity settings to decide whether workloads are allowed to communicate with each other in private datacenters, private clouds, and shared network environments (private datacenter and public cloud).

By default, the Private Data Center connectivity setting is set and intended for workloads that are hosted in private datacenters, which do not have duplicate IP addresses in the network. When your network environment hosts workloads in your own private datacenter and in a public cloud, and you want to change this setting, contact Illumio Support.

Offline Timers

You can configure Offline Timers in **Settings > Offline Timers** and choose appropriate settings for your workloads.



NOTE

To configure Offline Timers, you must be the Global Organization Owner for your PCE or a member of the Global Administrator role.



WARNING

Disabling the Offline Timer setting degrades your security posture because the PCE will not remove IP addresses that belonged to workloads that have been disconnected from those that were allowed to communicate with the disconnected workloads. You need to remove the disconnected workloads from the PCE to ensure that its IP addresses are removed from the policy.

The PCE isolates a workload from the other workloads when the workload goes offline. The VEN sends a heartbeat message to the PCE every 5 minutes and a goodbye message when it is gracefully shutdown. The PCE marks a workload offline when these conditions occur:

- The PCE hasn't received a heartbeat message from:
 - Server VENs: for 3600 seconds (1 hour).
 - Endpoint VENs: for 24 hours
- The PCE receives a goodbye message from the VEN.

Under the following conditions, you can change the default Offline Timer settings before putting your workloads in enforcement:

- The default setting might potentially disrupt your critical applications.
- Application availability is more important than security.

**NOTE**

How you configure this setting is a tradeoff between benefiting from an increased zero-churn outage time window versus increasing the window of time where IP addresses could be reused. You should weigh the operational and security benefits and find a balance suitable for your applications.

Decommission and IP Cleanup Timer

Sets how much time must elapse before a managed workload is marked "offline" after it sends a goodbye message. By default, the High Security setting is:

- Server VENs: Wait 15 minutes .
- Endpoint VENs: Wait 1 day.

Wait 1 hour/1 day - High Security (Default)

The PCE performs the following actions:

1. Listens for Goodbye messages from the VEN.
2. Pushes an updated policy to the peer workloads that were previously allowed to communicate with the removed workloads.
3. Immediately cleans up those workloads IP addresses from its active policy.

- *Never remove IP addresses - Highest Availability*

This setting has the following affect on the PCE:

- Ignores Goodbye messages from workloads.
- Keeps all IP addresses in policy and never automatically remove unused IP addresses.
- Requires a removal of those unused IP addresses.
- *Custom Timeout*

Enter a time period (minimum: 0 seconds).

The PCE performs the following actions:

- Listens for Goodbye messages from the VEN.
- Waits for the specified time period before cleanup of those workloads IP addresses from its active policy.
- Pushes an updated policy to the peer workloads that were previously allowed to communicate with the removed workloads.

Disconnect and Quarantine Timer

Sets how much time must elapse before a managed workload is marked "offline" after the PCE has received no heartbeat from the VEN. By default, the High Security setting is:

- Server VENs: Wait 1 hour.
- Endpoint VENs: Wait 1 day.

Wait 1 hour/1 day - High Security (Default)

The PCE performs the following actions:

1. Waits for the configured time to receive a heartbeat from the disconnected workloads and then quarantines workloads that do not respond within that time period.
2. Removes the quarantined workloads IP addresses from its active policy.
3. Pushes an updated policy to the peer workloads that were previously allowed to communicate with the quarantined workloads.

Never remove IP addresses - Highest Availability

This setting has the following affect on the PCE:

- Never disconnects or quarantines workloads that fail to heartbeat.
- Keeps all IP addresses in policy and never automatically removes unused IP addresses.
- Requires a removal of those unused IP addresses.

Custom Timeout

Enter a time period (minimum: 300 seconds).

The PCE performs the following actions:

1. Waits for the specified time period for the VEN to heartbeat.
2. Quarantines those workloads that do not respond within that time period.
3. Removes the quarantined workloads IP addresses from its active policy.
4. Pushes an updated policy to the peer workloads that were previously allowed to communicate with the quarantined workloads.

Disconnect and Quarantine Warning

Sets how much time must elapse before the PCE emits a warning event to indicate that the VEN missed heartbeats. The server VEN will appear in a warning state on the VEN pages.

The default settings are:

- Server VENs: Wait one-quarter of the Disconnect and Quarantine Timer.
- Endpoint VENs: Disabled.

Wait one-quarter of the Disconnect and Quarantine Timer - (Default) (applies to Server VENs only)

The PCE performs the following actions:

1. Wait one-quarter of the *Disconnect and Quarantine Timer* setting for the server VEN to heartbeat before emitting a warning event indicating that the server VEN has missed heartbeats. The server VEN appears in a warning state on the VEN pages.
2. If the *Disconnect and Quarantine Timer* is set to *Never remove IP addresses - Highest Availability*, the PCE emits a warning event 15 minutes after receiving the previous VEN heartbeat.

3. If you set a custom time of 20 minutes or less for the *Disconnect and Quarantine Timer* and the PCE receives no heartbeat from the VEN at least 5 minutes after receiving the previous heartbeat, the PCE emits a warning event to indicate the missed heartbeat. The endpoint VEN will appear in a warning state on the VEN pages.

Custom Timeout (applies to Server and Endpoint VENs)

Enter a time period greater than 5 minutes (300 seconds) and less than the value specified for the Disconnect and Quarantine Timer.

1. Waits for the specified time period for the VEN to heartbeat.
2. VENs appear in a warning state on the VEN pages.

Set the IP Version for Workloads

This section describes how to enforce a preference for IPv4 over IPv6 addresses.

Change Linux Workloads to Prefer IPv4

To ensure that your paired Linux VEN workloads prefer IPv4 over IPv6 addresses in your PCE organization, edit the `/etc/gai.conf` file on the VEN by adding the following line:

```
precedence ::ffff:0:0/96 100
```

This change will cause `getaddrinfo` system calls to return the IPv4 addresses before IPv6 addresses.

This method works when you assign IPv4 addresses to your workloads. However, it doesn't work when your workloads only have IPv6 addresses (meaning, no IPv4 addresses for the hosts) or the software installed is hard coded to look for IPv6 addresses.

Change Windows Workloads to Prefer IPv4

When you choose to allow only IPv4 traffic for your PCE organization, the VENs on your workloads drop IPv6 traffic when they are in Enforced mode. This decision can lead to delays and communication failures in applications because applications will wait for IPv6 connection attempts to time out before attempting to connect over IPv4.

The problem occurs because, by default, the Windows OS prefers IPv6 over IPv4 and will attempt to connect over IPv6 before IPv4. As a workaround, you can change the order of connection attempts so that IPv4 is preferred over IPv6. With this change, applications will connect over IPv4 first and succeed or fail as governed by the workload's firewall policies.

For information about changing the connection order to prefer IPv4 over IPv6, see the Microsoft KB article [Guidance for configuring IPv6 in Windows for advanced users](#).

As explained in the KB article, run the following command and reboot the Windows workload:

```
reg add hklm\system\currentcontrolset\services\tcpip6\parameters /v DisabledComponents /t REG_DWORD /d 0x20
```

To avoid rebooting the Windows workload, run the following commands:

```
netsh interface ipv6 delete prefixpolicy ::ffff:0:0/96
netsh interface ipv6 add prefixpolicy ::ffff:0:0/96 60 4
```

Manage Security Settings

You can manage security settings by accessing the page **Settings -> Security**:

Security for		Options	Description
VENS (Versions 20.2.0 and higher)	IPv6 traffic	Allow IPv6 traffic	Allowed based on policy
		Block IPv6 traffic	Blocked only in Enforcement state. Always allowed on AIX and Solaris workloads
VENS (Versions lower than 20.2.0)	IPv6 traffic	Allow IPv6 traffic	All IPv6 traffic allowed
		Block IPv6 traffic	Blocked only in Enforcement state. Always allowed on AIX and Solaris workloads
IKE Authentication	Authentication type	PSK	Use Pre-shared Keys for authentication
		Certificate	Use certificates for authentication
Public cloud configuration	NAT Detection	Private Data Center or	For workloads in a known public cloud (such as AWS or Azure) the public IP address of the workload as seen by the PCE is distributed along with the IP addresses of the interfaces on the workload. Use this setting only if there are no shared SNAT IP addresses for egress traffic from the public cloud workloads.
		Public Cloud with 1:1 NAT (default)	
		Public Cloud with SNAT/NAT Gateway (recommended setting if using a NAT gateway in AWS or Azure or the default outbound access in Azure)	The PCE will ignore the public IP address of the workload in policy computation. This setting is used in environments where workloads in a known public cloud (e.g, AWS or Azure) that connect to other workloads or the PCE outside the VPC or cloud via the SNAT IP address or SNAT pool (e.g, NAT Gateway in AWS) as the public IP seen by the PCE is not specific to any workloads. Only the IP address of the network interfaces on the workload (usually the private IP addresses) is distributed in the policy.

Enable IP Forwarding

(For Linux VENS only)

In PCE versions earlier than 21.5.10, IP forwarding is automatically enabled for hosts in a container cluster that is reported by Kubelink to the PCE or hosts explicitly set to use the Container Inherit Host Policy feature.

Starting in PCE version 21.5.10, you can enable IP forwarding on hosts without using any container segmentation features. To enable this feature, contact Illumio Support.

1. In the PCE web console, choose **Security > IP Forwarding**. The IP Forwarding tab appears if the feature is enabled.

**NOTE**

Use the API call to the PCE to enable this feature so it appears in the Security menu as an option.

2. In this tab, you can use labels and label groups to enable IP forwarding for the workloads that match the label combination. Use combinations of Role, Application, Environment, and Location labels and label groups in the same way that you would to specify workloads for any other purpose; for example, in a Rule or any of the tabs under the Security Settings page.

Workloads with IP forwarding enabled will configure the host firewall to allow all forwarded traffic without visibility, including traffic forwarded through the host.

SecureConnect Setup

Enterprises have requirements to encrypt in transit data in many environments, particularly in PCI and other regulated environments. Encrypting in transit data is straightforward for an enterprise when the data is moving between datacenters. An enterprise can deploy dedicated security appliances (such as VPN concentrators) to implement IPsec-based communication across open untrusted networks.

However, what if an enterprise needs to encrypt in transit data within a VLAN, datacenter, or PCI environment, or from a cloud location to an enterprise datacenter? Deploying a dedicated security appliance to protect every workload is no longer feasible, especially in public cloud environments. Additionally, configuring and managing IPsec connections becomes more difficult as the number of hosts increases.

SecureConnect Features

SecureConnect has the following key features.

Supported Platforms

SecureConnect works for connections between Linux workloads, between Windows workloads, and between Linux and Windows workloads.

IPsec Implementation

SecureConnect implements a subset of the IPsec protocol called Encapsulating Security Payload (ESP), which provides confidentiality, data-origin authentication, connectionless integrity, an anti-replay service, and limited traffic-flow confidentiality.

In its implementation of ESP, SecureConnect uses IPsec transport mode. Using transport mode, only the original payload is encrypted between the workloads. The original IP header information is unchanged so all network routing remains the same. However, the protocol being used will be changed to reflect the transport mode (ESP).

Making this change causes no underlying interfaces to change or be created or any other underlying networking infrastructure changes. Using this approach simply obfuscates the data between endpoint workloads by encrypting the data between them.

If SecureConnect is unable to secure traffic between two workloads with IPsec, it will block unencrypted traffic when the policy was configured to encrypt that traffic.

IKE Versions Used for SecureConnect

SecureConnect connections between workloads use the following versions of Internet Key Exchange (IKE) based on workload operating system:

- Linux ↔ Linux: IKEv2
- Windows ↔ Windows: IKEv1
- Windows ↔ Linux: IKEv1

For a list of supported operating systems for managed workloads, see [VEN OS Support and Package Dependencies](#) on the Illumio Support portal.

Existing IPsec Configuration on Windows Systems

Installing a VEN on a Windows system does not change the existing Windows IPsec configuration, even though SecureConnect is not enabled. The VEN still captures all logging events (`event.log`, `platform.log`) from the Windows system that relate to IPsec thereby tracking all IPsec activity.

Performance

The CPU processing power that a workload uses determines the capacity of the encryption. The packet size and throughput determine the amount of power that is required to process the encrypted traffic using this feature.

In practice, enabling SecureConnect for a workload is unlikely to cause a big spike in CPU processing or a decrease in network throughput. However, Illumio recommends benchmarking performance before enabling SecureConnect and comparing results after enabling it.

Prerequisites, Limitations, and Caveats

Before configuring your workloads to use SecureConnect, review the following prerequisites and limitations, and consider the following caveats.

VEN Versions

To use PKI certificates with SecureConnect, your workloads must be running VEN version 17.2 or later.

Maximum Transmission Unit (MTU) Size

IPsec connections cannot assemble fragmented packets. Therefore, a high MTU size can disrupt SecureConnect for the workloads running on that host.

Illumio recommends setting the MTU size at 1400 or lower when enabling SecureConnect for a workload.

Ports

Enabling SecureConnect for a workload routes all traffic for that workload through the SecureConnect connection using ports 500/UDP and 4500/UDP for NAT traversal and for environments where ESP traffic is not allowed on the network (for example, when using

Amazon Web Services). You must allow 500/UDP and 4500/UDP to traverse your network for SecureConnect.

Unsupported SecureConnect Usage

SecureConnect is not supported in the following situations:

- SecureConnect cannot be used between a workload and unmanaged entities, such as the label “Any (0.0.0.0/0 and ::/0)” (such as, the internet).
- SecureConnect is not supported on virtual services.
- SecureConnect is not supported on workloads in the Idle policy state. If you enable it for a rule that applies to workloads that are in both Idle and non-Idle policy states, you can impact the traffic between these workloads.
- SecureConnect is not supported on AIX and Solaris platforms.

SecureConnect and Build and Test Policy States

When you configure workloads to use SecureConnect be aware of the following caveat.

SecureConnect encrypts traffic for workloads running in all policy states except Idle. If misconfigured, you could inadvertently block traffic for workloads running in the Build and Test policy states.

SecureConnect Host-to-Host Encryption

When you configure workloads to use SecureConnect be aware of the following caveat.

SecureConnect encrypts traffic between workloads on a host-to-host basis. Consider the following example.



No.	Provision Status	Status	Providers	Providing Service	Consumers	Note
1	ADDITION PENDING	Enabled	Database	MYSQL 80 TCP	SecureConnect Off Database	

In this example, it appears that enabling SecureConnect will only affect MySQL traffic. However, when you enable SecureConnect for a rule to encrypt traffic between a database workload and a web workload over port 3306, the traffic on all ports between the database and web workloads is protected by IPsec encryption.

Use Pre-Shared Keys with SecureConnect

SecureConnect supports the use of pre-shared keys (generated by the PCE) or client-side PKI certificates for IKE authentication.

You can configure SecureConnect to use pre-shared keys (PSKs) to build IPsec tunnels that are automatically generated by the PCE. SecureConnect uses one key per organization. All the workloads in that organization share the one PSK. SecureConnect uses a randomly generated 64-character alpha-numeric string, for example:

```
c4aeb6230c508063db3e3e1fac185bea9c4d17b4642a87e091d11c9564fbd075
```


When SecureConnect is enabled for a workload, you can extract the PSK from a file in the `/opt/illumio` directory, where the VEN stores it. You cannot force the PCE to regenerate and apply a new PSK. If you feel the PSK has been compromised, contact [Technical Support](#).

**NOTE**

Illumio customers accessing the PCE from the Illumio cloud can have multiple Organizations. However, the Illumio Core PCE does not support multiple Organizations when you have installed the PCE in your datacenter.

asfasdfasdf

Configure SecureConnect to Use Pre-Shared Keys

You can configure SecureConnect to use pre-shared keys (PSKs) for IKE authentication and IPsec communication between managed workloads. SecureConnect uses one key per Organization. All the workloads in that organization share the one PSK. SecureConnect generates a random 64-character alpha-numeric string for this key.

1. From the PCE navigation menu, choose **Settings > Security Settings**.
2. Choose **Edit > Configure SecureConnect**.
The page refreshes with the settings for SecureConnect.
3. In the Default IPsec Authority field, select the **PSK** option.
4. Click **Save**.

Use PKI Certificates with SecureConnect

SecureConnect allows you to use client-side PKI certificates for IKE authentication and IPsec communication between managed workloads. If you have a certificate management infrastructure in place, you can leverage it for IKE authentication between workloads because it provides higher security compared to using pre-shared keys (PSKs).

Certificate-based SecureConnect works for connections between Linux workloads, between Windows workloads, and between Linux and Windows workloads.

The IPsec configuration uses the certificate with the distinguished name from the issuer field that you specify during PCE configuration for IKE peer authentication.

Requirements and Caveats

- You must have a PKI infrastructure to distribute, manage, and revoke certificates for your workloads. The PCE does not manage certificates or deliver them to your workloads.
- The PCE supports configuring only one global CA ID for your organization.
- Only use certificates obtained from trusted sources.
- The VEN on a workload uses a Certificate Authority ID (CA ID) to authenticate and establish a secure connection with a peer workload.
- Connected workloads must have CA identity certificates signed by the same root certificate authority. When workloads on either end of a connection use different CA IDs, the

IKE negotiation between the workloads will fail and the workloads will not be able to communicate with each other.


Leaf certificate X.509 field requirement

- Version 3
- Subject Name DN must contain Common Name (example: OU=VEN, CN=centos6.ilabs.io)
- SubjectAltName (required for better compatibility) must contain an email address field that is identical to the Common Name of DN (example: DNS:centos6, email:centos6@ilabs.io)
- Must contain key usage with
 - Digital Signature
 - Key Encipherment
 - Data Encipherment
 - Key Agreement
- Must contain Extended key Usage with
 - IPSec End System
 - IPSec User
 - TLS Web Server Authentication (optional for macOS X compatibility)
- Must Contain Authority Key Identifier

Set up Certificates on Workloads

To use PKI certificates with SecureConnect, you must set up certificates on your Windows and Linux workloads independently.

File Requirements

File	Requirements
Issuer's certificate	<p>The global CA certificate, either root or intermediate, in PEM or DER format</p> <div>  <p>NOTE On Linux, the issuer's certificate must be readable by the Illumio user.</p> </div>
pkcs12 container	<p>Archive containing the public key, private key, and identity certificate generated for the workload host.</p> <p>Sign the identity certificate using the global root certificate.</p> <p>You can password protect the container and private key but do not password protect the public key.</p>

Installation Locations

Windows Store

Use the Windows OS (for example Microsoft Management Console (MMC)) to import the files into these locations of the local machine store (not into your user store).

- Root certificate: Trusted Root Certificate Store
- pkcs12 container: Personal ("My") certificate store

Linux Directories

Copy the files into the following Linux directories. (You cannot change these directories.)

- Root certificate: `/opt/illumio_ven/etc/ipsed.d/cacert`
- pkcs12 container: `/opt/illumio_ven/etc/ipsed.d/private`

Configure PKI Certificates

You can use client-side PKI certificates for IKE authentication and IPsec communication between managed workloads. The PCE supports configuring only one global CA ID for your organization. Configuring SecureConnect to use certificates applies the setting to All Roles, All Applications, All Environments, and All Locations.

Configuring SecureConnect to use PKI certificates in the global Security Settings page does not manage certificates for your organization or deliver them to your workloads.



NOTE

You must set up certificates on your Windows and Linux workloads independently. For information, see [Requirements for Certificate Setup on Workloads \[27\]](#).

1. Go to **Settings > Security Settings**.
2. Choose **Edit > Configure SecureConnect**.
3. In the Default IPsec Authority field, select **Certificate Authority**.
4. In the Global Certificate ID field, enter the distinguished name from the Issuer field of your trusted root certificate. (This certificate is used globally for all workloads in your organization enabled with SecureConnect.)
5. Click **Save**.

AdminConnect Setup

Using AdminConnect, you can control access to network resources based on Public Key Infrastructure (PKI) certificates. Because the feature bases identity on cryptographic identity associated with the certificates and not IP addresses, mapping users to IP addresses (common for firewall configuration) is not required.

With AdminConnect, a workload can use the certificates-based identity of a client to verify its authenticity before allowing it to connect.

For more information, see [SecureConnect Setup \[23\]](#) and [AdminConnect Setup \[28\]](#).

Certificates for AdminConnect

AdminConnect relies on PKI certificates for relationship-based access control of workloads.

The feature uses the same certificate infrastructure enabled for SecureConnect. If you have not set up a certificate for SecureConnect, see [Configure SecureConnect to Use Certificates \[28\]](#).

The same prerequisites and limitations for certificate setup apply to AdminConnect. Additionally, because you can use AdminConnect to control access for laptops, certificates on laptops must meet these additional requirements:

- The certificate must have a unique Subject Name and Subject Alt Name.
- The certificate must be enabled with all extended key usage to check trust validation.

Secure Laptops with AdminConnect

You can use Illumio to authenticate laptops and grant them access to managed workloads. To manage a laptop with AdminConnect, complete the following tasks:

1. Deploy a PKI certificate on the laptop. See [Certificates for AdminConnect. \[28\]](#)
2. Add the laptop to the PCE by creating an unmanaged workload and assign the appropriate labels to it to be used for rule writing
3. Create rules using those labels to grant access to the managed workloads. For information, see "Enable AdminConnect for a Rule" in the Security Policy Guide.
4. Configure IPsec on a laptop.

To add a laptop to the PCE by creating an unmanaged workload:

To manage a laptop with AdminConnect, add the laptop to the PCE as an unmanaged workload.

1. Choose **Workloads > Add > Add Unmanaged Workload**.
2. Complete the fields in the General, Labels, Attributes, and Processes sections.
3. In the Machine Authentication ID field, enter all or part of the DN string from the Issuer field of the end entity certificate (CA Subject Name). For example:
CN=win2k12, O=Illumio, OU=Portal, ST=CA, C=US, L=Sunnyvale



TIP

Enter the exact string that you get from the `openssl` command output.

4. Click **Save**.

To configure IPsec on a laptop:

To use the AdminConnect feature with laptops in your organization, you must configure IPsec for these clients.

See the Microsoft Technet article [Netsh Commands for Internet Protocol Security \(IPsec\)](#) for information about using netsh to configure IPsec.

See also the following examples for information about the IPsec settings required to manage laptops with the AdminConnect feature.

```
PS C:\WINDOWS\system32> netsh advfirewall show global
```

```
Global Settings:
```

```
-----
IPsec:
StrongCRLCheck                0:Disabled
SAIdleTimeMin                 5min
DefaultExemptions             NeighborDiscovery,DHCP
IPsecThroughNAT               Server and client behind NAT
AuthzUserGrp                  None
AuthzComputerGrp              None
AuthzUserGrpTransport         None
AuthzComputerGrpTransport     None

StatefulFTP                   Enable
StatefulPPTP                  Enable
```

```
Main Mode:
KeyLifetime                   60min,0sess
SecMethods                    ECDHP384-AES256-SHA384
ForceDH                       Yes
```

```
Categories:
BootTimeRuleCategory          Windows Firewall
FirewallRuleCategory           Windows Firewall
StealthRuleCategory            Windows Firewall
ConSecRuleCategory             Windows Firewall
```

```
Ok.
```

```
PS C:\WINDOWS\system32> netsh advfirewall consec show rule name=all
```

```
Rule Name:                      telnet
-----
Enabled:                        Yes
Profiles:                       Domain,Private,Public
Type:                            Static
Mode:                            Transport
Endpoint1:                       Any
Endpoint2:                       10.6.3.189/32,10.6.4.35/32,192.168.41.163/32
Port1:                           Any
Port2:                           23
Protocol:                        TCP
Action:                          RequireInRequireOut
Auth1:                           ComputerKerb,ComputerCert
Auth1CAName:                      CN=MACA, O=Company, OU=engineering,
S=CA, C=US, L=Sunnyvale, E=user@sample.com
Auth1CertMapping:                 No
Auth1ExcludeCAName:              No
Auth1CertType:                    Intermediate
Auth1HealthCert:                 No
MainModeSecMethods:              ECDHP384-AES256-SHA384
QuickModeSecMethods:             ESP:SHA1-AES256+60min+100256kb
```

ApplyAuthorization:	No
Ok.	

Access Configuration for PCE

This section describes how to configure the PCE to control access.

Role-based Access Control

This section describes the concepts of role-based access control (RBAC) and how it works with the PCE.

Overview of Role-based Access Control

Security-oriented companies should grant employees the exact permissions they need based on their role. Illumio Core uses role-based access control (RBAC) to deliver security at an enterprise scale in the following ways:

- Assign your users the least required privilege they need to perform their jobs.
Limit access for your users to the smallest operation-set they need to perform their jobs; for example, monitor for security events.
- Implement separation of duties.
Delegate the responsibility to manage a zone to a specific team or delegate authority to application teams; for example, delegate a team to manage security for the US-West Dev zone, or assign the DevOps team to set security policy for the HRM application they manage.
- Grant access to users based on two dimensions: roles and scopes.
Each role grants access to a set of capabilities in Illumio Core. Scopes define the workloads in your organization that users can access and are based on three labels: Application, Environment, and Location. The scopes specify the boundaries of the sphere of influence granted to a user.
For example, a user can be added to the Ruleset Provisioner role with the scope Application CRM, Environment Staging, and Location US. With that access, the user could provision rulesets for workloads that are part of your CRM application in the Staging environment located in the US.
- Centrally manage user authentication and authorization for Illumio Core.
Configure single sign-on with your corporate Identity Provider (IdP) and designate which external IdP groups should have access roles. Group membership is managed by your IdP while resource authorization is configured in Illumio Core.

Use Cases

Illumio designed our RBAC feature around a set of use cases based on the way that enterprises manage the security of the computing assets in their environment. These use cases encompass common security workflows for the modern, security-conscious enterprise. The personas include different levels of security professionals.

Support the Security Workflow

Customers can configure the RBAC feature to support any type of responsibility bifurcation that they have in their workflow models. For example, the following workflows are supported:

- Architect-level professionals define all security policy for an enterprise by adding rulesets and rules in the PCE.
- Junior-level professionals provision rulesets and rules to workloads during maintenance windows. Junior personnel cannot edit any policy items in the Illumio PCE.
- Some users only view the infrastructure and alert senior team members when security issues occur.

Manage Security for Specific Workloads

When you combine Illumio Core RBAC roles with scopes, you can secure access for IT teams who support specific applications or different geographic locations. For example, customers could delegate authority for workloads in the following ways:

- To manage security for workloads around silos; for example, a particular cloud provider like AWS.
- To decentralize their security policy to specific application teams allowing them to act quickly when managing application security without waiting for the central security team.
- To bifurcate the security of their infrastructure in such a way that one user is responsible only for the West coast assets and another user is responsible for the East coast assets.

Features of Role-based Access Control

Built-in Roles

Illumio Core includes seven roles that grant users access to perform operations. Each role is matched with a scope. See [About Roles, Scopes, and Granted Access \[33\]](#) for information.

Granular Permissions

You can assign multiple roles to one user and by mixing and matching the different roles, you can achieve different levels of granularity of permissions.

You can grant different permissions to different users for different resources by defining scopes. For example, you might allow some users complete access to add rulesets for all workloads in your staging environment. For other users, you might grant access to all workloads in all environments. Users can be assigned exactly one role, representing their singular job function while other users can be assigned multiple roles, representing multiple job functions.

Identity Federation Using External Users and Groups

You can connect to external LDAP directories to manage users and user groups by configuring single sign-on (SSO) for the PCE.

Using this feature, you can create and manage users locally in PCE, or use an IdP to manage users and user groups from an existing directory. External user and user groups authenticate with the external IdPs.

Custom Role Assignments

You can customize access to suit your organization by specifying specific scopes for the Ruleset Manager and Ruleset Provisioner roles.

Audit Information

You can access an audit trail of user activity through the following reports:

- The User Activity page, which displays the authentication details for each user, when they logged in, and whether they are online.
- The Organization Events page, which displays when Organization Owners granted users access, when users logged in and out, and the actions they performed.

About Roles, Scopes, and Granted Access

Illumio Core includes seven 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 Read Only	View any resource or organization setting They cannot perform any operations.
Global Policy Object Provisioner	Provision rules containing IP lists, services, and label groups They cannot provision rulesets, virtual services, or virtual servers, or add, modify, or delete existing policy items.



NOTE

You can add, modify, and delete your API keys because you own them.

About the Read Only User Role

The Read Only User role applies to all users in your organization—local, external, and users who are members of external groups managed by your IdP. This role allows users to view resources in Illumio Core when they are not explicitly assigned to roles and scopes in the PCE.

For example, you configure single sign-on for your corporate Microsoft Active Directory Federation Services (AD FS) so that users managed by AD FS can log into the PCE by using their corporate usernames and passwords. However, you haven't added all your exter-

nal users to the PCE or assigned them to roles. These users can still log into the PCE by authenticating with the corporate IdP and view resources in the PCE.

The Read Only User role is not listed in the **Role-Based Access > Global Roles** or **Scoped Roles** pages because it is considered a default, catchall type of role. Users have access to this role on an organization-wide basis because you either enable or disable it for your entire organization. Additionally, you do not see it in the list of a user's role assignments when you view the user's details page (**Role-Based Access > Users and Groups**). However, when the role is enabled for your organization, you see it listed in the **Role-Based Access > User Activity** details for each user.





NOTE



You can enable and disable the Read Only User role from the **Role-Based Access > Global Roles > Global Read Only** page.

When the Read Only User role is disabled for your organization, users who are not assigned to roles cannot access Illumio managed resources. When attempting to log into the PCE, they are still authenticated by their corporate IdP but the PCE immediately logs them out because they do not have access (even read-only access) to any Illumio managed assets.

Roles with Custom Scopes

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

Role	Granted Access
Full Rule-set Manager	<ul style="list-style-type: none"> Add, edit, and delete all rulesets within the specified scope. Add, edit, and delete rules when the provider matches the specified scope. The rule consumer can match any scope. <div>  <p>NOTE You can choose the All Applications, All Environments, and All Locations scope with the Full Ruleset Manager role.</p> </div>
Limited Ruleset Manager	<ul style="list-style-type: none"> 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. <div>  <p>NOTE You cannot choose the All Applications, All Environments, and All Locations scope with the Limited Ruleset Manager role.</p> </div>

Role	Granted Access
Ruleset Provisioner	<p>Provision rulesets within specified scope.</p> <div>  <p>NOTE You can choose the All Applications, All Environments, and All Locations scope and custom scopes with the Ruleset Provisioner role.</p> </div>
Workload Manager	<p>Manage workloads and pairing profiles within the specified scope. Read-only access provided to all other resources.</p> <div>  <p>NOTE The 19.1.0 PCE does not support unpairing multiple managed workloads via the REST API when you are logged in as a Workload Manager. You can unpair workloads using the PCE web console because it restricts selection of workloads by the user's scope. However, via the REST API, the bulk unpair operation fails when multiple workloads are selected and one or more of the workloads are out of the user's scope.</p> </div>

Workload Manager Role

Use Case 1

You want to use scripts in your development environment to programmatically spin up and bring down workloads; your scripts create pairing profiles and generate pairing keys without you granting elevated Admin privileges to the scripts.

Use Case 2

Your application teams are in charge of changing the security posture of workloads, such as changing the policy enforcement states. You want to allow your application teams to manage workload security without granting them broad privileges, such as All | All | All access.

Use Case 3

You want to prevent your PCE users from accidentally changing workload labels by moving the workloads in Illumination.

Solution

Users with the Workload Manager role can create, update, and delete workloads and pairing profiles. This role is a scoped role; when you assign a user to a scope, they can only manage workloads within the allocated scope. The Workload Manager can pair, unpair, and suspend VENs and change the policy state. It is an additive role; you can assign the Workload Manager role to a user and combine it with any other PCE role to provide additional privileges for that user.

Configuration

1. Create a local user with “None” or Global Read Only role.
2. Assign the Workload Manager role to the user.
3. (Optional) Provide the invitation link to the new workload manager user.
4. The workload manager can then log into the PCE and manage workloads and pairing profiles per the allocated scope.

The Workload Manager role is available under Scoped Roles. Users assigned this role can view applications that are outside their scopes but can only modify those applications that are within their scopes.



NOTE

A workload manager user cannot clear traffic counters from workloads within their scope.

Example: Limited Ruleset Manager Role

A user has the role Full Ruleset Manager role and access to the following scope:

All Applications | Production Environment | All Locations

The user can create and manage:

- Any ruleset that matches the Production environment
- Intra- or extra-scope rules that match this scope:
All Applications | Production Environment | All Locations
Where the provider and consumer of the rule are both within the Production environment scope.

For intra-scope rules, all workloads can communicate within their group (as defined by the scope), so the rule consumer is not restricted. However, in extra-scope rules, the Environment label of the resource selected as the consumer must match the label in the scope exactly.

The user cannot create a rule with the scope “All | All | All” because that scope is broader than the user’s access, which is only for the Production environment.

Because the user is a member of the Limited Ruleset Manager role, the user cannot manage custom iptables rules and the following resources cannot be selected as consumers in extra-scope rules:

- IP lists
- Label groups
- User groups
- Workloads

Combine Roles to Support Security Workflows

Illumio includes fine-grained roles to manage security policy. The roles control different aspects of the security workflow. By mixing and matching them, you can effectively control the access needed by your company.

Ruleset Only Roles

You can add users to the Full Ruleset Manager and Ruleset Provisioner roles so that they can edit the security policies on the workloads within their assigned scopes without affecting other entities, such as services, virtual services, or virtual servers.

These users can write rules for their workloads and provision them when the rules do not have dependencies on global objects, such as services or IP lists.

Ruleset Plus Global Policy Object Provisioner Roles

You can add users to the Ruleset Manager (Full or Limited) role and the Global Policy Object Provisioner role so that they can control the security policy for workloads.

These users can create rulesets within their assigned scopes and write rules that are not dependent on global objects. However, they can provision any workloads, even those containing services, IP lists, and label groups.

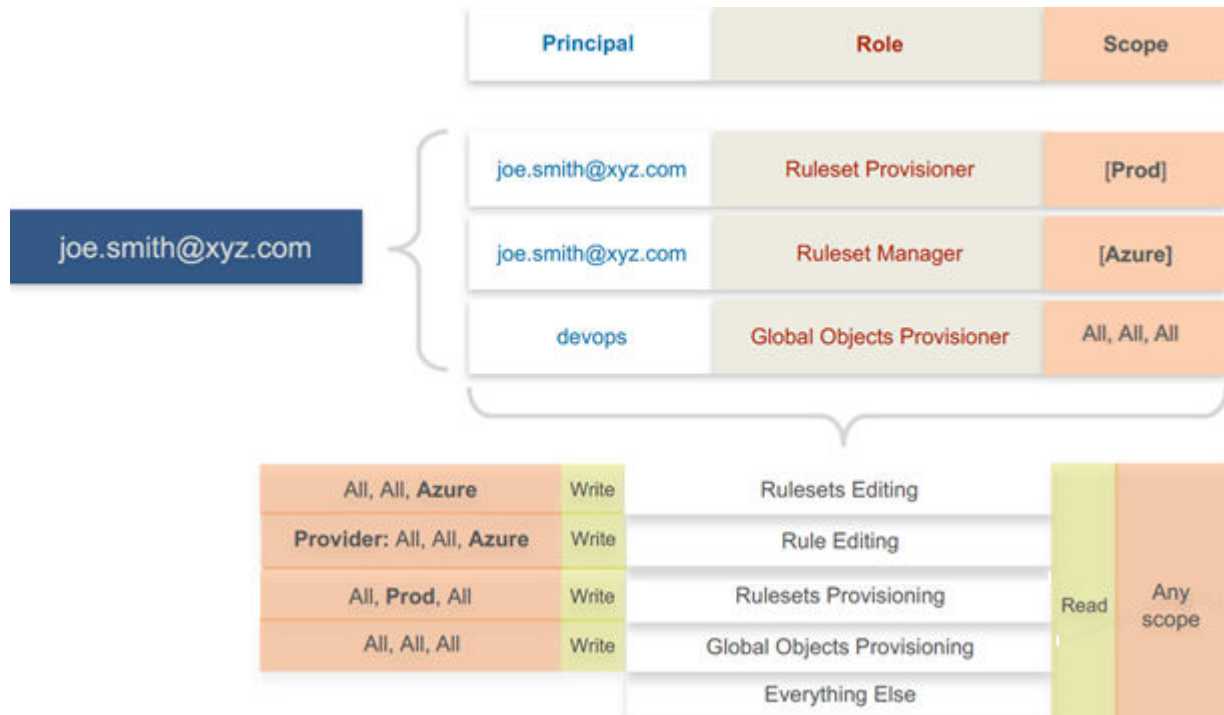
Global Organization Owner or Administrator Roles

You can add architect-level professionals to the Global Organization Owner or Global Administrator role so that they can define all security policy for an enterprise.

They have the capability to modify global objects, such as services and labels, add workloads, pair workloads, and change workload modes to function as a security policy administrator.

Role Access is Additive

In the following example, Joe Smith is added to two user roles and one external group and each is assigned a specific role and scope. Joe's ability to manage security for his company is a union of the roles and scopes he is assigned to.



Example Role Workflows

The following example shows the hand offs between a user who is a member of the Global Organization Owner role and a member of a Ruleset Manager role.

1. An Organization Owner grants access to one or more scopes for a Ruleset Manager by selecting specific labels, which define the permitted scopes for the Ruleset Manager.
2. The Ruleset Manager logs in and creates rules that conform to the specified scopes, as defined by the labels that are accessible to that user.
3. The Ruleset Manager has read-only access to all other PCE resources, such as services or rulesets with different scopes from the scopes that the Ruleset Manager can access.
4. The Organization Owner reviews the rules created by the Ruleset Manager and provisions them as needed.

Prerequisites and Limitations

- You must be a member of the Global Organization Owner role to manage users, roles, and scopes in the PCE.
- Configuring SSO for an Illumio supported IdP is required for using RBAC with external users and groups.
If you have not configured SSO, you can still add external users and external groups to the PCE; however, these users will not be able to log into the PCE because they will not be able to reach the IdP or SAML server to authenticate.
- Illumio resources that are not labeled are not access restricted and are accessible by all users.
- External users who are designated by username and not an email address in your IdP will not receive an automatic invitation to access the PCE. You must send them the PCE URL so they can log in.
- You cannot change the primary designation for users and groups in the PCE; specifically, the email address for a local user, the username or email address for an external user, or the contents of the External Group field for an external group. To change these values, you must delete the users or groups and re-add them to the PCE.

- An App Owner who is in charge of the application in both production and development environments does not have permissions to write extra-scope rules between production and development.

Local users are not locked out of their accounts when they fail to log in. After 5 consecutive failures, the PCE emails the user that their account might be compromised.

Locked users retain all their granted access to scopes in the PCE; however, they cannot log into the PCE.

Setup for Role-based Access Control

This section describes how to configure role-based access control (RBAC) for the PCE.



NOTE

Permission to configure these settings is dependent on your role.

Add a Scoped Role

Add a scoped role to create fine-grained access control to manage security policy for your workloads.

By defining scopes, you can grant different permissions to different users for different resources. For example, you might allow some users to add rulesets for all workloads in your staging environment. You might grant access to all workloads in all environments for other users.

When adding a scoped role:

- use the Access Wizard
- Define the scope of the role by selecting labels or label groups for applications, environment, and location.
- Add a local user, external user, or user group to the role.
- Select roles and confirm your choice.

Manage a Local User

Local users are created in the PCE (an IdP does not manage them). When they log into the PCE, they must enter their email addresses and passwords. The Illumio PCE encrypts and stores their passwords.

When you install the PCE, the first user account it creates is a local user. You can create additional local users as a backup in case your external IdP goes offline or the SAML server is inaccessible.

To add a local user:

- In the Local Users tab, click **Add**.
- Enter a name and an email address. The email address must use the format xxxx@yyyy.zzzz and be 255 characters or less.
You can add email addresses with an apostrophe (') in them. In the PCE, you can have duplicate names for local users, but you cannot have duplicate email addresses.
The PCE emails the user to the address you specified an invitation to with a link to create their Illumio user account. The link in the invitation email is valid only for 7 days, after which it expires.
- Select a role for the user: None, Global Organization Owner, Global Administrator, or Global Read Only.

You can change a user's role membership after adding them by going to the user's details page or from a role details page. The "My Roles" feature allows you to view the list of assigned permissions (roles).

To remove a local user

Select it in the Users and Groups and remove it.

When you remove a local user while the user is online, the PCE logs the user out as soon as the user is removed.

The user is removed from the Local Users tab; however, the user remains in the User Activity page and is designated as offline. The user's actions remain in the Organization Events page.

You can re-add the user to the PCE as a local or external user with the same name and email address or username.

To edit a local user

In Users and Groups, find the user you want to edit. change the user's name and save.

You cannot edit a user's email address. You must remove and re-add the user with the new email address.

Changing a local user's name only changes it in the RBAC Roles and Users and Groups pages. The name is not changed in the user's profile or on the RBAC User Activity pages.



NOTE

Local and external users can change their names when they create their accounts or from their profiles.

To convert a local user

In Users and Groups, select the name of the user and click **Convert**.

You can convert a local user to an external user so that your corporate IdP manages the user authentication credentials. When you convert a user to an external user, the user retains all their role memberships.

To invite a local user

In Users and Groups, select the name of the user and click **Re-Invite**.

You can send a new email to users to create their account when they haven't responded to the original email. An invitation remains valid for 7 days.

To lock or unlock a local user

In Users and Groups, select the name of the user and click **Lock**.

Local users are locked out of their accounts when they fail to log in after five consecutive failures.

Locked users retain all their granted access to scopes in the PCE; however, they cannot log into the PCE. When an account is locked, the PCE web console reports that the username or password is invalid even when a user enters valid credentials. The user's account resets after 15 minutes and does not require an Illumio administrator to unlock it.

Add or Remove an External User

Using RBAC, you can control access to Illumio Core for users who a corporate IdP externally authenticates. Your corporate IdP manages authentication so that when these users log into the PCE, they are redirected to the IdP to authenticate. The PCE does not validate their usernames or passwords.

Using RBAC, you control the access external users have to Illumio Core features and functionality. When you add an external user to the PCE, you specify that user's access by assigning the user to Illumio roles and scopes.

To add an external user:

Use the External Users tab to click Add and enter a name, email address, or username.

Whether you enter an email address or username for the user depends on how you have configured your IdP to identify corporate users. The username can contain up to 225 alphanumeric and special characters (. @ / _ % + -). In the PCE, you can have duplicate names for external users, but you cannot have duplicate email addresses or usernames.

When your IdP is configured to identify users by using email addresses, the PCE emails the user at the address you specify an invitation with a link to create their Illumio user account. If your IdP is configured to use usernames, you must provide the user your Illumio PCE web console URL.

Select the role: None, Global Organization Owner, Global Administrator, or Global Read Only.

Users without a role (None) can still log into the PCE to view resources when Read Only User access to the PCE is enabled. You can enable and disable Read Only User access in the Global Read Only role.

You can change a user's role membership after adding them by going to the user's details page or from a role details page.

To change an external user's name, click **Edit User** from the user's details page. You cannot edit the email address or username for an external user. You must remove and re-add the user with the new information.

To remove an external user:

Use the External Users tab to select the user you want to remove and click **Remove**.

Removing an external user removes the user from the External Users tab and all the user's RBAC role memberships. Your corporate IdP still manages the user's authentication.

If Read Only User access to the PCE is enabled for your organization, the user can still log into the PCE and view resources after you remove the user.

When you remove an external user while the user is online, the PCE logs the user out for their next action after being removed.

Add or Remove an External Group

The RBAC feature in Illumio Core integrates with the user groups maintained in your corporate IdP so you can manage user authentication centrally for the Illumio Core. In the PCE, you assign roles and scopes to the groups managed by your IdP to control the access that Illumio users have to their Illumio managed resources.

With user groups, you can authorize your teams to manage the security for the applications they manage without waiting for a centralized security team to delegate authority.

When a user who is a member of an external group logs into the PCE, the corporate IdP authenticates the user and returns the list of groups the user belongs to. For each of those groups, the PCE determines what roles and scopes are assigned to the group. The user is granted access to the resources associated with the roles and scopes.

A user can belong to multiple external groups. When a user belongs to multiple groups, the user is granted access to Illumio resources based on the most permissive role and scopes defined for each group.

To add an external group:

- Use the External Users tab to add an external group
- In the External Group field, enter the group name as it's configured in your IdP.
In your IdP, the group is designated by a simple group name (for example, "Sales") or by a group name in distinguished name (DN) format (for example, "CN=Sales, OU=West").

To verify the correct format to enter the PCE, check the **memberOf** attribute in the SAML assertion from your IdP. The **memberOf** attribute is a multiple-value attribute that contains a list of distinguished names for groups that contain the group.

To change an external group's name, click **Edit Group** from the group's details page. You cannot edit the External Group field. You must remove and re-add the group with the new information.

To remove an external group: Click **Edit Group** from the group's details page to change an external group's name.

Use the External Users tab to remove an external group, select it, and click **Remove**.

Removing an external group from the PCE removes all the group's RBAC role memberships and, therefore, removes access for all the group members. Your corporate IdP still manages user authentication for the group members.

If Read Only User access to the PCE is enabled, the external group members can still log into the PCE and view resources after you remove the group.

Change Users and Groups Added to Roles

When you change the membership for a role, the affected users must log out and log in to access the new capabilities.

When you revoke a user's access to scopes or global objects while the user is online, the PCE logs them out of the next action they can take after revoking their access.

- In Global Roles, click the name of the role you want to assign users or groups to
- To remove a user or group from the role, select it and click **Remove**.
- To add a user or group to a role, click **Add**.
- From the first drop-down list, select what (Any Principal Type, Local Users, External Users, or External Groups) you want to add to the role.
Selecting what you want to add filters the second list to display only those types of users or user groups.
- Select the user or group to add to the role.
- Click **Grant Access**.

Alternatively, you can select users or groups to add to roles from the **Role-Based Access > User and Groups** details pages, and select **Add** and follow the steps in the Access Wizard.

View User Activity

You can access a historical audit trail of user activity through the following reports:

- **User Activity:** Go to **Role-Based Access > User Activity**
 - Displays session details for each user, including their status, email address, and when they were last logged in.
 - Click a user to view all the roles and scopes that are assigned to that user.

The User Activity page also displays users who were removed and are designated as offline.

**NOTE**

The names that appear in the User Activity pages can be different from the **Role-Based Access > Users and Groups** pages when users edit their profiles or an Organization Owner changes names in the **Role-Based Access > Users and Groups** pages.

- **Organization Events:** Go to **Troubleshooting > Organization Events**

The Organization Events page provides an ongoing log of all events in the PCE. For example, it captures actions, such as users logging in and logging out and failed log-in attempts, when a system object is created, modified, deleted, or provisioned, and when a workload is paired or unpaired.

Each of these events has a severity level and are exportable in JSON format. You can narrow the search for many events by event type, severity, or time filters.

Change Your Profile Settings

If you want to change the password you use to access the PCE web console, you can do so from your User menu located at the top right corner of the PCE web console.

To change your password

- In My Profile, click on **Change Password**.
- Enter your current password and then your new password twice.
- Click **Change Password**.

Color Vision Deficiency Mode

Users with color vision deficiency (Deuteranopia, Protanopia, or Tritanopia) can select Color Vision Deficiency mode, making it easier for them to distinguish between blocked and allowed traffic lines in the Illumination map. This mode can be enabled on a per-user basis.

The color vision deficiency mode is disabled by default.

To enable color vision deficiency mode

- In My Profile, Accessibility section, select the **Color Vision Deficiency** button.
-

**NOTE**

To restore the default setting, select the **Normal Vision** button.

Role-based Access for Application Owners

The enhancements made to the Role-based Access Control (RBAC) framework in the Illumio Core 20.1.0 release enable organizations to address several use cases related to application owners.

Overview

These enhancements include:

- Delegation of policy writing to downstream application teams.
- Assigning read-only privileges to application owners. Those users get read access based on the assigned scopes.
- Flexibility to assign read/write or read-only privileges to the same user for different applications. For example, the same user can have read/write privileges in a staging environment but has read-only privileges in a production environment.

Although the RBAC controls in releases prior to Illumio Core 20.1.0 restricted "writes" based on user role and scope, users had visibility into all aspects of the PCE irrespective of the role. With these new RBAC controls, application owners get visibility into the applications within their assigned scopes, specifically the PCE information relevant to their applications. Depending on the user's role, application owners can:

- Read/write policies to manage application segmentation.
- View inbound and outbound traffic flows as well as use Explorer.
- View labeled objects used in policies.
- View details of global objects such as, IP Lists and Services used by their applications.

Benefits

The key benefits of the RBAC framework in the PCE are as follows:

- Provides a label based approach to define user permissions.
- Provides roles based on application owner personas to manage application segmentation.
- Provides a building block based approach to stack permissions for users.
- Offers flexibility to delegate read/write and read-only privileges to same user for different sets of applications.
- Enables enforcement of least privilege by hiding information outside of an application scope.
- Allows application owners to effectively manage segmentation for their applications.

Updates to Roles

Illumio Core provides two types of user roles - Global and Scoped. It also provides the ability to stack multiple roles for the same user. A PCE owner can assign multiple roles to the same user. The resulting set of permissions is the summation of all permissions included with each stacked. With these updates:

- Existing scoped roles were enhanced to restrict reads by scope.
- The new scope-based *read-only* role limits read access by labels.
- Scoped users get limited visibility into objects 1-hop away (this applies to Explorer, App Group Maps, Rule Search, and Traffic).
- Global read-only is disabled by default for new PCE installations.
- PCE performance and scale enhanced to support concurrently active users.

Global Roles

Global roles allow the user to view everything and perform operations globally. The four Global roles are :

- Global Organization Owner: Allowed to manage all aspects of the PCE, including user management.
- Global Administrator: Allowed to manage most aspects of the PCE, except user management.

- Global Viewer: Allowed to view everything within the PCE in a read-only capacity. This role was previously called "Global Read-only".
- Global Policy Object Provisioner: Allowed to provision global objects that require provisioning, such as Services and Label Groups.

Scoped Roles

The Scoped roles are defined using labels. The permissions included with the assigned role apply only to the assigned scope, where the scope is defined using a combination of as many label types as you have defined (and with only one label value per type). To provide permissions to different applications for a user, each of the application scopes has to be added to the same user.

All the Scoped roles have been enhanced to restrict reads and writes by Scope. The Scoped roles are :

- Ruleset Viewer: A new scope-based read-only role. A user with this role has read-only permissions within the assigned scope. The user can view policy, application groups, incoming and outgoing traffic, and labeled objects, such as workloads, within the assigned scope.
- Ruleset Manager (Limited or Full): An existing scope-based read/write role. A user with this role can read/write policy within the assigned scope. The user can also view application groups, incoming and outgoing traffic, and labeled objects within the assigned scope.
- Ruleset Provisioner: This role allows a user to provision changes to scoped objects, provided the objects are inside the user's assigned scope. A user with this role can also provision changes to policies within the assigned scope. The user can also view application groups, incoming and outgoing traffic, and labeled objects within the assigned scope.
- Workload Manager: This role allows a user to perform workload-specific operations such as pairing, unpairing, label assignment, and changing policy state. A user with this role cannot view policies and traffic and cannot provision changes.

Configuration

The Global Read-only user setting should be disabled to enforce scoped reads for users with scoped roles. To disable this setting, make sure that the *Read Only User* setting under **Access Management > Global Roles > Global Viewer** is set to **Off**.



NOTE

In PCE versions 20.1.0 and higher, the Global Read-only user setting is disabled by default.

On PCE versions upgraded from prior releases, this setting must be manually turned **off** for users to have reads restricted by scope. If this setting is set **On**, users with scoped roles will get global visibility by default.

Figure 1. Global Viewer Setup

The screenshot displays the 'Global Roles' configuration page. At the top, the breadcrumb navigation is 'Home > Access > Global Roles'. The page title is 'Global Viewer'. Below the title, there are several configuration options: 'Scope' is set to 'All', 'Role' is 'Global Viewer', 'Granted Access' has a 'Show' button, and 'Read Only User' is a toggle switch currently set to 'Off' with a 'Turn On' button. Below these options are 'Add' and 'Remove' buttons. A 'Refresh' button is located on the right side of the table. The table, titled 'Principals and Roles', shows a list of users assigned to the 'Global Viewer' role. The table has columns for 'Type', 'Name', 'Email/Username/Group Name', and 'Roles'. The first row shows a user named 'Aditeya' with email 'aditeya.pandey@illumio.com'. The second row shows a user named 'asdfsdf' with email 'greg.konush+303@illumio.com'. The third row shows a user named 'asdfsdf' with email 'greg.konush+44@illumio.com'. The fourth row shows a user named 'asdfsdf' with email 'sadsfsdf@illumio.com'. The fifth row shows a user named 'asdfsdfdsaf' with email 'asdfsdf@illumio.com'. The table indicates that there are 1 to 50 of 90 total entries.

Type	Name	Email/Username/Group Name	Roles
<input type="checkbox"/>	Aditeya	aditeya.pandey@illumio.com	Global Viewer
<input type="checkbox"/>	asdfsdf	greg.konush+303@illumio.com	Global Viewer
<input type="checkbox"/>	asdfsdf	greg.konush+44@illumio.com	Global Viewer
<input type="checkbox"/>	asdfsdf	sadsfsdf@illumio.com	Global Viewer
<input type="checkbox"/>	asdfsdfdsaf	asdfsdf@illumio.com	Global Viewer

Manage Global Owners

Facet Searches for Scoped Roles

The Scopes page now features a search bar with auto-complete and facets. This is restricted to users with a Global Organization Owner role. To use this feature, navigate to **Access Management > Scopes**. The search bar allows Organization Owners to query a list of users by a user's role. They can search by labels and label groups to get a list of users with the selected label(s) in their assigned scope(s), or for users with no labels assigned. They can also select Principals to search for a specific user.

Ruleset Viewer

Ruleset Viewer is a new scope-based read-only role. When assigned, a user get read-only visibility into the assigned application scope. As a Ruleset Viewer, you can view all the Rulesets and Rules within the assigned scope. However, you cannot edit any of the rules or create new rules. You can use Policy Generator to preview the policies that will be generated. However, you are not allowed to save policy after previewing it using Policy Generator.

A Ruleset Viewer is allowed to view everything that a Ruleset Manager with the same scope is allowed to view. This includes traffic flows, labeled objects, application groups, global objects, and so on. The only difference between a Ruleset Manager and a Ruleset Viewer is the absence of write privileges for a Ruleset Viewer. A Ruleset Manager is allowed to create and update policy within the application scope.

Scoped Roles and Permissions

The following table provides a summary of the different permissions provided with each of the scoped roles.

- (R) = Restricted based on scope
- (T) = Restricted based on resource type
- --- = Not applicable

Page	Ruleset Viewer (Scoped Read-Only)	Ruleset Manager	Ruleset Provisioner	Workload Manager	Application Owner (Combined Permissions)
Traffic - Illumination, App Group, Explorer					
Illumination Location Map	---	---	---	---	---
App Group Policy Map	Read (R)	Read (R)	Read (R)	---	Read (R)
App Group Vulnerability Map	Read (R)	Read (R)	Read (R)	---	Read (R)
App Group List	Read (R)	Read (R)	Read (R)		Read (R)
Explorer	Read (R)	Read (R)	Read (R)	---	Read (R)
Blocked Traffic	Read (R)	Read (R)	Read (R)	---	Read (R)
Policy					
Policy Generator	Read (R)	Read+Write (R)	Read (R)	---	Read+Write (R)
Rulesets and Rules	Read (R)	Read+Write (R)	Read (R)	---	Read+Write (R)
Rule Search	Read (R)	Read (R)	Read (R)	---	Read (R)
Policy Check	Read (R)	Read (R)	Read (R)	---	Read (R)
Provisioning Draft Changes	Read (R)	Read (R)	Read+Write (R)	---	Read+Write (R)
Policy Versions	Read (R)	Read (R)	Read (R)	---	Read (R)
Provisioning Status	Read (R)	Read (R)	Read (R)	---	Read (R)
Labeled Objects					
Workloads	Read (R)	Read (R)	Read (R)	Read+Write (R)	Read+Write (R)
Container Workloads	Read (R)	Read (R)	Read (R)	Read (R)	Read (R)
Virtual Enforcement Nodes	Read (R)	Read (R)	Read (R)	Read+Write (R)	Read+Write (R)
Pairing Profiles	---	---	---	Read+Write (R)	Read+Write (R)
Virtual Services	Read (R)	Read (R)	Read (R)	Read (R)	Read (R)
Virtual Servers	Read	Read	Read	Read	Read

Page	Ruleset Viewer (Scoped Read-Only)	Ruleset Manager	Ruleset Provisioner	Workload Manager	Application Owner (Combined Permissions)
Global Policy Objects					
Services	Read	Read	Read	Read	Read
IP Lists	Read	Read	Read	Read	Read
User Groups	Read	Read	Read	Read	Read
Labels	Read	Read	Read	Read	Read
Label Groups	Read	Read	Read	Read	Read
Settings					
Segmentation Templates	---	---	---	---	---
Role-Based Access Global Roles	---	---	---	---	---
Role-Based Access Scoped Roles	---	---	---	---	---
Role-Based Access Users and Groups	---	---	---	---	---
Role-Based Access User Activity	---	---	---	---	---
Load Balancers	---	---	---	---	---
Container Clusters	---	---	---	---	---
Bi-directional Routing Networks	---	---	---	---	---
Event Settings	---	---	---	---	---
Setting Security	---	---	---	---	---
Setting Single Sign-On	---	---	---	---	---
Setting Password Policy	---	---	---	---	---
Setting Offline Timers	---	---	---	---	---

Page	Ruleset Viewer (Scoped Read-Only)	Ruleset Manager	Ruleset Provisioner	Workload Manager	Application Owner (Combined Permissions)
VEN Library	---	---	---	Read	Read
My Profile	Read+Write	Read+Write	Read+Write	Read+Write	Read+Write
My API Keys	Read+Write	Read+Write	Read+Write	Read+Write	Read+Write
Other					
Support Reports	---	---	---	Read+Write (R)	Read+Write (R)
Events	---	---	---	---	---
Reports	Read (R, T)	Read (R, T)	Read (R, T)	Read (R, T)	Read (R)
Support	Read	Read	Read	Read	Read
PCE Health	---	---	---	---	---
Product Version	Read	Read	Read	Read	Read
Help	Read	Read	Read	Read	Read
Terms	Read	Read	Read	Read	Read
Privacy	Read	Read	Read	Read	Read
Patents	Read	Read	Read	Read	Read
About Illumio	Read	Read	Read	Read	Read

Scoped Users and PCE

Each scoped role has different permissions that impact an application owner's visibility into various aspects of the PCE. Application owners can be assigned scoped roles that come with different permissions.

Navigation Menus

The PCE navigation menu options vary based on the user's role. The navigation menu options available for Application Owner are limited. For example, a user is logged in as a Global Organization Owner has more (complete) menu options displayed than when a user logs in as a scoped user (Application Owner).

The following table provides the menu options available for different scoped users.

- Y = Yes (menu option is displayed for the user)
- N/A = Not applicable (menu option is hidden from the user)

Page	Ruleset Viewer	Ruleset Manager	Ruleset Provisioner	Workload Manager
Illumination Map	N/A	N/A	N/A	N/A
Role-based Access	N/A	N/A	N/A	N/A
Policy Objects > Segmentation Templates	N/A	N/A	N/A	N/A
Policy Objects > Pairing Profiles	N/A	N/A	N/A	Y
Infrastructure	N/A	N/A	N/A	N/A
Troubleshooting > Events	N/A	N/A	N/A	N/A
Troubleshooting > Support Reports	N/A	N/A	N/A	Y
Settings	N/A	N/A	N/A	See row below
Settings > VEN Library	N/A	N/A	N/A	Y
PCE Health	N/A	N/A	N/A	N/A
App Groups > Map	Y	Y	Y	N/A (App Group Members are visible)
App Groups > List	Y	Y	Y	Y
App Groups > Vulnerability Map	Y	Y	Y	N/A
Explorer	Y	Y	Y	N/A
Policy Generator	Y	Y	Y	N/A
Rulesets and Rules	Y	Y	Y	N/A
Rule Search	Y	Y	Y	N/A
Workload Management > Workloads	Y	Y	Y	Y
Workload Management > Container Workloads	Y	Y	Y	Y
Workload Management > Virtual Enforcement Nodes (Agents)	Y	Y	Y	Y
Provision > Draft Changes	Y	Y	Y	N/A
Provision > Policy Versions	Y	Y	Y	N/A
Policy Objects > IP Lists	Y	Y	Y	Y
Policy Objects > Services	Y	Y	Y	Y
Policy Objects > Labels	Y	Y	Y	Y

Page	Ruleset Viewer	Ruleset Manager	Ruleset Provisioner	Workload Manager
Policy Objects > User Groups	Y	Y	Y	Y
Policy Objects > Label Groups	Y	Y	Y	Y
Policy Objects > Virtual Services	Y	Y	Y	Y
Policy Objects > Virtual Servers	Y	Y	Y	Y
Troubleshooting > Blocked Traffic	Y	Y	Y	N/A
Troubleshooting > Export Reports	Y	Y	Y	Y
Troubleshooting > Policy Check	Y	Y	Y	N/A
Troubleshooting > Product Version	Y	Y	Y	Y
Support	Y	Y	Y	Y
My Profile	Y	Y	Y	Y
My Roles	Y	Y	Y	Y
My API Keys	Y	Y	Y	Y
Help	Y	Y	Y	Y
Terms	Y	Y	Y	Y
Patents	Y	Y	Y	Y
Privacy	Y	Y	Y	Y
About Illumio	Y	Y	Y	Y

Landing Page

The PCE landing page changes dynamically based on the user's role. The Illumination page opens when you log in to your account as an Organization Owner. However, when you log in as a Scoped user, the landing page changes to the App Groups List page where you can see the list of App Groups assigned.

Labeled Objects

The scope of the user filters labeled objects, such as workloads. On the Workloads page, you will only see the list of the workloads within the application scope. You cannot see any workloads that are outside the application scope. This applies to any labeled object, such as workloads, containers, Virtual Services, and Virtual Enforcement Nodes (VENs).

The menu functions and buttons change dynamically to reflect a user's permissions. If logged in as a Ruleset Manager, you cannot manage workloads. So, all the workload-specific operations buttons are disabled. However, you can view the list of workloads within the scope and get details for individual workloads, except for Virtual Servers.

**NOTE**

While Virtual Servers are considered labeled objects, they are visible to all scoped users regardless of object scope.

Facet Searches and Auto-complete

The search bar with auto-complete and facets is scoped for labeled objects and Rulesets. For example, if you search for Application Labels, you can only select the Application Labels under the assigned scope. This applies to other label types such as Environment labels and Location labels. However, Role labels are excluded since Role labels are not part of the user scope. The restriction of visibility by scope applies to facets such as hostname, IP address, etc. The search bar automatically filters the facets to the list of facets in the user's assigned scope.

Global Objects

Scoped users get complete read-only visibility into all global objects. This includes IP Lists, services, labels, label groups, and user groups. However, scoped users cannot create, modify, or provision global objects.

**NOTE**

Only the Global Organization Owner and Global Administrator can create, modify, and provision global objects.

Rulesets and Rules

Scoped users, except Workload Managers, can see rulesets and rules that apply to their applications. A Ruleset Manager can edit the ruleset, whereas the other scoped roles (Ruleset Viewer and Ruleset Provisioner) can view rulesets. A scoped user can see all the rules within the application ruleset.

When label groups are used within the scope of a ruleset, a Ruleset Manager may not be allowed to edit the ruleset and its rules even if there is a scope match between the user's assigned scope and the underlying scope of the ruleset. The user will, however, be able to view the rules within such a ruleset.

In addition, scoped users can also see rules that apply to their applications. For example, scoped users can view rules written by other applications that apply to their application. To see those rules, click **Rule Search** from the navigation menu.

On the Rule Search page, a scoped user can see all the rules that apply to their application. This includes rules for incoming and outgoing traffic flows. The rules highlighted in the screenshot below are the outbound rules which are for your application. The application owner provides visibility to all the rules that are applied to your application.

Policy Generator and Explorer

With Policy Generator, scoped users can generate policies only for their applications. Only Ruleset Managers can generate policies with Policy Generator. Ruleset Viewers can preview Policy Generator without the ability to save the policy.

Explorer views are also filtered for scoped users. To use Explorer, one of the endpoints has to be within the scoped user's application. The same applies to Blocked Traffic.

My Roles

"My Roles" is a new feature that allows you to view the list of assigned permissions (roles).

Configure Access Restrictions and Trusted Proxy IPs

To employ automation for managing the PCE environment, you can use API Keys created by an admin user and automate PCE management tasks. This section tells how you can restrict the use of API keys and the PCE web interface by IP address. In this way, you can block API requests and users coming in from non-allowed IP addresses.

Configure Access Restrictions

This section tells how to use the Illumio web console UI to configure access restrictions. You can also configure access restrictions programmatically using the REST API calls described in "Access Restrictions and Trusted Proxy IPs" in the REST API Developer Guide.

- You must have the global Org Owner role to view or change access restrictions.
- A maximum of 50 access restrictions can be defined.

To configure access restrictions:

1. Log in to the PCE web console as a user with the Global Org Owner role.
2. Open the menu and choose **Access Management - Access Restrictions**.
The Access Restriction page opens with a list that shows which IP addresses are allowed and where the restrictions have been applied.
3. To add a new restriction, click **Add**.
The Add Access Restriction page opens.
Provide the required attributes:
 - Provide a name.
 - In **Restriction Applies To**, choose User Session, API Key, or Both. Access restrictions can be applied to these different types of user authentication.
 - List a maximum of eight IPv4 addresses or CIDR blocks.
4. Click **Edit** to edit the restriction.
5. View the access restrictions applied to local users. The default is blank, no restrictions.
6. You can assign access restrictions to local and external users or user groups. To add a local user:
 - a. Click **Add**.
 - b. In **Access Restriction**, choose the type of access restriction.
 - c. Click **Add**.
7. View the local user's detail page. To modify the user settings, click **Edit User**.
8. Use the Edit User dialog to apply restrictions.

If an Org Owner assigns an access restriction to any Org Owner, a warning is shown, because this can result in the Org Owner user losing access to the PCE.

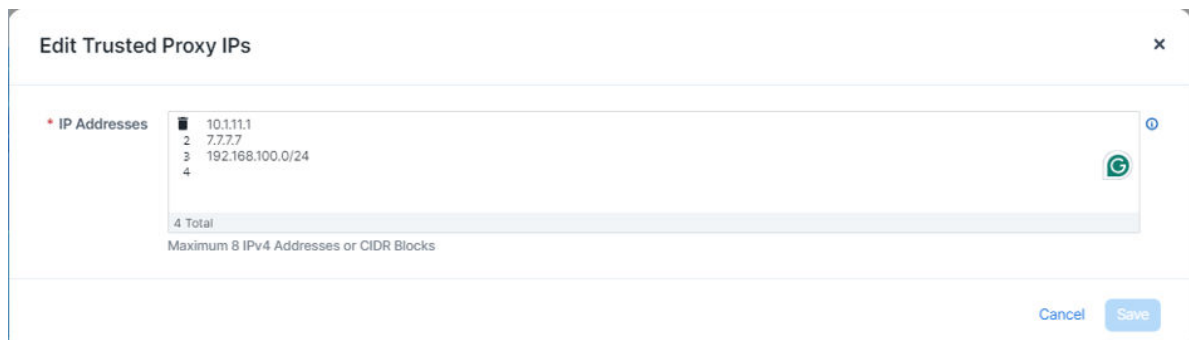
9. View the list of API keys in the API Keys page and the Event page.

Configure Trusted Proxy IPs

This section tells how to use the Illumio web console UI to configure trusted proxy IPs. You can also configure trusted proxy IPs programmatically using the REST API calls as described in "Access Restrictions and Trusted Proxy IPs" in the REST API Developer Guide.

When a client is connected to the PCE's haproxy server, this connection can traverse one or more load balancers or proxies. Therefore, the source IP address of a client connection to haproxy might not be the actual public IP address of the client.

1. Log in to the PCE web console as a user with the Global Org Owner role.
2. Select **Settings > Trusted Proxy**.
3. In the Trusted Proxy IPs page, click **Edit**.
4. A list of trusted proxy IPs is displayed. Proxy configuration can have upto 8 Trusted Proxy IPs.
5. To remove any of the proxies from the list, select the checkbox in front of the proxy address and click **Remove**.
6. To edit Trusted Proxy IPs, click **Edit**.
7. In the Edit Trusted Proxy IPs dialog box, you can add a proxy IP address to the list, or delete any of the existing addresses by hovering over the number in front of the address and then clicking the Trash Can icon that shows up.



Edit Trusted Proxy IPs

* IP Addresses

1	10.1.1.1
2	7.7.7.7
3	192.168.100.0/24
4	

4 Total

Maximum 8 IPv4 Addresses or CIDR Blocks

Cancel Save

8. Once you have added or deleted the proxy addresses for your needs, click **Save**.

Manage API Keys

You can add and edit API keys using the PCE console;

Creating API Keys

1. In the Web console, type "API keys" in the Search field.
2. In the API Keys page, click **Add**.
3. In the "Create API Key" pop-up dialog, add the
 - a. Key Name
 - b. Description of the key
 - c. Org ID
4. Click Create.
5. The confirmation dialog appears to show the data for the created API key.

API Key Created

This is the only time these credentials will be available to download. You can manage and recreate these credentials at any time.

Name	Pubs-key
Description	Pubs group key
Key ID	13b0b856607c48a49
Authentication Username	api_13b0b856607c48a49
Secret	1b04e723f8e0ada762daa00980bbbb987916e215a5b5baf4139652d0b903274e

Close

Download Credentials

- To download the credentials, click on **Download Credentials**.
You can download the credentials only after the key is created. You can, however, manage the credentials at any time.
- The credentials will be downloaded in the default download directory on your hard drive, with the name API-Key-<your-key-name>. The format of the credential is a TXT file.

```
{ "key_id": "13b0b856607c48a49", "auth_username": "api_13b0b856607c48a49",  
  "secret": "1b04e723f8e0ada762daa00980bbbb987916e215a5b5baf4139652d0b903274e" }
```

Editing Expiration of API Keys

To edit expiration of the Service account API keys using the PCE console:

- Select **Settings > API Keys**.
- On the API Key Settings page, click **Edit**.
- By default, API Key for Service Account expires in:
Select from the dropdown list: **Never expires**, **1 day**, **30 days**, **60 days**, or **90 days**.
If you change this setting, expiration of the existing API keys will not be impacted.
- Keep expired API keys for:
Select from the dropdown list: **1 day**, **30 days**, **60 days**, **90 days**, or **custom**.

Password Policy Configuration

The PCE enforces password policies that only a Global Organization Owner can configure. In the PCE web console, you set password policies that the PCE enforces, such as password length, composition (required number and types of characters), and password expiration, re-use, and history.

About Password Policy for the PCE

You need to be a Global Organization Owner to view the Password Policy feature under the Settings > Authentication menu options.

Prior to Illumio Core 18.2.0, a Global Organization Owner set the password in the PCE by using the PCE runtime script. The settings in the PCE runtime script are the same as before Illumio Core 18.2.0, except that the password length can now be set to a maximum of 64 characters.

**NOTE**

The Password Policy feature is not applicable for organizations using SAML authentication.

**NOTE**

Permission to edit this setting is dependent on your role.

Password Requirements

The password requirements you set are displayed to users when they are required to change their passwords. You can set the minimum character length, ranging from a minimum of 8 characters to a maximum of 64 characters. The default length is 8 characters.

A Global Organization Owner should configure passwords based on the following categories:

- Uppercase English letters
- Lowercase English letters
- Numbers 0 through 9 inclusive
- Any of the following special characters: ! @ # \$ % ^ & * < > ? .

**WARNING**

Any other special characters are neither tested nor supported.

You have to select at least three of the above categories. The default password requirement is one number, one uppercase character, and one lowercase character. You can set the password to use either one or two characters from each category.

Password Expiration and Reuse

You can set the password expiration range from 1 day to 999 days. The default setting for password expiration is “Never.”

You can set the password reuse history from 1 to 24 passwords before a user can reuse the old password. The default setting is five password changes before reuse of the password is allowed.

**NOTE**

The number of password changes before password reuse is allowed is the value you enter + 1 (the current password). For example, when you specify 3, the number of passwords before reuse is allowed is 4.

You can also set the similarity of a password by not allowing a user to change their password unless it changes from a minimum of 1 to a maximum of 4 characters and positions from their current password.

Allowable password reuse and password history can be set to from 1 to 24 passwords before reuse is allowed. The default setting for password reuse is five password changes before reuse is permitted.

Caveats

- When a Global Organization Owner increases the required minimum password length policy or increases the password complexity requirements and enables the password expiration (1-999 days), all the existing users must reset their passwords based on the new policy.
- When a Global Organization Owner configures the password to never expire, all users who were migrated from an older release to 18.2.0 must reset their passwords when they next log in.

Change Password Policy Settings

1. From the PCE web console menu, choose **Access > Authentication**.
2. In the Authentication Settings screen, choose the Authentication Method to authenticate users for accessing the PCE:
 LOCAL (IN USE) : User will sign in to the PCE only with a local credential provided by the user's organization password policy.
 SAML (IN USE) : SAML users can also authenticate to the PCE using local credentials.
 LDAP: LDAP user can also authenticate to the PCE using local credentials>
3. Once you decide which option to take, click on the **Configure** button.
4. Depending on the authentication method, these are the available options:
 Choose option LOCAL, SAML, or LDAP:

LOCAL (in use)**Password requirements**

Min lengths	8 characters
Character categories	A-Z (required), a-z (required), 0-9 (required)
Min characters per category	1

LOCAL (in use)**Password expiration and reuse**

Expiration	Never
Reuse history	1 password changes
Similarity	1 character and position from the current password

Session timeout

The session expiration timeout values must be set accordingly to balance security and usability so that your users can comfortably complete operations within the PCE web console without their session frequently expiring. The timeout value is dependent on how critical the application and its data are. For example, you might set the timeout to 3-5 minutes for high-value applications and 15-30 minutes for low-risk applications.

The changed session timeout value applies to new browser sessions. Existing browser sessions are not affected when the session timeout value is changed.

The PCE Org owner can go to **Access > Authentication > Local** to configure Session Timeout. This PCE session timeout is applicable to any user belonging to the same organization, regardless whether they are local or external users.

Timeout	30 minutes
---------	------------

SAML (in use)**Information from Identity provider**

SAML Identity provider certificate

```
-----BEGIN CERTIFICATE----- MIICpDC-
CAYwCCQD05WZzgX RugDANBgkqhkiG9w0BAQsFADAUMRIwEAYDVQQD-
DA1sb2NhbgHvc 3QwHhcNMTgxMTE0MjAyNmM2WhcNMjgxMTE0Mj-
jAyNmM2WjAUMRIw EAYDVQQDDA1sb2NhbgHvc3QwggEiMA0GCSqGSIb3DQEBB-
QUAA4I BDwAwggEKaoIBAQDXs/OhH90IPQ8qBrUMqzQZb5MI72fu+Ay0s
P8gI1v8RiUqSl+WJNo8s9L8GNI9hnQT+OXg99PNmoE41xiAlnx
qx8T78Qxb9zX3uc4hec+9bMSF7iieUiFXWQQRiUVM3g8TWI6B5g
Uapt0vZcxNok2eNhiFvVTLgPzB06vb2/yU68ilwQ8wz/MGO00Un/ 1Rw3LORy-
nEAluMeT6terWtX8JQGbvclqYddnXD86Y5MOP1AXU+ 1w1w1JfxD0uKiuOHJv-
NYfJjkisEbDis9b0/E00SyayVA7ABELaw QTfeWM6xLrNhZCTGeQiKb4XHMBgeliA-
loEvNDDofKbLDQrWUyIf7 TAgMBAAEwDQYJKoZIhvcNAQELBQADggEBANlhqsZs-
FUng7kc+B5a vMmOXbCNjMsaASBULsX+akexhyJdMZUxmN6wfljZ3F0wxvFuhe-
Ta ZpkplUtC+2E9YlxY//FxOX/YyvNT/xfOBzqZ9SCsNxpCBsSRK5X4
DS+2jGQuz3fwbJDxTXP4sKNUZ/E9Z+dC9Npdq7xtcXr7pWhI2qe
M08E9LdvfWLcsqq8Z0VtxyHYZYh8KN0Q6ObfK1sPC4QZ/292B
xm2ckxsWDTyONV8ytLQKwp93exxqmzpbz6qi23y0B4u4af+/SW9 ukjzD/
atP34bY1YjeLBCsKEgylndTVgypAZSEy46kJ9mAu6t3r4/gEg XTMYQDtrPA= -----END
CERTIFICATE-----
```

Remote login URL	https://hohoho.illumio.com
Logout landing URL	https://hohoho.illumios.com/logout

Information from Identity provider

Authentication method	unspecified
-----------------------	-------------

SAML (in use)	
Force re-authentication	no
Sign SAML request	no
SAML version	2.0
Issuer URL	https://2x2testlab360.ilabs.io:8443/login
NameID format	urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
Assertion consumer URL	https://2x2testlab360.mylabs.io:8443/login/acs/6b5243ef-2305-4ffd-bf81-4fa97fb91a5b
Logout URL	https://2x2testlab360.mylabs.io:8443/login/logout/6b5243ef-2305-4ffd-bf81-4fa97fb91a5b
Timeout	30 minutes

5. LDAP authentication is not active. Click **Turn On** to apply on all the LDAP servers.
6. To create an LDAP server, click on **Create Server**.
To continue with LDAP server configuration, see the "LDAP Authentication" topic.

Authentication

The Illumio PCE supports the use of either SAML SSO or LDAP as an external authentication method. Both SAML SSO and LDAP cannot be used at the same time. When LDAP is turned on, the use of SAML SSO, if already configured, is disabled. Similarly, enabling SAML SSO after LDAP is enabled will disable LDAP authentication.

SAML SSO Authentication

When you use a third-party SAML-based Identity provider (IdP) to manage user authentication in your organization, you can configure that IdP to work with the PCE. By configuring a single sign-on (SSO) IdP in the PCE, you can validate usernames and passwords against your own user management system, rather than having to create additional user passwords managed by the Illumio Core.

Illumio Core currently supports the following SAML-based IdPs:

- Azure AD
- Microsoft Active Directory Federation Services (AD FS)
- Okta
- OneLogin
- Ping Identity



NOTE

You can use other SAML-based IdPs; however, configuring those IdPs is your responsibility as an Illumio customer.

Before you configure SSO in the PCE, you need to configure SSO on your chosen IdP and obtain the required SSO information. After obtaining the IdP SSO information, log into the PCE web console and complete the configuration.

PCE Information Needed to Configure SSO

Before you configure SSO in the PCE, obtain the following information from your IdP:

- x.509 certificate
- Remote Login URL
- Logout Landing URL

The PCE supports the following optional attributes in the SAML response from the IdP:

- User.FirstName - First Name
- User.LastName - Last Name
- User.MemberOf - Member of

Details

User email address is the primary attribute used by the PCE to uniquely identify users.



IMPORTANT

The client browser must have access to both the PCE and the IdP service. The Illumio PCE uses HTTP-redirect binding to transmit SAML messages.

To obtain the SSO information from the PCE:

1. From the PCE web console menu, choose **Access Management > Authentication**.
2. On the Authentication Settings screen, locate the SAML configuration panel and click **Configure**.
3. Use the displayed information (as shown in the example below) while configuring your specific IdP.

Information for Identity Provider

Authentication Method	Unspecified
Force Re-authentication	No
SAML Version	2.0
Issuer	https://c[REDACTED]3/login
NameID Format	urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
Assertion Consumer URL	https://[REDACTED]3/login/acs/a63e[REDACTED]49598e
Logout URL	https://[REDACTED]43/login/logout/a63e[REDACTED]49598e

**NOTE**

Even though the SAML NameID format specifies an emailAddress, the PCE can support any unique identifier such as, userPrincipalName (UPN), common name (CN), or samAccountName as long as the IdP is configured to map to the corresponding unique user identifier.

Signing for SAML Requests

There are four new APIs you can use to sign SAML requests:

- GET /authentication_settings/saml_configs
- GET /authentication_settings/saml_configs/:uuid
- PUT /authentication_settings/saml_configs/:uuid
- POST /authentication_settings/saml_configs/:uuid/pce_signing_cert

These APIs are covered in detail in REST API Developer Guide.

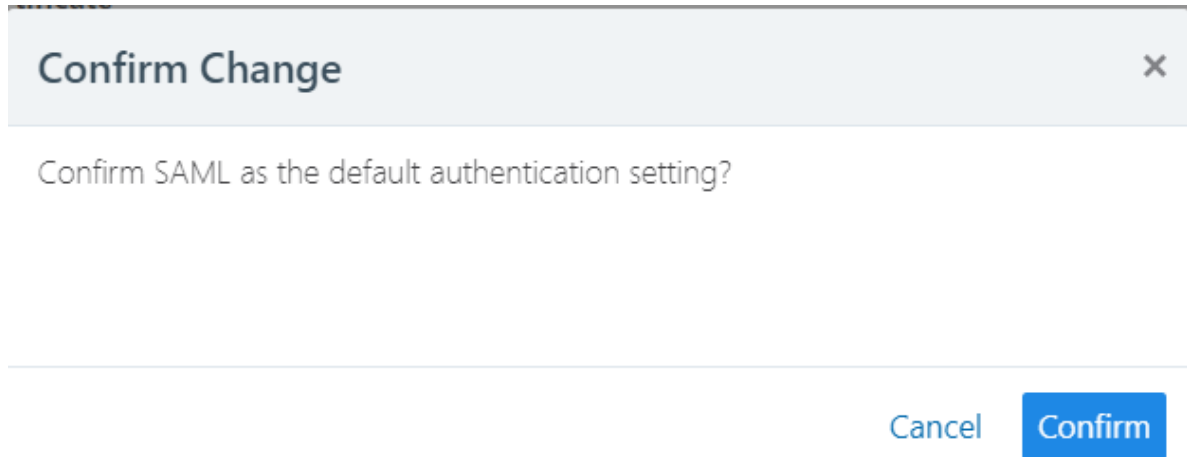
Signing of SAML requests is, however, disabled by default.

To enable SAML request signing:

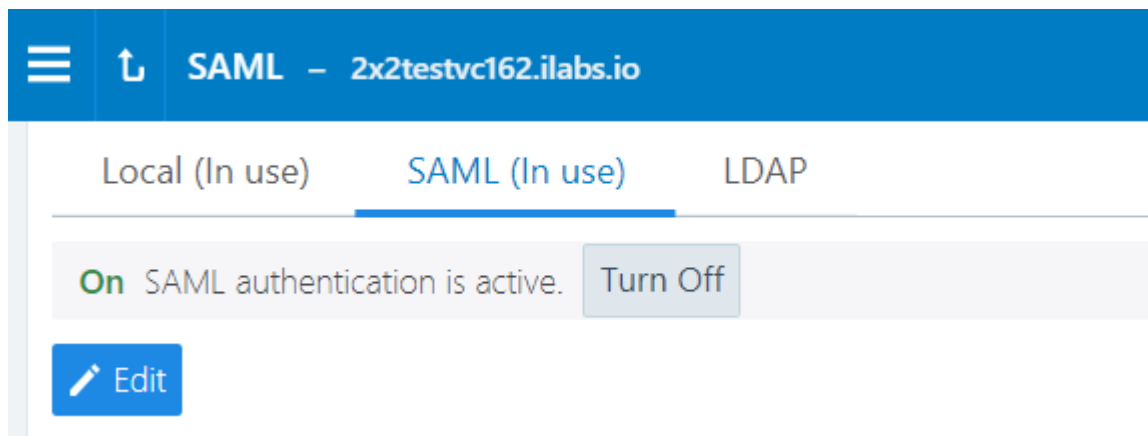
1. Using the Web Console, go to **Access Management > Authentication**.
2. In the *Authentication Setting* screen, select **Configure** button for SAML.
3. In the SAML screen, click **Turn On**.

The screenshot displays the SAML configuration interface. At the top, a blue header bar shows the breadcrumb 'SAML - 2x2testvc162.ilabs.io'. Below the header, there are tabs for 'Local (In use)', 'SAML', and 'LDAP'. A red status bar indicates 'Off SAML authentication is not active. Click Turn On to enable SAML.' with a green 'Turn On' button. An 'Edit' button is also present. The configuration is organized into two main sections: 'Information from Identity Provider' and 'Information for Identity Provider'. The first section includes fields for 'SAML Identity Provider Certificate', 'Remote Login URL', and 'Logout Landing URL'. The second section includes fields for 'Authentication Method' (Unspecified), 'Force Re-authentication' (No), 'Sign SAML Request' (No), 'SAML Version' (2.0), 'Issuer URL' (https://2x2testvc162.ilabs.io:8443/login), 'NameID Format' (urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress), 'Assertion Consumer URL' (https://2x2testvc162.ilabs.io:8443/login/acs/2f762c04-b327-42e8-ae0a-2954366d5ed8), and 'Logout URL' (https://2x2testvc162.ilabs.io:8443/login/logout/2f762c04-b327-42e8-ae0a-2954366d5ed8).

4. In the pop-up screen, click **Confirm**.



The updated SAML screen shows that SAML authentication is active.



If necessary, you can disable it at any time.

Once configured using these steps, the lifetime of the SAML certificate is ten years.

Active Directory Single Sign-on

This section describes how to configure Microsoft Active Directory Federation Services (AD FS) 3.0 for Single Sign-on (SSO) 2.0 authentication with the PCE.

Overview of AD FS SSO Configuration

To enable AD FS for the PCE, the PCE needs three fields returned as claims from:

- NameID
- Surname
- Given Name

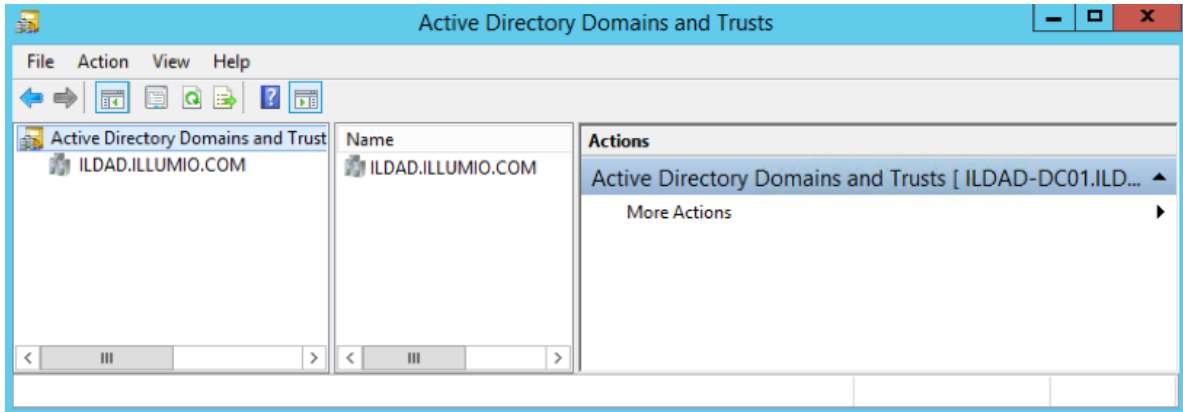
There are two ways for AD FS to produce the NameID claim for an SSO user. The first uses the email field in an Active Directory user account for the NameID.

The second way to return a NameID of an Active Directory user is to use the User Principal Name (UPN). Each user created in Active Directory has an extension to their username that's ADUserName@yourADDomanName. For example, a user named "test" in an Active Directory domain called "testing.com" would have a UPN of test@testing.com.

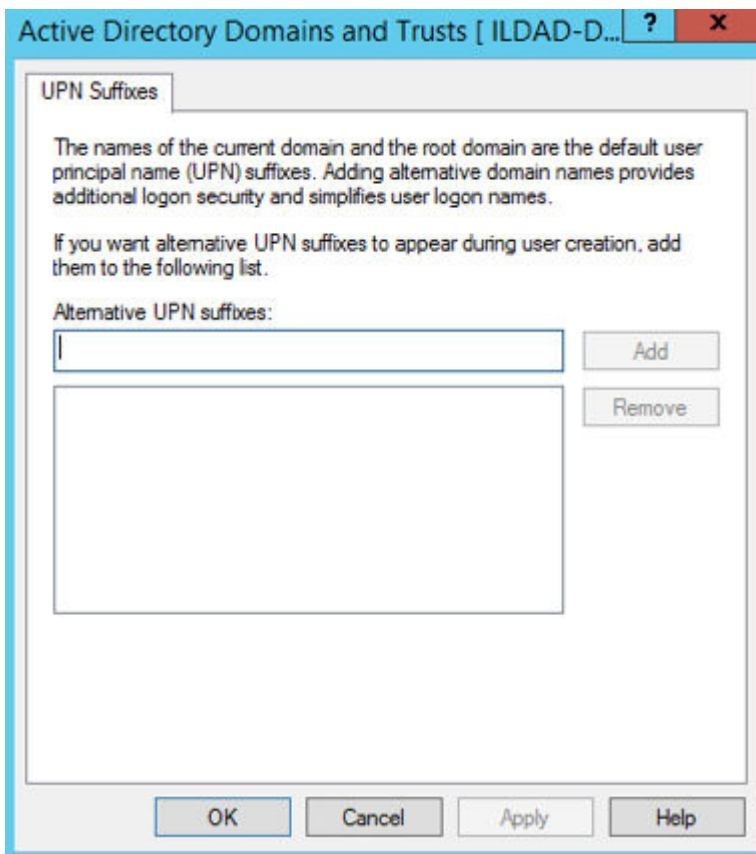
Configure AD Users to Use Different UPN Suffixes

To configure different UPN suffix as the source for NameID:

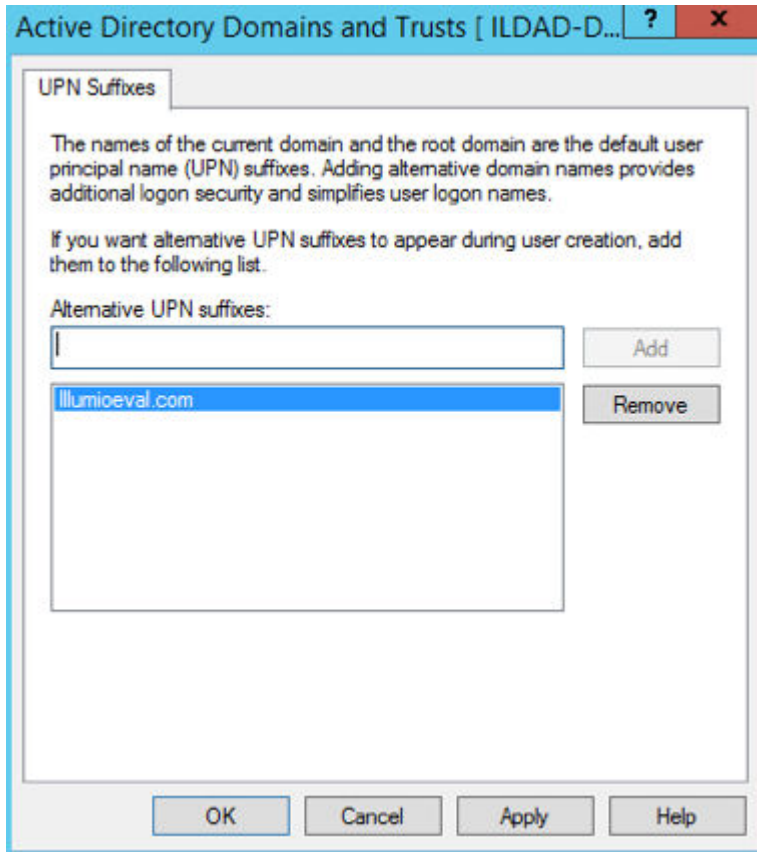
1. Add a UPN suffix. On your system under Server Manager Tools, click **Active Directory Domains and Trusts**.



2. From the left side of the window, right-click Active Directory Domains and Trusts, and select **Properties**. In this dialog, you can create new suffixes for Active Directory usernames.



3. Create a suffix that matches the external namespace you'll be using and click **Add**.



You can now assign an Active Directory user your custom UPN for the SAML response.

4. You can add multiple UPNs if needed. As shown below, you can select the UPN created in the previous steps.

The screenshot shows the 'test Properties' dialog box with the 'Account' tab selected. The 'User logon name' is 'test' and the domain is '@ILDAD.ILLUMIO.COM'. The 'User logon name (pre-Windows 2000)' is 'ILDAD\'. The 'Account options' section shows 'Password never expires' checked. The 'Account expires' section shows 'Never' selected.

Your UPN configuration is set up and you can begin configuring AD FS for SSO with the PCE.

Initial AD FS SSO Configuration

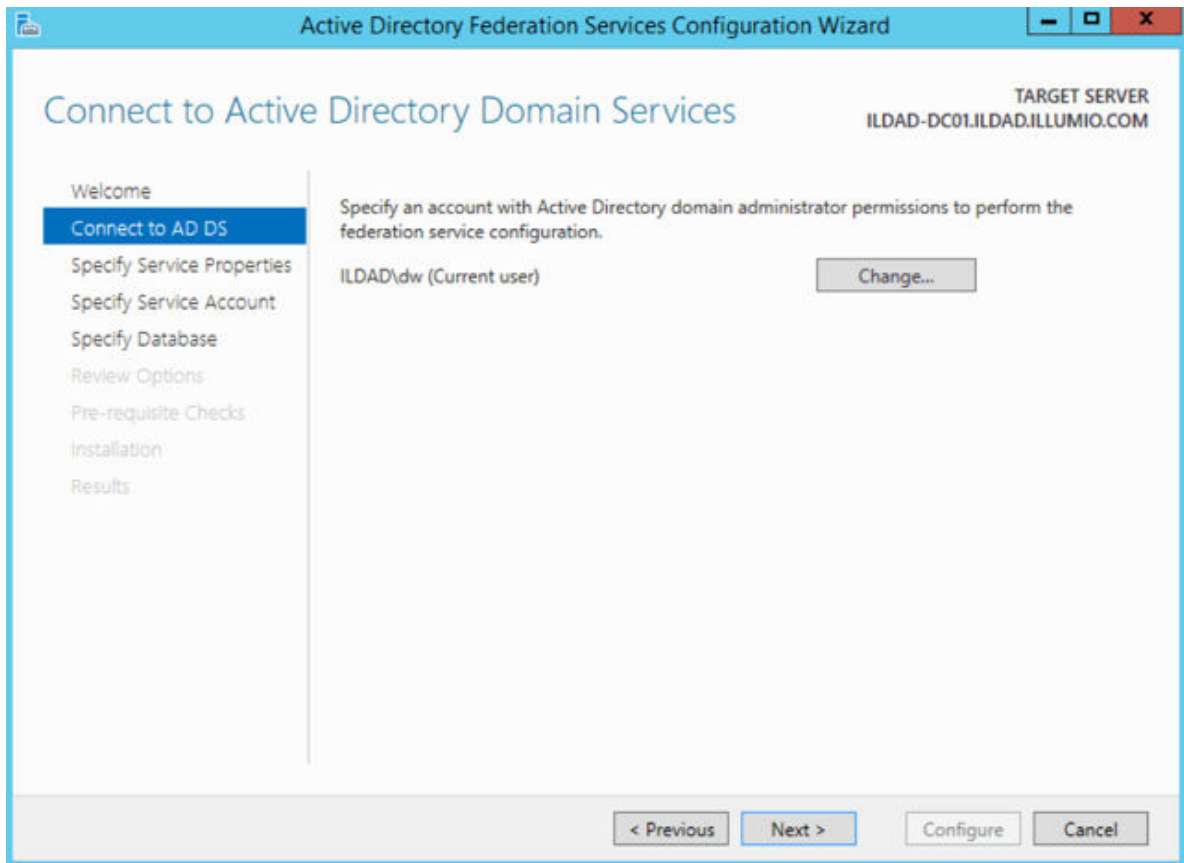
This task explains how to perform the initial configuration of AD FS to be your SSO IdP for Illumio Core.

To configure AD FS:

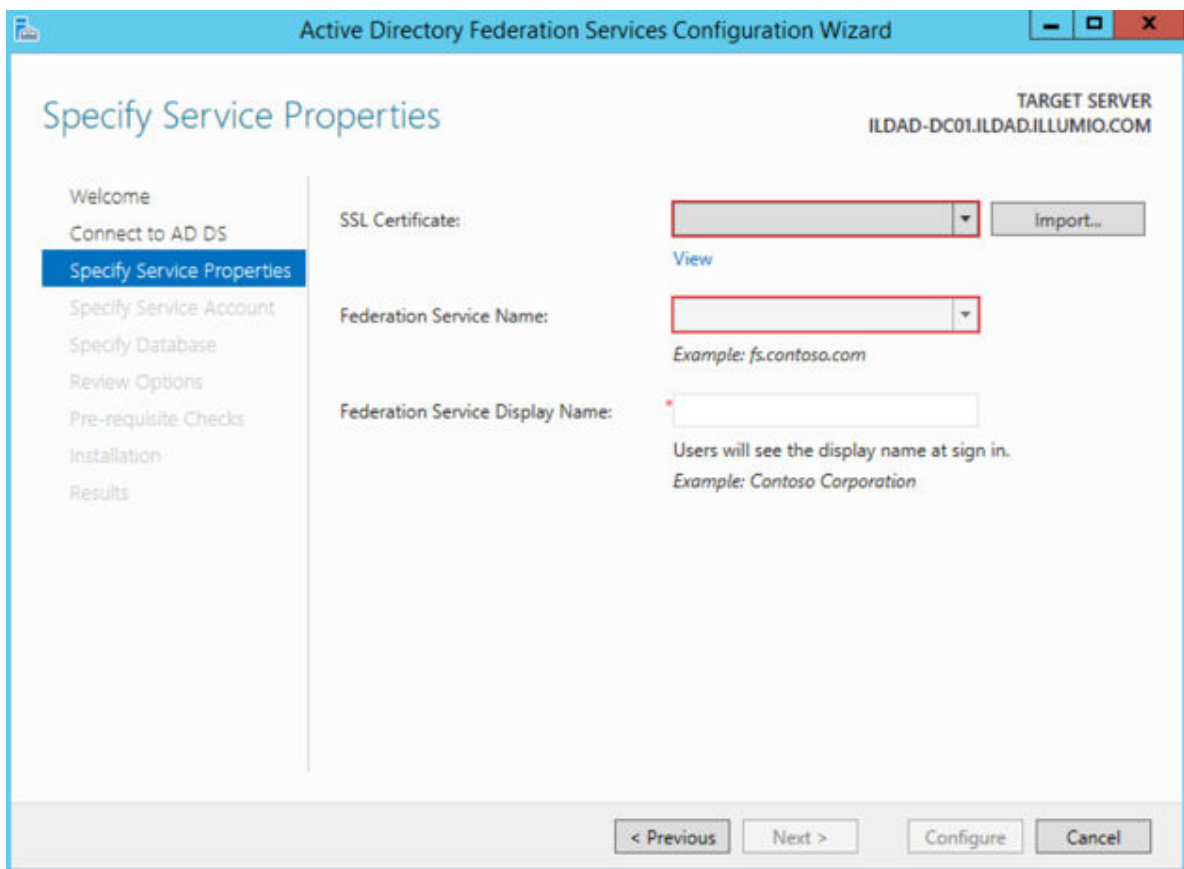
1. Open Microsoft Server Manager and click the notification icon.



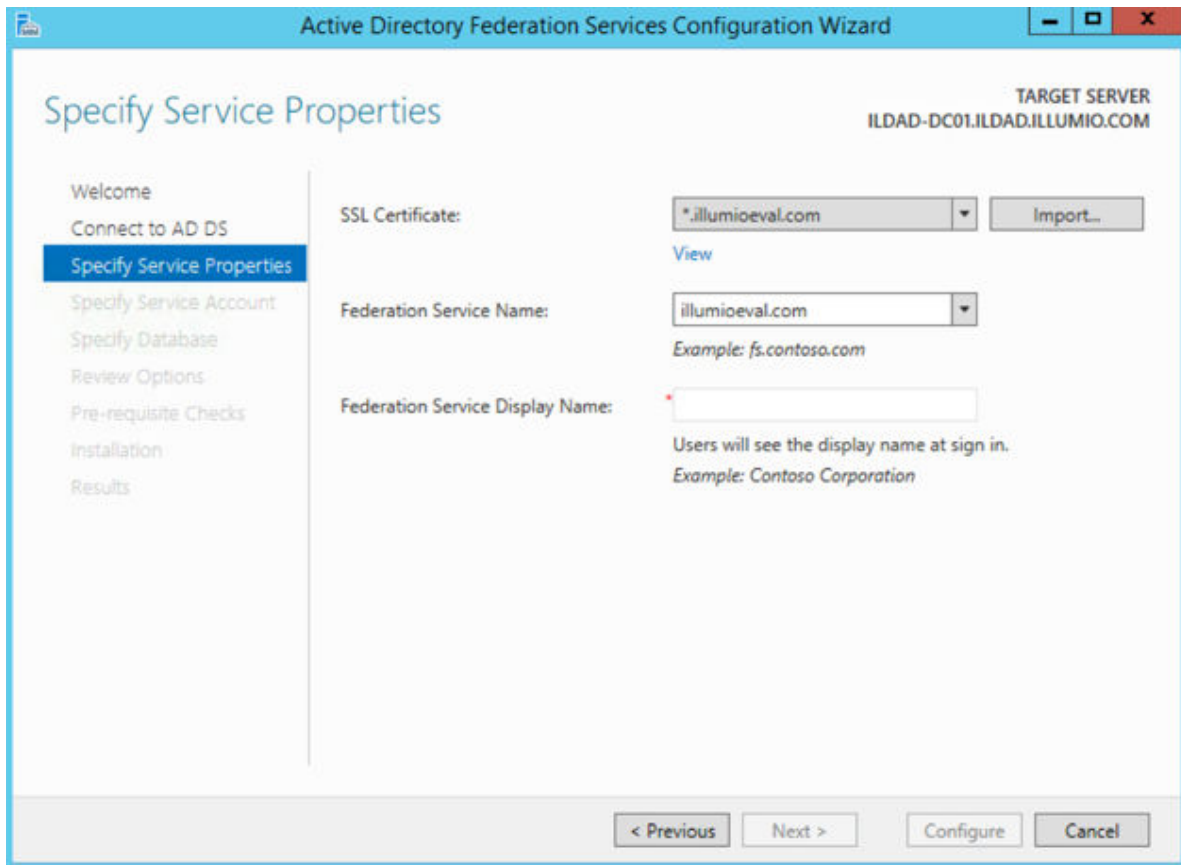
2. Click the "Configure the federation service on this server" link.
3. Select "Create the first federation server in a federation server farm" option and click **Next**.
4. Specify a domain admin account for AD FS configuration.



5. Select or import a certificate. This certificate can be a self-signed certificate.

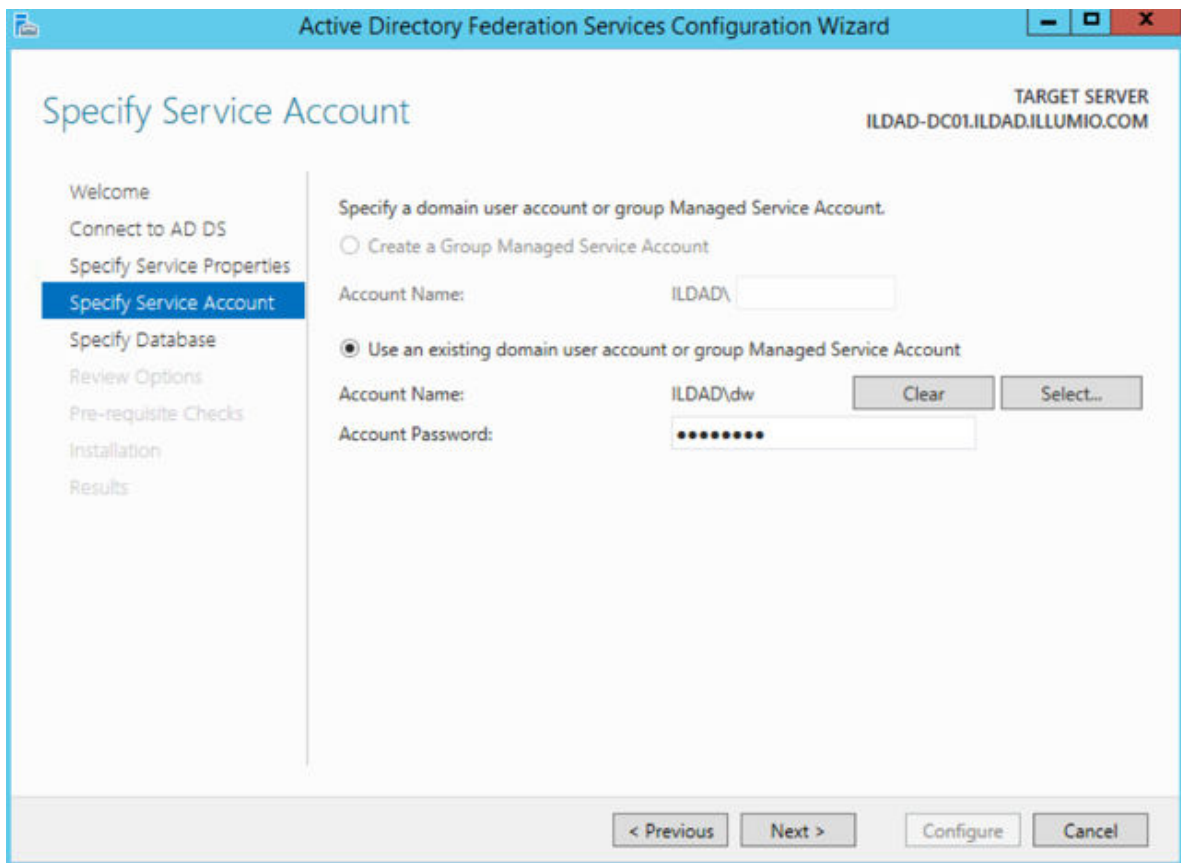


6. Specify your Federation Service Name, enter a display name for this instance of AD FS, and click **Next**



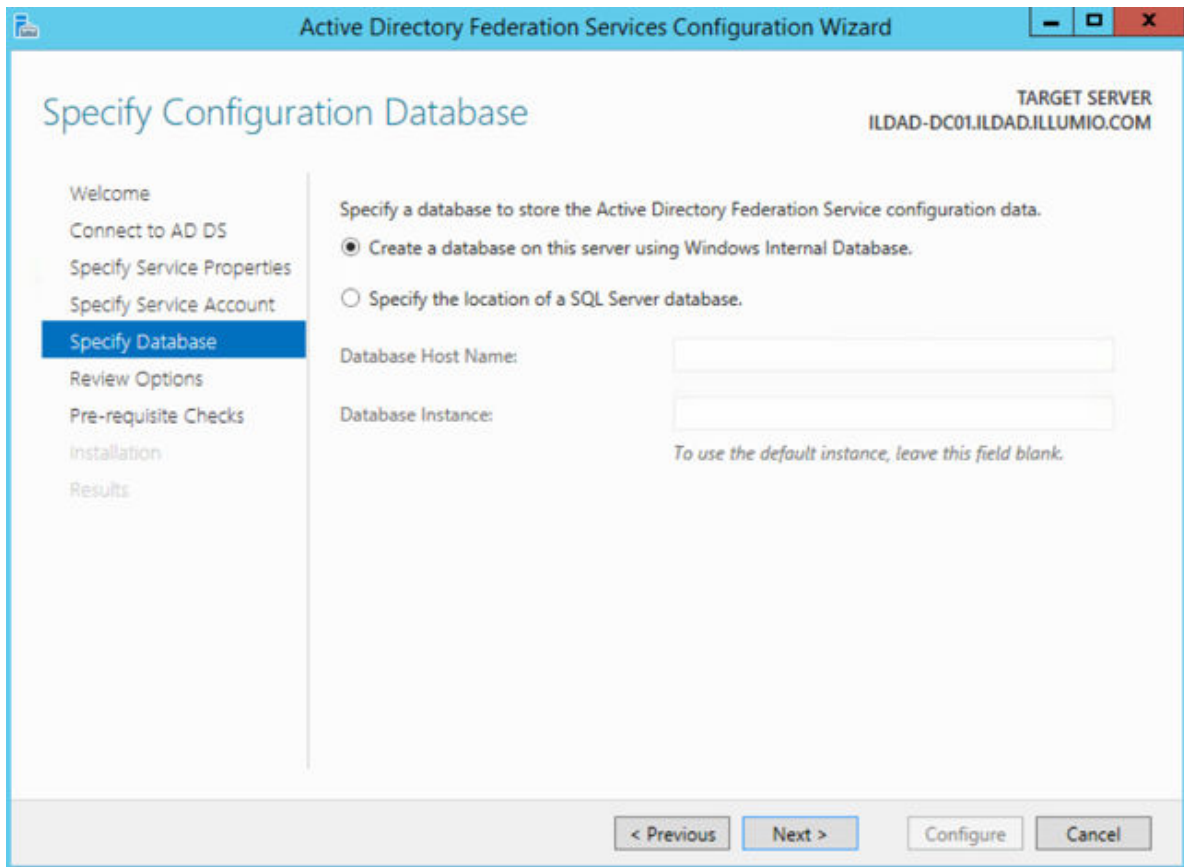
The screenshot shows the 'Specify Service Properties' step of the Active Directory Federation Services Configuration Wizard. The title bar reads 'Active Directory Federation Services Configuration Wizard'. The left sidebar contains a list of steps: Welcome, Connect to AD DS, Specify Service Properties (highlighted), Specify Service Account, Specify Database, Review Options, Pre-requisite Checks, Installation, and Results. The main area is titled 'Specify Service Properties' and shows the 'TARGET SERVER' as 'ILDAD-DC01.ILDAD.ILLUMIO.COM'. It includes fields for 'SSL Certificate' (set to '*.illumioeval.com' with an 'Import...' button), 'Federation Service Name' (set to 'illumioeval.com' with an example 'fs.contoso.com'), and 'Federation Service Display Name' (empty with an example 'Contoso Corporation'). Navigation buttons at the bottom are '< Previous', 'Next >', 'Configure', and 'Cancel'.

7. Specify your service account and click **Next**.



The screenshot shows the 'Specify Service Account' step of the Active Directory Federation Services Configuration Wizard. The title bar reads 'Active Directory Federation Services Configuration Wizard'. The left sidebar contains a list of steps: Welcome, Connect to AD DS, Specify Service Properties, Specify Service Account (highlighted), Specify Database, Review Options, Pre-requisite Checks, Installation, and Results. The main area is titled 'Specify Service Account' and shows the 'TARGET SERVER' as 'ILDAD-DC01.ILDAD.ILLUMIO.COM'. It includes a section 'Specify a domain user account or group Managed Service Account.' with two radio buttons: 'Create a Group Managed Service Account' (unselected) and 'Use an existing domain user account or group Managed Service Account' (selected). The 'Account Name' field is set to 'ILDAD\dw' with a 'Clear' button and a 'Select...' button. The 'Account Password' field is masked with dots. Navigation buttons at the bottom are '< Previous', 'Next >', 'Configure', and 'Cancel'.

8. Select "Create a database on this server using Windows Internal Database" or choose the SQL server option, and click **Next**.



The screenshot shows the 'Specify Configuration Database' step of the Active Directory Federation Services Configuration Wizard. The window title is 'Active Directory Federation Services Configuration Wizard'. The target server is 'ILDAD-DC01.ILDAD.ILLUMIO.COM'. The left sidebar lists the steps: Welcome, Connect to AD DS, Specify Service Properties, Specify Service Account, Specify Database (selected), Review Options, Pre-requisite Checks, Installation, and Results. The main area contains the instruction 'Specify a database to store the Active Directory Federation Service configuration data.' with two radio button options: 'Create a database on this server using Windows Internal Database.' (selected) and 'Specify the location of a SQL Server database.' Below these are input fields for 'Database Host Name:' and 'Database Instance:'. A note states 'To use the default instance, leave this field blank.' At the bottom are buttons for '< Previous', 'Next >', 'Configure', and 'Cancel'.

Active Directory Federation Services Configuration Wizard

TARGET SERVER
ILDAD-DC01.ILDAD.ILLUMIO.COM

Specify Configuration Database

Welcome
Connect to AD DS
Specify Service Properties
Specify Service Account
Specify Database
Review Options
Pre-requisite Checks
Installation
Results

Specify a database to store the Active Directory Federation Service configuration data.

☒ Create a database on this server using Windows Internal Database.

☐ Specify the location of a SQL Server database.

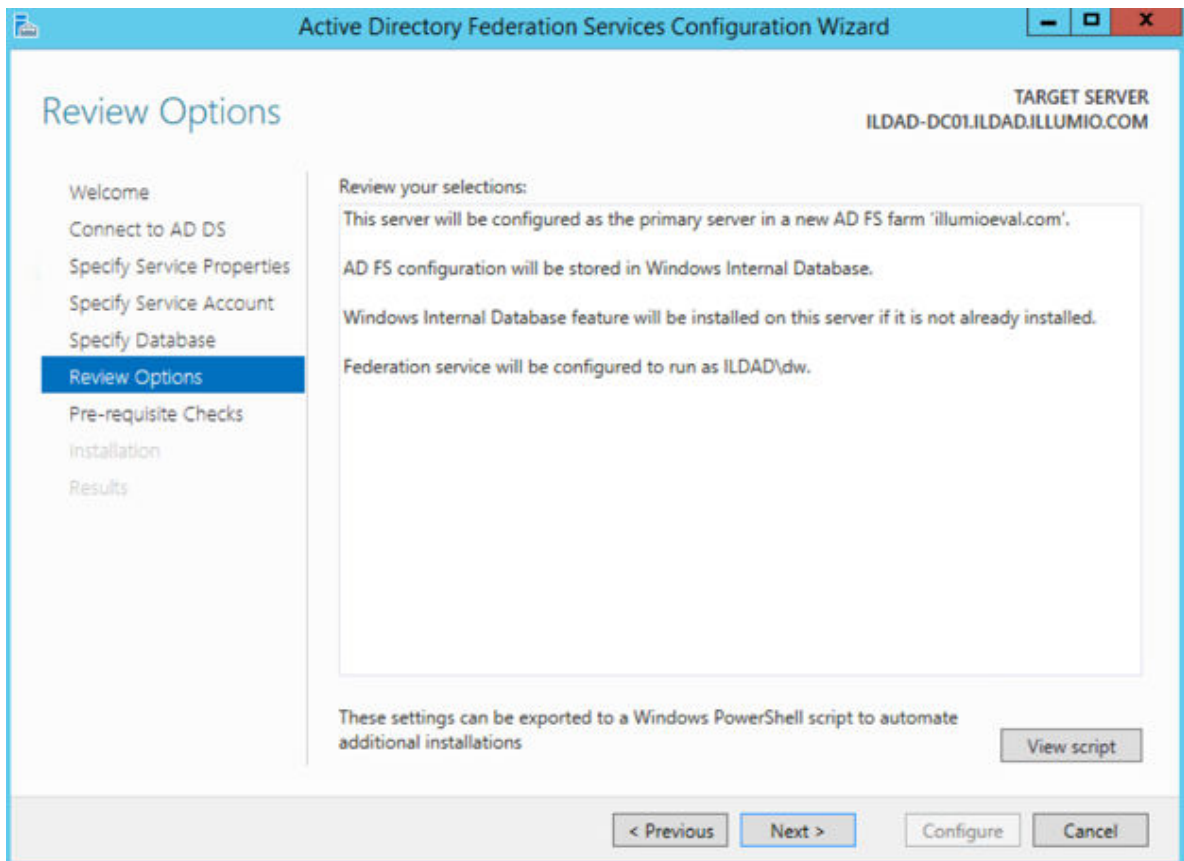
Database Host Name:

Database Instance:

To use the default instance, leave this field blank.

< Previous Next > Configure Cancel

9. Review your selected options and click **Next**.



The screenshot shows the 'Review Options' step of the Active Directory Federation Services Configuration Wizard. The window title is 'Active Directory Federation Services Configuration Wizard'. The target server is 'ILDAD-DC01.ILDAD.ILLUMIO.COM'. The left sidebar lists the steps: Welcome, Connect to AD DS, Specify Service Properties, Specify Service Account, Specify Database, Review Options (selected), Pre-requisite Checks, Installation, and Results. The main area contains the instruction 'Review your selections:' followed by a summary of the configuration: 'This server will be configured as the primary server in a new AD FS farm 'illumioeval.com'.', 'AD FS configuration will be stored in Windows Internal Database.', 'Windows Internal Database feature will be installed on this server if it is not already installed.', and 'Federation service will be configured to run as ILDAD\dw.' At the bottom, there is a note 'These settings can be exported to a Windows PowerShell script to automate additional installations' and a 'View script' button. At the bottom are buttons for '< Previous', 'Next >', 'Configure', and 'Cancel'.

Active Directory Federation Services Configuration Wizard

TARGET SERVER
ILDAD-DC01.ILDAD.ILLUMIO.COM

Review Options

Welcome
Connect to AD DS
Specify Service Properties
Specify Service Account
Specify Database
Review Options
Pre-requisite Checks
Installation
Results

Review your selections:

This server will be configured as the primary server in a new AD FS farm 'illumioeval.com'.

AD FS configuration will be stored in Windows Internal Database.

Windows Internal Database feature will be installed on this server if it is not already installed.

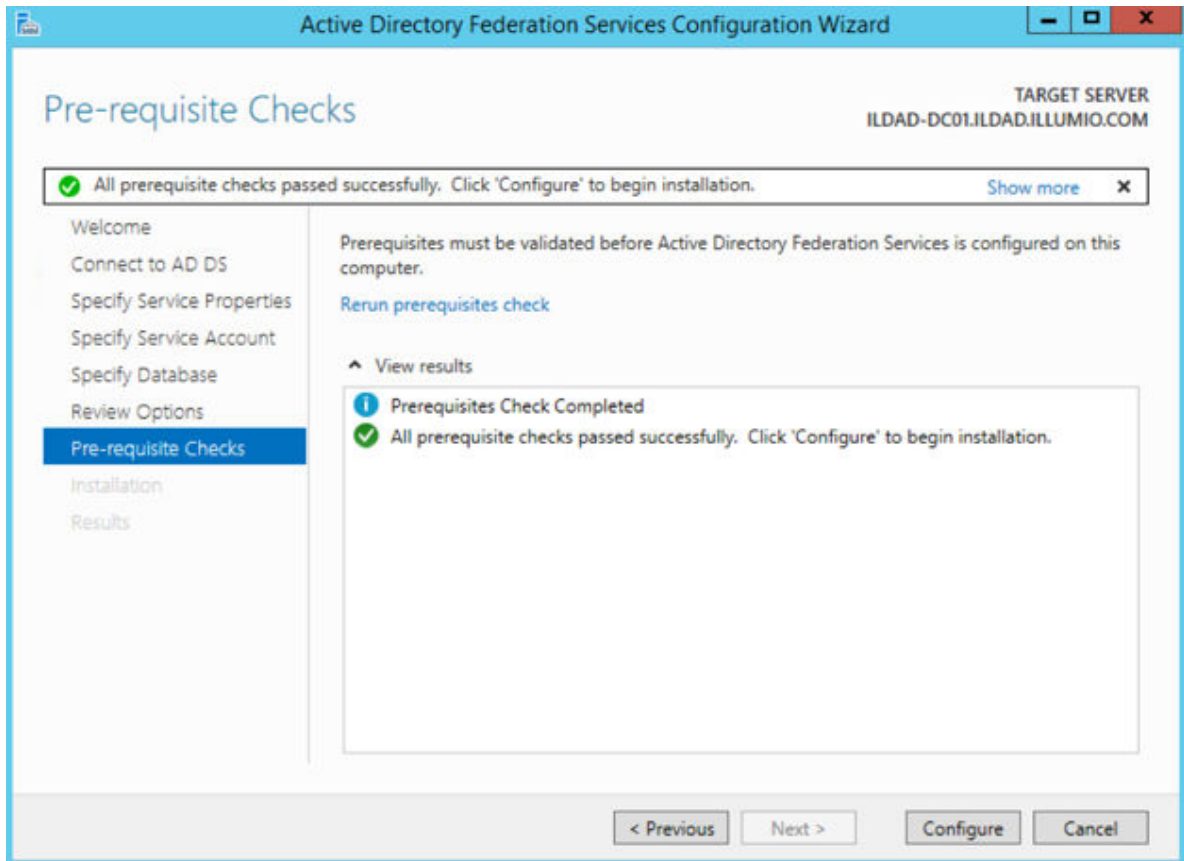
Federation service will be configured to run as ILDAD\dw.

These settings can be exported to a Windows PowerShell script to automate additional installations

View script

< Previous Next > Configure Cancel

- 10 Click **Configure** to finish the basic configuration of AD FS.



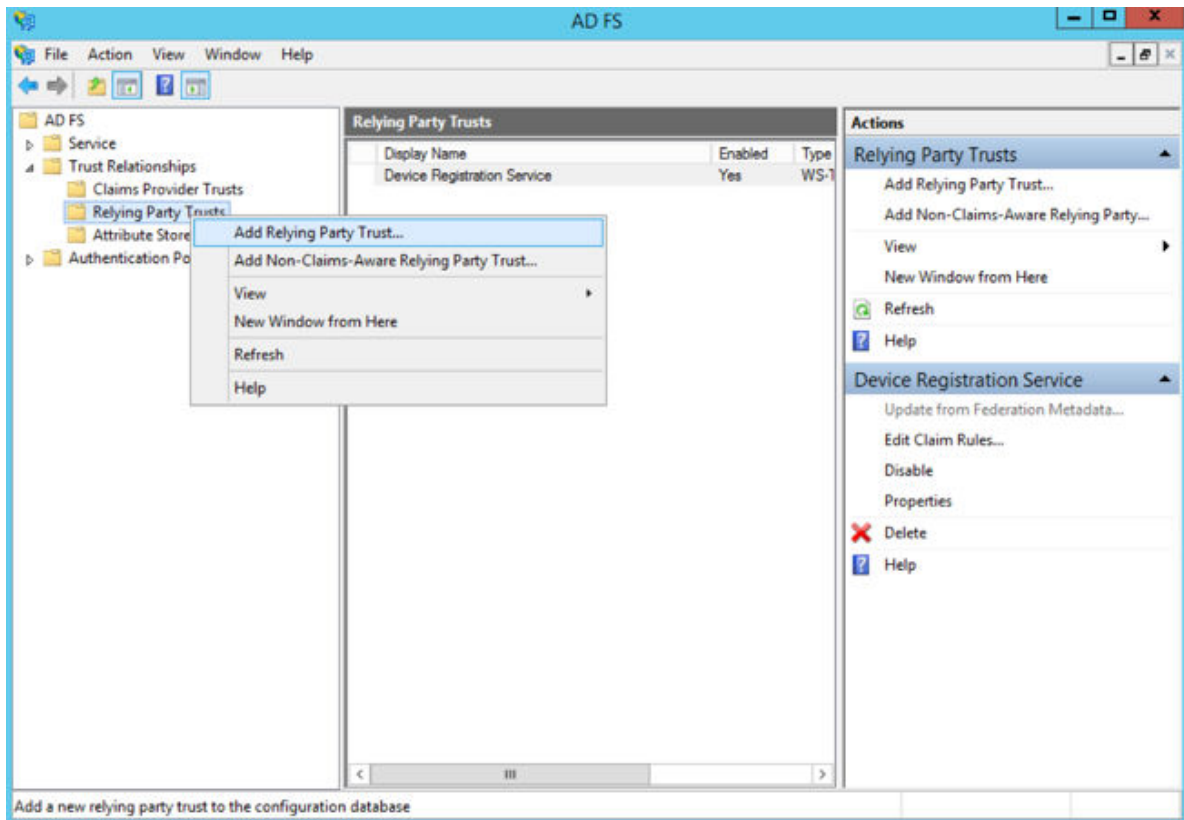
11. In the results screen, click **Close**.

AD FS is now installed with the basic configuration on this host.

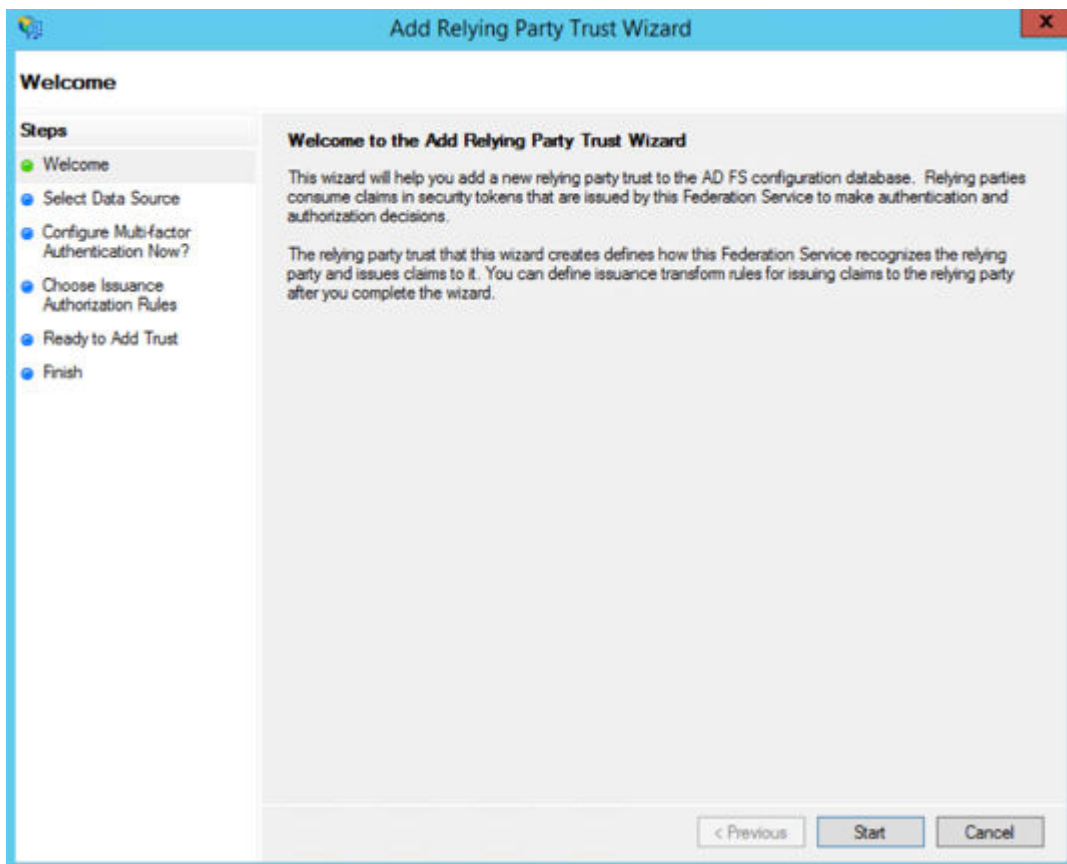
Create a Relying Party Trust

To start configuring AD FS for SSO with the PCE, you need to create a Relying Party Trust for your Illumio PCE.

1. From Server Manager/Tools, open the AD FS Manager.
2. From the left panel, choose **Relying Party Trusts > Add Relying Party Trust**.



The Add Relying Party Trust Wizard appears.



3. Click **Start**.
4. Select the "Enter data about the relying party manually" option and click **Next**.

The screenshot shows the 'Add Relying Party Trust Wizard' window. The title bar is blue with the text 'Add Relying Party Trust Wizard' and a close button. The main area is titled 'Select Data Source'. On the left, a 'Steps' pane lists the wizard's steps: Welcome, Select Data Source (highlighted), Specify Display Name, Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main content area has the instruction 'Select an option that this wizard will use to obtain data about this relying party:'. There are three radio button options: 1. 'Import data about the relying party published online or on a local network' with a description and a text field for 'Federation metadata address (host name or URL)'. 2. 'Import data about the relying party from a file' with a description and a text field for 'Federation metadata file location:' with a 'Browse...' button. 3. 'Enter data about the relying party manually' (selected) with a description. At the bottom right are buttons for '< Previous', 'Next >', and 'Cancel'.

Add Relying Party Trust Wizard

Select Data Source

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Select an option that this wizard will use to obtain data about this relying party:

☐ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

☐ Import data about the relying party from a file

Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location:

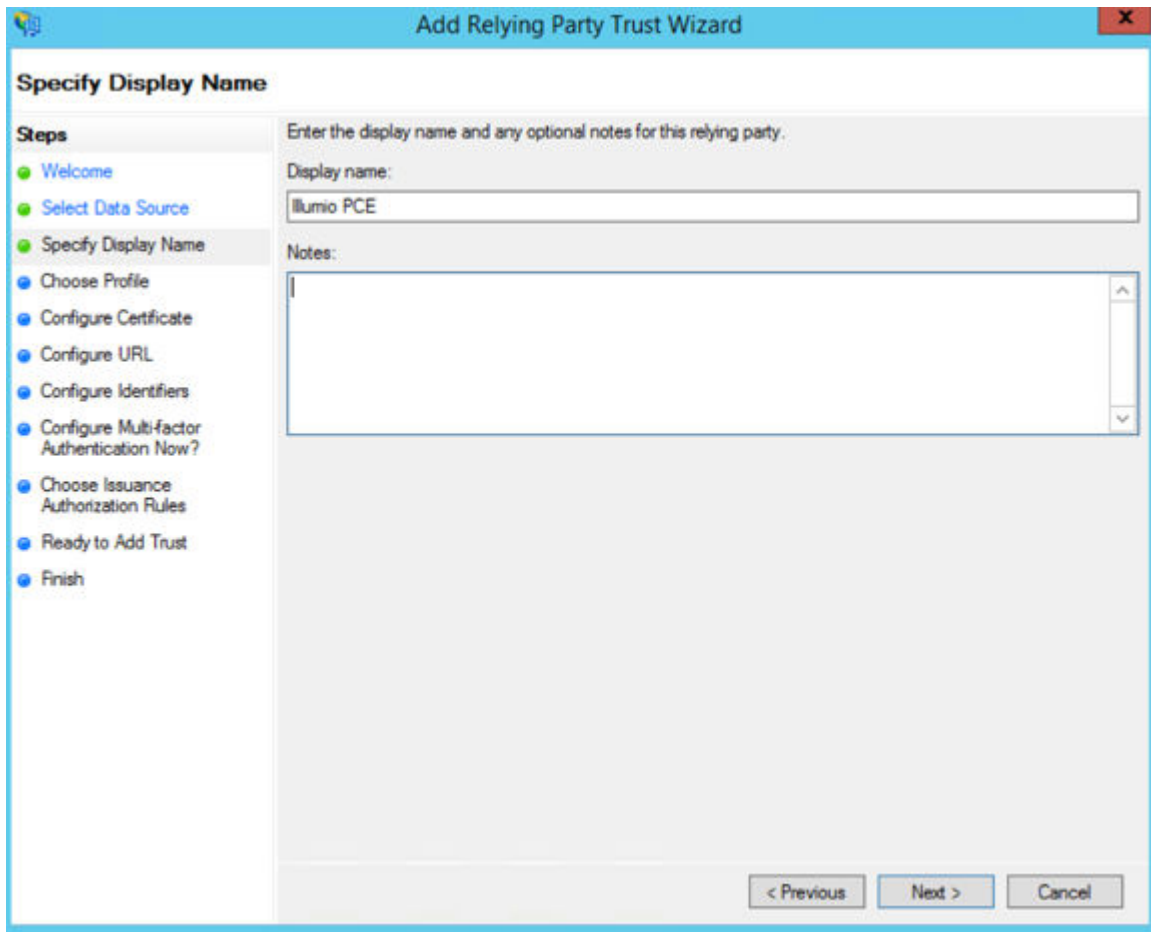
Browse...

☒ Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

< Previous Next > Cancel

5. Name your Relying Party Trust and click **Next**.



The image shows a screenshot of the "Add Relying Party Trust Wizard" window, specifically the "Specify Display Name" step. The window has a blue title bar with the text "Add Relying Party Trust Wizard" and a close button. On the left, there is a "Steps" pane with a list of steps: Welcome, Select Data Source, Specify Display Name (highlighted), Choose Profile, Configure Certificate, Configure URL, Configure Identifiers, Configure Multi-factor Authentication Now?, Choose Issuance Authorization Rules, Ready to Add Trust, and Finish. The main area of the wizard is titled "Specify Display Name" and contains the instruction "Enter the display name and any optional notes for this relying party." Below this instruction, there is a "Display name:" label followed by a text box containing "Illumio PCE". Below the text box is a "Notes:" label followed by a large text area. At the bottom right of the wizard, there are three buttons: "< Previous", "Next >", and "Cancel".

Add Relying Party Trust Wizard

Specify Display Name

Enter the display name and any optional notes for this relying party.

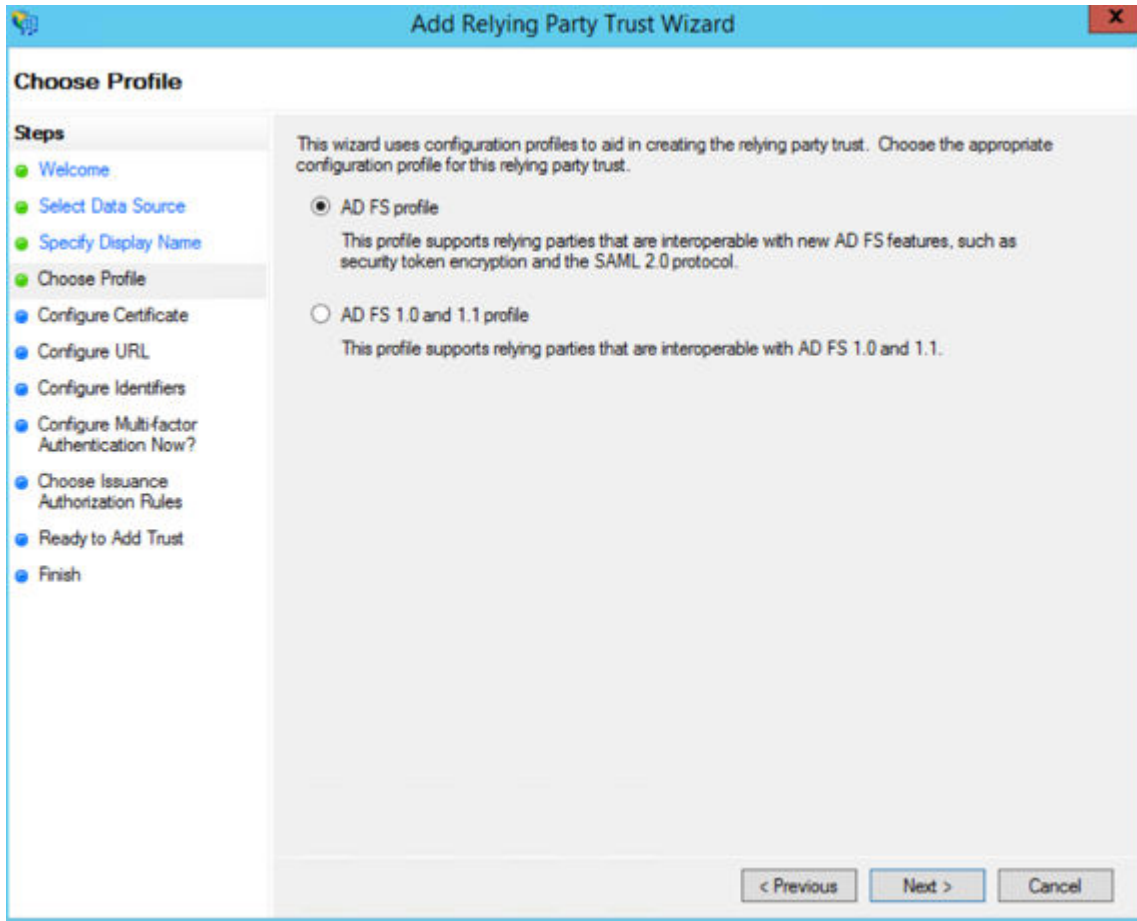
Display name:

Illumio PCE

Notes:

< Previous Next > Cancel

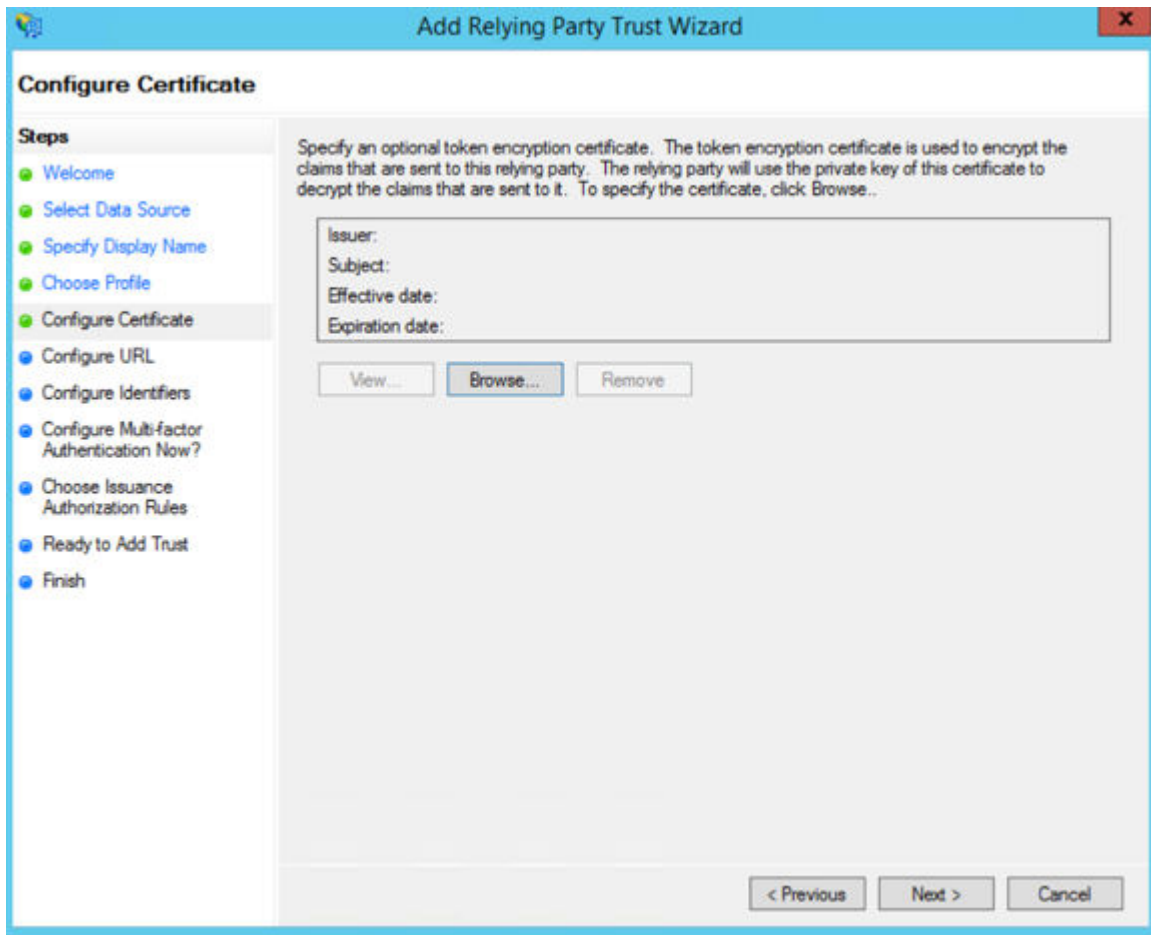
6. Select "ADFS profile" and click **Next**.



7. When you have a separate certificate for token encryption, browse to, select it, and click **Next**.

**NOTE**

To use the standard AD FS certificate (created during AD FS installation) for token signing, don't select anything in this step and click **Next**.

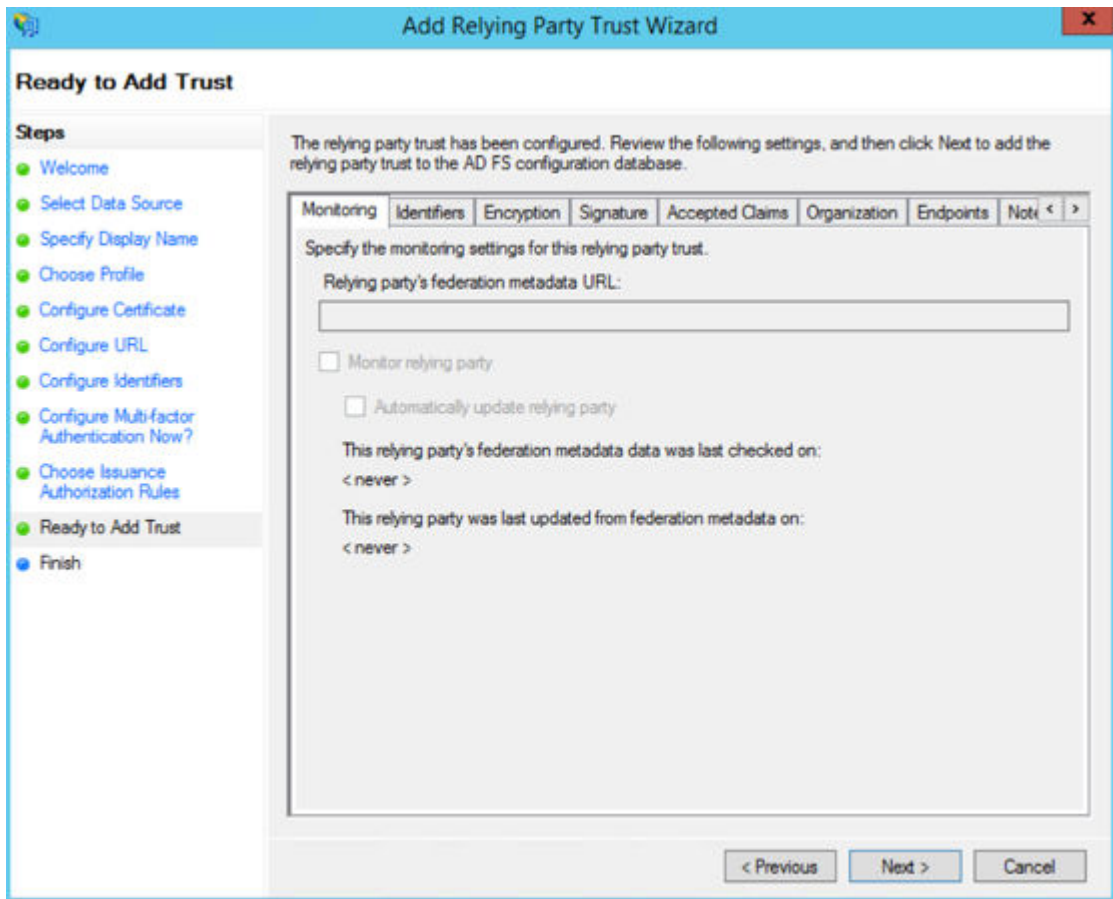


8. Select "Enable support for the SAML 2.0 WebSSO protocol." In the Relying party SAML 2.0 SSO service URL field, add your "Assertion Consumer URL" (obtained from the PCE web console).

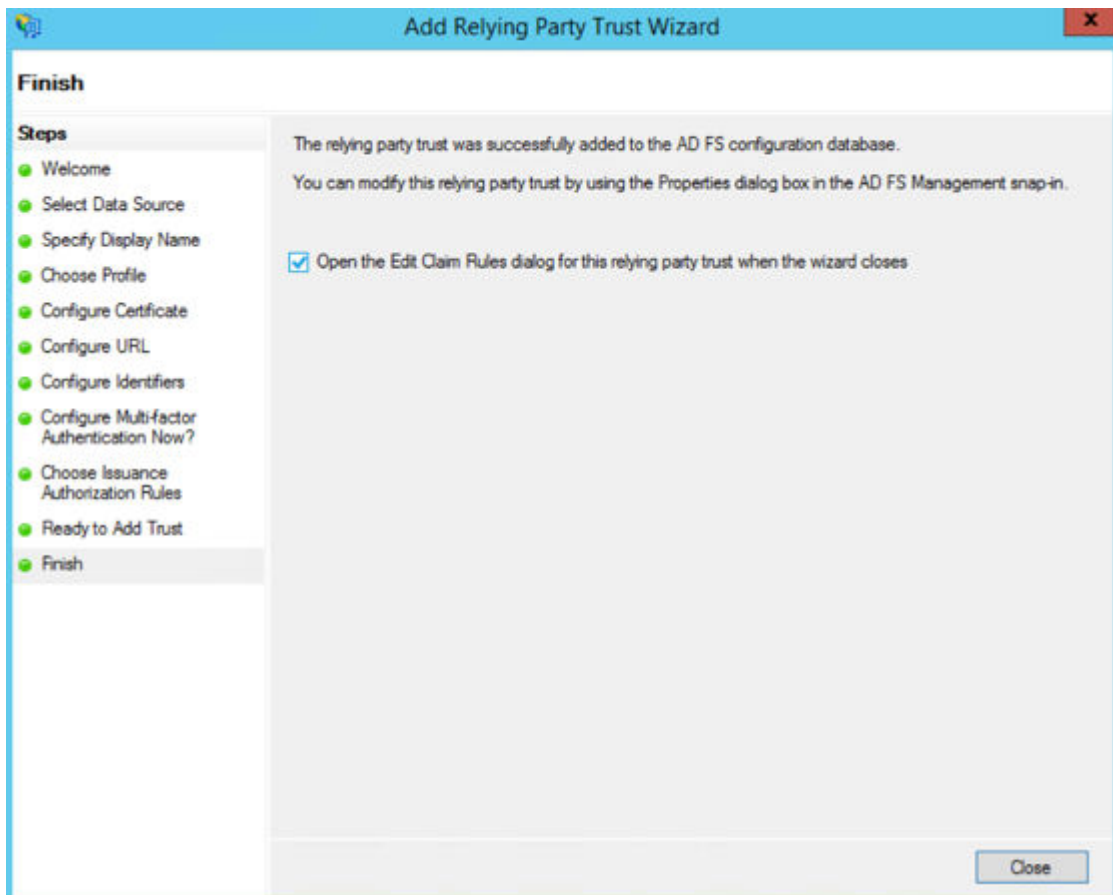
To locate the “Assertion Consumer URL,” go to **Settings > Authentication > Information for Identity Provider** in the PCE web console:

Information for Identity Provider	
Default User Role	Read Only
SAML Version	2.0
Issuer	https://pce-mnc.illumioeval.com:8443/login
NameID Format	urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
Assertion Consumer URL	https://pce-mnc.illumioeval.com:8443/login/acs/2402fb18-3d75-4432-ab6d-10475897b476
Logout URL	https://pce-mnc.illumioeval.com:8443/login/logout/2402fb18-3d75-4432-ab6d-10475897b476

9. On the Configure Identifiers page, use the same URL for the Relying party trust identifier, without the `/acs/<randomNumbers>`.
For example: `https://pce.domain.com:8443/login`.
Click **Next**.
10. Select the radio button “I do not want to configure multi-factor authentication settings for this relying party at this time” and click **Next**.
11. Select “Permit all users to access this relying party” and click **Next**.
12. On the Ready to Add Trust page, click **Next**.



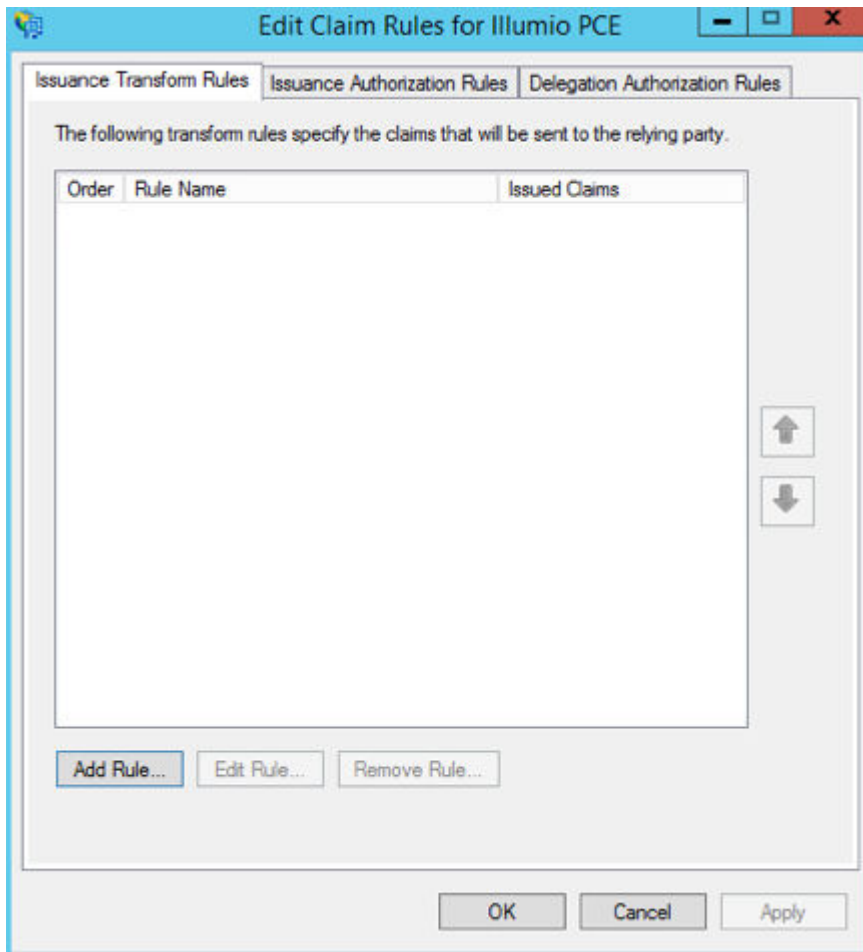
13. Leave the Open the Edit Claim Rules checkbox selected and click **Close**.



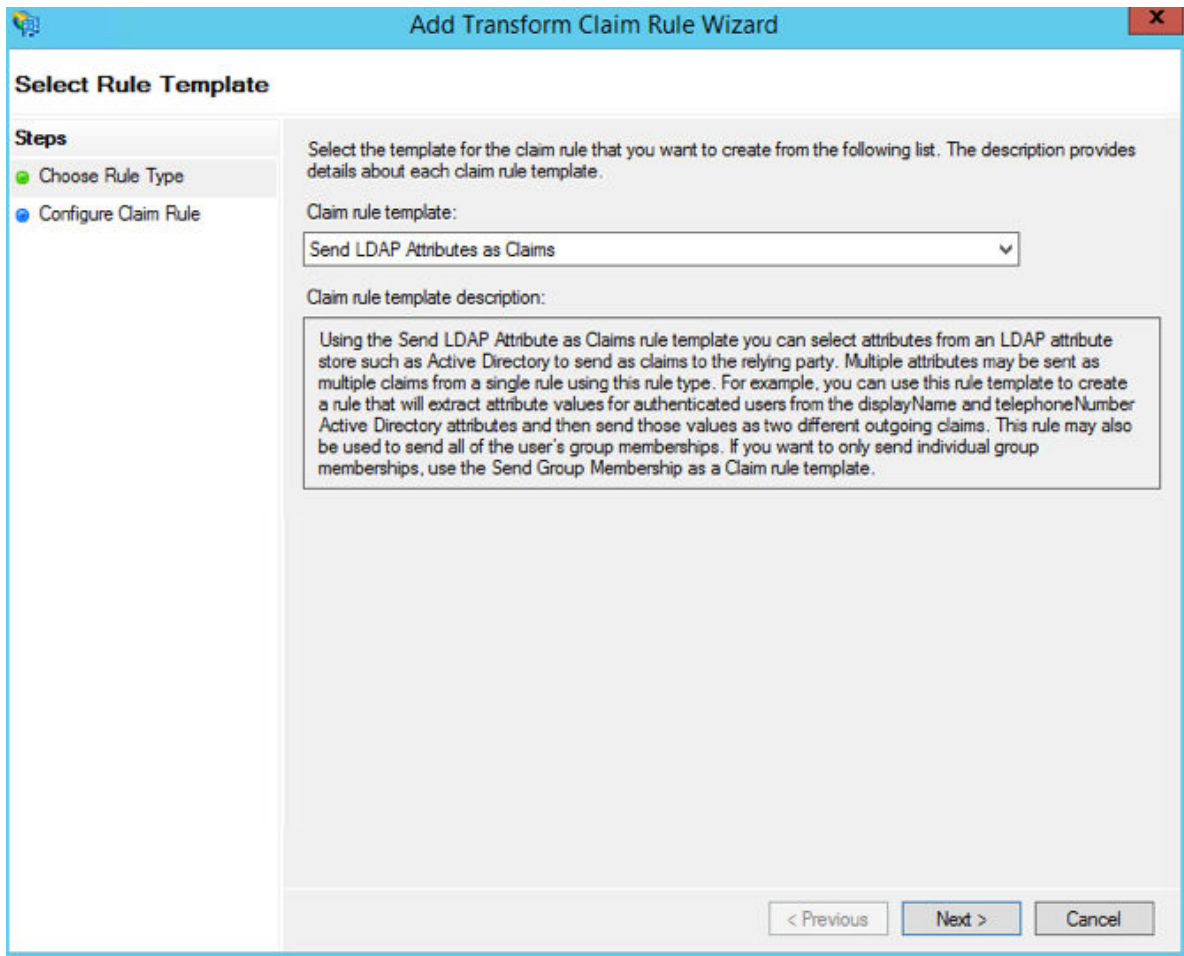
Create Claim Rules

You need to create claim rules to enable proper communication between AD FS and the PCE.

1. In the Edit Claim Rules dialog, click **Add Rule**.



2. Under Select Rule Template, select "Send LDAP Attributes as Claims" and click **Next**.



3. Name the Claim rule "Illumio Attributes" and select **Active Directory** as the Attribute store. Under the first attribute, select "User-Principal-Name" and "E-Mail Address" as the outgoing. Select "Surname" and type the custom field name of "User.LastName" in the outgoing field. Repeat the values for "Given-Name" and "User.FirstName" and click **Finish**.

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:
Illumio Attributes

Rule template: Send LDAP Attributes as Claims

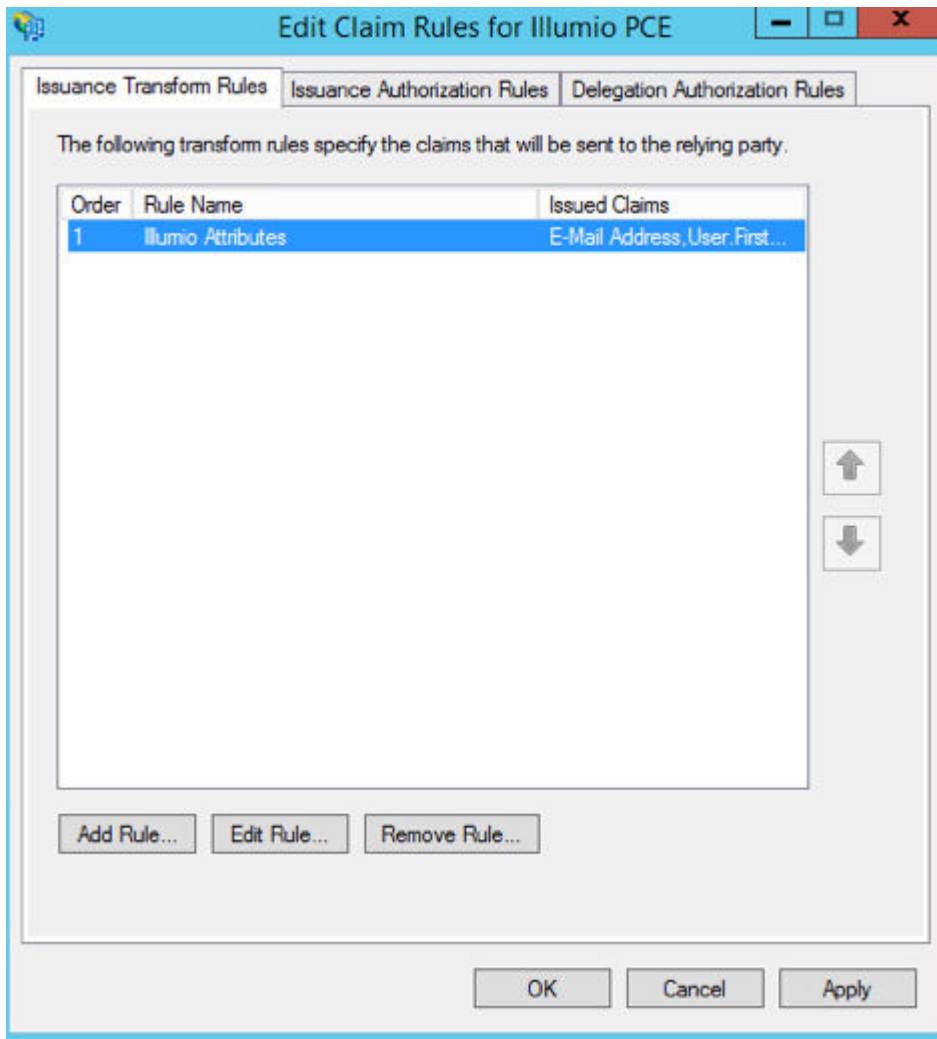
Attribute store:
Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	User-Principal-Name	E-Mail Address
	Surname	User.LastName
	Given-Name	User.FirstName
*		

< Previous Finish Cancel

4. In the Edit Claim Rules dialog with your new rule added, click **Add Rule** to add the final rule.



5. Under the Claim Rule Template, select “Transform and Incoming Claim” and click **Next**.

The screenshot shows a Windows-style dialog box titled "Add Transform Claim Rule Wizard". It has a blue header bar with a close button (X) in the top right corner. The main content area is titled "Select Rule Template". On the left, there is a "Steps" sidebar with two items: "Choose Rule Type" (marked with a green dot) and "Configure Claim Rule" (marked with a blue dot). The main area contains the following text: "Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template." Below this is a label "Claim rule template:" followed by a dropdown menu showing "Transform an Incoming Claim". Underneath is a label "Claim rule template description:" followed by a text box containing the following text: "Using the Transform an Incoming Claim rule template you can select an incoming claim, change its claim type, and optionally change its claim value. For example, you can use this rule template to create a rule that will send a role claim with the same claim value of an incoming group claim. You can also use this rule to send a group claim with a claim value of 'Purchasers' when there is an incoming group claim with a value of 'Admins'. Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims vary based on the rules being edited. For more information on the sources of incoming claims, click Help." At the bottom right of the dialog are three buttons: "< Previous", "Next >" (highlighted with a blue border), and "Cancel".

6. Name the rule "Email to NameID Transform" and change the incoming claim type to "E-Mail Address." Set the Outgoing claim type to "Name ID" and the Outgoing name ID format to "Email" and click **Finish**.

The screenshot shows the 'Add Transform Claim Rule Wizard' window, specifically the 'Configure Rule' step. The window has a blue title bar with the text 'Add Transform Claim Rule Wizard' and a close button. On the left, there is a 'Steps' sidebar with two items: 'Choose Rule Type' (highlighted with a green dot) and 'Configure Claim Rule' (with a green dot). The main area contains a descriptive paragraph: 'You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.' Below this, there are several configuration fields: 'Claim rule name' (text box with 'Email to NameID Transform'), 'Rule template' (dropdown with 'Transform an Incoming Claim'), 'Incoming claim type' (dropdown with 'E-Mail Address'), 'Incoming name ID format' (dropdown with 'Unspecified'), 'Outgoing claim type' (dropdown with 'Name ID'), and 'Outgoing name ID format' (dropdown with 'Email'). There are three radio button options: 'Pass through all claim values' (selected), 'Replace an incoming claim value with a different outgoing claim value' (with sub-fields for 'Incoming claim value' and 'Outgoing claim value' and a 'Browse...' button), and 'Replace incoming e-mail suffix claims with a new e-mail suffix' (with a 'New e-mail suffix' field and an example 'fabrikam.com'). At the bottom right, there are three buttons: '< Previous', 'Finish', and 'Cancel'.

Add Transform Claim Rule Wizard

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name:

Rule template: Transform an Incoming Claim

Incoming claim type:

Incoming name ID format:

Outgoing claim type:

Outgoing name ID format:

☒ Pass through all claim values

☐ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

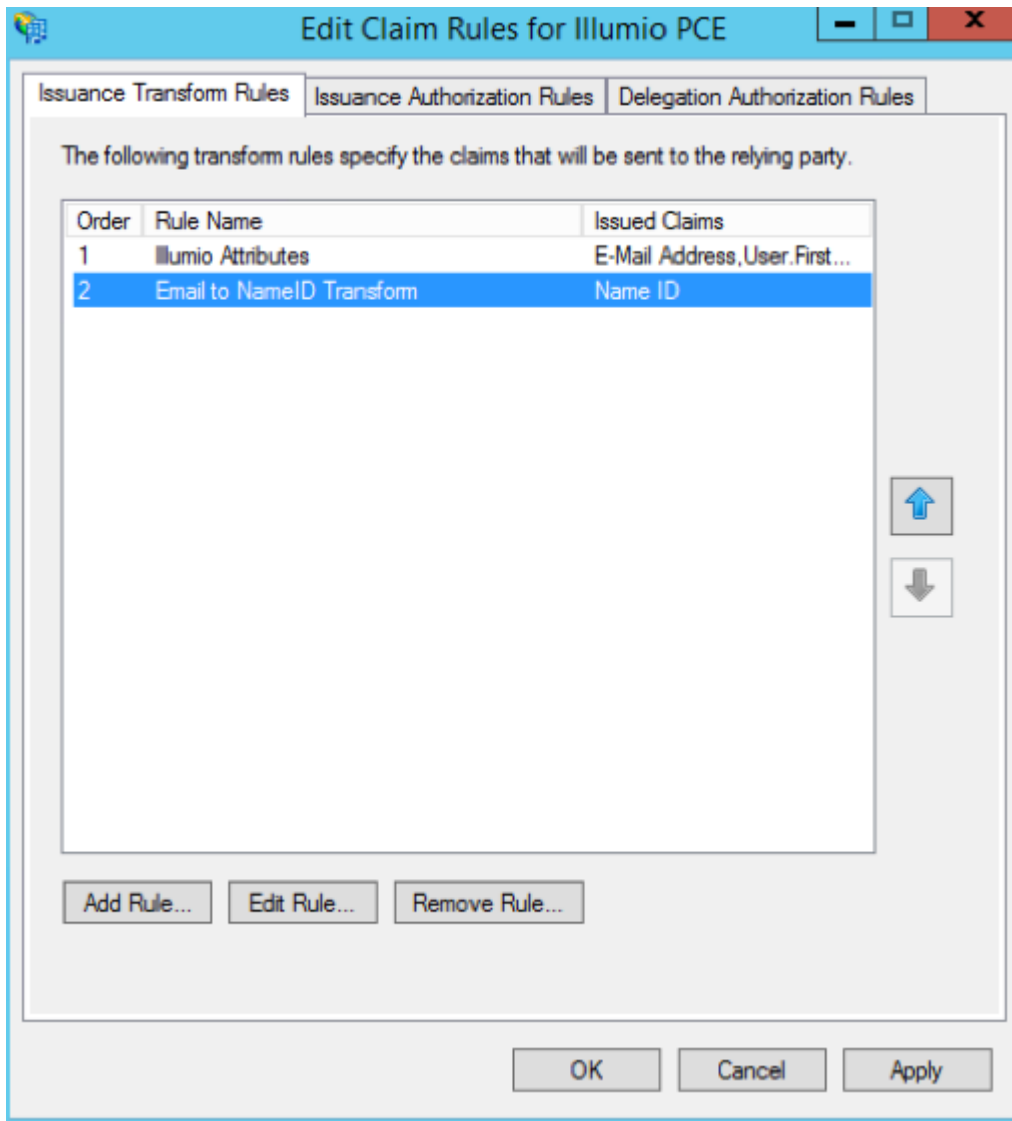
Outgoing claim value:

☐ Replace incoming e-mail suffix claims with a new e-mail suffix

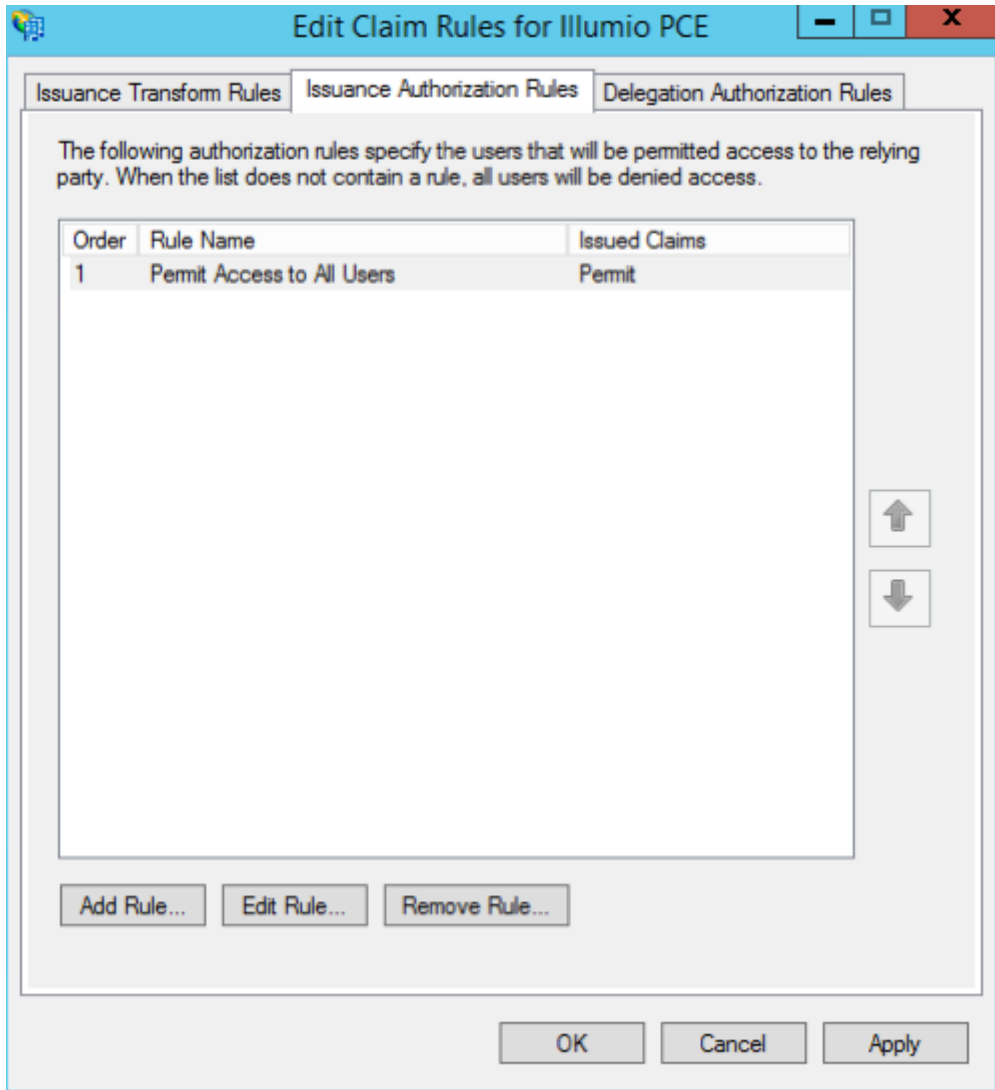
New e-mail suffix:

Example: fabrikam.com

The Edit Claim Rules window opens.



7. (Windows 2016 and Windows 2019) Skip to step 12.
The Edit Claim Rules window has three tabs. You have already filled out the first tab. The other two tabs are not available in Windows 2016 or Windows 2019. Therefore, skip steps 8 - 11.
8. Select the Issuance Authorization Rules tab.
9. To allow all your Active Directory Users to access the PCE, leave the “Permit Access to All Users” as is. Otherwise, you should restrict access to a single group or groups of users.



10 Select "Permit or Deny Users Based on an Incoming Claim" and click **Next**.

.

The screenshot shows a Windows-style dialog box titled "Add Issuance Authorization Claim Rule Wizard". On the left, a "Steps" pane lists two steps: "Choose Rule Type" (selected with a green dot) and "Configure Claim Rule" (with a blue dot). The main area is titled "Select Rule Template" and contains the following text: "Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template." Below this is a "Claim rule template:" label and a dropdown menu showing "Permit or Deny Users Based on an Incoming Claim". Underneath is a "Claim rule template description:" label and a text box containing the following text: "Using the Permit or Deny Users Based on an Incoming Claim rule template you can permit or deny users access to the relying party based on the type and value of an incoming claim. For example, you can use this rule template to create a rule that will permit only users that have a group claim with a value of 'Domain Admins'. If you want to permit all users to access the relying party, use the Permit All Users rule template. Users who are permitted to access the relying party from the federation service may still be denied service by the relying party." At the bottom right are three buttons: "< Previous", "Next >", and "Cancel".

11. Name the rule "AD FS Users" and change the Incoming claim type to "Group SID" (you might have to scroll to find it). In Incoming claim value, browse to the group of users you want to give access. Make sure "Permit access" is selected and click **Finish**.

The screenshot shows the 'Add Issuance Authorization Claim Rule Wizard' window, specifically the 'Configure Rule' step. The window has a blue title bar and a sidebar on the left with two steps: 'Choose Rule Type' and 'Configure Claim Rule'. The main area contains the following fields and options:

- Claim rule name:** A text box containing 'AD FS Users'.
- Rule template:** 'Authorize Users Based on an Incoming Claim'.
- Incoming claim type:** A dropdown menu showing 'Group SID'.
- Incoming claim value:** A text box containing 'ILDAD\ADFS Users' and a 'Browse...' button.
- Access options:** Two radio buttons: 'Permit access to users with this incoming claim' (selected) and 'Deny access to users with this incoming claim'.
- Navigation buttons:** '< Previous', 'Finish', and 'Cancel' at the bottom right.

12. If you are using RBAC with groups, you need to create a Group Claim Rule. To add groups to AD FS claim rule configuration, click **Edit Rule**. Add the requirement for "LDAP Attribute: memberOf" by selecting the Outgoing Claim Type as "User.MemberOf." Click **OK**.

Edit Rule - Groups

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:
Groups

Rule template: Send LDAP Attributes as Claims

Attribute store:
Active Directory

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	Token-Groups - Unqualified Names	User.MemberOf
*		

View Rule Language... OK Cancel

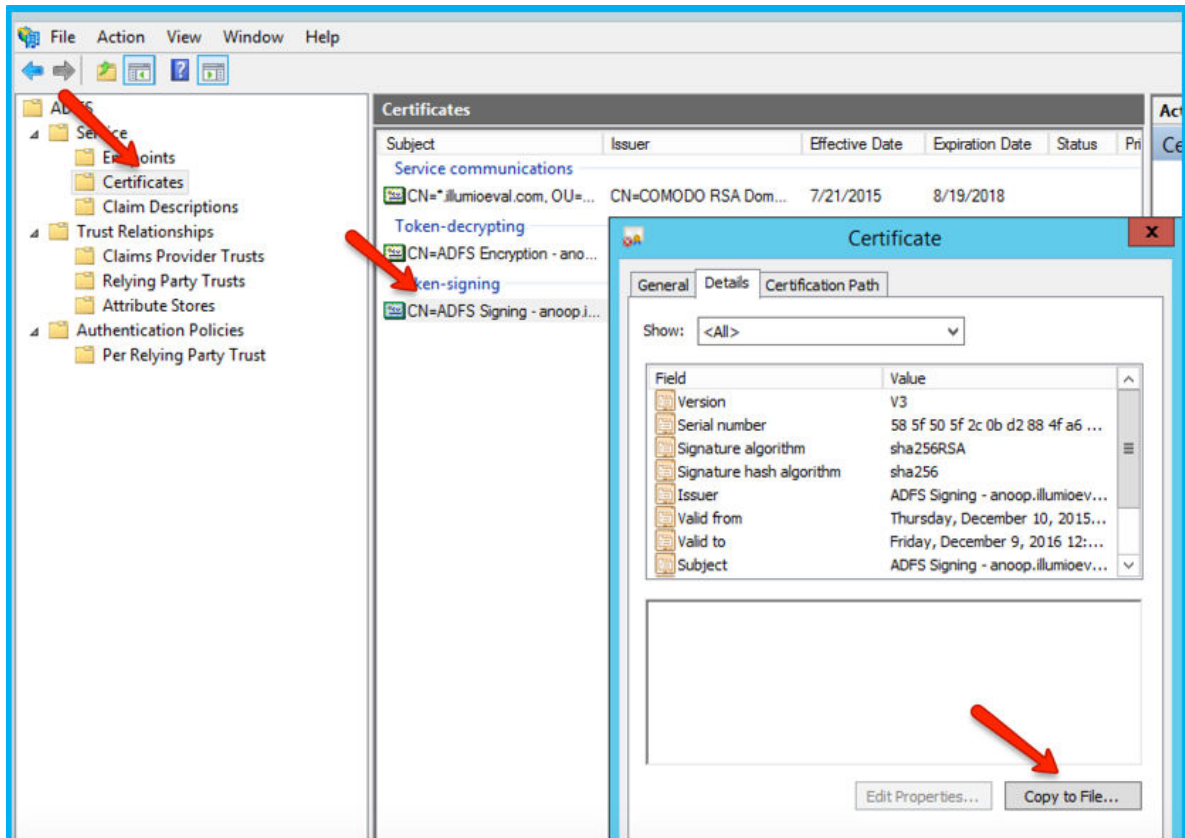
Obtain ADFS SSO Information for the PCE

Before you can configure the PCE to use AD FS for SSO, obtain the following information from your AD FS configuration:

- x.509 certificate supplied by ADFS
- Remote Login URL
- Logout Landing URL

To obtain the AD FS SSO information for the PCE:

1. To find the certificate in your AD FS configuration, log into the AD FS server and open the management console.
2. Browse to the certificates and export the Token-Signing certificate.
3. Right-click the certificate and select **View Certificate**.
4. Select the **Details** tab.
5. Click **Copy to File**.



6. When the Certificate Export Wizard launches, click **Next**.
7. Verify that the “No - do not export the private key” option is selected and click **Next**.
8. Select Base 64 encoded binary X.509 (.cer) and click **Next**.
9. Select where you want to save the file, name the file, and click **Next**.
10. Click **Finish**.
- .
11. After exporting the certificate to a file, open the file with a text editor. Copy and paste the contents of the exported x.509 certificate, including the **BEGIN CERTIFICATE** and **END CERTIFICATE** delimiters in to the SAML Identity Provider Certificate field.
12. To find the **Remote Login URL** (which AD FS calls “Sign-On URL”), download and open the following metadata file from your AD FS server by navigating to <https://server.mydomain/FederationMetadata/2007-06/FederationMetadata.xml> and search for SingleSignOnService.

```
format:persistent</NameIDFormat><NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid
-format:transient</NameIDFormat><SingleSignOnService
```

```
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://.illumio.com/adfs/ls/"><SingleSignOnService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://anoop.illumioeval.com/adfs/ls/"><Attribute
Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"
```

13. To find the **Logout Landing URL** for the PCE, you can use the login URL of the PCE (preferred):

```
https://<myPCNameAndPort>/login
```

Or, a generic logout URL of AD FS:

```
https://<URLToMyADFSServer>/adfs/ls/?wa=wsignout1.0
```

You are now ready to configure the PCE to use AD FS for SSO.

Configure the PCE for AD FS SSO

Before you configure the PCE to use Microsoft AD FS for SSO, make sure you have the following information provided by your AD FS, which you configure in the PCE web console:

- x.509 certificate supplied by ADFS
- Remote Login URL
- Logout Landing URL

For more information, see [Obtain ADFS SSO Information for the PCE \[88\]](#).



NOTE

When SSO is configured in Illumio Core and for the IdP, the preferences in Illumio Core are used. When SSO is not configured in Illumio Core, the default IdP settings are used.

To configure the PCE for AD FS:

1. From the PCE web console menu, choose **Settings > SSO Config**.
2. Click **Edit**.
3. Select the Enabled checkbox next to SAML Status.
4. In the Information From Identity Provider section, enter the following information:

- SAML Identity Provider Certificate
 - Remote Login URL
 - Logout Landing URL
5. Select the authentication method from the drop-down list:
 - **Unspecified:** Uses the IdP default authentication mechanism.
 - **Password Protected Transport:** Requires the user to log in with a password using a protected session; select this option and check the Force Re-authorization checkbox to force user re-authorization.
 6. To require users to re-enter their login information to access Illumio (even if the session is still valid), check the Force Re-authorization checkbox. This allows users to log into the PCE using a different login than their default computer login and is disabled by default.

**NOTE**

You must select "Password Protected Transport" as the authentication method and check the Force Re-authorization checkbox to force users to re-authenticate.

7. Click **Save**.
Your PCE is now configured to use AD FS for SSO authentication.

Azure AD Single Sign-on

This topic describes how to configure Azure Active Directory (AD) to provide SSO authentication to the Illumio PCE.

**TIP**

Because you'll configure settings in both the Illumio PCE Web Console and in Azure AD, have both applications open in adjacent browser tabs.

Prerequisites

To perform this configuration, you need the following:

- An Azure AD subscription. If you don't have a subscription, you can get a [free account](#).
- An Illumio single sign-on (SSO) enabled subscription.

STEP 1: Obtain URLs from the Illumio PCE Web Console

In this step you'll copy and preserve URLs from the Illumio PCE for use in Step2.

1. Log in to the PCE as a Global Organization Owner.
2. Go to **Access Management > Authentication**.
3. On the **SAML** tile, click **Configure**.
4. Copy and preserve the following URLs needed to complete the Azure configuration in a later step:

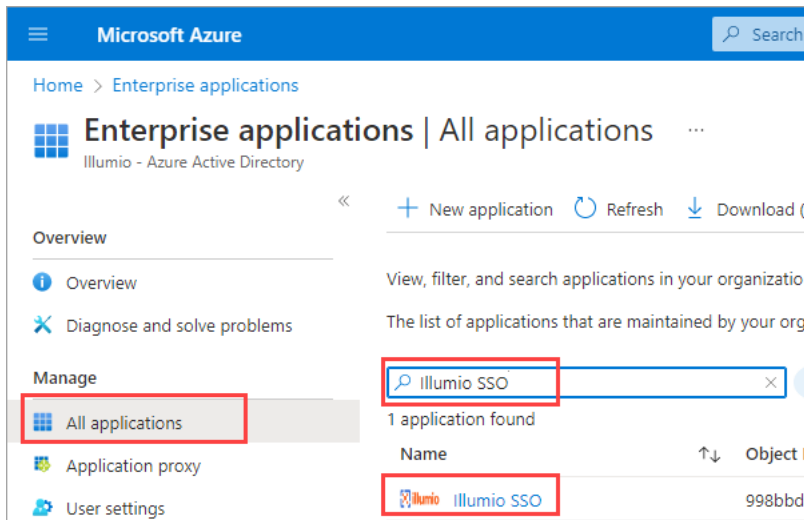
**TIP**

Make sure to replace the x's in the URLs below with the actual values from your implementation.

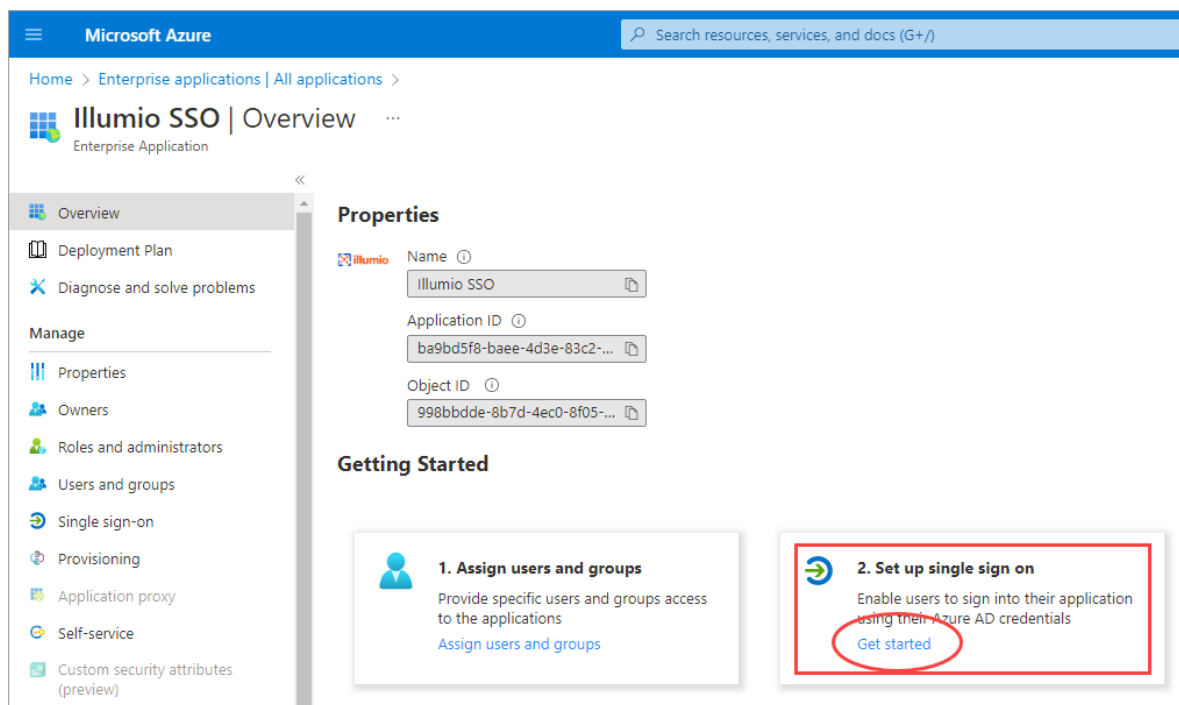
STEP 2: Configure SSO settings in Azure AD**NOTE**

Only an Azure Application Administrator can configure Azure AD.

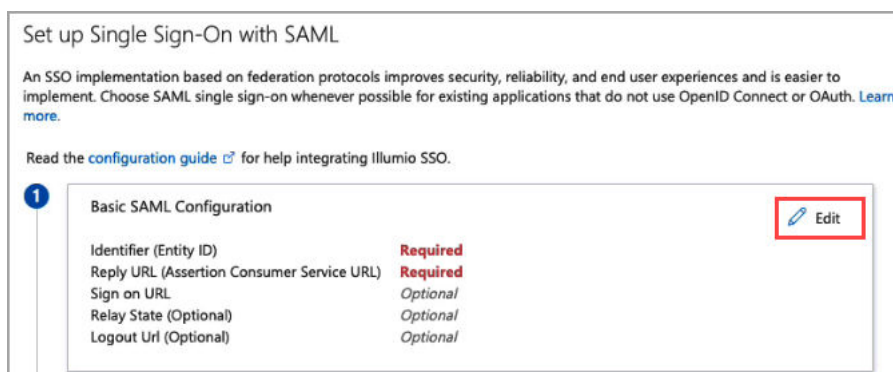
1. In a different browser tab, log in to Azure AD as an Application Administrator.
2. Go to **Enterprise applications > All applications**.
3. Search for the **Illumio SSO** app and then click the app.



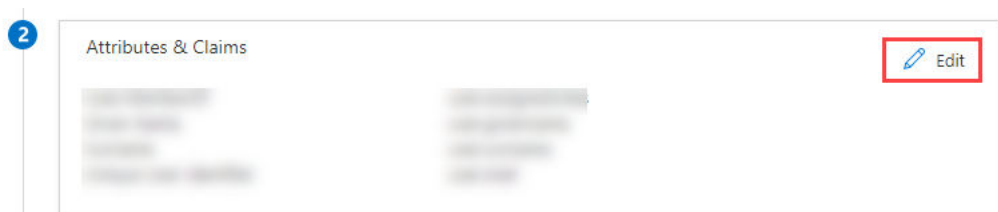
4. In the center of the page under **Getting Started**, click **Get started** on the **Set up single sign on** tile.



5. If prompted to select a single sign-on method, click **SAML**.
6. Configure Basic SAML:
 - a. On the **Set up Single-Sign On with SAML** page **Basic SAML Configuration** tile, click **Edit**.



- b. On the **Basic SAML Configuration** panel that opens, populate the fields with the values you copied and preserved.
 - In the **Identifier (Entity ID)** field, paste the **Issuer URL** you copied from the Illumio PCE.
 - In the **Reply URL (Assertion Consumer Service URL)** field, click **Add reply URL** and then paste the **Assertion Source URL** you copied from the Illumio PCE. **Note:** Your Reply URL must have a subdomain such as www, wd2, wd3, wd3-impl, wd5, wd5-impl. For example, *http://www.myIllumio.com* will work but *http://myIllumio.com* won't.
 - c. Click **Save** and close the **Basic SAML Configuration** panel.
7. Click **Edit** on the **Attributes & Claims** tile.



8. Under **Required claim**, update the **Claim name**:

Attributes & Claims ...

+ Add new claim + Add a group claim Columns Got feedback?

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.mail [nameid-forma...]

Additional claims

Claim name	Type	Value

Advanced settings

- Click the three dots.
 - On the **Manage claim** page, click in the **Source attribute** field and select **user.mail** from the dropdown.
 - Click **Save**.
9. Back on the **Attributes & Claims** page, delete **all** of the existing claims in the **Additional claims** section by clicking the three dots for each one and then clicking **Delete**.

Additional claims

Claim name	Type	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailadd...	SAML	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname

- 10 Click **Add new claim** and add three new claims:

Attributes & Claims ...

+ Add new claim + Add a group claim Columns Got feedback?

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.mail [nameid-forma...]

Additional claims

Claim name	Type	Value
Given Name	SAML	user.givenname
Surname	SAML	user.surname
User.MemberOf	SAML	user.assignedroles

Given Name

Surname



User.MemberOf


STEP 3: Obtain SAML certificate and URLs from Azure AD

In this step, you'll download a certificate and copy two URLs that you'll later paste into the Illumio PCE SAML setup.

- On the **SAML Certificates** tile, click **Download** for the **Certificate (Base64)** certificate and save the certificate to your computer.

SAML Certificates

Token signing certificate		 Edit
Status	Active	
Thumbprint	A1 [REDACTED]	
Expiration	10/5/2025, 2:20:54 PM	
Notification Email	haider.jarral@illumio.com	
App Federation Metadata Url	https://login.microsoftonline.com/68b76eeb-dd53... 	
Certificate (Base64)	Download	
Certificate (Raw)	Download	
Federation Metadata XML	Download	




Verification certificates (optional) (Preview)  Edit

Required	No
Active	0
Expired	0

- On the **Set up Illumio SSO** tile, copy and preserve the following URLs that you'll later paste into the Illumio PCE SAML setup.

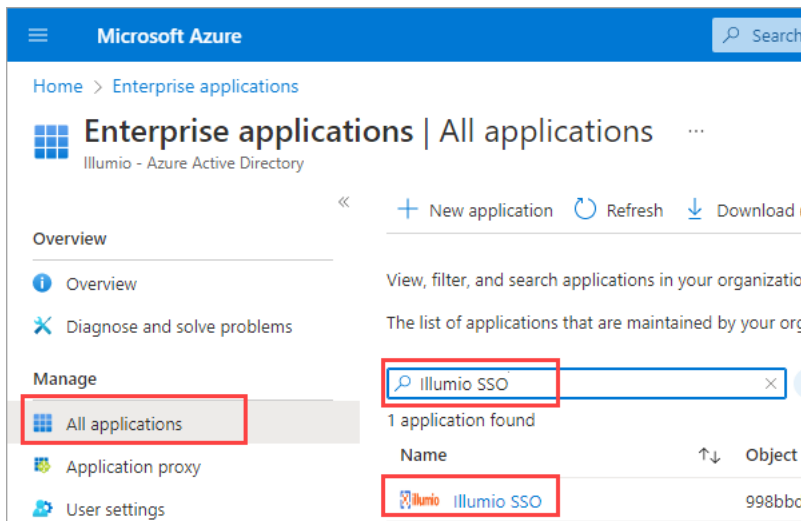
Set up Illumio SSO

You'll need to configure the application to link with Azure AD.

Login URL	https://login.microsoftonline.com/68b76eeb-dd53.. 
Azure AD Identifier	https://sts.windows.net/68b76eeb-dd53-4531-955.. 
Logout URL	https://login.microsoftonline.com/68b76eeb-dd53.. 

STEP 3: Create and assign a test user in Azure AD

- In Azure, go to **Azure Active Directory**.
- In the left pane, click **Users** and then **All users**.
- Click **+ New user**.
- In the **User** properties:
 - In the **Name** field, enter a name (Example.Name).
 - In the **User name** field, enter the user name in the form of an email address (Example.Name@example.com).
 - Select **Show password**, and then make a note of the value that appears in the **Password** box.
- Click **Create**.
- Go to **Home > Azure Active Directory**.
- Under **Overview > Manage**, click **Enterprise applications > All applications**.
- Search for and click the **Illumio SSO** app.



9. In the left pane under **Manage**, click **Users and Groups**.
10. Click **+ Add user/group**.
- .
11. On the **Add Assignment** page, click **Users and groups**.
12. In the **Users and groups** panel that opens, click the user you created in a previous step (Example.Name).
13. Click **Select**.
14. On the **Add Assignment** page under **Select a role**, click one of the roles you created in a previous step.
15. Click **Assign**.

STEP 4: Configure SAML SSO settings in the Illumio PCE

In this procedure you'll paste the following information that you copied and preserved from Azure:

- Certificate (Base64)
- Azure Login URL
- Logout URL

1. In the Illumio PCE Web Console, go to **Access Management > Authentication**.
2. On the **SAML** tile, click **Configure**.
3. Click **Edit**.
4. In the **Information from Identity Destination** section, enter the following information that you obtained from Azure AD:
 - **SAML Identity Destination Certificate**: Open the certificate that you downloaded and then copy and paste the contents.
 - **Remote Login URL**: Paste the Login URL you copied from Azure AD.
 - **Logout Landing URL**: Paste the Logout URL you copied from Azure AD.
5. In the **Information for Identity Destination** section:
 - a. Choose an authentication method:
 - **Unspecified** uses the IdP default authentication mechanism.
 - **Password Protected Transport** requires the user to log in with a password in a protected session.
 - b. If you want to require users to re-enter login credentials to access Illumio (even if the session is still valid), select **Force Re-authentication**. This allows users to log in to the PCE using login credentials different from their default computer login credentials.
6. Click **Save**.

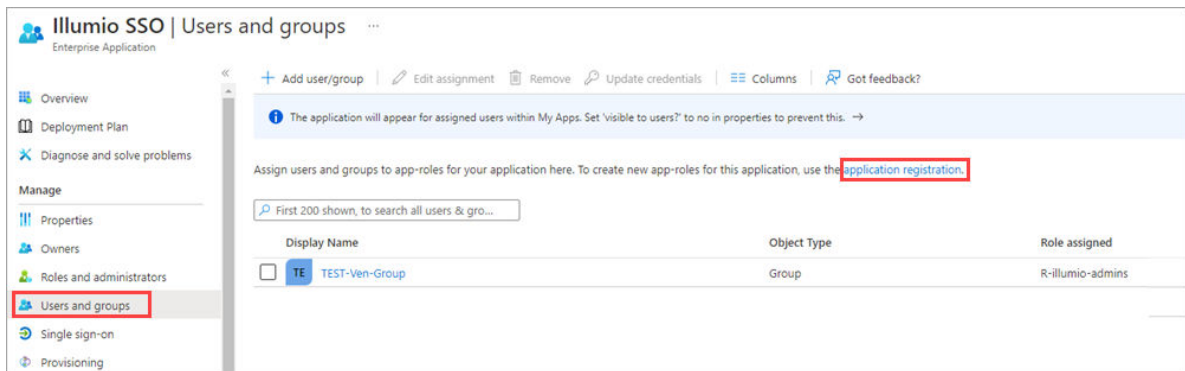
STEP 5: Create App Roles in Azure AD

In this step you'll create app roles in Azure AD that you'll map to roles in the Illumio PCE Web Console.

For reference in this step, here's a list of the Global Roles available in the PCE Web Console:

- Global Organization Owner
- Global Administrator
- Global Viewer
- Globally Policy Object Provisioner

1. In Azure AD, go to **Users and Groups** and then click **application registration**.



2. Create the roles you want by clicking **+ Create app role** and entering the required information for each role:
 - **Display name:** For example, enter one of the Global Roles that appear in the PCE Web Console.
 - **Value:** This must match the name you'll enter in the **Add External Groups** dialog box.
 - **Description:** The description will appear as help text in the app assignment and consent experiences.
3. Click **Apply** for each role that you create.
4. Delete the default app role **msiam_access**.

Note: You first need to disable the default app role before you can delete it.

 - a. Click **msiam_access** to open the **Edit app role** panel.
 - b. Deselect **Do you want to enable the app role?**
 - c. Click **Apply**. The side panel closes.
 - d. Click **msiam_access** again to open the **Edit app role** panel again.
 - e. Click **Delete**.

When you're done creating roles in Azure AD, the **App roles** section should look similar to this:

App roles				
App roles are custom roles to assign permissions to users or apps. The application defines and publishes the app roles and interprets as permissions during authorization.				
How do I assign App roles				
Display name	Description	Allowed member types	Value	ID
Global Organization O...	Global Organization Owner	Users/Groups	GOO	309c156d
Global Administrator	Global Administrator	Users/Groups	GA	f6473e65-
Global Viewer	Global Viewer	Users/Groups	GV	cb677852
Global Policy Object P...	Global Policy Object Provisioner	Users/Groups	GPOP	d07b17b1

STEP 6: Assign users and groups to app roles in Azure AD

In this step, you'll assign users and groups to the app roles you created.

1. In Azure AD, go to **Users and groups**.
2. Select the Illumio SSO app.
3. Click **Remove** to remove the current app assignments.
4. Click **Yes** to confirm removal.
5. Click **Add user/group**.
6. On the **Add Assignment** page, assign desired role(s) to users or groups:
 - a. Under **User and groups**, click **None Selected**.
 - b. In the **Users and groups** panel that opens, search for your desired user/group, click to select it, and then click **Select** at the bottom of the panel.
 - c. Back on the **Add Assignment** page, under **Select a role***, click **None Selected**.
 - d. In the **Select a role** panel that opens, find and click the role you want to assign, and then click **Select** at the bottom of the panel.
 - e. Back on the **Add Assignment** page, click **Assign** at the bottom of the page.
 - f. Repeat these sub-steps for each user and/or to which you want to assign app roles.

STEP 7: Add External Groups and assign roles in the PCE Web Console

In this step, you'll add external groups in the PCE Web Console and assign them the relevant global or scoped roles in Illumio RBAC.



TIP

Alternatively, you can add individual users by going to the **External Users** tab and following the onscreen prompts.

1. On the PCE Web Console, go to **Access Management > External Groups**.
2. Click **Add**.
3. In the **Add External Group** dialog box:
 - Enter a **Name**.
 - Enter an **External Group**.



IMPORTANT

This must match the **Value** that you specified for the app role.

- Click **Add**.

4. Repeat for additional groups.

Add External Group

*

Name

Global Organization Owner

*

External Group

GOO

Cancel

Add

Access Management – External Groups	
Global Roles	Scopes
External Groups	External Users
<div><div>+ Add</div><div>– Remove</div></div>	
Select a principal	
Customize columns	
<input type="checkbox"/>	Name
<input type="checkbox"/>	Global Administrator
<input type="checkbox"/>	Global Organization Owner
<input type="checkbox"/>	Global Policy Object Provisioner
<input type="checkbox"/>	Global Viewer

5. Click to open a group you created in the above step.
6. Click **Add Role > Add Global Role** or **Add Scoped Role**.
7. In the **Access Wizard**, select the appropriate **Role** and then click **Grant Access**.
8. Repeat for additional groups.

Access Management – Access Wizard

Scope All

Name ml-test

Email or Username ml-test-group

1 Select Roles

- ☒ **Global Viewer**
Global read-only access to all resources
- ☐ **Global Policy Object Provisioner**
Provision Services, IP Lists, Label Groups, and Security Settings. Read-only access to all other resources.
- ☐ **Global Administrator**
Manage all resources and Security Settings. Cannot manage users and roles.
- ☐ **Global Organization Owner**
Manage all resources, users and Security Settings.

Summary Scope All

Principals ml-test

Role Please select a role

[Cancel](#) [Grant Access](#)

STEP 8: Turn on SAML authentication in the PCE Web Console

1. In the PCE Web Console, go to **Access Management > Authentication**.
2. On the SAML tile, click **Configure**.
3. On the SAML page, click **Turn On** and then click **Confirm**.

SAML

Local (In use) **SAML** LDAP

Off SAML authentication is not active. Click Turn On to enable SAML

[Turn On](#)

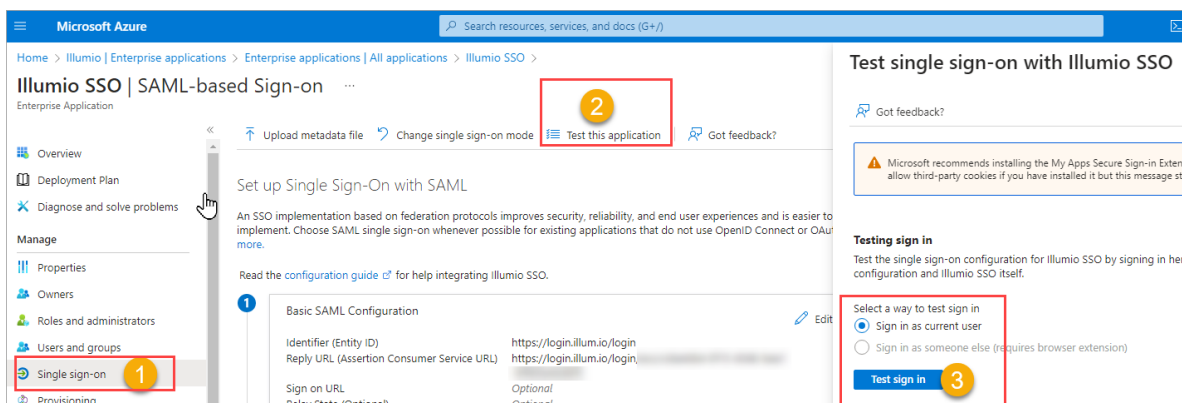
[Edit](#)

SSO method SAML

STEP 9: Test SSO

Perform this procedure to test the SSO authentication you configured in the previous steps.

1. In Azure AD, go to **Single sign-on**.
2. Click **Test this application**.
3. In the panel that opens, select a way to sign in and then click **Test sign in**.



4. If the test is successful, the PCE will log you in to the **Welcome to Illumio** screen.

Okta Single Sign-on

This section explains how to configure SSO for user authentication with the PCE using Okta as your IdP.

Prerequisite for Okta SSO

Before you begin, make sure you have the following information from your Okta account:

- x.509 certificate
- Remote Login URL
- Logout Landing URL



NOTE

Your PCE user account must have Owner or Admin privileges to perform this task.

Configure the PCE for Okta SSO

1. From the PCE web console menu, choose **Access Management > Authentication**.
2. On the Authentication Settings screen, locate the SAML configuration panel and click **Configure**.
3. Enter the following information:
 - **SAML Identity Provider Certificate:** Paste your Okta x.509 certificate (in PEM text format):
 - **Remote Login URL:** Enter the Okta Remote Login URL.
 - **Logout Landing URL:** Enter the Okta Logout Landing URL.
4. In the Information for Identity Provider section, choose the Access Level for the users who will use Okta to authenticate with the PCE. When you select No Access, SSO users from your Okta account will have to be added manually before they can log into the PCE.
5. In the Information for Identity Provider section, make note of the following fields:
 - Issuer
 - Assertion Consumer URL

6. Select the authentication method from the drop-down list:
 - **Unspecified:** Uses the IdP default authentication mechanism.
 - **Password Protected Transport:** Requires the user to log in with a password using a protected session.
7. To require users to re-enter their login information to access Illumio (even if the session is still valid), check the Force Re-authentication checkbox. This allows users to log into the PCE using a different login than their default computer login and is disabled by default.

**NOTE**

When SSO is configured both in Illumio Core and for the IdP, the preferences in Illumio Core are used. When SSO is not configured in Illumio Core, the default IdP settings are used.

8. Click **Save**.
9. Log into your Okta account.
10. Select the Illumio Core app, select the General tab, and click **Edit**.
- .
11. Enter the values you copied from the Information for Identity Provider section of the PCE SSO Configuration page.

The screenshot shows the Okta Admin Console interface. At the top is a blue navigation bar with the Okta logo and links to Dashboard, Directory, Applications, Security, Reports, and Settings. Below this is a card for the 'Illumio ASP' application, which is 'Active'. Below the card are tabs for General, Sign On, Import, People, and Groups. The 'General' tab is selected. Below the tabs is the 'App Settings' modal. The modal has a 'Cancel' button in the top right. It contains the following fields and options:

- Application label:** Illumio ASP. Below the field is the text: 'This label displays under the app on your home page'.
- Assertion Consumer URL:** https://[redacted].com/login/acs/bcc9a9f5-2be8-42cc-9626-f[redacted]. Below the field is the text: 'Please, enter your Assertion Consumer URL'.
- Issuer:** https://[redacted].com/login. Below the field is the text: 'Please, enter your Issuer'.
- Application visibility:** Two checkboxes:
 - ☐ Do not display application icon to users
 - ☐ Do not display application icon in the Okta Mobile App

A red box highlights the 'Assertion Consumer URL' and 'Issuer' fields and their respective labels.

12. Click **Save**.

Your PCE is now configured to use Okta SSO for authenticating users with the PCE.

OneLogin Single Sign-on

This section describes how to configure SSO for OneLogin.

Configure SSO for OneLogin

This task shows you how to configure SSO for authenticating users with the PCE using OneLogin as your Identity Provider (IdP).

Before you begin, make sure you have the following information from your OneLogin account:

- x.509 certificate
- SAML 2.0 Endpoint (HTTP)
- SLO Endpoint (HTTP)



NOTE

Your PCE user account must have Owner or Admin privileges to perform this task

To configure the PCE for OneLogin SSO:

1. From the PCE web console menu, choose **Settings > SSO Config**.
2. Click **Edit**.
3. Select the Enabled checkbox for SAML Status.
4. Enter the following information:
 - **SAML Identity Provider Certificate:** Paste your OneLogin x.509 certificate (in PEM text format).
 - **Remote Login URL:** Enter the OneLogin SAML 2.0 Endpoint (HTTP) URL.
 - **Logout Landing URL:** Enter the OneLogin SLO Endpoint (HTTP) URL.
5. In the Information for Identity Provider section, choose the Access Level for the users who use OneLogin to authenticate with the PCE. When you select No Access, SSO users from your OneLogin account will have to be added manually before they can log in to the PCE.
6. In the Information for Identity Provider section, make note of the following fields:
 - Issuer
 - Assertion Consumer URL
 - Logout URL

You will enter this information into your OneLogin SSO configuration.
7. Select the authentication method from the drop-down list:
 - **Unspecified:** Uses the IdP default authentication mechanism.
 - **Password Protected Transport:** Requires the user to log in with a password using a protected session.
8. To require users to re-enter their login information to access Illumio (even if the session is still valid), check the Force Re-authentication checkbox. This allows users to log in to the PCE using a different login than their default computer login and is disabled by default.

**NOTE**

When SSO is configured both in Illumio Core and for the IdP, the preferences in Illumio Core are used. When SSO is not configured in Illumio Core, the default IdP settings are used.

9. Click **Save**.
10. Log in to your OneLogin account.
- .
11. Select the Illumio Core app, and then click the Configuration tab.
12. Enter the values copied from the Information for Identity Provider section of the PCE SSO configuration page.

USERS APPS ACTIVITY SETTINGS

← Illumio ASP MORE ACTIONS SAVE

Info **Configuration** Parameters Rules SSO Access Users

Application Details

Issuer

Assertion Consumer URL

Logout URL

Enter PCE 'Information for Identity Provider' here

This information may be found on the SSO Config page of the PCE web console (located under the User menu).

13. Click **Save**.
- Your PCE is now configured to use OneLogin SSO for authenticating users with the PCE.

Ping Identity Single Sign-on

This section explains how to configure SSO for authentication users with the PCE using Ping Identity as your Identity Provider (IdP).

Configure SSO for Ping Identity

Before you begin, make sure you have this information from your Ping Identity SSO account:

- x.509 certificate
- Remote Login URL
- Logout Landing URL

**NOTE**

Your PCE user account must have Owner or Admin privileges to perform this task.

To configure the PCE for Ping Identity SSO:

1. From the PCE web console menu, choose **Access Management > Authentication**.
2. On the **SAML** tile, click **Configure**.
3. On the SAML page, click **Edit**.
4. In the Information From Identity Provider section, enter the following information:
 - **SAML Identity Provider Certificate:** Paste your Ping Identity x.509 certificate (in PEM text format).
 - **Remote Login URL:** Enter the Ping Identity Remote Login URL.
 - **Logout Landing URL:** Enter the Ping Identity Logout Landing URL.
5. In the Information for Identity Provider section, make note of the following fields:
 - Issuer
 - NameID Format
 - Assertion Consumer URL
 - Logout URL
6. Select the authentication method from the drop-down list:
 - **Unspecified:** Uses the IdP default authentication mechanism.
 - **Password Protected Transport:** Requires the user to log in with a password using a protected session.
7. To require users to re-enter their login information to access Illumio (even if the session is still valid), check the Force Re-authentication checkbox. This allows users to log in to the PCE using a different login than their default computer login and is disabled by default.



NOTE

When SSO is configured both in Illumio Core and for the IdP, the preferences in Illumio Core are used. When SSO is not configured in Illumio Core, the default IdP settings are used.

8. Click **Save**.
9. Click **Turn On** to enable SAML, and then click **Confirm**.
10. Log in to your Ping Identity account.
- .
11. Select the Applications tab and add the Illumio app.
12. Click **Edit** and enter the following values you just noted from Illumio:
 - **ACS URL:** Enter the value from the Assertion Consumer URL field in the PCE web console.
 - **Entity ID:** Enter the value from the Issuer field in the PCE web console.
 - **Single Logout Endpoint:** Enter the value from the Logout URL field in the PCE web console.
 - **Single Logout Response Endpoint:** Enter the value from the Logout URL field in the PCE web console.

The screenshot shows the 'My Applications' configuration page in the Ping Identity Admin console. The page is titled 'My Applications' and shows a list of applications. The application 'Illumio ASP' is selected, and its configuration page is displayed. The configuration page is titled '1. Configure your connection' and contains several fields for SSO configuration. The fields are: 'ACS URL' (https://\$(Enter Assertion Consumer U), 'Entity ID' (\$(Enter Issuer from the SSO Config p), 'Target Resource' (empty), 'Single Logout Endpoint' (https://\$(Enter Logout URL from the S), 'Single Logout Response Endpoint' (https://\$(Enter Logout URL from the S), 'Verification Certificate' (Choose File, No file chosen), 'Force Re-authentication' (checkbox), and 'PingOne dock URL' (Default PingOne dock URL: https://sso.connect.pingidentity.com/sso/sp/intsso?saasid=27af9ebf-f019-44f8-9b31-c6dc51dae78c&idpid=58d7f05a-ad70-4da6-812f-5706dc3a27a7, Use Custom URL). The 'Continue to Next Step' button is highlighted.

Welcome, [Admin Pelham](#)

[Dashboard](#) [Applications](#) [Users](#) [Setup](#) [Account](#) [Help](#)

[My Applications](#) [Application Catalog](#)

My Applications

[Applications](#) / [My Applications](#)

Applications you've added to your account are listed here.

- Active applications are enabled for single sign-on (SSO).
- Details displays the application details.

Application Name	Type	Status	Enabled
Illumio ASP	SAML	Incomplete	Yes <input type="checkbox"/> Remove

1. Configure your connection

Assign the attribute values for single sign-on (SSO) to the application.

Upload Metadata [Or use URL](#)

ACS URL *

Replace the parameter(s) '\$(Enter Assertion Consumer URL from the SSO Config page of the PCE web console)' above with your configuration information.

Entity ID *

Replace the parameter(s) '\$(Enter Issuer from the SSO Config page of the PCE web console)' above with your configuration information.

Target Resource

Single Logout Endpoint *

Single Logout Response Endpoint *

Verification Certificate No file chosen

Force Re-authentication ☐

PingOne dock URL

Default PingOne dock URL

NEXT: Attribute Mapping

13. Click **Continue to Next Step**.

14. You will now configure the SAML_SUBJECT attribute mapping. Under Advanced Attribute Mapping, next to the Name ID Format to send to SP, select `urn:oa-sis:names:tc:SAML:1.1:nameid-format:emailAddress`.

Advanced Attribute Options

Advanced Attribute Options for SAML_SUBJECT

Advanced Attribute Options

NameIDFormat ⓘ

Name ID Format to send to SP:

urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified

urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName

urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName

urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified

urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos

urn:oasis:names:tc:SAML:2.0:nameid-format:entity

urn:oasis:names:tc:SAML:2.0:nameid-format:persistent

Attribute Mapping

You can build an attribute mapping using

An example of a possible SAML_SUBJECT

firstName + "." + lastName + "

SAML_SUBJECT = SAML_SUBJECT

IDP Attribute Name or Literal Value	As Literal	Function
1 SAML_SUBJECT	<input type="checkbox"/> As Literal	

Close

Save

15. Click **Save.**

Your PCE is now configured to use Ping Identity SSO for authenticating users with the PCE.

VEN Administration Guide

Overview of VEN Administration

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

About This Administration Guide

This guide shows you how use `illumio-ven-ctl` (for Linux, AIX, and Solaris) and `illumio-ven-ctl.ps1` (for Windows) and other commands to administer the Virtual Enforcement Node (VEN) on a managed workload for operational tasks such as start/stop, suspend, and other functions on the VEN and with the Policy Compute Engine (PCE) in an on-premise deployment.

How To Use This Guide

The VEN Administration Guide has several main divisions:

- Overview of VEN Software Architecture and Description of Components.
- VEN deployment models
- Command-line-oriented sections with syntax examples for `illumio-ven-ctl` for on-workload managing the VEN.
- Basic Theory of VEN Operations.

Before Reading This Guide

Illumio recommends that you be familiar with the following topics before you follow the procedures in this guide:

- Your organization's security goals
- The Illumio Core platform
- General computer system administration of Linux and Windows operating systems, including startup/shutdown, and common processes or services
- Linux/UNIX shell (bash) and Windows command line
- TCP/IP networks, including protocols and well-known ports

Notational Conventions in This Guide

- Newly introduced terminology is italicized. Example: *activation code* (also known as pairing key)
- Command-line examples are monospace. Example: `illumio-ven-ctl --activate`
- Arguments on command lines are monospace italics. Example: `illumio-ven-ctl --activate activation_code`
- In some examples, the output might be shown across several lines but is actually on one single line.
- Command input or output lines not essential to an example are sometimes omitted, as indicated by three periods in a row. Example:

```
...
some command or command output
...
```

VEN Architecture and Components

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

Basic Concepts for Illumio Core Software

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

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

Once installed, the VEN performs the following tasks:

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

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

Activation or Pairing

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

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

Pairing and Activating the VEN

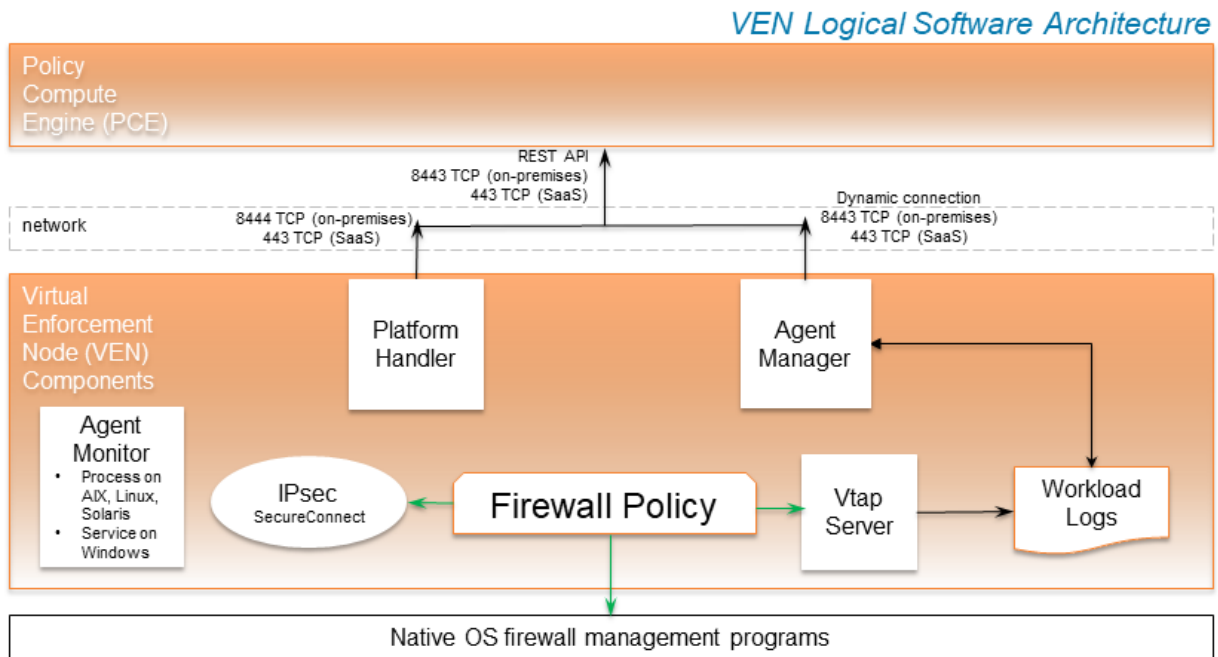
1	The VEN is installed.	The PCE remains unaware the VEN is present.
2	The VEN and the PCE are paired.	The PCE uses a pairing key (activation code) to pair with the VEN. After pairing, the PCE becomes aware of the VEN.
3	The VEN is activated.	The VEN uses an activation code generated by the PCE. After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

Unpairing or Deactivating the VEN

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

VEN Architectural Diagram

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



1. The VEN reports to the PCE the status of the workloads.
2. The PCE computes a unique security policy for each managed workload and transmits it to the VEN.
3. The VEN receives the policy and it programs a firewall by using the firewall platform of the OS. The VEN supports the following firewall platforms:
 - a. iptables (older Linux)
 - b. nftables (newer Linux)
 - c. Packet Filter (newer Solaris)
 - d. Ipfilter (older Solaris)
 - e. Windows Filtering Platform (Windows)
4. When the VEN is finished programming a firewall for each workload, it reports back to the PCE. The PCE then considers these workloads as having a *synced* policy.

Main Components of the VEN

VEN Process	Description	Linux/AIX/Solaris User	Windows User
AgentManager	<ul style="list-style-type: none"> Manages PCE-driven uninstallation and upgrades. All actions relating to active service reporting. Mines the workload's system information, such as network interfaces, and listening processes, and sends them to the PCE. Sends heartbeats to the PCE. Calls netstat periodically for connection status through a shell script or with a direct program call. 	root	LOCAL SYSTEM
Platform-Handler	<ul style="list-style-type: none"> Firewall configuration via native OS mechanisms. Tamper detection and protection. Upgrades and uninstallation. 	root	LOCAL SYSTEM
VtapServer	<ul style="list-style-type: none"> Windows: VTAP runs under the "Local System" account. Retrieves traffic flow data from the ilwfp kernel mode driver (Windows) or firewall (other platforms) and generates flow logs in a database. Receives events from the firewall on blocked packets and allowed connections. 	root	LOCAL SYSTEM
AgentMonitor	<ul style="list-style-type: none"> Service account: NT Authority/Local System Monitors VEN processes or services and restarts them when necessary. 	root	LOCAL SYSTEM

SecureConnect Architecture

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

IPsec runs as root in LOCAL SYSTEM.

VEN Interactions with Files and Components

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

The VEN interacts with the following files and components:

Linux/AIX/Solaris

Function	Description	File/Location
Root file	DATA_ROOT is a variable that points to a filepath.	/opt/illumio_ven_data (by default)
Package repository	INSTALL_ROOT is a variable that points to a filepath.	/opt/illumio_ven (by default)
System initialization	Initializes system	/etc/illumio_ven (typically)

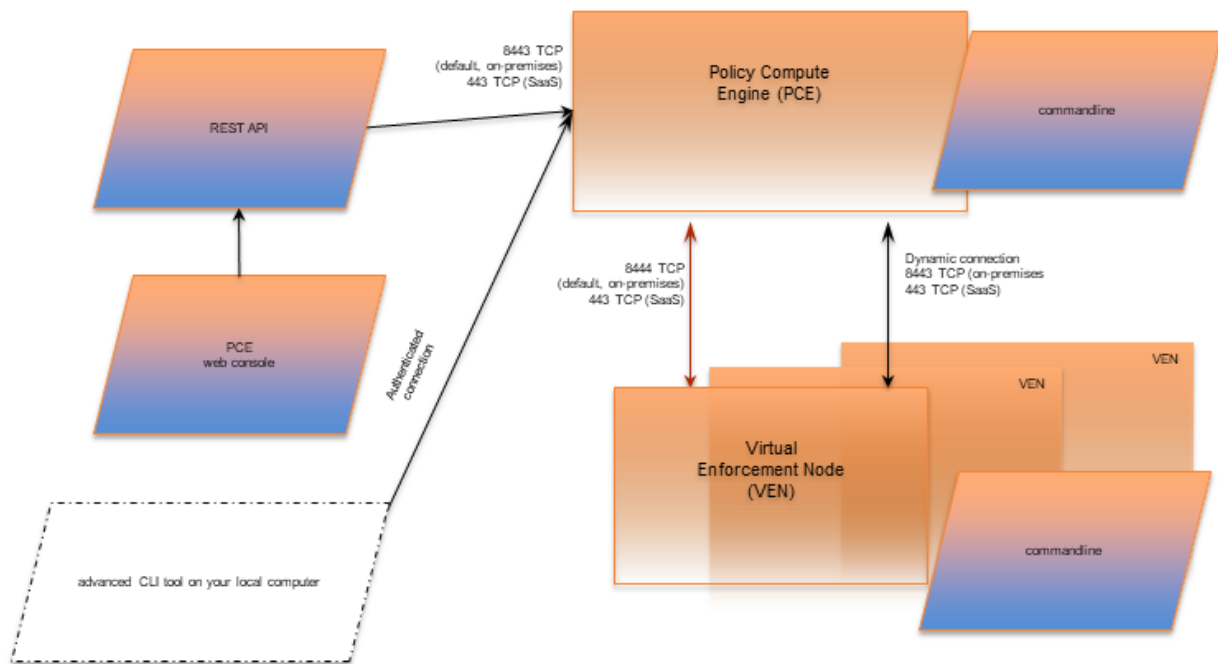
Function	Description	File/Location
Persistent install log	Persistent install log	<code>/var/log/illumio.log</code>
Firewall	Dynamically adds IPs to ipsets:	Snoop on special packets.
	Strongswan IPSec system.	Snoop on Security Associations.
	Read system files (e.g., netstat).	<code>/proc</code>

Windows

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

Management Interfaces for the VEN and PCE

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

PCE and VEN Management Interfaces

Interface	Notes	See...
PCE web console	With the PCE web console, you can perform many common tasks for managing Illumio Core.	Security Policy Guide
PCE command line	Use of the command line directly on the PCE. A primary management tool on the PCE is the command line <code>illumio-pce-ctl</code> control script. You can perform many common tasks for managing the Illumio Core on the PCE command line, including installing and updating the VEN.	PCE Administration Guide
PCE advanced command-line tool	From your own local computer, you can run the PCE advanced CLI tool for many management tasks on the PCE's resource objects: <ul style="list-style-type: none"> Importing vulnerability data for analysis with Illumination®. Importing/exporting security policy rules. Managing security policy rules and rule sets, labels, and other resources. 	PCE CLI Tool Guide
REST API	With the Illumio Core REST API, you can perform many common management tasks. One use is to automate the management of large groups of workloads, rather than each workload individually. The endpoint for REST API requests is the PCE itself, not the workload; the REST API does not communicate directly with the VEN.	REST API Developer Guide
VEN command line	A primary management tool on the VEN command line is the <code>illumio-ven-ctl</code> control script.	VEN Administration Guide

VEN Supported Interfaces

Windows

- Ethernet
- Tunnel
- WLAN (Endpoint only)
- PPP (Endpoint only)

Linux/Unix

- Ethernet
- Tunnel
- Infiniband
- GRE
- Loopback

About VEN Administration on Workloads

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

Workload Policy States

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

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

VEN Enforcement Characteristics

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

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

Work-load En-force-ment State	VEN Mode	VEN Visibility Level	Log Traffic
Idle	Idle	Limited	Limited
Visibility Only	Illumina-ted	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 Collec-tion	VEN logs byte counts in addition to connection details for allowed, blocked, and potentially blocked traffic

Work-load En-force-ment State	VEN Mode	VEN Visibility Level	Log Traffic
Selective	Selective	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
Full	Enforced	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

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

VEN Features by Initial Release

The following tables list key Illumio Core features by their introductory release.

VEN Features in Release Pre-19.3.0

Feature	Initial Release
Firewall coexistence	Pre-19.3.0
illumio-ven-ctl start/stop/activate/unpair	Pre-19.3.0
illumio-ven-ctl unpair open[saved]recommended	Pre-19.3.0
illumio-ven-ctl suspend	Pre-19.3.0
IPSec (SecureConnect)	Pre-19.3.0
Kerberos PKI-based Pairing on Solaris/AIX	Pre-19.3.0
PCE Repo Upgrade	Pre-19.3.0
Process-based Policies	Pre-19.3.0
Solaris Zone Support	Pre-19.3.0

Feature	Initial Release
Support report	Pre-19.3.0

VEN Features in Release 19.3.x

Feature	Initial Release
Compatibility Report for IPv6 Support	19.3
Custom iptable Rules	19.3
Easy installation of VEN on container hosts	19.3
Ignored Interfaces on Windows VENs	19.3
Management of Conntrack Table Size	19.3
Modes: idle, illuminated, enforced	19.3
nftables for RHEL 8	19.3
Solaris 11.4 Support	19.3
Support Reports New Options	19.3
Faster Supercluster Full Restore	19.3.0
FQDN policy on Domain controller/DNS server	19.3.0
State Table Sizes on AIX and Solaris	19.3.0
illumio-ven-ctl deactivate	19.3.0
CRI-O Support	19.3.1
Loadbalancer TCP port 8302 and	19.3.1
TCP+UDP port 8302 Enhancements	
Docker/ContainerD/CRIO	19.3.1
SLES on Power Series hardware	19.3.2
Oracle Exadata Support	19.3.4
Oracle ZDLRA Support	19.3.4
FQDN-Based Rules Enhancements	19.3.5
LDAP Authentication	19.3.5
Aggressive Tampering Protection for nftables	19.3.6
Illumio Core REST API	19.3.6

Feature	Initial Release
Debian 11 Support	19.3.7
IBM Z Support	19.3.7

VEN Features in Release 20.x

Feature	Initial Release
Agent Monitor	20.1.0
REJECT Rules	20.1.0
Workloads and VENs Separation	20.1.0
Flow Duration Attributes	20.2.0
IPv6 for Linux and Windows VENs	20.2.0
IPv6 for VEN	20.2.0
IPv6 is Enabled by Default on Datacenter VENs	20.2.0
Software Management from PCE	20.2.0
Stopped Status	20.2.0
Tamper Detection	20.2.0
Clone Detection	20.2.0 (Edge 20.1, Core 20.2)
Selective Enforcement	20.2.0-PCE

VEN Features in Release 21.x

Feature	Initial Release
Core 21.2.0, Illumio previewed the Reports feature	21.2.0
Enforcement Boundaries	21.2.0
Linux Pairing Script Activation for Proxy Servers	21.2.0
Network-Specific Policy	21.2.0
Uninterrupted Traffic between the VEN and the PCE	21.2.0
Network_deny List	21.2.0-PCE
Adaptive User Segmentation	21.2.0-VEN
Explorer Allows Label Search of All Types	21.2.1
Open Source Package Updates for 21.2.1	21.2.1

Feature	Initial Release
RHEL 8 support for PCE	21.2.1
Supercluster 8-Region Support in 21.2.1	21.2.1
Syslog Forwarding Change	21.2.1
Threshold Configuration Settings	21.2.1
File Settings Option	21.2.1
VEN Package Format Changes	21.2.1
Proxy Fallback Enhancement on Windows	21.2.4
Robustness and Reliability	21.5.0
Run as a Different User with AUS on Windows	21.5.0
IBM Z with RHEL 7 and RHEL 8	21.5.11
Label-based Security Setting for IP Forwarding	21.5.11

VEN Features in Release 21.x-C (Container)

Feature	Initial Release
Containerized VEN	21.2.0-C VEN
Containerized VEN Base Image	21.2.1-C-VEN

VEN Features in Release 22.x

Feature	Initial Release
Advanced Diags (strace/tcpdump)	22.5.0
Configurable Time for Heartbeat Warning Events	22.2.0
Disable and Enable Enforcement Boundaries	22.2.0
Essential Rule Coverage in Illumination and Explorer	22.2.0
Firewall Script Logging	22.2.0
Traffic Flow Query Report	22.2.0
Wireless Connections and VPNs	22.2.0

VEN Features in Release 23.x

Feature	Initial Release
Extended RHEL 5 Support	23.2.0
Configurable enforcement node type (server or endpoint) in pairing profile	23.2.0

Major VEN Features by Supported OS

The following table lists key VEN features by supported platform.

Feature	Windows	Windows Edge	Linux	RHEL 5	C- VEN	Cen- tOS8	AIX	Solaris	MacOS (Endpoint)
Firewall	WFP	WFP	IPTables	IPTables	IPTables	NFTables	IPFilter	IPFilter/PF	PF
Firewall coexistence	✓	✓	✓	✓	✓	✓	-	-	✓
Container support	-	-	✓	✓	✓	✓	-	-	-
IPv6	✓	✓	✓	-	✓	✓	-	✓	✓
PCE repo upgrade	✓	✓	✓	✓	-	✓	-	-	✓
Aggressive Tampering Detection	✓	✓	✓	✓	-	-	-	-	-
Process-based policies	✓	✓	-	-	-	-	-	-	-
Extended process path/args (vtap)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Flow-byte counting	✓	✓	✓	-	-	-	-	-	-
Kerberos	✓	✓	✓	✓	✓	✓	✓	✓	✓

Fea- ture	Win- dows	Win- dows Edge	Li- nux	RHEL 5	C- VEN	Cen- tOS8	AIX	So- la- ris	Ma- cOS (End- point)
FIPS	✓	✓	✓	✓	✓	✓	✓	✓	-
FQDN Policies	✓	✓	✓	-	✓	✓	-	-	✓
FQDN Traffic report- ing	✓	✓	✓	✓	✓	✓	-	-	-
IPSec (Secure- Con- nect)	✓	✓	✓	✓	✓	✓	-	-	-
Installer	MSI; EXE (from 21.2.1)	MSI; EXE (from 21.2.1)	pkg	pkg	apk; rpm (from 19.3.2)	pkg	bff	pkg	dmg
Pairing script (oneliner from PCE UI)	✓	✓	✓	✓	✓	✓	-	-	✓
Process- based policies	✓	✓	o e- bpf	o e-bpf	-	-	-	-	o (P1) networ- kexten- sion

**NOTE**

On RHEL 5, machine authentication is not supported.

VEN Policy Sync States

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

- **Active (Syncing):** Policy is currently being applied to the workload. Appears if the VEN is not currently heartbeating but the PCE has not received a goodbye event from the VN, and the disconnect & quarantine threshold timer has not yet been reached. This is appropriate because, from the PCE's point of view, the VEN status is not stopped and the policy sync status is Syncing. Compare with [Syncing \[121\]](#).

**NOTE**

A workload may also have a status of Active (Syncing) if there is a high rate of policy changes taking place, either from user provisioning actions or from VEN environmental policy changes (for example, new VENs being activated or old VENs being deactivated/unpaired).

- **Syncing:** Appears if the PCE has received a goodbye event from a VEN but the decommission offline timer threshold has not yet been reached. This is appropriate because the VEN, although stopped, is not yet removed from policy and therefore has not yet been marked as **Offline**. When the offline timer expires, the VEN's status transitions to **Stopped** and its IP is removed from policy. Compare with [Active \(Syncing\)](#) [120].
- **Active:** The most recent policy provisioning was successful, no unwanted changes to the workload's firewall have been reported, none of the configured SecureConnect connections are in an erroneous state, and all VEN processes are running correctly.
 - For more information on SecureConnect, see Security Policy Guide.
- **Staged:** The PCE has successfully sent policy to the VEN, and it is staged and scheduled to be applied at a later time. This state only appears when you have configured the Policy Update Mode for the workload to use Static Policy. See Static Policy and Staged Policy for information. For information, see "Types of Illumio Policy" in the Security Policy Guide.
- **Error:** One of the following errors has been reported by the VEN:
 - The most recent policy provisioning has failed.
 - Unwanted changes to the workload's firewall have been reported.
 - At least one VEN process is not running correctly.
 - There is a SecureConnect or Machine Authentication policy, but leaf certificates are not set up properly.
- **Warning:** At least one SecureConnect connection is in an erroneous state, and either the most recent policy provisioning was successful or no unwanted changes to the workload's firewall have been reported.
- **Suspended:** Used by admins to debug. Rules programmed into the platform firewall (including custom iptables rules) are removed completely. No Illumio-related processes are running on the workload.

VEN Health Status on Workloads

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

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

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

VEN Process Health

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

Workload Clone Alerts

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

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



NOTE

Automatic Cloned VEN Remediation

For on-prem domain joined Windows workloads, cloned VENs support automatic clone remediation by detecting changes to the workload's domain Security identifier (SID). After the VEN reports such changes to the PCE, the PCE tells the clone to re-activate itself, after which the cloned VEN is remediated and becomes a distinct agent from the original VEN.

VEN Software Management from PCE

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

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

Stopped VEN Status

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

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

Aggressive Tampering Protection for nftables

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

VEN Proxy Support on Linux, AIX, and Solaris

VEN proxy support includes Linux, AIX, Solaris, and Windows devices.

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

Support on IBM Z With RHEL 7 and RHEL 8

In the Illumio Core 19.3 release, Illumio supports installing and operating the VEN on IBM Z systems running Red Hat Enterprise Linux 7 (RHEL 7) and RHEL 8.

Support on SLES 11 SP2

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

From the SLES 11 SP2 Latest Updates:

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

From the SLES 11 SP4 DVD:

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

VEN File Settings Option

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

VEN File Setting: `IPFILTER_TCPCLOSED=<value>`

Ipfilter Setting: `fr_tcpclosed=<value>`

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

Debian 11 Support

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

Windows VEN Proxy Fallback Enhancement

Starting from Illumio Core 21.2.1 and 21.2.2, the VEN automatically detects a web proxy. However, it always attempts to connect directly to the PCE first. In this release, Illumio enhanced the heuristic in the VEN for falling back to the configured web proxy. After an attempt fails to connect to the PCE directly due to an HTTPS intercepting proxy, the VEN falls back to use the configured web proxy.

VEN Enhancements in 21.5.11

The following enhancements were added in Illumio Core 21.5.11.

Support on IBM Z With RHEL 7 and RHEL 8

In this release, the system supports installing and operating the VEN on IBM Z systems running Red Hat Enterprise Linux 7 (RHEL 7) and RHEL 8.

Label-based Security Setting for IP Forwarding

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

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

Uninterrupted Traffic Between the VEN and the PCE

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

IPv6 Support and Features for the VEN

In Illumio Core 20.2.0 and later releases, the VEN supports both IPv4 and Ipv6 address versions and the IP address version appears correctly in the PCE; for example, in the Workload section of the VEN summary page in the PCE web console.

You can configure how the PCE treats IPv6 traffic from workloads. For more information, see "Allow or Block IPv6 Traffic" in the PCE Administration Guide.

The VEN supports IPv6 in the following ways.

IPv6 is Enabled by Default on Datacenter VENs

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

The default settings are as follows:

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

IPv6 Support for Linux and Windows VENs

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

VEN Compatibility Report for IPv6 Support

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

The following command and command options are supported:

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

`illumio-ven-ctl` General Syntax



The `illumio-ven-ctl` is a primary tool for managing VENs on individual workloads. The script varies slightly by platform.

Set PATH Environment Variable

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

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

Command Line Syntax by Platform

Platform	Command	Notes
Linux/AIX/Solaris	illumio-ven-ctl	 IMPORTANT Parameters for the subcommands are preceded by two hyphens: --option1 var --option2 var ...
Windows	illumio-ven-ctl.exe	 IMPORTANT Parameters for the script are preceded by a single hyphen: -option1 var -option2 var ...

Linux/AIX/Solaris Command Line Help

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

Windows Command Line Help

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

Useful VEN and OS Commands

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

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

Verify VEN Version Number

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

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

```
# /opt/illumio_ven/illumio-ven-ctlversion 21.5.0-xxxx
```

- Run the following command on a Windows workload:

```
<VEN Installation Directory>\illumio-ven-ctl.exe version
```

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

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

Commonly Used VEN Commands

Platform	Command	Description
Linux	<code>/opt/illumio-ven/illumio-ven-ctl</code>	VEN Linux shell control script to control VEN control VEN settings and functions
	<code>/opt/illumio-ven/bin/agent_status.sh</code>	Alternative to <code>illumio-ven-ctl status</code>
	<code>ps</code>	Native OS command to list all system processes
	<code>chkconfig</code>	Native OS command to update and query run-level information for system services
Windows	<code>tasklist /svc</code>	Native OS command to display system services
	<code>wf.msc</code>	Native OS command to manage the Windows firewall
AIX/Solaris	<code>/opt/illumio-ven/illumio-ven-ctl</code>	VEN AIX/Solaris shell control script to control VEN control VEN settings and functions
	<code>/opt/illumio-ven/bin/agent_status.sh</code>	Alternative to <code>illumio-ven-ctl status</code>
	<code>/opt/illumio-ven/bin/agent_status.sh</code>	Alternative to <code>illumio-ven-ctl status</code>
	<code>ps</code>	Native OS command to list all system processes
AIX	<code>lssrc</code>	Native OS command to list OS subsystem status
Solaris	<code>svcs</code>	Native OS command to list OS service status

illumio-ven-ctl Command Options by OS

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

Com-mand	Descrip-tion	AIX	Cen-tOS	De-bian	RHEL	So-la-ris	SUSE	Ubun-tu	Win-dows
acti-vate <op-tions>	Activate VEN.	Y	Y	Y	Y	Y	Y	Y	Y
backup	Backup VEN data.	—	Y	Y	Y	—	Y	Y	Y
check-env	Check VEN run-time_env.yml settings.	Y	Y	Y	Y	Y	Y	Y	Y
con-ncheck	Query VEN policy.	Y	Y	Y	Y	Y	Y	Y	
con-nec-tivi-ty-test	Test connec-tivity with PCE.	Y	Y	Y	Y	Y	Y	Y	Y
deac-tivate <op-tions>	Deactivate VEN without uninstalling.	Y	Y	Y	Y	Y	Y	Y	Y
gen-sup-por-tre-report <op-tions>	Generate VEN support re-ports.	Y	Y	Y	Y	Y	Y	Y	Y
pre-prepare	Prepare VEN image.	Y	Y	Y	Y	Y	Y	Y	Y
re-start	Restart VEN services.	Y	Y	Y	Y	Y	Y	Y	Y
re-store	Restore VEN dataillumio-ven-ctl.	—	Y	Y	Y	—	Y	Y	Y
start	Start VEN services.	Y	Y	Y	Y	Y	Y	Y	Y
status	Report VEN status.	Y	Y	Y	Y	Y	Y	Y	Y
stop	Stop VEN services.	Y	Y	Y	Y	Y	Y	Y	Y
sus-pend	Suspend VEN (enter emer-gency state).	Y	Y	Y	Y	Y	Y	Y	Y

Com-mand	Descrip-tion	AIX	Cen-tOS	De-bian	RHEL	So-la-ris	SUSE	Ubun-tu	Win-dows
<code>unpair <op-tions></code>	Unpair VEN.	—	Y	Y	Y	Y	Y	Y	Y
<code>unsuspend</code>	Unsuspend VEN (exit emergency state).	Y	Y	Y	Y	Y	Y	Y	Y
<code>version</code>	Display VEN version.	Y	Y	Y	Y	Y	Y	Y	Y
<code>workloads</code>	Report VEN workload status.	—	Y	Y	—	—	Y	Y	—

VEN State

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

VEN Startup and Shutdown

This topic provides information on starting and stopping VENs.

VEN Startup and Shutdown (illumio.com)

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


Start Up VENs

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

Automatic Startup

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

Plat-form	Command	Notes
Linux/AIX/Solaris	<code>/etc/rc.d/init.d/illumio-ven</code> Or <code>/etc/init.d/illumio-ven</code>	Installs firewall kernel modules if necessary, sets firewall to the desired state.

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

Manual Startup

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

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

Shut Down VENs

At shutdown, the VEN sends a “goodbye” message to the PCE. The PCE marks the workload as offline and initiates a policy recomputation. After the new policy is distributed throughout the network, the workload without the VEN is effectively isolated from the network.

Linux/AIX/Solaris Workload Shutdown

Platform	Command	Notes
Linux/AIX/Solaris/RHEL/CentOS	<code>illumio-ven-ctl stop</code>	<ul style="list-style-type: none"> Stops all VEN processes. The VEN sends a “goodbye” message to the PCE.
Windows	None needed.	<ul style="list-style-type: none"> Service Control Manager (SCM) stops all VEN services. The VEN sends a “goodbye” message to the PCE.

Disable and Enable VENs (Windows only)

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

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

Platform	Action	Command
Windows	• Enable	PS C:\Program Files\Illumio> .\illumio-ven-ctl.ps1 enable
	• Disable:	PS C:\Program Files\Illumio> .\illumio-ven-ctl.ps1 disable

VEN Suspension

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



IMPORTANT

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

About VEN Suspension

When a VEN is suspended, the following is true:

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

Properties of a suspended VEN:

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

- If the PCE is rebooted, the VEN remains suspended.

When a VEN is unsuspended:

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

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

- The REST API
For more information on this method, see "VEN Operations" in the REST API Developer Guide.
- The command line
- The PCE web console
For more information, see [Mark VEN as Suspended Using the PCE Web Console \[133\]](#) in this topic.

Linux VEN: Back Up Custom iptables/NAT Rules



NOTE

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

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

Suspend and Unsuspend Commands

Platform	Action	Command	Notes
Linux/ Unix	• Suspend	<code>\$ illumio-ven-ctl suspend</code> Suspending the VEN... The VEN has been suspended. PCE was notified.	On Linux, be sure to backup your custom configuration. See Linux VEN: Back Up iptables/NAT Rules [132] .
	• Unsuspend	<code>\$ illumio-ven-ctl unsuspend</code> Unsuspending the VEN... The VEN has been unsuspended. PCE was notified.	

Platform	Action	Command	Notes
Windows	<ul style="list-style-type: none"> Suspend Unsuspend 	<pre><VEN Installation Directory>\illumio-ven-ctl.exe suspend Suspending the VEN... The VEN has been suspended. PCE was notified. <VEN Installation Directory>\illumio-ven-ctl.exe unsuspend Unsuspending the VEN... The VEN has been unsuspended. PCE was notified.</pre>	

Mark VEN as Suspended Using the PCE Web Console

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



NOTE

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

To mark a VEN Suspended:

1. Go to **Servers & Endpoints > Workloads**.
2. Click the **VENs** tab.
3. Click the name of the VEN you want to mark as suspended.
4. On the VEN's detail page, click **Mark as Suspended**.
5. Click **Suspend** to confirm the VEN suspension.

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

To clear a VEN's Suspension status:

1. Go to **Servers & Endpoints > Workloads**.
2. Click the **VENs** tab.
3. Click the name of a VEN marked as suspended that you want to mark as unsuspended.
4. On the VEN's detail page, click **Clear Suspension**.
5. Click **Clear** to confirm.

Disable VEN Suspension on Workloads

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

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

**NOTE**

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

Linux VENs

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

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

Examples:

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

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

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

Windows VENs

Disabling the suspend command:

```
<ven_installation_filename>.exe <options> VEN_NO_SUSPEND=1
```

Available options include:

- /install
- /log logfile.log
- /quiet

Example:

```
ven_install_filename.exe /install EN_NO_SUSPEND=1
```

AIX VENs

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

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

Example:

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

Solaris VENs

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

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

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

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

Change the copied file in the following way:

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

Deactivate and Unpair VENs

VEN Deactivation and Unpairing

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

This section describes how to deactivate and unpair the VEN software.

Deactivate and Unpair VENs

This topic describes how to deactivate and unpair VENs by operating system. Additionally, it explains the security implications for performing these tasks and makes recommendations on how to properly deactivate and unpair VENs.

See [VEN Unpairing Details \[138\]](#).

Deactivate Using VEN Command Line

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

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

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

Linux/AIX/Solaris

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

Windows

```
<VEN Installation Directory>\illumio-ven-ctl.exe deactivate
```

Unpair Using VEN Command Line

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

Linux/AIX/Solaris

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

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



NOTE

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

Unpair Options on Linux/AIX/Solaris

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



IMPORTANT

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

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



IMPORTANT

Security Implications: Depending on how old the iptables configuration is on the workload, VEN removal could impact the application.

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



IMPORTANT

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

Windows

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

```
<VEN Installation Directory>\illumio-ven-ctl.exe unpair [recommended | saved | open | unmanaged]
```

Unpair Options on Windows

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



IMPORTANT

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

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



IMPORTANT

Security Implications: Depending on how old the WFP configuration was on the workload, VEN removal could impact the application.

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



IMPORTANT

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

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

Unpair Using System Commands

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



IMPORTANT

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

Linux

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

Windows

- Use the Control Panel to uninstall the VEN.

AIX

- `installp -u illumio-ven`

Solaris

- `pkgrm illumio-ven`

VEN Unpairing Details

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

Linux/AIX/Solaris

- Unpairs the VEN from the PCE.
 - Sends a "deactivate" message to the PCE.
- Restores the host firewall state to the requested or open state if no state is specified.
Possible values of the state are:
 - Open: All ports are open after VEN uninstalls.
 - Saved: The firewall is restored to its state just before the VEN was installed.
- Uninstalls the `illumio-ven` package.
 - Removes program and data files.
 - Removes repo and GPG files and package.

Windows

- Unpairs the VEN from the PCE.
 - Sends a "deactivate" message to PCE.
- Stops all VEN services.
- Unregisters services from Service Control Manager.
- Restores Windows Firewall to requested state.
 - Open: All ports are open after VEN uninstalls.
 - Saved: Restore the firewall to its state just before the VEN was installed.
- Removes Program Files and ProgramData directories.
- Removes VEN registry keys.
- Removes Certificate.
- Unregisters VEN Event provider.

Support Report During Unpairing

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

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

Monitor and Diagnose VEN Status

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

VEN-to-PCE Communication

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

Details about VEN-to-PCE Communication

On Prem

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

- Port 8443 - HTTPS requests
- Port 8444 - long-lived TLS-over-TCP connection

SaaS

The VEN communicates with the Illumio Core Cloud PCE over Port 443 for both HTTPS requests and the long-lived TLS-over-TCP connection.

The VEN uses Transport Level Security (TLS) to connect to the PCE. The PCE certificate must be trusted by the VEN before communication can occur.

The VEN sends the following details to the PCE:

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

The VEN receives the following details from the PCE:

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

Configurable Time for Heartbeat Warning

You can change the threshold for the time the VEN goes without a heartbeat and goes into the Warning state. To change the 15-minute threshold in the PCE interface:

1. Go to **Settings > Offline Timers**.
2. Click **Edit**.
3. In the **Disconnect and Quarantine** section, select **Custom Timeout**.
4. Specify a wait time.
5. Click **Save**.

VEN Connectivity

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

VEN Support for IPv6 Traffic

You can configure how VENs support IPv6 traffic. Go to **Settings > Security** and click the General tab:

For VEN releases 20.2.0 and later, choose one of these options:

- Allow IPv6 traffic according to your policy
- Block IPv6 traffic only when in Full Enforcement. (Traffic will always be allowed on AIX and Solaris workstations.)

For VEN releases pre-20.2.0, choose one of these options:

- Allow all IPv6 traffic
- Block IPv6 traffic only when in Full Enforcement. (Traffic will always be allowed on AIX and Solaris workstations.)

Communication Frequency

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

Function	Frequency	Notes
Firewall policy updates	Real-time if lightning bolts are enabled.	If lightning bolts are displayed or the channel is not functional, policy updates are communicated to the VEN by a heartbeat action.
Active service reporting	See note.	<ul style="list-style-type: none"> • AgentManager performs all active service reporting tasks. • At start-up, a snapshot of processes and ports is sent to the PCE. • Every 24 hours, a snapshot of <i>all</i> listening processes is taken and sent to the PCE.

Function	Frequency	Notes
Interface reports and changes	Event driven.	Only if there are changes to the interfaces; otherwise, no data are sent.
Traffic flow log	Every 10 minutes.	<ul style="list-style-type: none"> The VEN checks if there are logs, and if so, sends them to the PCE. If the PCE is inaccessible, the VEN retains flow summaries for the previous 24 hours but purges logs that are older than 24 hours, with the oldest log at every 24-hour mark. When logs are purged, the VEN locally logs an alert, which is posted to the PCE as an event when connectivity is restored.
Heartbeat	Every 5 minutes.	If the PCE does not receive three consecutive heartbeats, an event is written to the PCE's event log. See also VEN Heartbeats and Lost Agents [141] .
Dead-peer interval	Configurable	Default is 60 minutes (or 12 heartbeats). See also VEN Offline Timers and Isolation [142] .
VEN tampering detection	Within a few seconds on Windows and Linux.	For more information, see Host Firewall Tampering Protection [153] .

VEN Heartbeats and Lost Agents

The VEN sends a heartbeat message every five minutes to the PCE to inform the PCE that it is up and running. If the VEN fails to send a heartbeat, check the workload where the VEN is installed and investigate any connectivity issues. If the VEN continues to fail to send a heartbeat, it eventually is marked Offline, which means it can no longer communicate with the PCE or other managed workloads.

PCE down or network issue and the VEN degraded state

- If the VEN cannot connect to the PCE either because the PCE is down or because of a network issue, the VEN continues to enforce the last-known-good policy while it tries to reconnect with the PCE.
- After missing three heartbeats, the VEN enters the *degraded state*. In the degraded state, the VEN ignores all the asynchronous commands received as lightning bolts from the PCE, except the commands for software upgrades and support reports.
- After connectivity to the PCE is restored, the VEN comes out of the degraded state after three successful heartbeats.

Failed authentication and the VEN minimal state

- If the VEN enters the degraded state because of failed authentications, the VEN enters a state called *minimal*. In the minimal state, the VEN only attempts to connect with the PCE every four hours through a heartbeat.
- If the authentication failure was temporary, the VEN exits the minimal state after its first successful connection to the PCE. Whenever the VEN enters the minimal state, it stops the VTAP service. VTAP is then restarted when the VEN exits the minimal state.
- If Kerberos authentication is used, the VEN attempts to refresh the agent token with a new Kerberos ticket before sending a heartbeat. If the authentication error is not recovered after four hours, the VEN sends a lost-agent message to the PCE which then logs a message in the Organization Events. The message informs the user that the VEN needs to be uninstalled or reinstalled manually on this workload.

VEN Offline Timers and Isolation

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

If the REST API call (goodbye) fails, or if the workload goes offline abruptly (for example, due to a power outage), the PCE stops receiving heartbeats from the workload. After the period of time configured in the PCE web console **Settings > Offline Timers** elapses, the PCE marks the workload offline and recomputes policies for the peer workloads to isolate the offline workload. If no time period has been configured, the default is 60 minutes, or 12 heartbeats.

The `system_task.agent_missed_heartbeats_check` alert triggers an alert to be sent at 25% of the time configured in the offline timer. For example, if the offline timer is configured to 1 hour, an alert is sent after the VEN has not sent a heartbeat for 15 minutes; if the offline timer is configured to 4 hours, an alert is sent after the VEN hasn't sent a heartbeat for 1 hour. If a user has customized the timer, the event will show up when 25% of the timer has elapsed.

Sampling Mode for VENs

If the VEN receives a sustained amount of high traffic per second from many individual connections, the VEN enters Sampling Mode to reduce the load. Sampling Mode is a protection mechanism to ensure that the VEN does not contribute to the consumption of CPU. In Sampling Mode, not every flow is reported. Instead, flows are periodically sampled and logged.

After CPU usage on the VEN decreases, Sampling Mode is disabled and each connection is reported to the VEN. The entry and exit from sampling-mode is automatically performed by the VEN depending on the load on the VEN.

Details about entering and exiting Sampling Mode are captured in `/opt/illumio_ven_data/log/vtap.log`. Look for `Entering` and `Exiting throttle state`.

Linux TCP Timeout Variable

For VENs installed on Linux workloads, the VEN relies on conntrack to manage the `nf_conntrack_tcp_timeout_established` variable.

By default, as soon as the VEN is installed, it sets the `nf_conntrack_tcp_timeout_established` frequency to eight hours (28,800 seconds). Setting this frequency manages workload memory by removing unused connections from the table and thereby increasing performance.

If you change the frequency via `sysctl`, it is reverted the next time the workload is rebooted or the next time the VEN's configuration file is read.

Wireless Connections and VPNs

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

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

**NOTE**

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

Show Amount of Data Transfer

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

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

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

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

The number of bytes includes:

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

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

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

Term	Description
dst_tbi	Destination Delta Bytes In Number of bytes received by the destination in the latest sampled interval, over the flows included in this flow-summary. This is the same as bytes sent by the source. Present in 'A', 'C', and 'T' flow-summaries. source = client = connection initiator, destination = server = connection responder.
dst_dbo	Destination Delta Bytes Out Number of bytes sent by the destination in the latest sampled interval, over the flows included in this flow-summary. This is the same as bytes received by the source. Present in 'A', 'C', and 'T' flow-summaries. source = client = connection initiator, destination = server = connection responder.
inter-val_sec T	Time Interval in Seconds Duration of latest sampled interval over which the above metrics are valid.

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

VEN Status Command and Options

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

The VEN Status Command

```
illumio-ven-ctl status
```

Returns the status of the VEN on the workload.

Linux/AIX/Solaris

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

Example Linux VEN Status return parameters

```
Status for illumio-control:
- Environment Illumio VEN Environment is setup
- venAgentMgr venAgentMgr (pid 23598) is running...
```



```
- IPsec IPsec feature not enabled
- venPlatformHandler venPlatformHandler (pid 23676) is running...
- venVtapServer venVtapServer (pid 23737) is running...
- venAgentMonitor active(running)
```

Agent state: enforced

Linux/AIX/Solaris VEN status field definitions

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

Windows

Example Windows VEN status command:

```
<VEN Installation Directory>\illumio-ven-ctl.exe status
```

Example Windows VEN status return parameters

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

Policy Option for VEN Status

```
illumio-ven-ctl status policy
```

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

Linux/AIX/Solaris

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

Windows

Example Windows VEN status policy command:

```
<VEN Installation Directory>\Illumio>\illumio-ven-ctl.exe status policy
```

Return Description

Example

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

VEN status policy field definitions

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

Health Option for VEN Status

```
illumio-ven-ctl status health
```

Returns whether or not the VEN can write logs locally.



NOTE

This is not the same as PCE health.

Linux/AIX/Solaris

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

Windows

Example Windows VEN status health command:

```
<VEN Installation Directory>\illumio_ven\illumio-ven-ctl status health
```

Return Description

Example

```
{
  "results": [
```

```

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

```

Linux/AIX/Solaris VEN status health field definitions

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

Status Connectivity Option for VEN Status

```
illumio-ven-ctl status connectivity
```

Returns the status of the VEN connectivity with the PCE.

Linux/AIX/Solaris

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

Windows

Example Windows VEN status connectivity command:

Return Description

Example

```

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

```

VEN status connectivity field definitions

Field Name	Definitions
<code>connectivity</code>	JSON object containing most of the connectivity status fields
<code>ips_returned</code>	Number of IP addresses returned for the PCE name
<code>pce</code>	PCE name
<code>port</code>	PCE port number
<code>results</code>	Array containing the PCE IP address, the test result, and the HTTP code
<code>ip</code>	PCE IP address
<code>result</code>	Result of test ("pass" or an error message)
<code>http_code</code>	HTTP code received when the VEN attempted to connect to the PCE IP address
<code>last_successful_hb</code>	Timestamp of the last VEN heartbeat received by the PCE
<code>time_now</code>	Timestamp of the current local time

VEN Logging

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

VEN Traffic Logging

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

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

Querying Flow Log Databases

The `sqlite` command-line tool, which comes with the VEN, is used to query the flow log databases.

Linux/AIX/Solaris Database Query Examples

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

Window Database Query Examples

Query Type	Example
Non-aggregated accepted flows	<code>"c:\Program Files\Illumio\bin\sqlite.exe" c:\ProgramData\Illumio\log\flow.db "select * from flow_view"</code>
Non-aggregated dropped flows	<code>"c:\Program Files\Illumio\bin\sqlite.exe" c:\ProgramData\Illumio\log\flow.db "select * from drop_flow_view"</code>
Aggregated accepted flows	<code>"c:\Program Files\Illumio\bin\sqlite.exe" c:\ProgramData\Illumio\log\flowsum.db "select * from flow_view"</code>
Aggregated dropped flows	<code>"c:\Program Files\Illumio\bin\sqlite.exe" c:\ProgramData\Illumio\log\flowsum.db "select * from drop_flow_view"</code>

List of Local Processes

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

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

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

VEN Firewall Script Logging

The Illumio firewall scripts log all errors and other key information into the `platform.log` file. This log file can help Illumio debug issues.

Traffic Flow Query Report

You can generate, schedule, and email reports which are based off saved and recent filters from Explorer for reporting. The CSV report is downloadable and can be emailed to the user.

Tuning the IPFilter State Table (AIX/Solaris)

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

About State Table Tuning

In most environments, the state table default values are sufficient to handle the number of network connections encountered by Solaris and AIX workloads. However, if your system has a very large number of network connections, you might need to tune the state table. You can do so either before or after VEN activation. Tuning the state table values persists through rebooting, restarting, and suspending the VEN.

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

- `fr_statemax`: 1,000,000
- `fr_statesize`: 250,007
- `fr_state_maxbucket`: 256
- `fr_tcpclosed`: 120

Set a Custom IPFilter State Table Size

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



NOTE

The following file that must be created by the `root` user or the Illumio VEN user `ilo-ven`: `/etc/default/illumio-agent`.

This file cannot be world-readable or -writeable.

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

VEN File Setting	ipfilter Setting	Description
<code>IPFIL- TER_STATE_MAX=<value></code>	<code>fr_statemax</code>	Maximum number of network connections stored in the state table. You must also set <code>IPFILTER_STATE_SIZE</code> .
<code>IPFIL- TER_STATE_SIZE=<value></code>	<code>fr_statesize</code>	Size of the hash table. Must be a prime number. You must also set <code>IPFIL- TER_STATE_MAX</code> . Recommended: Set the hash table size to 1/4 of the number in <code>fr_statemax</code> . This setting allows each hash bucket to contain about 4 states.

VEN File Setting	ipfilter Setting	Description
IPFILTER_STATE_MAXBUCKET=<value>	fr_state_max-bucket	Number of allowed hash collisions before the VEN starts dropping network connections Recommended: Increase this value beyond the default value to avoid dropping network connections.
IPFILTER_TPCPCLOSED=<value>	fr_tcpclosed	Option introduced and supported for Illumio Core 21.2.1 VEN and later. To support NFS traffic so that the workload does not drop this traffic even when a rule exists in the PCE allowing the traffic. This issue occurs due to TCP port number reuse. Recommended: Illumio customers have found that setting the value for the IPFILTER_TPCPCLOSED option to 2 (2 equals 1 second) resolved the issue.

**NOTE**

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

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

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

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

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

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

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

Manage Conntrack Table Size (Linux)

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

About Managing the State Table

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

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

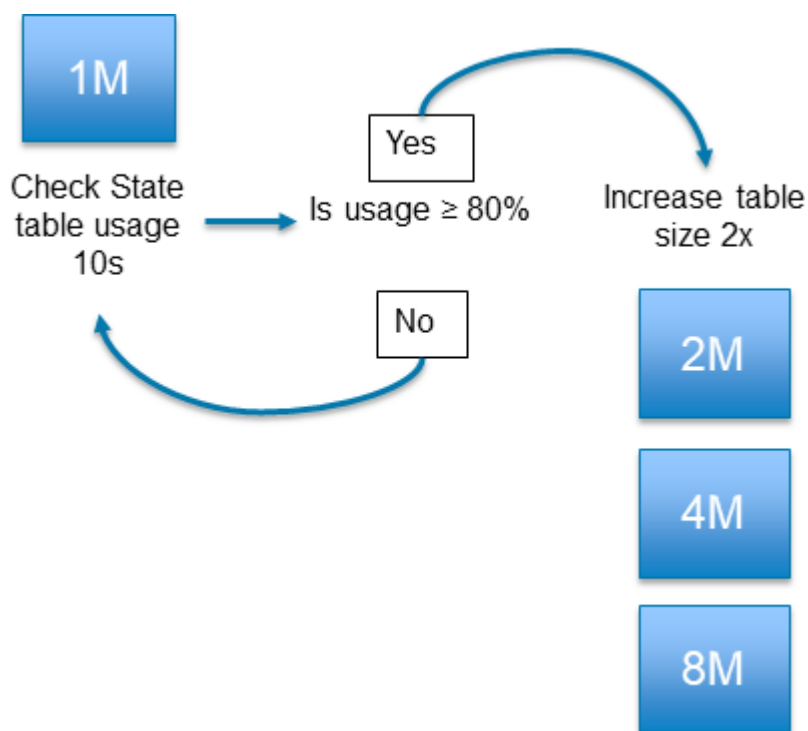
For more information about AIX and Solaris, see [Tuning the IP Filter State Table \(AIX/Solaris\) \[150\]](#).

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

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

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

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



Customizing the VEN Adjustment Behavior

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

Setting	Default	Description
FW_STATE_TABLE_AUTO_RESIZE	True	Indicates whether auto resize of the Conntrack table is required.

Setting	Default	Description
CONNTRACK_MAX	1000000	<ul style="list-style-type: none"> Defines the maximum number of Conntrack table entries. Configures the system value for <code>/proc/sys/net/nf_conntrack_max</code>
CONNTRACK_HASH_SIZE	256000	<ul style="list-style-type: none"> Defines the starting size of the Conntrack hash table. Configures the system value for <code>/sys/module/nf_conntrack/parameters/hashsize</code>

**NOTE**

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

Restrictions for VEN Adjustment

Customizing the VEN adjustment behavior has the following restrictions:

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

VEN Firewall Tampering Detection

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

Automatic History of Firewall Changes

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

Host Firewall Tampering Protection

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

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

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

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

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

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


Host Firewall Tampering Alerts

Host firewall tampering alerts can be viewed:

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

View Tampering Alerts on VEN Host

Workload OS	Procedure
Linux	<p>As root, separately execute the following commands:</p> <p>Tail the VEN log file to see suspected tampering events and hash comparisons:</p> <pre>\$ tail -f /opt/illumio_ven_data/log/platform.log</pre> <pre>INFO: Possible tamper detected... INFO: FW iptables checksums ... (compares security policy hashes to see if anything changed)</pre>

Work-load OS	Procedure
Windows	Check <code>\programdata\illumio\log\platform.log</code> and search <code>"!!!Tampering detected"</code>
<div>  <p>NOTE This alter displays "Filtering Platform Policy Change" when a tampering event is detected. Double-click the alert for detailed information.</p> </div>	

View Tampering Alerts Sent to PCE

PCE Web Console

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

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

Illumio Core REST APIs

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

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

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

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

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

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

```
{
  "href": "/orgs/1/events/some_event_ID",
  "timestamp": "2019-06-17T05:42:10.419Z",
  "pce_fqdn": "someName.someDomain",
  "created_by": {
    "agent": {
      "href": "/orgs/1/agents/xxxxx",
      "hostname": "someHostname"
    }
  },
  "event_type": "agent.tampering",
  "status": "success",
  "severity": "err",
}
```

```

    "action": {
      "uuid": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
      "api_endpoint": "FILTERED",
      "api_method": "PUT",
      "http_status_code": 204,
      "src_ip": "xx.xxx.xx.xx"
    },
    "resource_changes": [],
    "notifications": [
      {
        "uuid": "yyyyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyyyy",
        "notification_type": "workload.oob_policy_changes",
        "info": {
          "tampering_revert_succeeded": true,
          "beginning_timestamp": "2019-06-17T05:42:10Z",
          "ending_timestamp": "2019-06-17T05:42:10Z",
          "num_events": 1
        }
      }
    ]
  }
}

```

Splunk or Other SIEM Software

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

VEN Tampering Protection

In Illumio Core and Illumio Endpoint 22.5.10 and later releases, you can protect the following types of VENs from unintended actions and tampering:

- Windows and Linux VENs running on servers
- Windows VENs running on endpoints

This feature protects the VEN itself from tampering versus protecting the workload host that the VEN is running on from being tampered with. For information about how the VEN detects tampering with the host firewall, see [VEN Firewall Tampering Detection \[153\]](#).

About Tampering Protection



NOTE

Before using this feature, complete the tasks in [Requirements for Using Tampering Protection \[157\]](#).

This feature protects VENs from unintended, accidental invocation of VEN CLI actions and installer commands that impact VEN functionality, and malicious attempts (including from System Administrators) to disable or uninstall the VEN, or otherwise render the VEN unusable.

Using this feature, you control the ability to run the following VEN administrative actions with the VEN CLI:

- Stopping the VEN; for information see [Shut Down VENs. \[130\]](#)
- Restarting the VEN; for information see [Start Up VENs. \[129\]](#)
- Suspending the VEN; for information, see [VEN Suspension. \[131\]](#)
- Deactivating the VEN; for information, see [Deactivate Using VEN Command Line. \[135\]](#)
- Unpairing the VEN from the PCE; for information, see [Unpair Using VEN Command Line. \[136\]](#)
- Upgrading the VEN on the server or endpoint; see the topics for managing the VENs using the CLI.



NOTE

Providing a maintenance token is not required when upgrading VENs by using the PCE web console.

- Uninstalling the VEN from the server or endpoint; see the topics for managing the VENs using the CLI.



NOTE

Providing a maintenance token is not required when uninstalling VENs from workloads by using the PCE web console.

This tampering protection restricts VEN CLI commands issued by all users, including the users who have administrative or root access to the VEN hosts (servers and endpoints).

Requirements for Using VEN Tampering Protection

To use this feature, you must complete the following requirements:

1. Enable the feature for your organization. See [Enable VEN Tampering Protection \[157\]](#).
2. Generate a maintenance token for all VENs or for specific VENs that you want protected. See [Generate VEN Maintenance Token. \[158\]](#)
To generate this token, users must be part of one of the following Illumio Authorization roles:
 - Global Organization Owner
 - Global Administrators
 - Workload Managers (only for the workloads to which the users have access)
 When you are part of the Workload Manager role, you can set up tampering protection for the VENs you have access to. See "Workload Manager Role" in the PCE Administration Guide for information.
3. Include the token when running VEN CLI commands. See [Manage VEN When Tampering Protection Enabled \[158\]](#).

Enable VEN Tampering Protection

Before you can generate maintenance tokens for VENs or use the tampering protection feature, you must enable it in the PCE web console for your organization.

1. From the PCE web console main menu, go to **Settings > VEN Operations**.

**IMPORTANT**

To access the Setting page for VEN Operations, you must be a member of the Global Organization Owner role. You cannot enable the VEN tampering protection feature without this level of Illumio authorization.

2. Click **Edit**.
3. In the Tampering Protection section, select **Yes** to require a maintenance token when running VEN commands on the VEN CTL.
4. Click **Save**.

Generate a VEN Maintenance Token

**NOTE**

Before you generate a VEN and Endpoint maintenance token, you must enable the feature for your organization.

You can generate maintenance tokens for all your VENs or for a specific VEN.

To generate a maintenance token:

1. Go to **Workloads** and click the **VENs** tab.
 - To generate support tokens for all of the VENs, click **Generate Maintenance Token**.
 - To generate a token for a specific VEN, click the name of a VEN to open the details page for that VEN, and then click **Generate Maintenance Token**.

A **Generate Maintenance Token** dialog box appears where you can generate tokens for all VENs or the specific VEN you selected.

**NOTE**

If the tampering protection feature is enabled for the PCE, the page includes a **Generate Maintenance Token** button. If the page does not include this button, you must enable the feature for your PCE. See [Enable VEN Tampering Protection \[157\]](#).

2. Specify the time period for the token: unlimited (will never expire or need to be regenerated) or a set time period. By default, the dialog box specifies 7 days for the time period.
3. Click **Generate**.

When ready, the dialog refreshes with the text string for the maintenance token and the timestamp for when the token was generated.
4. Copy the text string for the token and store it in a secure location. You will need to provide this string on the command line when you run VEN commands using the VEN CLI.
5. Click **Done** to close the dialog box.

Manage a VEN when Tampering Protection Enabled

When you've enabled tampering protection for a VEN, you must include the new parameter `maintenance-token <token>` on the VEN command line after the action you want to run.

See the following examples. On Windows, include one dash with the parameter (`-maintenance-token <token>`); on Linux, include two dashes (`--maintenance-token <token>`) to run the parameter.

When enabled, running the VEN actions without specifying the token will fail.



NOTE

Not all VEN actions support using a maintenance token for tampering protection. See [About Tampering Protection \[156\]](#) for the list of supported actions.

When enabled, the VEN validates the maintenance token and the token expiration date, and runs the commands as usual.

When the token expires, you can regenerate it in the PCE web console.

Example: Windows Command Line to Run Protected VENs

```
<VEN Installation Directory>\illumio-ven-ctl.exe stop
Maintenance token is required for this operation.
<VEN Installation Directory>\illumio-ven-ctl.exe stop
-maintenance-token eyJhY3Rpb25zIjpuWxsLCJleHBpcmVzX2F0IjpuWxsLCJhZ2VudF9p
ZHMlOm51bGwsIm9yZl9pZCI6MX0=.MGUCMHSfLNS8yGHgFY0D3CuFvi+L8m6VUVI9FHRzT31sn37
F+
GsKecpSnbR8abYuSoz2wgIxALhrtjAXZNN8unxLuN8WO/kcLONz7gwboRCT/Sc2FdwXAkLvioh+9
jyU80BeAj5poA==Stopping venAgentMonitorSvc
Stopping venPlatformHandlerSvc
Stopping venVtapServerSvc
Stopping venAgentMgrSvc
Success
<VEN Installation Directory>\Illumio>
```

Example: Linux Command Line to Run Protected VENs

```
[root@localhost illumio_ven]# ./illumio-ven-ctl unpair open noreport
Maintenance token is required for this operation.
[root@localhost illumio_ven]# ./illumio-ven-ctl unpair --maintenance-token
eyJhY3Rpb25zIjpuWxsLCJleHBpcmVzX2F0IjpuWxsLCJhZ2VudF9pZHMlOm51bGwsIm9yZl9p
ZCI6
6MX0=.MGUCMHSfLNS8yGHgFY0D3CuFvi+L8m6VUVI9FHRzT31sn37F+GsKecpSnbR8abYuSoz2wg
IxAL
hrtjAXZNN8unxLuN8WO/kcLONz7gwboRCT/Sc2FdwXAkLvioh+9jyU80BeAj5poA== open
noreport
Stopping venAgentMonitor:    ...done.
Stopping venVtapServer:     ...done.
Stopping IPSec:             ...done.
Stopping venPlatformHandler: ...done.
Stopping venAgentMgr:       ...done.
Checking agent state
```

```

...done.
* Flush IPv4    ...done.
...done.
Unloading modules    ...done.Illumio VEN is being uninstalled...
2023-01-17T12:51:01-0800 Uninstalling Illumio .....
2023-01-17T12:51:04-08:00 Stopped all daemons
2023-01-17T12:51:04-08:00 Init scripts disabled
2023-01-17T12:51:04-08:00 VEN state on uninstall: enforced
2023-01-17T12:51:04-0800 Deactivating Illumio VEN .....
2023-01-17T12:51:05-0800 Agent 15 Org 1 successfully deactivated
2023-01-17T12:51:05-0800 Deactivation complete
2023-01-17T12:51:05-08:00 /opt/illumio_ven/system/etc/init.d/illumio-
firewall
disable -w workload/c3364c6d-43f7-43fd-a4e4-9eb6258808b4/current
2023-01-17T12:51:07-08:00 Firewall Rules successfully restored
2023-01-17T12:51:07-08:00 Removed ilo-ven user entries
2023-01-17T12:51:07-08:00 Removed data distribution tree from /opt
2023-01-17T12:51:07-08:00 Removed binary distribution tree from /opt
2023-01-17T12:51:07-0800 Uninstall successful
VEN has been SUCCESSFULLY unpaired with Illumio
[root@localhost illumio_ven]#

```

Windows VEN Installer Changes

When you enable the VEN tampering protection feature, the Windows VEN installer can include the new `MAINTENANCE_TOKEN` parameter for the `upgrade`, `uninstall`, and `repair` commands, as shown in the following examples.

Upgrade a VEN

```
ven_installer.exe /install /quiet /log ven_install.log MAINTENANCE_TOKEN=xxx
```

Uninstall a VEN

```
ven_installer.exe /uninstall /quiet /log ven_uninstall.log
MAINTENANCE_TOKEN=xxx
```

Repair a VEN

```
ven_installer.exe /repair /quiet /log ven_repair.log MAINTENANCE_TOKEN=xxx
```

VEN Support Reports

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



NOTE

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

Generate a VEN Support Report from the PCE UI

1. In the PCE web console, go to **Workloads**.
2. Click the **VENs** tab.
3. Click the name of a VEN to go to its details page.
4. Click **Generate Support Bundle**. Generating the bundle may take up to 10 minutes.
5. When the bundle is finished generating, click **Download**.

Generate Linux/AIX/Solaris Support Report Using CLI

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

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



NOTE

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

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

To generate a VEN support report for a Linux workload:

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

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

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

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

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

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

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

Generate Windows Support Report Using CLI

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

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

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

To generate a VEN support report

```
illumio-ven-ctl.exe gen-supportreport
```

To bypass the confirmation prompt

```
illumio-ven-ctl.exe gen-supportreport -noprompt yes
```

VEN Troubleshooting

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

Windows: Enable Base Filtering Engine (BFE)

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

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

Linux: ignored_interface

The Linux `ignored_interface` inhibits PCE policy updates.

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

When a VEN interface is placed in the `ignore_interface` list, the any flow state over the interface won't be kept by conntrack any longer. (The conntrack table on Linux stores information on network connections.) If the connection on TCP port 8444 to the PCE is reinitialized, any arriving packets from the PCE are dropped, because the packets do not have any state in conntrack.

The VEN heartbeat eventually restores connections, but meanwhile the VEN implements any policy sent by lightning bolt from the PCE.

VEN Troubleshooting Tools

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

- A VEN connectivity checking tool called `venconch` for workloads is available on the Illumio Support site.
- A VEN compatibility checking feature is available in the PCE web console for paired workloads.

Commands to Obtain Firewall Snapshot

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

Linux

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

Windows

- `netsh wfp show state`

Solaris

```
ipfstat -ionv
```

AIX

```
ipfstat -ionv
```

Troubleshooting Tips**Connectivity Issues**

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

- Determine if all workloads are unable to communicate or just a subset of the workloads are reported as disconnected. If the PCE reports that all workloads are offline, check if PCE is reachable from workloads.
- If a subset of workloads are down, check if there are differences in network configuration between those and the workloads that are connected, and if they are contributing to PCE being unreachable.
- Check if any workloads that are unable to communicate are located behind NAT devices, firewalls, or remote data centers.
- Ensure the following port configuration:
 - On Prem
 - Port 8443 - HTTPS requests
 - Port 8444 - long-lived TLS-over-TCP connection
 - SaaS
 - Port 443 for both HTTPS requests and the long-lived TLS-over-TCP connection
- If running in a public cloud instance:
 - For AWS, ensure security groups permit TCP port 443.
 - For Azure, ensure that Endpoints are configured to allow traffic.

VEN Process Issues

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

- **Linux:** Run `/opt/illumio/illumio-ven-ctl status`
- **Windows:** Execute `tasklist`

Ensure the following processes are running and active:

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

Errors in the VEN Logs

Review the VEN log files to find any errors generated by the system (sudo required):

- Logs in Data_Dir/log directory

To look for any errors in the log files, execute `grep -ir ERROR *`

To check for firewall updates, view the `platform.log` file. Look for logs related to firewall updates; for example:

```
2014-07-26T22:20:41Z INFO:: Enforcement mode is: XXXX
2014-07-26T22:20:41Z INFO:: Is fw update yes
2014-07-26T22:20:41Z INFO:: Is ipset update yes
2014-07-26T22:20:41Z INFO:: saved fw-json
```

- Check heartbeat logs for records related to update messages from the PCE. See the following example heartbeats:

```
2014-07-26T22:43:12Z Received HELLO from EventService.
2014-07-26T22:43:12Z Sent ACK to EventService.
Events - f/w updates etc.
2014-07-26T22:34:11Z Received EVENT from EventService.
2014-07-26T22:34:11Z Added EVENT from EventService to PLATFORM handler
thread message queue
```

```
iptables-save | grep 443 | grep allow_out
-A tcp_allow_out -d 54.185.43.60/32 -p tcp -m multiport --dports 443
-m conntrack --ctstate NEW -j NFLOG --nflog-prefix "0x800000000000025f "
--nflog-threshold 1
-A tcp_allow_out -d 54.185.43.60/32 -p tcp -m multiport --dports 443
-m conntrack --ctstate NEW -j ACCEPT
-A tcp_allow_out -d 204.51.153.0/27 -p tcp -m multiport --dports 443
-m conntrack --ctstate NEW -j NFLOG --nflog-prefix "0x8000000000000265 "
--nflog-threshold 1
-A tcp_allow_out -d 204.51.153.0/27 -p tcp -m multiport --dports 443
-m conntrack --ctstate NEW -j ACCEPT
iptables-save | grep 444 | grep allow_out
-A tcp_allow_out -d 54.185.43.60/32 -p tcp -m multiport --dports 444
-m conntrack --ctstate NEW -j NFLOG --nflog-prefix "0x8000000000000266 "
--nflog-threshold 1
-A tcp_allow_out -d 54.185.43.60/32 -p tcp -m multiport --dports 444
-m conntrack --ctstate NEW -j ACCEPT
```

Policy Sync Might Require Reboot

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

Event Viewer Stops Logging

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

Events Administration and REST APIs

Overview of Events Administration

This section describes how to do typical administration tasks related to PCE events.

Before You Begin

Illumio 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

About This Guide

This guide provides the following information to administer your PCE deployment:

- 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](#)

Notational Conventions in This Guide

- Newly introduced terminology is italicized. Example: *activation code* (also known as pairing key)
- Command-line examples are monospace. Example: `illumio-ven-ctl --activate`
- Arguments on command lines are monospace italics. Example: `illumio-ven-ctl --activate activation_code`
- In some examples, the output might be shown across several lines but is actually on one single line.
- Command input or output lines not essential to an example are sometimes omitted, as indicated by three periods in a row. Example:

```
...  
some command or command output  
...
```

Events Framework

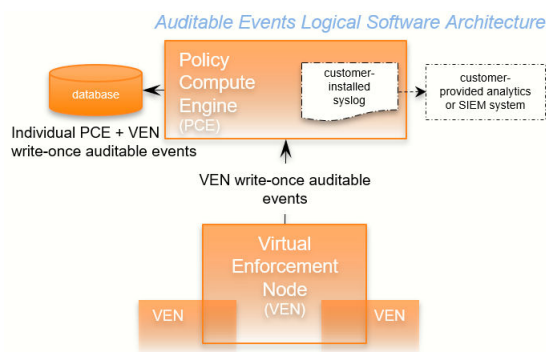
The Illumio events framework provides an information-rich, deep foundation for actionable insights into the operations of Illumio Core.

Overview of the Framework

Auditable events are records of transactions collected from the following management interfaces:

- PCE web console
- REST API
- PCE command-line tools
- VEN command-line tools

All actions that change the configuration of the PCE, security policy, and the VENs are recorded, including workload firewall tampering.



As required by auditing standards, every recorded change includes a reference to the program that made the change, the change's timestamp, and other fields. After recording, the auditable events are read-only.

Auditable events comply with the [Common Criteria Class FAU Security Audit requirements](#) standard for auditing.

Auditing Needs Satisfied by Framework

Need	Description	See topic...
Audit and Compliance	Evidence to show that resources are managed according to rules and regulatory standards.	Events Record Information [169]
Resource Lifecycle Tracking	All information necessary to track a resource through creation, modification, and deletion.	Events Lifecycle for Resources [167]
Operations	Trace of recent changes to resources.	Events Lifecycle for Resources [167]
Security	Evidence to show which changes failed, such as incorrect user permissions or failed authentication.	User Password Update Failed (JSON) [187]

Benefits of Events Framework

The events framework in the Illumio Core provides the following benefits:

- Exceeds industry standards
- Delivers complete content
 - Comprehensive set of event types
 - Includes more than 200 events
 - Additional notable system events are generated
- Easily accessible interfaces to capture events:
 - Event Viewer in the PCE web console
 - REST API with filtering
 - SIEM integration
 - Events are the same across all interfaces
- Designed for customer ease of use
 - Flattened, common structure for all events
 - Eliminates former duplicate or multiple events for single actions
 - Streamed via syslog in JSON, CEF, or LEEF format
 - Create/Update/Delete REST APIs recorded as events
 - Read APIs/GET requests are not recorded, because they do not change the Illumio Core.

Events Lifecycle for Resources

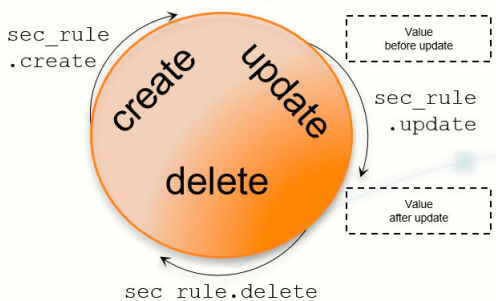
Illumio resources progress through the lifecycle stages (creation, updating, deletion) and Illumio Core records them with the appropriate event types.

About the Lifecycle

Many resources have a lifecycle from creation through update to deletion. For example, the events related to a security policy rule (identified by the resource name `sec_rule`) are recorded with the following event types.

- `sec_rule.create`
- `sec_rule.update`: Update events record with the values of the resource object both before and after the event for a lifecycle audit trail.
- `sec_rule.delete`

Auditable Events: Lifecycle of a Resource



Other Resource Lifecycles

Some resources have unique characteristics and do not follow the create-update-delete pattern. For example, workloads have the following event types:

- `workload.update`
- `workload.upgrade`
- `workload.redetect_network`
- `workload.recalc_rules`
- `workload.soft_delete`
- `workload.delete`
- `workload.undelete`

Events Described

This section describes the concepts and types of PCE events.

Event Types, Syntax, and Record Format

When working with events, it is important to recognize their type, REST API schema, syntax, and record information.

Types of Events

The Illumio Core includes the following general categories of auditable events:

- Organizational events: Organizational events are further grouped by their source:
 - API-related events: Events occurring from a use of the REST API, including the PCE web console
 - System-related events: Events caused by some system-related occurrence
- Traffic events

Anonymized Database Dumps

To troubleshoot customer-reported issues, Illumio Customer Support sometimes requests that you supply an anonymized dump of the PCE database.

To safeguard your organization's privacy, the event information is not included in the anonymized database dump.

REST API Events Schema

The Events schema in JSON is downloadable from this documentation portal in the zipfile of the REST API schemas. From the documentation portal Home page, go to the **Develop** category > **REST API Public Schemas (Archive File)**.

Event Syntax

The names of recorded auditable events in have the following general syntax:

```
resource.verb[.success_or_failure]
```

Where:

- `resource` is a PCE and VEN object, such as PCE `user` or VEN `agent` component.

- `verb` describes the action of the event on that resource.
- In CEF and LEEF formats, the success or failure of the verb is included in the recorded event type. This indicator is not needed in the JSON format.

Events Record Information

The following information is included in a event record, which answers the who, what, where, how, and when:

Type of information	Description
Who	<ul style="list-style-type: none"> • VEN identified by hostname and agent href, and after Release 22.3, VEN href • User identified by username and href • PCE system identified by "system"
What	<p>The action that triggered the event, including the following data:</p> <ul style="list-style-type: none"> • Resource type + operation + success or failure • Application Request ID • Status of successful events and failed events: <ul style="list-style-type: none"> • In case of failure, exception type and exception message. • All failures related to security, such as authentication and authorization. • Severity as INFO, WARNING, ERROR. • The pre-change and post-change values of the affected resources.
Where	<p>The target resource of the action, composed of the following data:</p> <ul style="list-style-type: none"> • Identifier of the target resource (primary field). • Friendly name for the target resource. For example: <ul style="list-style-type: none"> • workload/VEN: <code>hostname</code> • user.username • ruleset, label, service, etc: name, key/value
How	API endpoint, method, HTTP status code, and source IP address of the request.
When	Timestamp of the event's occurrence. This timestamp is <i>not</i> the time the event was recorded.

Event Record Structure

Regardless of export format (JSON, CEF, or LEEF), the records and fields for all events share a common structure. This common structure of composite events makes post-processing of event data easier.

Bulk change operations on many resources simultaneously are recorded as individual operations on the resource within a single composite event. Failed attempts to change a configuration, such as incorrect authentication, are also collected.

Common Fields

Field Name	Description
<code>href</code>	Unique event identifier; contains a UUID.
<code>timestamp</code>	Exact time that the event occurred in RFC 3339 format with fractional seconds.

Field Name	Description
<code>pce_fqdn</code>	The fully qualified domain name of the PCE; especially useful for Supercluster deployments or if there are multiple PCEs sending data to the SIEM server.
<code>created_by</code>	Identifies creator of the event; could be a user, the system, or a workload.
<code>event_type</code>	Name of the event; for more information, see the List of Event Types [171] table.
<code>status</code>	“Success” or “failure;” if the status is null, the event is for information only and doesn’t indicate success or failure.
<code>severity</code>	“Informational,” “warning,” or “error” indicating the severity of the event.
<code>version</code>	Schema version for events.

Events Displayed in PCE Web Console

The PCE web console provides an ongoing log of all Organization events that occur in the PCE. For example, Organization events capture actions such as users logging in and logging out, and failed login attempts; when a system object is created, modified, deleted, or provisioned; when a workload is paired or unpaired; and so on.

From the platform and API perspective, Organization events are referred to internally as `auditable_events` and are generated by the `auditable_events_service`.

You can use the filter at the top of the page to search for events by type of event, event severity level, and when the event occurred.

Cross-Site Request Forgery Protection

A cross-site request forgery (CSRF) is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is an application functionality using predictable URL or form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a website has for a user.

For more details on this attack, see the [CSRF article](#) on the Web Application Security Consortium website.

Illumio Core can notify you of this type of attack in the following ways:

- The PCE web console logs the attack as an Organization Event called “CSRF token validation failure.”
- The event is logged in the Illumio Core REST API as `authz_csrf_validation_failure` in the `audit_log_events_get.schema`.
- The event `authz_csrf_validation_failure` appears in the PCE syslog output if you have deployed the PCE as a software.

**IMPORTANT**

When you see this event occur, you should immediately investigate the issue because the request might not have originated from a valid user.

List of Event Types

The following table provides the types of JSON events generated and their description. For each of these events, the CEF/LEEF success or failure events generated are the event name followed by `.success` or `.failure`.

For example, the CEF/LEEF success event for `agent.activate` is `agent.activate.success` and the failure event is `agent.activate.failure`.

Each event can generate a variety of notification messages. See [Notification Messages in Events \[181\]](#).

JSON Event Type	Description
<code>access_restriction.create</code>	Access restriction created
<code>access_restriction.delete</code>	Access restriction deleted
<code>access_restriction.update</code>	Access restriction updated
<code>agent.activate</code>	Agent paired
<code>agent.activate_clone</code>	Agent clone activated
<code>agent.clone_detected</code>	Agent clone detected
<code>agent.deactivate</code>	Agent unpaired
<code>agent.generate_maintenance_token</code>	Generate maintenance token for any agent
<code>agent.goodbye</code>	Agent disconnected
<code>agent.machine_identifier</code>	Agent machine identifiers updated
<code>agent.refresh_token</code>	Agent refreshed token
<code>agent.request_policy</code>	Policy request sent
<code>agent.request_upgrade</code>	VEN upgrade request sent
<code>agent.service_not_available</code>	Agent reported a service not running
<code>agent.suspend</code>	Agent suspended
<code>agent.tampering</code>	Agent firewall tampered

JSON Event Type	Description
<code>agent.unsuspend</code>	Agent unsuspended
<code>agent.update</code>	Agent properties updated.
<code>agent.update_interactive_users</code>	Agent interactive users updated
<code>agent.update_iptables_href</code>	Agent updated existing iptables href
<code>agent.update_running_containers</code>	Agent updated existing containers
<code>agent.upload_existing_ip_table_rules</code>	Agent existing IP tables uploaded
<code>agent.upload_support_report</code>	Agent support report uploaded
<code>agent_support_report_request.create</code>	Agent support report request created
<code>agent_support_report_request.delete</code>	Agent support report request deleted
<code>agents.clear_conditions</code>	Condition cleared from a list of VENS
<code>agents.unpair</code>	Multiple agents unpaired
<code>api_key.create</code>	API key created
<code>api_key.delete</code>	API key deleted
<code>api_key.update</code>	API key updated
<code>auth_security_principal.create</code>	RBAC auth security principal created
<code>auth_security_principal.delete</code>	RBAC auth security principal deleted
<code>auth_security_principal.update</code>	RBAC auth security principal updated
<code>authentication_settings.update</code>	Authentication settings updated
<code>cluster.create</code>	PCE cluster created
<code>cluster.delete</code>	PCE cluster deleted
<code>cluster.update</code>	PCE cluster updated
<code>container_workload.update</code>	Container workload updated
<code>container_cluster.create</code>	Container cluster created
<code>container_cluster.delete</code>	Container cluster deleted
<code>container_cluster.update</code>	Container cluster updated
<code>container_cluster.update_label_map</code>	Container cluster label mappings updated all at once
<code>container_cluster.update_services</code>	Container cluster services updated, created, or deleted by Kubelink
<code>container_workload_profile.create</code>	Container workload profile created

JSON Event Type	Description
container_workload_profile.delete	Container workload profile deleted
container_workload_profile.update	Container workload profile updated
database.temp_table_autocleanup_started	DB temp table cleanup started
database.temp_table_autocleanup_completed	DB temp table cleanup completed
domain.create	Domain created
domain.delete	Domain deleted
domain.update	Domain updated
enforcement_boundary.create	Enforcement boundary created
enforcement_boundary.delete	Enforcement boundary deleted
enforcement_boundary.update	Enforcement boundary updated
event_settings.update	Event settings updated
firewall_settings.update	Global policy settings updated
group.create	Group created
group.update	Group updated
ip_list.create	IP list created
ip_list.delete	IP list deleted
ip_list.update	IP list updated
ip_lists.delete	IP lists deleted
ip_tables_rule.create	IP tables rules created
ip_tables_rule.delete	IP tables rules deleted
ip_tables_rule.update	IP tables rules updated
job.delete	Job deleted
label.create	Label created
label.delete	Label deleted
label.update	Label updated
label_group.create	Label group created
label_group.delete	Label group deleted
label_group.update	Label group updated

JSON Event Type	Description
labels.delete	Labels deleted
ldap_config.create	LDAP configuration created
ldap_config.delete	LDAP configuration deleted
ldap_config.update	LDAP configuration updated
ldap_config.verify_connection	LDAP server connection verified
license.delete	License deleted
license.update	License updated
login_proxy_ldap_config.create	Interservice call to login service to create LDAP config
login_proxy_ldap_config.delete	Interservice call to login service to delete LDAP config
login_proxy_ldap_config.update	Interservice call to login service to update LDAP config
login_proxy_ldap_config.verify_connection	Interservice call to login service to verify connection to the LDAP server
login_proxy_msp_tenants.create	New MSP tenant created
login_proxy_msp_tenants.delete	MSP tenant deleted
login_proxy_msp_tenants.update	MSP tenant updated
login_proxy_orgs.create	New managed organization created
login_proxy_orgs.delete	Managed organization deleted
login_proxy_orgs.update	Managed organization updated
lost_agent.found	Lost agent found
network.create	Network created
network.delete	Network deleted
network.update	Network updated
network_device.ack_enforcement_instructions_applied	Enforcement instruction applied to a network device
network_device.assign_workload	Existing or new unmanaged workload assigned to a network device
network_device.create	Network device created
network_device.delete	Network device deleted
network_device.update	Network device updated
network_devices.ack_multi_enforcement_instructions_applied	Enforcement instructions applied to multiple network devices

JSON Event Type	Description
<code>network_endpoint.create</code>	Network endpoint created
<code>network_endpoint.delete</code>	Network endpoint deleted
<code>network_endpoint.update</code>	Network endpoint updated
<code>network_enforcement_node.activate</code>	Network enforcement node activated
<code>network_enforcement_node.clear_conditions</code>	Network enforcement node conditions cleared
<code>network_enforcement_node.deactivate</code>	Network enforcement node deactivated
<code>network_enforcement_node.degraded</code>	Network enforcement node failed or primary lost connectivity to secondary
<code>network_enforcement_node.missed_heartbeats</code>	Network enforcement node did not heartbeat for more than 15 minutes
<code>network_enforcement_node.missed_heartbeats_check</code>	Network enforcement node missed heartbeats check
<code>network_enforcement_node.network_devices_network_endpoints_workloads</code>	Workload added to network endpoint
<code>network_enforcement_node.policy_ack</code>	Network enforcement node acknowledgment of policy
<code>network_enforcement_node.request_policy</code>	Network enforcement node policy requested
<code>network_enforcement_node.update_status</code>	Network enforcement node reports when switches are not reachable
<code>network_enforcement_nodes.clear_conditions</code>	A condition was cleared from a list of network enforcement nodes
<code>nfc.activate</code>	Network function controller created
<code>nfc.delete</code>	Network function controller deleted
<code>nfc.update_discovered_virtual_servers</code>	Network function controller virtual servers discovered
<code>nfc.update_policy_status</code>	Network function controller policy status
<code>nfc.update_slb_state</code>	Network function controller SLB state updated
<code>org.create</code>	Organization created
<code>org.recalc_rules</code>	Rules for organization recalculated
<code>org.update</code>	Organization information updated
<code>pairing_profile.create</code>	Pairing profile created
<code>pairing_profile.create_pairing_key</code>	Pairing profile pairing key created
<code>pairing_profile.delete</code>	Pairing profile deleted

JSON Event Type	Description
pairing_profile.update	Pairing profile updated
pairing_profile.delete_all_pairing_keys	Pairing keys deleted from pairing profile
pairing_profiles.delete	Pairing profiles deleted
password_policy.create	Password policy created
password_policy.delete	Password policy deleted
password_policy.update	Password policy updated
permission.create	RBAC permission created
permission.delete	RBAC permission deleted
permission.update	RBAC permission updated
radius_config.create	Create domain RADIUS configuration
radius_config.delete	Delete domain RADIUS configuration
radius_config.update	Update domain RADIUS configuration
radius_config.verify_shared_secret	Verify RADIUS shared secret
request.authentication_failed	API request authentication failed
request.authorization_failed	API request authorization failed
request.internal_server_error	API request failed due to internal server error
request.service_unavailable	API request failed due to unavailable service
request.unknown_server_error	API request failed due to unknown server error
resource.create	Login resource created
resource.delete	Login resource deleted
resource.update	Login resource updated
rule_set.create	Rule set created
rule_set.delete	Rule set deleted
rule_set.update	Rule set updated
rule_sets.delete	Rule sets deleted
saml_acs.update	SAML assertion consumer services updated
saml_config.create	SAML configuration created
saml_config.delete	SAML configuration deleted

JSON Event Type	Description
saml_config.pce_signing_cert	Generate a new cert for signing SAML AuthN requests
saml_config.update	SAML configuration updated
saml_sp_config.create	SAML Service Provider created
saml_sp_config.delete	SAML Service Provider deleted
saml_sp_config.update	SAML Service Provider updated
sec_policy.create	Security policy created
sec_policy_pending.delete	Pending security policy deleted
sec_policy.restore	Security policy restored
sec_rule.create	Security policy rules created
sec_rule.delete	Security policy rules deleted
sec_rule.update	Security policy rules updated
secure_connect_gateway.create	SecureConnect gateway created
secure_connect_gateway.delete	SecureConnect gateway deleted
secure_connect_gateway.update	SecureConnect gateway updated
security_principal.create	RBAC security principal created
security_principal.delete	RBAC security principal bulk deleted
security_principal.update	RBAC security principal bulk updated
security_principals.bulk_create	RBAC security principals bulk created
service.create	Service created
service.delete	Service deleted
service.update	Service updated
service_account.create	Service account created
service_account.delete	Service account deleted
service_account.update	Service account updated
service_binding.create	Service binding created
service_binding.delete	Service binding created
service_bindings.delete	Service bindings deleted
service_bindings.delete	Service binding deleted

JSON Event Type	Description
<code>services.delete</code>	Services deleted
<code>settings.update</code>	Explorer settings updated
<code>slb.create</code>	Server load balancer created
<code>slb.delete</code>	Server load balancer deleted
<code>slb.update</code>	Server load balancer updated
<code>support_report.upload</code>	Support report uploaded
<code>syslog_destination.create</code>	syslog remote destination created
<code>syslog_destination.delete</code>	syslog remote destination deleted
<code>syslog_destination.update</code>	syslog remote destination updated
<code>system_task.agent_missed_heartbeats_check</code>	Agent missed heartbeats
<code>system_task.agent_missing_heartbeats_after_upgrade</code>	VEN missing heartbeat after upgrade
<code>system_task.agent_offline_check</code>	Agents marked offline
<code>system_task.agent_self_signed_certs_check</code>	VEN self signed certificate housekeeping check
<code>system_task.agent_settings_invalidation_error_state_check</code>	VEN settings invalidation error state check
<code>system_task.agent_uninstall_timeout</code>	VEN uninstall timeout
<code>system_task.clear_auth_recover_condition</code>	Clear VEN authentication recovery condition
<code>system_task.compute_policy_for_unmanaged_workloads</code>	Compute policy for unmanaged workloads
<code>system_task.delete_expired_service_account_api_keys</code>	An expired service account <code>api_key</code> was successfully deleted
<code>system_task.delete_old_cached_perspectives</code>	Delete old cached perspectives
<code>system_task.endpoint_offline_check</code>	Endpoint marked offline
<code>system_task.provision_container_cluster_services</code>	Container cluster services provisioned
<code>system_task.prune_old_log_events</code>	Event pruning completed
<code>system_task.remove_stale_zone_subnets</code>	Stale zone subnets removed
<code>system_task.set_server_sync_check</code>	Set server synced
<code>system_task.vacuum_deactivated_agent_and_deleted_workloads</code>	Deactivated and deleted workloads have been vacuumed

JSON Event Type	Description
traffic_collector_setting.create	Traffic collector setting created
traffic_collector_setting.delete	Traffic collector setting deleted
traffic_collector_setting.update	Traffic collector setting updated
trusted_proxy_ips.update	Trusted proxy IPs created or updated
user.accept_invitation	User invitation accepted
user.authenticate	User authenticated
user.create	User created
user.delete	User deleted
user.invite	User invited
user.login	User logged in
user.login_session_terminated	User login session terminated
user.logout	User logged
user.pce_session_terminated	User session terminated
user.reset_password	User password reset
user.sign_in	User session created
user.sign_out	User session terminated
user.update	User information updated
user.update_password	User password updated
user.use_expired_password	User entered expired password
user.verify_mfa	User verified MFA
users.auth_token	Auth token returned for user authentication on PCE
user_local_profile.create	User local profile created
user_local_profile.delete	User local profile deleted
user_local_profile.reinvite	User local profile reinvited
user_local_profile.update_password	User local password updated
ven_settings.update	VEN settings updated
ven_software.upgrade	VEN software release upgraded
ven_software_release.create	VEN software release created

JSON Event Type	Description
<code>ven_software_release.delete</code>	VEN software release deleted
<code>ven_software_release.deploy</code>	VEN software release deployed
<code>ven_software_release.update</code>	VEN software release updated
<code>ven_software_releases.set_default_version</code>	Default VEN software version set
<code>virtual_server.create</code>	Virtual server created
<code>virtual_server.delete</code>	Virtual server created
<code>virtual_server.update</code>	Virtual server updated
<code>virtual_service.create</code>	Virtual service created
<code>virtual_service.delete</code>	Virtual service deleted
<code>virtual_service.update</code>	Virtual service updated
<code>virtual_services.bulk_create</code>	Virtual services created in bulk
<code>virtual_services.bulk_update</code>	Virtual services updated in bulk
<code>vulnerability.create</code>	Vulnerability record created
<code>vulnerability.delete</code>	Vulnerability record deleted
<code>vulnerability.update</code>	Vulnerability record updated
<code>vulnerability_report.delete</code>	Vulnerability report deleted
<code>vulnerability_report.update</code>	Vulnerability report updated
<code>workload.create</code>	Workload created
<code>workload.delete</code>	Workload deleted
<code>workload.online</code>	Workload online
<code>workload.recalc_rules</code>	Workload policy recalculated
<code>workload.redetect_network</code>	Workload network redetected
<code>workload.undelete</code>	Workload undeleted
<code>workload.update</code>	Workload settings updated
<code>workload.upgrade</code>	Workload upgraded
<code>workload_interface.create</code>	Workload interface created
<code>workload_interface.delete</code>	Workload interface deleted
<code>workload_interface.update</code>	Workload interface updated

JSON Event Type	Description
<code>workload_interfaces.update</code>	Workload interfaces updated For example, IP address changes, new interface added, and interface shut down.
<code>workload_service_report.update</code>	Workload service report updated
<code>workload_settings.update</code>	Workload settings updated
<code>workloads.apply_policy</code>	Workloads policies applied
<code>workloads.bulk_create</code>	Workloads created in bulk
<code>workloads.bulk_delete</code>	Workloads deleted in bulk
<code>workloads.bulk_update</code>	Workloads updated in bulk
<code>workloads.remove_labels</code>	Workloads labels removed
<code>workloads.set_flow_reporting_frequency</code>	Workload flow reporting frequency changed
<code>workloads.set_labels</code>	Workload labels applied
<code>workloads.unpair</code>	Workloads unpaired
<code>workloads.update</code>	Workloads updated

Notification Messages in Events

Events can generate a variety of notifications that are appended after the event type:

- `agent.clone_detected`
- `agent.fw_state_table_threshold_exceeded`
- `agent.missed_heartbeats`
- `agent.missing_heartbeats_after_upgrade`
- `agent.policy_deploy_failed`
- `agent.policy_deploy_succeeded`
- `agent.process_failed`
- `agent.service_not_available`
- `agent.upgrade_requested`
- `agent.upgrade_successful`
- `agent.upgrade_time_out`
- `container_cluster.duplicate_machine_id`
- `container_cluster.region_mismatch`
- `container_workload.invalid_pairing_config`
- `container_workload.not_created`
- `database.temp_table_autocleanup_completed`
- `database.temp_table_autocleanup_started`
- `hard_limit.exceeded`
- `pce.application_started`
- `pce.application_stopped`
- `remote_syslog.reachable`

- `remote_syslog.unreachable`
- `request.authentication_failed`
- `request.authorization_failed`
- `request.internal_server_error`
- `request.invalid`
- `request.service_unavailable`
- `request.unknown_server_error`
- `sec_policy.restore`
- `soft_limit.exceeded`
- `system_task.event_pruning_completed`
- `system_task.hard_limit_recovery_completed`
- `user.csrf_validation_failed`
- `user.login_failed`
- `user.login_failure_count_exceeded`
- `user.login_session_created`
- `user.login_session_terminated`
- `user.pce_session_created`
- `user.pce_session_terminated`
- `user.pw_change_failure`
- `user.pw_changed`
- `user.pw_complexity_not_met`
- `user.pw_reset_completed`
- `user.pw_reset_requested`
- `virtual_service.not_created`
- `workload.duplicate_interface_reported`
- `workload.nat_rules_present`
- `workload.offline_after_ven_goodbye`
- `workload.online`
- `workload.oob_policy_changes`
- `workload.partial_policy_delivered`
- `workload.update_mismatched_interfaces`
- `workloads.flow_reporting_frequency_updated`

Common Criteria Only Events

The following table lists the types of JSON events that are generated and their descriptions.

For each of these events, the CEF/LEEF success or failure events generated are the event name followed by `.success` or `.failure`.

For example, the CEF/LEEF success event for `agent.update` is `agent.update.success` and the failure event is `agent.update.failure`.

JSON Event Type	Description
<code>pce.application_started</code>	PCE application started
<code>pce.application_stopped</code>	PCE application stopped

JSON Event Type	Description
<code>remote_syslog.reachable</code>	Remote syslog destination reachable
<code>remote_syslog.unreachable</code>	Remote syslog destination not reachable
<code>tls_channel.establish</code>	TLS channel established
<code>tls_channel.terminate</code>	TLS channel terminated

View and Export Events

By default, you can view events in the PCE web console or by using the PCE command line. You can then export Organization events using the PCE web console.

View Events in PCE Web Console

By default, the PCE web console shows events that occur in your organization, such as when a workload is paired, if a pairing failed, when a user logs in or logs out, when a user fails to authenticate, and so on.

If you want to see only certain events you can filter by event type to see events that interest you most. You can also search for Organization events by their universally unique identifier (UUID), and filter events by their severity.

You can also export the list of organization events as a CSV file.

To view Organization events:

1. From the PCE web console menu, choose **Troubleshooting > Events**.
2. As the top of the page, you can use the Event Filter to filter the list by event type.

Event	Description	Severity	Status	Timestamp	Generated By
event.update	Event config updated	Informational	Success	07/28/2018, 21:27:20	admin@devtest103.ilabs.io
user.login	User session created (on PCE)	Informational	Success	07/28/2018, 21:24:23	admin@devtest103.ilabs.io
user.sign_in	User session created (on Login)	Informational	Success	07/28/2018, 21:24:22	admin@devtest103.ilabs.io
user.authentication_failed	User authentication failed	Error	Failure	07/28/2018, 21:24:19	anonymous
user.authentication_failed	User authentication failed	Error	Failure	07/28/2018, 21:00:24	anonymous
user.authentication_failed	User authentication failed	Error	Failure	07/28/2018, 20:59:51	anonymous
user.authorization_failed	User authorization failed	Error	Failure	07/28/2018, 20:49:17	System



NOTE

In the Events Viewer, the suggested values for the filters are generated from all possible values. For example, the “Generated By” filter shows all users on the system. However, the actual results displayed by that filter might not contain any data.

VEN Event Not Displayed in PCE Web Console

The following events related to VENs are not currently viewable in the PCE web console. This is a two-column list of event names.

VEN Events not shown in PCE Web Console	
fw_tampering_revert_failure	lost_agent
fw_tampering_reverted	missing_os_updates
fw_tampering_subsystem_failure	pce_incompat_api_version
invoke_powershell_failure	pce_incompat_version
ipsec_conn_state_change	pce_reachable
ipsec_conn_state_failure	pce_unreachable
ipsec_monitoring_failure	proc_config_failure
ipsec_monitoring_started	proc_envsetup_failure
ipsec_monitoring_stopped	proc_init_failure
ipsec_subsystem_failure	proc_malloc_failure
ipsec_subsystem_started	proc_restart_failure
ipsec_subsystem_stopped	proc_started
refresh_token_failure	proc_stopped
refresh_token_success	

VEN href Added to Events Information

After the 22.3.0 upgrade, all events created by a VEN includes the VEN href as well as the previously included Agent href. The VEN href can be used to query the VEN API, obtain the workload record, and execute various operations on the VEN from the PCE.

View Events Using PCE Command Line

Run this command at any runlevel to display:

- The total number of events
- The average number of events per day

```
$ sudo -u ilo-pce illumio-pce-db-management events-db events-db-show
```

Run this command at any runlevel to display:

- The amount of disk space used by events
- The total number of events

```
$ sudo -u ilo-pce illumio-pce-db-management events-db disk-usage-show
```


Export Events Using PCE Web Console

You can export all Organization events, or export a filtered list organization events to a CSV file.

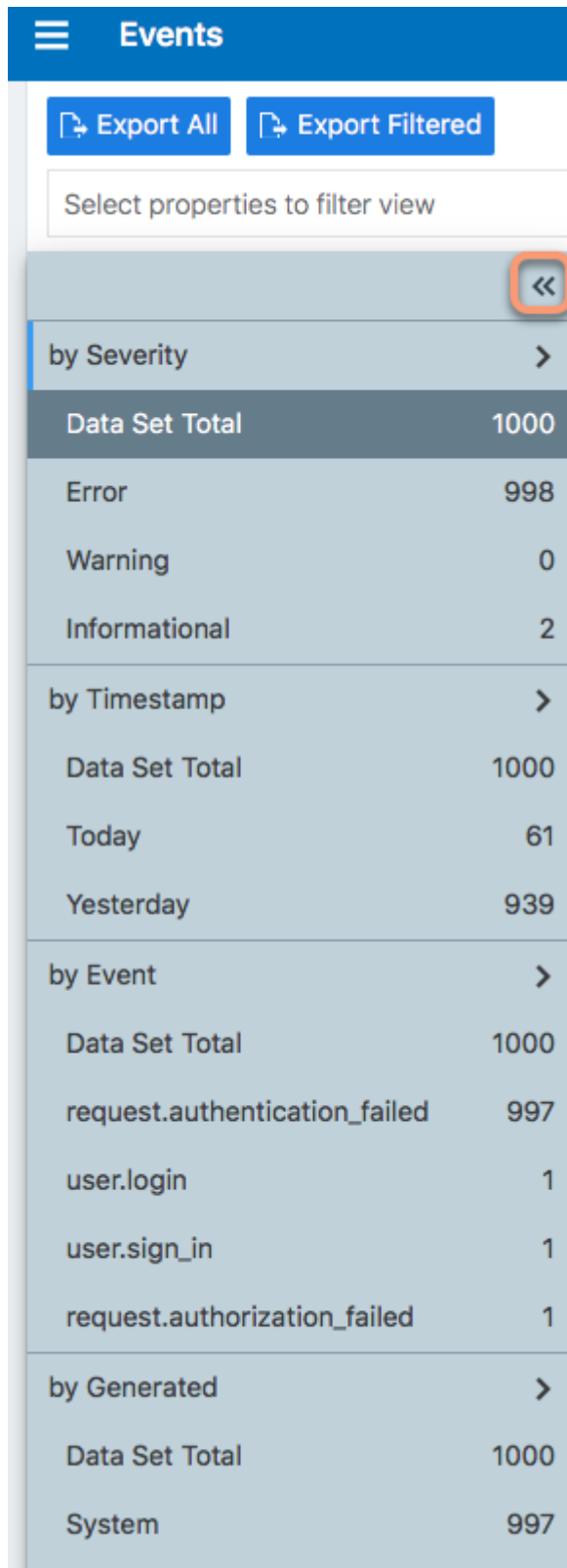
To export events:

1. From the PCE web console menu, choose **Troubleshooting > Events**.
You see a list of events based on the activities performed.
2. Click **Export > Export All** to export all Organization events.
3. To export a filtered list of a events, filter the list and then click **Export > Export Filtered** to export only the filtered view.
4. To search for events based on event type, severity, status, timestamp, and who generated them, use the search filter:

The screenshot shows the 'Events' page in the PCE web console. At the top, there's a blue header with a hamburger menu icon and the word 'Events'. Below the header, there are two buttons: 'Export All' and 'Export Filtered'. A text input field below these buttons says 'Select properties to filter view'. The main content area is a table of events. On the left side of the table, there is a sidebar with a list of event types and their descriptions, along with filter options for Severity, Status, Timestamp, and Generated By. The table columns are Description, Severity, Status, and Timestamp. The events listed include 'org.recalc_rules', 'agent.activate_clone', 'agent.clone_detected', 'agent.request_policy', 'agent.tampering', and 'agent.update_interactive_users'.

Event – 6 of 234 Total	Description	Severity	Status	Timestamp
org.recalc_rules Admin forced recalculation of policy	User session created	Informational	Success	01/21/2019, 01:00:00
	User login	Informational	Success	01/21/2019, 01:00:00
agent.activate_clone Agent clone activated	Request authorization failed	Error	Failure	01/21/2019, 01:00:00
agent.clone_detected Agent clone detected				
agent.request_policy Agent fetched policy				
agent.tampering Agent firewall tampered				
agent.update_interactive_users Agent interactive users updated				
Type to show more Events				
Severity				
Status				
Timestamp				
Generated By				

5. For a faster filtering via the browser, use the following field:



The screenshot shows the 'Events' page in the Illumio interface. At the top, there are two buttons: 'Export All' and 'Export Filtered'. Below them is a text input field labeled 'Select properties to filter view'. The sidebar on the left contains a list of filter categories, each with a right-pointing chevron. The 'by Severity' category is currently selected, and its details are shown in the main table. An orange box highlights the left-pointing chevron icon at the top of the sidebar.

by Severity	
Data Set Total	1000
Error	998
Warning	0
Informational	2

by Timestamp	
Data Set Total	1000
Today	61
Yesterday	939

by Event	
Data Set Total	1000
request.authentication_failed	997
user.login	1
user.sign_in	1
request.authorization_failed	1

by Generated	
Data Set Total	1000
System	997

Examples of Events

This section presents examples of recorded events in JSON, CEF, and LEEF for various auditing needs.

User Password Update Failed (JSON)

This example event shows a user password change that failed validation. Event type `user.update_password` shows `"status": "failure"`, and the notification shows that the user's attempted new password did not meet complexity requirements.

```
{
  "href": "/orgs/1/events/xxxxxxx-39bd-43f1-a680-cc17c6984925",
  "timestamp": "2018-08-29T22:07:00.978Z",
  "pce_fqdn": "pcel.bigco.com",
  "created_by": {
    "system": {}
  },
  "event_type": "user.update_password",
  "status": "failure",
  "severity": "info",
  "action": {
    "uuid": "xxxxxxx-a5f7-4975-a2a5-b4dbd8b74493",
    "api_endpoint": "/login/users/password/update",
    "api_method": "PUT",
    "http_status_code": 302,
    "src_ip": "10.3.6.116"
  },
  "resource_changes": [],
  "notifications": [{
    "uuid": "xxxxxxx-7b8e-4205-a62a-1f070d8a0ee2",
    "notification_type": "user.pw_complexity_not_met",
    "info": null
  }, {
    "uuid": "xxxxxxx-9721-4971-b613-d15aa67a4ee7",
    "notification_type": "user.pw_change_failure",
    "info": {
      "reason": "Password must have minimum of 1 new
character(s)"
    }
  }],
  "version": 2
}
```

Resource Updated (JSON)

This example shows the before and after values of a successful update event `rule_set.update`. The name of the ruleset changed from `"before": "rule_set_2"` to `"after": "rule_set_3"`.

```
{ "href": "/orgs/1/events/xxxxxxx-8033-4f1a-83e9-fde57c425807",
  "timestamp": "2018-08-29T22:04:04.733Z",
  "pce_fqdn": "pcel.bigco.com",
  "created_by": {
    "user": {
      "href": "/users/1",
      "username": "albert.einstein@bigco.com"
    }
  },
  "event_type": "rule_set.update",
  "status": "success",
```

```

"severity": "info",
"action": {
"uuid": "xxxxxxxx-7488-480b-9ef9-0cd2a8496004",
"api_endpoint": "/api/v2/orgs/1/sec_policy/draft/rule_sets/6",
"api_method": "PUT",
"http_status_code": 204,
"src_ip": "10.3.6.116"
},
"resource_changes": [{
"uuid": "xxxxxxxx-1d13-4e5e-8f0b-e0e8bccc44e0",
"resource": {
"rule_set": {
"href": "/orgs/1/sec_policy/draft/rule_sets/6",
"name": "rule_set_3",
"scopes": [
[ {
"label": {
"href": "/orgs/1/labels/19",
"key": "app",
"value": "app2"
}
}, {
"label": {
"href": "/orgs/1/labels/20",
"key": "env",
"value": "env2"
}
}, {
"label": {
"href": "/orgs/1/labels/21",
"key": "loc",
"value": "loc2"
}
}
]
]
}
},
"changes": {
"name": {
"before": "rule_set_2",
"after": "rule_set_3"
}
},
"change_type": "update"
}],
"notifications": [],
"version": 2
}

```

Security Rule Created (JSON)

In this example of a successful `sec_rule` composite event, a new security rule is created. Because this is a creation event, the `before` values are `null`.

```

{ "href": "/orgs/1/events/xxxxxxxx-6d29-4905-ad32-ee863fb63697",
"timestamp": "2018-08-29T21:48:28.954Z",

```

```

"pce_fqdn": "pce24.bigco.com",
"created_by": {
  "user": {
    "href": "/users/1",
    "username": "albert.einstein@bigco.com"
  }
},
"event_type": "sec_rule.create",
"status": "success",
"severity": "info",
"action": {
  "uuid": "xxxxxxxx-165b-4e06-aaac-60e4d8b0b9a0",
  "api_endpoint": "/api/v2/orgs/1/sec_policy/draft/rule_sets/1/sec_rules",
  "api_method": "POST",
  "http_status_code": 201,
  "src_ip": "10.6.1.156"
},
"resource_changes": [{
  "uuid": "9fcf6feb-bf25-4de8-a68a-a50598df4cf6",
  "resource": {
    "sec_rule": {
      "href": "/orgs/1/sec_policy/draft/rule_sets/1/sec_rules/5"
    }
  },
  "changes": {
    "rule_list": {
      "before": null,
      "after": {
        "href": "/orgs/1/sec_policy/draft/rule_sets/1"
      }
    }
  },
  "description": {
    "before": null,
    "after": "WinRM HTTP/HTTPS and RDP"
  },
  "type": {
    "before": null,
    "after": "SecRule"
  },
  "resolve_labels": {
    "before": null,
    "after": "1010"
  },
  "providers": {
    "created": [{
      "provider": true,
      "actors": "ams"
    }]
  },
  "consumers": {
    "created": [{
      "provider": false,
      "actors": "ams"
    }], {
      "provider": false,

```

```

"ip_list": {
  "href": "/orgs/1/sec_policy/draft/ip_lists/1"
}
}],
},
"ingress_services": {
  "created": [{
    "href": "/orgs/1/sec_policy/draft/services/7",
    "name": "WinRM HTTP/HTTPS and RDP"
  }]
},
},
"change_type": "create"
}],
"notifications": [],
"version": 2
}

```

User Logged In (JSON)

```

[
{
  "href": "/orgs/1/events/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
  "timestamp": "2019-06-25T23:34:12.948Z",
  "pce_fqdn": "someFullyQualifiedDomainName",
  "created_by": {
    "user": {
      "href": "/users/1",
      "username": "someUser@someDomain"
    }
  },
  "event_type": "user.sign_in",
  "status": "success",
  "severity": "info",
  "action": {
    "uuid": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
    "api_endpoint": "/login/users/sign_in",
    "api_method": "POST",
    "http_status_code": 302,
    "src_ip": "xxx.xxx.xx.x"
  },
  "resource_changes": [
    {
      "uuid": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
      "resource": {
        "user": {
          "href": "/users/1",
          "type": "local",
          "username": "someUser@someDomain"
        }
      }
    }
  ],
  "changes": {
    "sign_in_count": {
      "before": 4,
      "after": 5
    }
  }
}
]

```

```

    },
    "change_type": "update"
  }
],
"notifications": [
  {
    "uuid": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
    "notification_type": "user.login_session_created",
    "info": {
      "user": {
        "href": "/users/1",
        "type": "local",
        "username": "someUser@someDomain"
      }
    }
  }
]
},
{
  "href": "/orgs/1/events/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
  "timestamp": "2019-06-25T23:34:15.147Z",
  "pce_fqdn": "someFullyQualifiedDomainName",
  "created_by": {
    "user": {
      "href": "/users/1",
      "username": "someUser@someDomain"
    }
  },
  "event_type": "user.login",
  "status": "success",
  "severity": "info",
  "action": {
    "uuid": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
    "api_endpoint": "/api/v2/users/login",
    "api_method": "GET",
    "http_status_code": 200,
    "src_ip": "xxx.xxx.xx.x"
  },
  "resource_changes": [

],
"notifications": [
  {
    "uuid": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
    "notification_type": "user.pce_session_created",
    "info": {
      "user": {
        "href": "/users/1",
        "username": "someUser@someDomain"
      }
    }
  }
]
}
]

```

User Logged Out (JSON)

```
[
{
  "href": "/orgs/1/events/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
  "timestamp": "2019-06-25T23:35:16.636Z",
  "pce_fqdn": "someFullyQualifiedDomainName",
  "created_by": {
    "user": {
      "href": "/users/1",
      "username": "someUser@someDomain"
    }
  },
  "event_type": "user.sign_out",
  "status": "success",
  "severity": "info",
  "action": {
    "uuid": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
    "api_endpoint": "/login/logout",
    "api_method": "GET",
    "http_status_code": 302,
    "src_ip": "xxx.xxx.xx.x"
  },
  "resource_changes": [

],
  "notifications": [
    {
      "uuid": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
      "notification_type": "user.login_session_terminated",
      "info": {
        "reason": "user_logout",
        "user": {
          "href": "/users/1",
          "username": "someUser@someDomain"
        }
      }
    }
  ]
},
{
  "href": "/orgs/1/events/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
  "timestamp": "2019-06-25T23:35:16.636Z",
  "pce_fqdn": "someFullyQualifiedDomainName",
  "created_by": {
    "user": {
      "href": "/users/1",
      "username": "someUser@someDomain"
    }
  },
  "event_type": "user.sign_out",
  "status": "success",
  "severity": "info",
  "action": {
    "uuid": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
```



```

    "api_endpoint": "/login/logout",
    "api_method": "GET",
    "http_status_code": 302,
    "src_ip": "xxx.xxx.xx.x"
  },
  "resource_changes": [

  ],
  "notifications": [
    {
      "uuid": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
      "notification_type": "user.login_session_terminated",
      "info": {
        "reason": "user_logout",
        "user": {
          "href": "/users/1",
          "username": "someUser@someDomain"
        }
      }
    }
  ]
}

```

Login Failed — Incorrect Username (JSON)

```

{
  "href": "/orgs/1/events/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
  "timestamp": "2019-06-25T23:35:41.560Z",
  "pce_fqdn": "someFullyQualifiedDomainName",
  "created_by": {
    "system": {
    }
  },
  "event_type": "user.sign_in",
  "status": "failure",
  "severity": "info",
  "action": {
    "uuid": "someFullyQualifiedDomainName",
    "api_endpoint": "/login/users/sign_in",
    "api_method": "POST",
    "http_status_code": 200,
    "src_ip": "xxx.xxx.xx.x"
  },
  "resource_changes": [

  ],
  "notifications": [
    {
      "uuid": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
      "notification_type": "user.login_failed",
      "info": {
        "associated_user": {
          "supplied_username": "invalid_username@someDomain"
        }
      }
    }
  ]
}

```

```

    }
  ]
}

```

Login Failed — Incorrect Password (JSON)

```

{
  "href": "/orgs/1/events/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
  "timestamp": "2019-06-25T23:35:27.649Z",
  "pce_fqdn": "someFullyQualifiedDomainName",
  "created_by": {
    "system": {
    }
  },
  "event_type": "user.sign_in",
  "status": "failure",
  "severity": "info",
  "action": {
    "uuid": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
    "api_endpoint": "/login/users/sign_in",
    "api_method": "POST",
    "http_status_code": 200,
    "src_ip": "xxx.xxx.xx.x"
  },
  "resource_changes": [
  ],
  "notifications": [
    {
      "uuid": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
      "notification_type": "user.login_failed",
      "info": {
        "associated_user": {
          "supplied_username": "someUser@someDomain"
        }
      }
    }
  ]
}

```

User Log Out (CEF)

This example of an event record in CEF shows a successful user log out.

```

CEF:0|Illumio|PCE|19.3.0|user.logout.success|User Logout Success|1|rt=Mar
06 2020
18:38:59.900 +0000 dvchost=mypce.com duser=system dst=10.6.5.4
outcome=success
cat=audit_events request=/api/v2/users/logout_from_jwt requestMethod=POST
reason=204
cs2= cs2Label=resource_changes
cs4=[{"uuid":"b5ba8bf0-7ca8-47fc-870f-6c61ddc1648d",
"notification_type":"user.pce_session_terminated","info":
{"reason":"user_logout",
"user":{"href":"/users/1","username":"testuser@mypce.com"}}}]
cs4Label=notifications

```

```
cn2=2 cn2Label=schema-version cs1Label=event_href cs1=/system_events/
e97bd255-4316-4b5e-a885-5b937f756f17
```

Workload Security Policy Updated (LEEF)

This example of an event record in LEEF shows a successful update of security policy for a workload's Ethernet interfaces.

```
LEEF:2.0|Illumio|PCE|18.2.0|interface_status.update.success|
src=xx.xxx.xxx.xxx
cat=organizational devTime=someUTCdatetime devTimeFormat=yyyy-mm-
dd'T'HH:mm:ss.ttttttZ
sev=1
usrName=albert.einstein url=/orgs/7/agents/someUUID version=2
pce_fqdn=someFQDN
created_by={"agent":{"href":"/orgs/7/agents/
someUUID","hostname":"someHostname"}}
action={"uuid":"someUUID",
"api_endpoint":"/api/v6/orgs/7/agents/xxxxxx/interface_statuses/update",
"api_method":"PUT","http_status_code":200,"src_ip":"someIP"}
resource_changes=[{"uuid":"someUUID",
"resource":{"workload":{"href":"/orgs/7/workloads/someUUID","name":null,
"hostname":"someHostname",
"labels":[{"href":"/orgs/7/labels/
xxxxxx","key":"loc","value":"test_place_1"},
{"href":"/orgs/7/labels/xxxxxx","key":"env","value":"test_env_1"},
{"href":"/orgs/7/labels/xxxxxx","key":"app","value":"test_app_1"},
{"href":"/orgs/7/labels/xxxxxx","key":"role","value":"test_access_1"}]}},
"changes":{"workload_interfaces":
{"updated":[{"resource":
{"href":"/orgs/7/workloads/someUUID/interfaces/eth1","name":"eth0",
"address":{"family":2,"addr":xxxxxxxx,"mask_addr":someMask}},
"changes":{"address":{"before":null,"after":
{"family":2,"addr":xxxxxxxx,"mask_addr":someMask}},
"cidr_block":{"before":null,"after":16},"default_gateway_address":
{"before":null,"after":
{"family":2,"addr":someGateway,"mask_addr":someMask}},
"link_state":{"before":"unknown","after":"up"},
"network":{"before":null,"after":{"href":"/orgs/7/networks/xx"}},
"network_detection_mode":{"before":null,"after":"single_private_brn"}}},
{"resource":{"href":"/orgs/7/workloads/someUUID/interfaces/eth1",
"name":"eth1","address":
{"family":2,"addr":someAddress,"mask_addr":someMask}},
"changes":{"address":{"before":null,"after":{"family":2,"addr":someAddress,
"mask_addr":someMask}},
"cidr_block":{"before":null,"after":16},"link_state":
{"before":"unknown","after":"up"},
"network":{"before":null,"after":{"href":"/orgs/7/networks/xx"}},
"network_detection_mode":{"before":null,"after":"single_private_brn"}}}]},
"change_type":"update"}] notifications=[] event_href=/orgs/7/events/someUUID
```

Differences from Previous Releases

The following table indicates which event names changed in the Illumio Core 18.2 release. If you are upgrading from a release prior to 18.2, be sure to use the current event name in your alert monitoring system.

Changed VEN Event Names

This table lists the names of VEN-related events prior to the Illumio Core 18.2 release and the names they were changed to in the 18.2 release.

Old Name Prior to 18.2	New Name as of 18.2
fw_config_change	agent.firewall_config
activation_success	agent.activate
activation_failure	
deactivation_success	agent.deactivate
deactivation_failure	

Events Monitoring Best Practices

The 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 the 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.

Monitoring Operational Practices

In addition to setting up an automated system, Illumio recommends implementing the following operational practices:

1. Determine the normal quantity of events from the Illumio Core and monitor the trend for changes; investigate spikes or reductions in the event generation rate.
2. Implement good operational practices to troubleshoot and investigate alerts, and to recover from events.
3. Do not monitor Illumio Core events in isolation. Monitor them as part of your overall system. Understanding the events in the context of your overall system activity can provide as much information as the events themselves.

Recommended Events to Monitor

As a best practice, Illumio recommends you monitor the following events at a minimum.

Events	Description
<p>Program name = <code>illumio_pce/system_health</code></p> <p>Severity = Warning, Error, or Fatal</p>	<p>Provides multiple systems metrics, such as CPU and memory data, for each node in a PCE cluster. The PCE generates these events every minute. The Severity field is particularly important. When system metrics exceed thresholds, the severity changes to warning, error, or fatal.</p> <p>For more information about the metrics and thresholds, see the PCE Administration Guide.</p> <p>Recommendation: Monitor <code>system_health</code> messages with a severity of warning or higher and correlate the event with other operational monitoring tools to determine if administrative intervention is required.</p>
<p><code>event_type="lost_agent.found"</code></p>	<p>Contains the information necessary to identify workloads with lost agents. A lost agent occurs when the PCE deletes a workload from its database but that workload still has a VEN running on it.</p> <p>Recommendation: Monitor <code>lost_agent.found</code> events and send alerts in case you need to pair the workloads' VENs with the PCE again.</p>
<p><code>event_type="system_task.agent_missed_heartbeats_check"</code></p>	<p>Lists the VENs that missed three heartbeats (usually 15 minutes). Typically, this event precedes the PCE taking the VENs offline to perform internal maintenance.</p> <p>This event triggers an alert to be sent at 25% of the time configured in the offline timer. For example, if the offline timer is configured to 1 hour, an alert is sent after the VEN has not sent a heartbeat for 15 minutes; if the offline timer is configured to 4 hours, an alert is sent after the VEN hasn't sent a heartbeat for 1 hour.</p> <p>Recommendation: Monitor these events for high-value workloads because the PCE can take these workloads offline when the VENs miss 12 heartbeats (usually 60 minutes).</p>
<p><code>event_type="system_task.agent_offline_check"</code></p>	<p>Lists VENs that the PCE has marked offline, usually because they missed 12 heartbeats. The VENs on these workloads haven't communicated with the PCE for an hour and it removed the workloads from policy.</p> <p>Recommendation: Monitor these events for high-value workloads because they indicate change in the affected workloads' security posture.</p>
<p><code>event_type="agent.suspend"</code></p>	<p>Indicates that the VEN is suspended and no longer protecting the workload. If you did not intentionally run the VEN suspend command on the workload, this event can indicate the workload is under attack.</p> <p>Recommendation: Monitor these events for high-value workloads.</p>
<p><code>event_type="agent.tampering"</code></p>	<p>Indicates tampering of the workload's Illumio managed firewall and that the VEN recovered the firewall. Firewall tampering is one of the first signs that a workload is compromised. During a tampering attempt, the VEN and PCE continue to protect the workload; however, you should investigate the cause of the event.</p> <p>Recommendation: Monitor these events for high-value workloads.</p>

Events	Description
event_type="agent.update"	<p>Contains the state data that the VEN regularly sends to the PCE. Typically, these events contain routine information; however, the VEN can attach a notice indicating the following issues:</p> <ul style="list-style-type: none"> Processes not running Policy deployment failure <p>Recommendation: Monitor <code>agent.update</code> events that include notifications because they indicate workloads that might require administrative intervention.</p>
event_type="rule_set.create"	<p>Contains the labels indicating the scope of a draft ruleset. Illumio Core generates these events when you create, update, or delete a draft ruleset. When you include "All Applications," "All Environments," or "All Locations" in a ruleset scope, the PCE represents that label type as a null HREF. Ruleset scopes that are overly broad affect a large number of workloads. Draft rulesets do not take effect until they are provisioned.</p> <p>Recommendation: Monitor these events to pinpoint ruleset scopes that are unintentionally overly broad.</p>
event_type="rule_set.update"	
event_type="rule_sets.delete"	
event_type="sec_rule.create"	<p>Contains labels indicating when all workloads affected, all services, or a label/label-group are used as a rule provider or consumer. Illumio Core generates these events when you create, update, or delete a draft ruleset. The removed or added labels could represent high-value applications or environments.</p> <p>Recommendation: Monitor these events for high-value labels.</p>
event_type="sec_rule.update"	
event_type="sec_rule.delete"	
event_type="sec_policy.create"	<p>[NEW in Illumio Core 19.3.0] Contains the <code>workloads_affected</code> field, which includes the number of workloads affected by a policy. Illumio Core generates this event when you provision draft policy that updates the policy on affected workloads. The number of affected workloads could be high or a significant percentage of your managed workloads.</p> <p>Recommendation: Monitor the <code>workloads_affected</code> field for a high number of affect workloads. If the number exceeds an acceptable threshold, investigate the associated the policy.</p>
event_type="agent.clone_detected"	<p>The PCE detects cloned VENs based on clone token mismatch. This is a special alert from the Illumio Core release 19.3.2 onwards, as clones have become a higher priority. Volume of these events make the severity level important and not the fact that these events occurred.</p> <p>Recommendation: If severity is 1 or 'error', some intervention may be needed.</p>



NOTE

Automatic Cloned VEN Remediation

For on-prem domain joined Windows workloads, cloned VENs support automatic clone remediation by detecting changes to the workload's domain Security identifier (SID). After the VEN reports such changes to the PCE, the PCE tells the clone to re-activate itself, after which the cloned VEN is remediated and becomes a distinct agent from the original VEN.

Events Setup

This section describes PCE settings related to events and how to use them to configure PCE behavior.

Requirements for Events Framework

To use the events framework, ensure that you allocate enough disk space for event data, and be familiar with the disk capacity requirements.

Database Sizing for Events

Disk space for a single event is estimated at an average 1,500 bytes.



CAUTION

As the number of events increases, the increase in disk space is not a straight line. The projections below are rough estimates. Disk usage can vary in production and depends on the type of messages stored.

Number of Events	Disk Space
25 million	38GB
50 million	58GB

Data and Disk Capacity for Events

For Illumio Core Cloud customers, Illumio Operations manages all data and disk capacity requirements and configuration for events; including the default events data retention period, database dumps with and without events data, and disk compacting.

For more information, contact your Illumio Support representative.

Events Preview Runtime Setting

If you participated in the preview of Events in 18.1.0, the preview was enabled by configuring a setting in your PCE `runtime_env.yml` file.



WARNING

Remove preview parameter from `runtime_env.yml`

Before you upgrade to the latest release, you must remove `v2_auditable_events_recording_enabled: true` from `runtime_env.yml`. Otherwise, the upgrade does not succeed.

Removing this preview parameter does not affect the collection of “organization events” records, which continue to be recorded.

To remove the Events preview setting:

1. Edit the `runtime_env.yml` file and remove the line `v2_auditable_events_recording_enabled`:

```
v2_auditable_events_recording_enabled: true
```

If you are not participating in any other previews, you can also remove the line `enable_preview_features`.

2. Save your changes.

Events Settings

The following section describes how to configure the Events Settings in the PCE web console.

Events Are Always Enabled

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 Settings in PCE Web Console

From the PCE web console, you can change the following event-related settings:

- **Event Severity:** Sets the severity level of events to record. Only messages at the set severity level and higher are recorded. The default severity is “Informational.”
- **Retention Period:** The system retains event records for a specified number of days; from 1 day to 200 days with the default period being 30 days.
- **Event Pruning:** The system automatically prunes events based on disk usage and the age of events; events older than the retention period are pruned. When pruning is complete, the `system_task.prune_old_log_events` event is recorded.
- **Event Format:** Sets the message output to one of the three formats. The selected message output format only applies to messages that are sent over syslog to a SIEM. The REST API always returns events in JSON.
 - JavaScript Object Notation (JSON): The default; accepted by Splunk and QRadar SIEMs
 - Common Event Format (CEF): Accepted by ArcSight
 - Log Event Extended Format (LEEF): Accepted by QRadar

Event Severity Levels

Severity	Description
Emergency	System is unusable

Severity	Description
Alert	Should be corrected immediately
Critical	Critical conditions
Error	Error conditions
Warning	Might indicate that an error will occur if action is not taken
Notice	Events that are unusual, but not error conditions
Informational	Normal operational messages that require no action
Debug	Information useful to developers for debugging the application

Output Format Change

The output format can be changed in the PCE web console:

- JSON (default)
- CEF
- LEEF

Records are in JSON format until you change to one of the other formats. Then, the new events are recorded in the new format; however, the earlier events are not changed to the selected format and they remain recorded in JSON.

Set Event Retention Values

You can set the event retention values depending on the specific conditions described below.

If you are using a SIEM, such as Splunk as the primary long-term storage for events and traffic in a dynamic environment, consider setting the event retention period to 7 days. On setting it to 7 days, you can use the PCE Troubleshooting or Events Viewer to quickly troubleshoot and diagnose events. The benefit of setting 7 days is that if an issue occurs on a Friday, it can still be diagnosed on the following Monday. A large number of events are generated in a dynamic environment, which increases the data stored (disk space used), backup size, and so on. The period of 7 days provides a good balance between disk usage and the ability to troubleshoot.



NOTE

A dynamic environment is when applications and infrastructure are subject to frequent changes; for example, usage of APIs, ETL, Containers, and so on.

If you are using a SIEM in a non-dynamic environment, consider setting the event retention period to 30 days. A smaller number of events are generated, and less disk space is used in a non-dynamic environment.

If you are not using a SIEM such as Splunk and the PCE is the primary storage for the events data used for reporting, diagnosis, and troubleshooting, set the event retention period as

per the organization's record retention policy, such as 30 days. If you generate quarterly reporting using events, set the event retention period to 90 days.

SIEM	Consideration	Value
Yes: Primary storage for events	If primary storage of events is not on the PCE	7 days (PCE troubleshooting) 1 day (minimum)
No: Not primary storage for events	If primary storage of events is on the PCE, consider the organization's record retention policy as well as the available disk and event growth pattern	30 days (default)
No	<ul style="list-style-type: none"> If the organization's record retention is more than 30 days If disk monitoring is not set up, it is required to set up disk monitoring 	As per your record retention policy 200 days (maximum)
Not applicable	If events data is not needed for reporting or troubleshooting	1 day (minimum)

If disk space availability and event growth projections indicate that the desired retention period cannot be safely supported, consider using a SIEM because the PCE might not store events for the desired period.



NOTE

Running the `illumio-pce-db-management events-db` command provides an output of the average number of events and the storage used.

Configure Events Settings in PCE Web Console

1. From the PCE web console menu, choose **Settings** > **Event Settings** to view your current settings.
2. Click **Edit** to change the settings.
 - For Event Severity, select from the following options:
 - Error
 - Warning
 - Informational
 - For Retention Period, enter the number of days you want to retain data.
 - For Event Format, select from the following options:
 - JSON
 - CEF
 - LEEF
3. Click **Save** once you're done.

Limits on Storage

From the Illumio Core 19.3.1 release onwards, the PCE will automatically limit the maximum number of events stored. The limits are set on the volume of events stored locally in the PCE database, so that the events recorded in the database do not fill up the disk. The limit is a percentage of the disk capacity, cumulative for all services that store events on the disk.



IMPORTANT

To change the default limits, contact Illumio Support.

The configuration limit includes both hard and soft limits.

- Soft limit: 20% of disk used by event storage
Aggressive pruning is triggered when the soft limit is reached. However, new events are still recorded while pruning. On the Events list page of the PCE Web Console, the `system_task.prune_old_log_events` event is displayed with the "Object creation soft limit exceeded" message and 'Severity: Informational'.
- Hard limit: 25% of disk used by event storage.
More aggressive pruning is triggered when the hard limit is reached. New events are not recorded while pruning. On the Events list page of the PCE Web Console, the `system_task.prune_old_log_events` event is displayed with the message "Object creation hard limit exceeded" message and 'Severity: Error'. The pruning continues until the soft limit level of 20% is reached. When this occurs, a `system_task.hard_limit_recovery_completed` event occurs, and the PCE starts to behave as it did for the soft limit conditions.

SIEM Integration for Events

For analysis or other needs, event data can be sent using syslog to your own analytics or SIEM systems.

About SIEM Integration

This guide also explains how to configure the PCE to securely transfer PCE event data in the following message formats to some associated SIEM systems:

- JavaScript Object Notation (JSON), needed for SIEM applications, such as Splunk®.
- Common Event Format (CEF), needed for SIEM applications, such as Micro Focus Arc-Sight®.
- Log Event Extended Format (LEEF), needed for SIEM applications, such as IBM QRadar®.

Syslog Forwarding

The PCE can export logs to syslog. You can also use the PCE's own internal syslog configuration.

Identify Events in Syslog Stream

Event records from the syslog stream are identified by the following string:

```
"version":2
```

AND

```
'"href":\s*" /orgs/[0-9]*/events' OR '"href":\s*" /system_events/ '
```

Forward Events to External Syslog Server

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**.

Add Repository

* Description

* Address

* Protocol

TCP

* Port

* TLS

Enabled

* Trusted CA Bundle

Choose File

no file selected

* Verify TLS

☒ Ensure that TLS peer's server certificate is valid

Cancel

OK

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 check-box to ensure that the TLS peer’s server certificate is valid.

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

After ensuring that the events are being forwarded as configured to the correct external syslog servers, you can choose to stop using the “Local” server by editing the local server setting and deselect all message types.



NOTE

You cannot delete the “Local” server.

Disable Health Check Forwarding

PCE system health messages are useful for PCE operations and monitoring. You can choose to forward them if they are needed on the remote destination.

For example, IBM QRadar is usually used by security personnel, who might not need to monitor the PCE system health. The Illumio App for QRadar does not process the PCE system health messages.

The PCE system health messages are only provided in key/value syslog format. They are not translatable into CEF, LEEF, or JSON formats. If your SIEM does not support processing key/value messages in syslog format, do not forward system health messages to those SIEMs. For example, IBM QRadar and Micro Focus ArcSight do not automatically parse these system health messages.

To disable syslog forwarding of health check messages:

1. From the PCE web console menu, choose **Settings > Event Settings**.
2. Click the Event listed under the **Events** column.

Event Settings

[Edit](#)

Events

Event Severity Informational
Only audit events of this severity or higher are saved

Retention Period 30 days
Audit events older than this are purged

Event Format JSON

Event Forwarding [+ Add](#) [- Remove](#) [Refresh](#)

Repository	Events
<input type="checkbox"/> Local	Organizational, System, Allowed, Potentially Blocked, Blocked, System Health Messages

3. Under the Events block, for the Status Logs entry, deselect **System Health Messages**. System health check is only available in key-value format. Selecting a new event format does not change the system health check format to CEF or LEEF.

<

Event Settings – (Edit Event Forwarding)

Save

Cancel

Forwarding

* PCE

de o

* Repository

☒ Local
Forward events to local syslog service

☐ test (10 UDI .1)
Forwarded event data is not encrypted

Add Repository

Events

Auditable Events

☒ Organizational Events
☒ System Events

Traffic Events

☒ Allowed
☐ Potentially Blocked
☐ Blocked

Status Logs

☐ System Health Messages
Only key-value format is supported

4. Click **Save**.



NOTE

IBM QRadar and HP ArcSight do not support system health messages. If you are using either of these for SIEM, make sure that you do not select the System Health Messages checkbox.

Traffic Flow Summaries

This section describes traffic flow summaries.

After you install a VEN on a workload and pair the VEN with the PCE, the VEN monitors each workload's traffic flows and sends the traffic flow summaries to the PCE.

Traffic summaries can be exported to syslog or Fluentd. If traffic data is configured for export, the PCE processes the received traffic flow summaries from each VEN and immediately sends them to syslog or Fluentd.

Traffic Flow Types and Properties

The Illumio Core logs traffic flows based on the Visibility setting. Events have attributes that can be Allowed, Blocked, or Potentially Blocked and might not appear in the traffic flow summary.

Visibility Settings

The table below indicates whether or not a traffic summary is logged as Allowed, Potentially Blocked, or Blocked depending on a workload's policy state.



NOTE

Traffic from workloads in the "Idle" policy state is not exported to syslog from the PCE.

Visibility	Logged in Traffic Flow Summary
Off	VEN does not log traffic connection information
Blocked - Low Detail	VEN logs connection information for blocked and potentially blocked traffic only
Blocked + Allowed - High Detail	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

Event Types

In a traffic flow summary, the event type is designated by Policy Decision (pd).



NOTE

An asterisk (*) indicates the attribute might not appear in the summary.

Event Attributes	Allowed (pd=0)	Potentially Blocked (pd=1)	Blocked (pd=2)	Unknown (pd=3)
version	✓	✓	✓	✓
count	✓	✓	✓	✓

Event Attributes	Allowed (pd=0)	Potentially Blocked (pd=1)	Blocked (pd=2)	Unknown (pd=3)
interval_sec	✓	✓	✓	✓
timestamp	✓	✓	✓	✓
dir	✓	✓	✓	✓
src_ip	✓	✓	✓	✓
dst_ip	✓	✓	✓	✓
proto	✓	✓	✓	✓
dst_prt	✓	✓	✓	✓
state	✓	✓	✓	✓
pd	✓	✓	✓	✓
code*	✓	✓	✓	✓
type*	✓	✓	✓	✓
dst_vulns*	✓	✓	✓	✓
fqdn*	✓	✓	✓	✓
un*	✓	✓	✗	✓
pn*	✓	✓	✗	✓
sn*	✓	✓	✗	✓
src_labels*	✓	✓	✓	✓
dst_labels*	✓	✓	✓	✓
src_hostname*	✓	✓	✓	✓
dst_hostname*	✓	✓	✓	✓
src_href*	✓	✓	✓	✓
dst_href*	✓	✓	✓	✓

Show Amount of Data Transfer

The JSON, CEF, and LEEF for the accurate byte count work events are related to the 'Show Amount of Data Transfer' preview feature available with the Illumio Core 20.2.0 release.

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

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

Destination Total Bytes Out: Number of bytes transferred out of provider:

```
dst_tbo
```

Destination Total Bytes In: Number of bytes transferred in to provider.

```
dst_tbi
```

To activate the 'Show Amount of Data Transfer' capability on the PCE, contact your Illumio representative.

LEEF Mapping

- LEEF field `x` contains JSON field `y`
- `srcBytes` contains `dst_tbo`
- `dstBytes` contains `dst_tbi`
- `dbi` contains `dst_dbi`
- `dbo` contains `dst_dbo`

CEF Mapping

- CEF field `cn2` is `dst_dbi` with `cn2Label` is "dbi"
- CEF field `cn3` is `dst_dbo` with `cn3Label` is "dbo"
- CEF field "in" is `dst_tbi`
- CEF field "out" is `dst_tbo`

Manage Traffic Flows Using REST API



You can use the following properties to manage traffic flows using the REST API.







NOTE



You should ignore and *not* use any extra properties that are not described in this document, such as `tbi`, `tbo`, `dbi`, and `dbo`.

Property	Description	Type	Re-quired	Possible Values
<code>version</code>	The version of the flow summary schema.	Integer	Yes	4

Property	Description	Type	Re-quired	Possible Values
timestamp	Indicates the time (RFC3339) when the first flow in the summary was created, represented in UTC. Format: <code>yyyy-MM-dd'T'HH:mm:ss.SSSSSSZ</code>	String	Yes	
interval_sec	Sample duration for the flows in the summary. Default is approximately 600 seconds (10 minutes), depending on the VEN's ability to report traffic and PCE's current load.	Integer	Yes	
dir	Direction of the first packet: in or out (I, O).	String	Yes	I, O
src_ip	Source IP of the flows.	String	Yes	
dst_ip	Destination IP of the flows.	String	Yes	
proto	Protocol number (0-255).	Integer	Yes	Minimum=0 Maximum=255
type	The ICMP message type associated with the first flow in the summary. This value exists only if protocol is ICMP (1). <div>  NOTE This information is included in blocked flows for VEN versions lower than 19.1.0. It is included in all flows for VEN version 19.1.0 and later. </div> Example: 3 for "Destination Unreachable."	Integer	No	Minimum=0 Maximum=255
code	The ICMP message code (subtype) associated with the first flow in the summary. This value exists only if protocol is ICMP (1). <div>  NOTE This information is included in blocked flows for VEN versions lower than 19.1.0. It is included in all flows for VEN version 19.1.0 and later. </div> Example: 1 for "Destination host unreachable."	Integer	No	Minimum=0 Maximum=255
dst_port	Destination port. This value exists only if protocol is not TCP (6) or UDP (17).	Integer	Yes	Minimum=0 Maximum=65535

Property	Description	Type	Re-quired	Possible Values
pd	<p>Policy decision value, which indicates if the flow was allowed, potentially blocked (but allowed), blocked, or unknown.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • 0 - Allowed traffic • 1 - Allowed traffic but will be blocked after policy enforcement • 2 - Blocked traffic • 3 - Unknown <div>  <p>NOTE Policy decision is “unknown” in the following cases:</p> <ul style="list-style-type: none"> • Flows uploaded using existing bulk API (<code>/orgs/<org_id>/agents/bulk_traffic_flows</code>). • Flows uploaded using Network Flow Ingest Application (<code>/orgs/<org_id>/traffic_data</code>). • Traffic reported by idle VENs and specifically those that have been reported with “s” state (snapshot). </div>	Integer	Yes	<p>Minimum=0</p> <p>Maximum=3</p>
count	Count of the number of flows in the flow summary.	Integer	Yes	
state	<p>Session state for the traffic flows in the flow summaries.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • Active (A): Connection was still open at the time the flow summary was logged. Applies to allowed and potentially blocked flows. • Closed (C): (Linux only) Connection closed at the time the flow summary was logged. Applies to allowed and potentially blocked flows. • Timed out (T): Connection timed out at the time the flow summary was logged. Applies to allowed and potentially blocked flows. Due to a limitation of WFP, a Windows VEN will report “T” even when the connection is closed at the time the flow summary was logged. • Snapshot (S): Snapshot of current connections to and from the VEN, which applies only to workloads whose policy state is set to Idle. Applies to allowed and potentially blocked flows. • New connection (N): Dropped TCP packet contains a SYN and is associated with a new connection. Applies to blocked TCP flows. The value is empty for blocked UDP flows. 	String	No	A, C, T, S, N

Property	Description	Type	Re- quired	Possible Values
pn	<p>The program name is associated with the first flow of the summary. It is supported on inbound flows for Linux and Windows VEN and on outbound flows for only Windows VEN.</p> <div>  <p>NOTE This information might not be available on short-lived processes, which are Linux-specific.</p> </div> <p>Currently, flows are aggregated, so this value might represent only the first process detected across all aggregated flows.</p> <p>If network communication is done by an OS component (or a driver), no process is associated with it.</p>	String	No	
un	<p>The username is associated with the first flow of the summary. It is supported on inbound flows for Linux and Windows VEN and on outbound flows for only Linux VEN.</p> <p>On Windows, it can include the username of the user account that initiated the connection.</p> <div>  <p>NOTE This information might not be available on short-lived processes.</p> </div>	String	No	
sn	Service name associated with the first flow in the summary. It is supported only on inbound flows on Windows VEN.	String	No	
src_hostname	Hostname of the source workload that reported the flow.	String	No	
src_href	HREF of the source workload that reported the flow.	String	No	
src_labels	Labels applied to the source workload.	Object	No	
	<div>  <p>NOTE The <code>src_hostname</code>, <code>src_href</code>, and <code>src_labels</code> values are not included in a traffic summary if the source of the flow is not an Illumio-labeled workload. For example, Internet traffic or a managed workload without any labels applied.</p> </div>			

Property	Description	Type	Re-quired	Possible Values
<code>dst_hostname</code>	Hostname of the destination workload that reported the flow.	String	No	
<code>dst_href</code>	HREF of the destination workload that reported the flow.	String	No	
<code>dst_labels</code>	Labels applied to the destination workload.	Object	No	
<div>  NOTE The <code>dst_hostname</code>, <code>dst_href</code>, and <code>dst_labels</code> values are not be included in a traffic summary if the destination of the flow is not an Illumio-labeled workload. For example, Internet traffic or a managed workload without any labels applied. </div>				
<code>dst_vulns</code>	Information about the vulnerabilities on the destination of the traffic flow with the specific port and protocol.	Object	No	
<div>  NOTE <ul style="list-style-type: none"> Vulnerabilities are defined by Common Vulnerabilities and Exposures (CVE), with identifiers and descriptive names from the U.S. Department of Homeland Security National Cybersecurity Center. The vulnerability information is sent only when the Vulnerability Maps feature is turned on via a license and the information is imported into the PCE from a Vulnerability Scanner, such as Qualys. </div>				
<code>fqdn</code>	Fully qualified domain name	String	No	

The following table describes the sub-properties for the `dst_vulns` property:

Sub-property	Description	Type	Required
<code>count</code>	The total number of existing vulnerabilities on the destination port and protocol.	Integer	No
<code>max_score</code>	The maximum of all the scores for the vulnerabilities on the destination port and protocol.	Number	No
<code>cve_ids</code>	The list of CVE-IDs associated with the vulnerabilities that have the maximum score. Up to 100 displayed .	Array	No

Export Traffic Flow Summaries

Decide where to export the traffic flow summaries: syslog or Fluentd.



CAUTION

By default, from the 19.3.0 release on, the PCE generates all traffic flow summaries and sends them to syslog.

If you have not configured syslog, the syslog data by default is written to a local disk. For example, it is written to `/var/log/messages`.

Export to Syslog

To configure and export the traffic flow summaries to a remote syslog, follow these steps:

1. From the PCE web console menu, choose **Settings > Event Settings**.
2. Enable a remote syslog destination.
3. Select specific traffic flow summaries to be sent to remote syslog.
This filters the selected traffic flow summaries and send those to the remote syslog.

To prevent the syslog data from being written to a local disk based on your preference, deselect the Events checkboxes on the **Settings > Event Settings > Local** page in the PCE web console. For more information, see [Events Settings. \[200\]](#)



NOTE

The generation of all traffic flow summaries is implemented to ensure that all of the traffic flow summaries are controlled from the PCE web console only.

This example shows the `runtime_env.yml` configuration to generate all types of flow summaries.

Export to Syslog

```
export_flow_summaries_to_syslog:
- accepted
- potentially_blocked
- blocked
```

This example shows the `runtime_env.yml` configuration if you do not want to generate any types of flow summaries.

Export to Syslog

```
export_flow_summaries_to_syslog:
- none
```

**NOTE**

Illumio does not currently support having a primary and secondary syslog configuration, with disaster recovery and failover.

You can configure it on a system syslog (local) and use the internal syslog configuration to send messages to local, which sends to system syslog.

Export to Fluentd

To generate and export the traffic flow summaries to Fluentd, follow these steps:

1. Set the `export_flow_summaries_to_fluentd` parameter in `runtime_env.yml`.
2. Set the `external_fluentd_aggregator_servers` parameter in `runtime_env.yml`.

This example shows the `runtime_env.yml` configuration to generate two types of flow summaries, out of the three possible types.

Export to Fluentd

```
external_fluentd_aggregator_servers:
- fluentd-server.domain.com:24224
export_flow_summaries_to_fluentd:
- accepted
- blocked
```

Flow Duration Attributes

The 20.2.0 VEN sends two new attributes to the syslog and fluentd output. The new attributes describe the flow duration and are appended to the flow data.

- **Delta flow duration in milliseconds (`ddms`):** The duration of the aggregate within the current sampling interval. This field enables you to calculate the bandwidth between two applications in a given sampling interval. The formula is $\text{dbo} (\text{delta bytes out}) / \text{delta_duration_ms}$, or $\text{dbi} / \text{delta_duration_ms}$.
- **Total flow duration in milliseconds (`tdms`):** The duration of the aggregate across all sampling intervals. This field enables you to calculate the average bandwidth of a connection between two applications. The formula is $\text{tbo} (\text{total bytes out}) / \text{total_duration_ms}$, or $\text{tbo} / \text{total_duration_ms}$. It also enables you to calculate the average volume of data in a connection between two applications. The formula is $\text{tbo} (\text{total bytes out}) / \text{count}$ (number of flows in an aggregate), or $\text{tbi} / \text{count}$.

Traffic Flow Summary Examples

The following topic provides examples of traffic flow summaries in JSON, CEF, and LEEF, and messages that appear in syslog.

JSON

```
{
  "interval_sec": 600,
  "count": 1,
  "tbi": 73,
  "tbo": 0,
  "pn": "example-daemon",
  "un": "example",
  "src_ip": "xxx.xxx.xx.xxx",
  "dst_ip": "xxx.x.x.xxx",
  "timestamp": "2018-05-23T16:07:12-07:00",
  "dir": "I",
  "proto": 17,
  "dst_port": 5353,
  "state": "T",
  "src_labels": {
    "app": "AppLabel",
    "env": "Development",
    "loc": "Cloud",
    "role": "Web"
  },
  "src_hostname": "test-ubuntu-3",
  "src_href": "/orgs/1/workloads/xxxxxxxx-7741-4f71-899b-d6f495326b3f",
  "dst_labels": {
    "app": "AppLabel",
    "env": "Development",
    "loc": "AppLocation",
    "role": "Database"
  },
  "dst_hostname": "test-ubuntu-2",
  "dst_href": "/orgs/1/workloads/xxxxxxxx-012d-4651-b181-c6f2b269889e",
  "pd": 1,
  "dst_vulns": {
    "count": 8,
    "max_score": 8.5,
    "cve_ids": [
      "CVE-2016-2181",
      "CVE-2017-2241"
    ]
  },
  "fqdn": "xxx.ubuntu.com",
  "version": 4
}
```

Syslog

```
2019-02-11T22:50:15.587390+00:00 level=info host=detest01 ip=100.1.0.1
program=illumio_pce/collector| sec=925415.586 sev=INFO pid=9944
tid=30003240
rid=bb8ff798-1ef2-44b1-b74e-f13b89995520 {"interval_sec":1074,
"count":1,"tbi":3608,
"tbo":0,"pn":"company-daemon","un":"company","src_ip":"10.0.2.15",
"dst_ip":"211.0.0.232",
"class":"M","timestamp":"2019-02-11T14:48:09-08:00","dir":"I",
"proto":17,
```

```
"dst_port":5353,"state":"T","src_labels":{"app":"AppName",
"env":"Development","loc":"Cloud","role":"Web"},
"src_hostname":"dev-ubuntu-1",
"src_href":"/orgs/1/workloads/773f3e81-5779-4753-b879-35alabe45838",
"dst_labels":{"app":"AppName","env":"Development","loc":"Cloud2",
"role":"Web"},
"dst_hostname":"dev-ubuntu-1","dst_href":"/orgs/1/workloads/
773f3e81-5779-4753-b879-35alabe45838","pd":0,"dst_vulns":{"count":1,
"max_score":3.7,
"cve_ids":["CVE-2013-2566","CVE-2015-2808"]},"fqdn":"xxx.ubuntu.com",
"version":4}
```

Allowed Flow Summary (pd = 0)

```
2016-01-12T05:23:30+00:00 level=info host=myhost ip=127.0.0.1
program=illumio_pce/
collector| sec=576210.952 sev=INFO pid=25386 tid=16135120 rid=0
{"interval_sec":1244,"count":3,"dbi":180,"dbo":180,"pn":"sshd","un":"root",
"src_ip":"10.6.0.129","dst_ip":"10.6.0.129","timestamp":"2017-08-16T13:23:57
-07:00",
"dir":"I","proto":6,"dst_port":22,"state":"A","dst_labels":
{"app":"test_app_1","env":
"test_env_1","loc":"test_place_1","role":"test_access_1"},"dst_hostname":"co
rp-vm-2",
"dst_href":"/orgs/1/workloads/5ddcc33b-b6a4-4a15-b600-64f433e4ab33","pd":0,
"version":4}
```

Potentially Blocked Flow Summary (pd = 1)

```
2016-01-12T05:29:21+00:00 level=info host=myhost ip=127.0.0.1
program=illumio_pce/
collector| sec=576561.327 sev=INFO pid=25386 tid=16135120 rid=0
sec=920149.541
sev=INFO pid=1372 tid=30276700 rid=136019d0-f9d8-45f3-ac99-f43dd8015675
{"interval_sec":600,"count":1,"tbi":229,"tbo":0,"src_ip":"172.16.40.5",
"dst_ip":"172.16.40.255","timestamp":"2017-08-16T14:45:58-07:00","dir":"I",
"proto":17,"dst_port":138,"state":"T","dst_labels":{"app":"test_app_1",
"env":"test_env_1","loc":"test_place_1","role":"test_access_1"},"dst_hostnam
e":
"corp-vm-2","dst_href":"/orgs/1/workloads/5ddcc33b-b6a4-4a15-
b600-64f433e4ab33",
"pd":1,"version":4}
```

Blocked Flow Summary (pd = 2)

```
2016-01-12T05:23:30+00:00 level=info host=myhost ip=127.0.0.1
program=illumio_pce/
collector| sec=576210.831 sev=INFO pid=25386 tid=16135120 rid=0
sec=915000.311
sev=INFO pid=1372 tid=30302280 rid=90a01be5-a3c1-44f9-84fd-3c3a5eaec1f8
{"interval_sec":589,"count":1,"src_ip":"10.6.1.89","dst_ip":"10.6.255.255",
"timestamp":"2017-08-16T13:22:09-07:00","dir":"I","proto":17,"dst_port":138,
"dst_labels":{"app":"test_app_1","env":"test_env_1","loc":"test_place_1",
"role":"test_access_1"},"dst_hostname":"corp-vm-1","dst_href":"/orgs/1/
workloads/
a83ba658-576b-4946-800a-b39ba2a2e81a","pd":2,"version":4}
```

Unknown Flow Summary (pd = 3)

```
2019-06-14T05:33:45.442561+00:00 level=info host=devtest0 ip=127.0.0.1
program=illumio_pce/collector| sec=490425.442 sev=INFO pid=12381
tid=32524120
rid=6ef5a6ac-8a9c-4f46-9180-c0c91ef94759
{"dst_port":1022,"proto":6,"count":20,
"interval_sec":600,"timestamp":"2019-06-06T21:03:57Z","src_ip":"10.23.2.7",
"dst_ip":"10.0.2.15","dir":"O","state":"S","pd":3,"src_href":"/orgs/1/
workloads/
a0d735ce-c55f-4a38-965f-bf6e98173598","dst_hostname":"workload1",
"dst_href":"/orgs/1/workloads/a20eblb5-10a4-419e-
b216-8b35c795a01e","src_labels":
{"app":"app","env":"Development","loc":"Amazon","role":"Load Balancer"}
,"version":4}
```

CEF

```
CEF:0|Illumio|PCE|2015.9.0|flow_potentially_blocked|Flow Potentially
Blocked|3|
act=potentially_blocked cat=flow_summary deviceDirection=0 dpt=137
src=someIPAddress
dst=someIPAddress proto=udp cnt=1 in=1638 out=0 rt=Jun 14 2018 01:50:14
cnl=120 cnlLabel=interval_sec cs2=T cs2Label=state cs6=/orgs/1/workloads/
someID cs6Label=dst_href
cs4={"app":"CRM","env":"Development","loc":"AppLocation",
"role":"Web"} cs4Label=dst_labels dhost=connectivity-check.someDomainName
cs1={"count":1,"max_score":3.7,"cve_ids":
["CVE-2013-2566","CVE-2015-2808"]}
cs1Label=dst_vulns dvchost=someDomainName
```

Unknown Flow Summary (pd = 3)

```
2019-06-14T21:02:55.146101+00:00 level=info host=devtest0 ip=127.0.0.1
program=illumio_pce/collector| sec=546175.145 sev=INFO pid=15416
tid=40627440
rid=f051856d-b9ee-4ac8-85ea-4cb857eefa82 CEF:0|Illumio|PCE|19.3.0|
flow_unknown|
Flow Unknown|1|act=unknown cat=flow_summary deviceDirection=0 dpt=22
src=10.0.2.2
dst=10.0.2.15 proto=tcp cnt=6 in=6 out=6 rt=Jun 14 2019 21:02:25
duser=root
dproc=sshd cnl=31 cnlLabel=interval_sec cs2=S cs2Label=state
dhost=workload1
cs6=/orgs/1/workloads/a20eblb5-10a4-419e-b216-8b35c795a01e
cs6Label=dst_href
dvchost=devtest0.ilabs.io msg=
{"trafclass_code":"U"}
```

LEEF

```
LEEF:2.0|Illumio|PCE|2015.9.0|flow_blocked|cat=flow_summary
devTime=2018-06-14T10:38:53-07:00 devTimeFormat=yyyy-MM-dd'T'HH:mm:ssX
proto=udp sev=5 src=someIPAddress dst=someIPAddress dstPort=5353 count=15
dir=I intervalSec=56728 dstHostname=someHostName dstHref=/orgs/1/workloads/
someID
```

```
dstLabels={"app":"CRM","env":"Development","loc":"Cloud","role":"Web"}
dstVulns={"count":2,"max_score":3.7} dstFqdn=someDomainName "cve_ids":
["CVE-2013-2566","CVE-2015-2808"]}
```

Unknown Flow Summary (pd = 3)

```
2019-06-14T19:25:53.524103+00:00 level=info host=devtest0 ip=127.0.0.1
program=illumio_pce/collector| sec=540353.474 sev=INFO pid=9960 tid=36072680
rid=49626dfa-d539-4cff-8999-1540df1a1f61 LEEF:2.0|Illumio|PCE|19.3.0|
flow_unknown|cat=flow_summary devTime=2019-06-06T21:03:57Z
devTimeFormat=yyyy-MM-dd'T'HH:mm:ssX proto=tcp sev=1 src=10.23.2.7
dst=10.0.2.15 dstPort=1022 count=20 dir=O intervalSec=600 state=S
srcHref=/orgs/1/workloads/a0d735ce-c55f-4a38-965f-bf6e98173598 srcLabels=
{"app":"app","env":"Staging","loc":"Azure","role":"API"}
dstHostname=workload1 dstHref=/orgs/1/workloads/a20eb1b5-10a4-419e-
b216-8b35c795a01e
```

Illumio Core PCE CLI Tool Guide 1.4.2

Overview of the CLI Tool

This topic provides an overview of the CLI Tool, describes the general syntax of the CLI Tool command, and lists the environment variables you can use to customize the CLI Tool.



IMPORTANT

See the *Illumio Core CLI Tool 1.4.0 Release Notes* and *Illumio Core CLI Tool 1.4.1 Release Notes* and *Illumio CORE CLI Tool 1.4.2 Release Notes* in your respective Illumio Core Technical Documentation portal for the updates to the CLI Tool for these releases.

About This Guide

The following sections provide useful information to help you get the most out of this guide.

CLI Tool Versioning

Illumio Core CLI Tool version 1.4.2 is compatible with Illumio Core PCE versions:

PCE 19.3.6-H2 (LTS)

PCE 21.2.4 (LTS)

PCE 21.5.20 (LTS)

PCE 22.1.1 (Standard)

PCE 22.2.0 (Standard)

The CLI Tool version numbering is independent from the release and version numbering of Illumio Core PCE and VEN. The CLI Tool works with multiple versions of the PCE and the VEN and does not necessarily need software changes in parallel with releases of the PCE or the VEN.



IMPORTANT

See the *Illumio Core CLI Tool 1.4.0 Release Notes*, *Illumio Core CLI Tool 1.4.1 Release Notes* and *Illumio Core CLI Tool 1.4.2 Release Notes* in your respective Illumio Core Technical Documentation portal for the updates to the CLI Tool for these releases.

How to Use This Guide

This guide includes several major sections:

- Overview to the CLI Tool
- Installation
- Formal syntax of the `ilo` command
- Tutorials for various operations
- Uploading vulnerability data
- Security policy import and export

Before Reading This Guide

Before performing the procedures in this guide, be familiar with the following information:

- The CLI Tool interacts with the PCE; therefore, be familiar with PCE concepts such as core and data nodes, workloads, and traffic. See the PCE Administration Guide.
- The CLI Tool is often used to upload vulnerability data; therefore, understand how vulnerability data is used in the PCE web console. See the "Vulnerability Maps" topic in Visualization Guide.
- The CLI Tool can be used with workload data; therefore, you must understand what workloads are. See the "VEN Architecture and Components" topic in the VEN Administration Guide.
- The CLI Tool can be used with security policy rules, rulesets, labels, and similar resources; therefore, be familiar with these concepts. See "The Illumio Policy Model" in the Security Policy Guide.

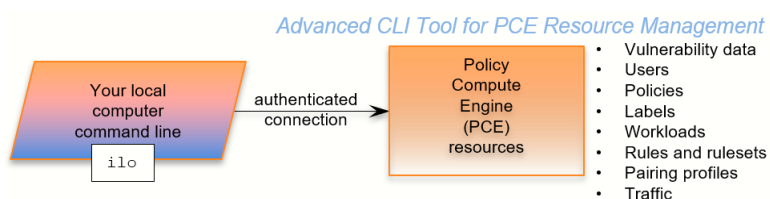
Notational Conventions in This Guide

- Newly introduced terminology is italicized. Example: *activation code* (also known as pairing key)
- Command-line examples are monospace. Example: `illumio-ven-ctl --activate`
- Arguments on command lines are monospace italics. Example: `illumio-ven-ctl --activate activation_code`
- In some examples, the output might be shown across several lines but is actually on one single line.
- Command input or output lines not essential to an example are sometimes omitted, as indicated by three periods in a row. Example:

```
...
some command or command output
...
```

CLI Tool and PCE Resource Management

With the Illumio CLI Tool, you can manage many of your PCE's resources directly from your local computer.



Some purposes of the CLI Tool include the following capabilities:

- Import vulnerability data for analysis with Illumination.
- Help with tasks such as directly importing workload information to create workloads in bulk.
- Create, view, and manage your organization's security policy rules, rulesets, labels, and other resources.



CAUTION

The CLI Tool is a powerful way to work with your PCE resources. Exercise caution to make sure that your use of the tool does not adversely affect your system. If possible, test your CLI Tool commands against a non-production system before using them on your production PCEs.

The CLI Tool is named `ilo`. It is a wrapper around the Illumio Core REST API. No knowledge of the REST API is required.

The `ilo` Command

This section describes the general syntax of the CLI Tool command, `ilo`, and tells how to use command-line help to get more specific syntax information.

Formal Syntax

The formal syntax for the `ilo` command is as follows:

```
ilo resource_or_specialCommand argument options
```

Where:

- `resource_or_specialCommand` represents either a resource managed by the PCE or a command that is not related to a particular resource.

A resource is an object that the PCE manages, such as a workload, label, or pairing profile. Example resource command on Linux (create a workload):

```
ilo workload create --name FriendlyWorkloadName --hostname
myWorkload.BigCo.com
```

A special command is a command that is not related to a specific resource. Special commands include `user`, `login`, `use_api_key`, and `node_available`.

Example special command on Windows (log out of PCE):

```
ilo user logout --id 6
```

- The `argument` represents an operation on the resource or special command.
- The `options` are allowed options for the `resource_or_specialCommand`. The specific option depends on the type of resource or special command.

CLI Tool Help

To get a complete list of all the available CLI Tool commands, use the `ilo` command without options. This command displays the high-level syntax of special commands, resources, and their allowable options.

For details about a resource's or special command's arguments, specify the name of the resource followed by the argument followed by the `--help` option. For example:

```
ilo workload create --help
```

HTTP Response Codes and Error Messages

This section describes the response codes and error messages that can be returned when you use CLI Tool commands.

REST API HTTP Response Codes

At the end of its output, the `ilo` command displays the REST API HTTP response code from the command. For example, a successful operation shows the following output:

```
...  
200, OK
```

Error Messages

For many syntactical or other types of errors, the CLI Tool displays a general message encouraging you to verify your syntax with the CLI Tool help:

```
The ilo command has encountered an error. Check your syntax with either of  
the  
following commands:
```

```
- ilo  
- ilo <command> --help
```

In addition, in some circumstances, the CLI Tool writes a detailed log of errors:

```
For detailed error messages, see the file:  
location-of-local-temp-directory/illumio-cli-error.log
```

Where `location-of-local-temp-directory` is as follows:

- Linux: `/tmp`
- Windows: `C:\Windows\Temp`

Environment Variables

Illumio provides Linux environment variables to allow users to customize operation of the CLI tool.

Environment Variable	Purpose
ILO_API_KEY_ID	API key for non-password based authentication and cookie less session with PCE. See "Authenticate with an API Key".
ILO_API_KEY_SECRET	API key secret for non-password based authentication and cookie less session with PCE. See "Authenticate with an API Key".
ILO_API_VERSION	API version to be used to execute CLI commands. Set this if you want to override the default API version. See "Set the Illumio ASP REST API Version." Default: v2. Example: \$ export ILO_API_VERSION=v1
ILO_CA_DIR	Directory that contains certificates. See "TLS/SSL Certificate for Access to the PCE".
ILO_CA_FILE	Absolute path to certificate file. See "TLS/SSL Certificate for Access to the PCE".
ILO_DISPLAY_CONFIG	Absolute path to the display configuration file that is to be used with the list command. See "Linux Save Specific Fields to File For Reuse".
ILO_INSECURE_PASSWORD	Provide a password for login. If this variable is set, the login password prompt does not appear, and this password is used instead. Do not use in a production system when authentication security is desired. Example: \$ export ILO_INSECURE_PASSWORD=myInsecurePassword
ILO_KERBEROS_SPN	Kerberos service principal name (SPN). Specify this variable when using Kerberos authentication.
ILO_LOGIN_SERVER	PCE login server FQDN. Use this variable when the login server FQDN is not the same as the PCE FQDN. See "Explicit Log into the PCE".
ILO_ORG_ID	Organization identifier for certificate-authenticated session with PCE. Value is always 1. Does not need to be explicitly set The environment variable is set by the system and should not be explicitly set. See "Authentication to PCE with API Key or Explicit Login".
ILO_PCE_VERSION	PCE version for the CLI to use. Default: 19.1.0 Example: \$ export ILO_PCE_VERSION=18.2.5
ILO_PREVIEW	Enable any preview features that are included in this release. To disable preview features, remove this variable from the environment.
ILO_SERVER	FQDN of PCE for login and authentication with PCE. See "Authentication to PCE with API Key or Explicit Login".
TSC_ACCESS_KEY	These two ENV variables have been added in the release 1.4.2 to set up the Tenable SC API keys, which are used for authentication.
TSC_SECRET_KEY	
TSC_HOST	Variable that specifies the target host for Tenable
QAP_HOST	Variable that specifies the target host for Qualys

Installation and Authentication

This section describes how to install the CLI Tool. It also describes how to set up authentication, how to upgrade the tool, and how to uninstall it.

Installation Prerequisites

This section details prerequisites and the installation of the CLI Tool. Be sure you meet the prerequisites in the checklist.

Prerequisite Checklist

- License for vulnerability data upload
- Vulnerability data for upload
- Functional PCE
- Supported operating systems
- TLS/SSL certificate for authenticating to the PCE
- API version set in configuration
- The CLI Tool installation program

License for Vulnerability Data

The Illumio Core Vulnerability Maps license is required to import vulnerability data into the Illumio PCE. For information about obtaining a license, contact Illumio Customer Support. For information on activating the license, see [Add the License for Vulnerability Data Upload \[240\]](#).

Upload Vulnerability Data

When you plan on using the CLI Tool to upload vulnerability data, make sure you have the data to upload in advance. See [Supported Vulnerability Data Sources \[243\]](#) for information.

Install Functional PCE

Because the CLI Tool is for managing resources on your PCE, you need to have already installed a fully functional PCE.

Supported Computer Operating Systems

The CLI Tool is supported on the following operating systems.

Linux

- Ubuntu 18.04
- Ubuntu 20.04
- Centos/RHEL 7.9
- Centos/RHEL 8.4

Microsoft Windows



NOTE

The CLI Tool is not supported on Windows 32-bit CPU architecture. Ensure that you run it on Windows 64-bit CPU architecture.

- Windows 2012 64 bit
- Windows 2016 64 bit
- Windows 10 64 bit

**NOTE**

CLI 1.4.2 is no longer supported on Windows 2008 R2 (EOL). The CLI Tool should work and can be used at your own risk.

TLS/SSL Certificate for Access to the PCE

You need a TLS/SSL certificate to securely connect to the PCE. Requirements for this certificate are provided in the PCE Installation and Upgrade Guide.

Alternative Trusted Certificate Store

To secure the connection to the PCE, by default, the CLI Tool relies on your computer's trusted certificate store to verify the PCE's TLS certificate. You can specify a different trusted store. When you have installed a self-signed certificate on the PCE, the alternative trusted store might be necessary.

Example: Set envvar for alternative trusted certificate store z

```
export ILO_CA_FILE=~/self-signed-cert.pem
```

Set the Illumio Core REST API Version

The CLI Tool uses v2 of the Illumio Core REST API by default.

Install, Upgrade, and Uninstall the CLI Tool

This section explains how to install, upgrade, or uninstall the CLI Tool on Linux or Windows.

Download the Installation Package

Download the CLI Tool installation package from the [Tools Catalog](#) page (login required) to a convenient location on your local computer.

Install Linux CLI Tool

The CLI Tool installer for Linux is delivered as an RPM for RedHat/CentOS and DEB for Debian/Ubuntu.

The CLI Tool is installed in the local binaries directory `/usr/local/bin`.

Log into your local Linux computer as a normal user and then use `sudo` to run one of the following commands.

RedHat/CentOS:

```
$ sudo rpm -ivh /path_to/nameOfCliRpmFile.rpm
```

Debian/Ubuntu:

```
$ sudo dpkg -i / path_to / nameOfCliDebFile .deb
```

Upgrade Linux CLI Tool

Log into your local Linux computer as a normal user and then use `sudo` to run one of the following commands.

RedHat/CentOS:

```
$ sudo rpm -Uvh /path_to/nameOfCliRpmFile.rpm
```

Debian/Ubuntu:

```
$ sudo dpkg -i / path_to / nameOfCliDebFile .deb
```

The same option, `-i`, is used for installation or upgrade.

Uninstall Linux CLI Tool

Log into your local Linux computer as a normal user and then use `sudo` to run one of the following commands.

RedHat/CentOS:

```
$ sudo rpm -e nameOfCliRpmFile
```

Debian/Ubuntu:

```
$ sudo dpkg -r nameOfCliDebFile
```

Install Windows CLI Tool

The CLI Tool installer for Windows is delivered as an .exe file.

Log into your local Windows computer as administrator and start the installation program in any of the following ways.

- In the Windows GUI, double-click the .exe file.
- In a cmd window, run the .exe.
- In a PowerShell window, run the .exe.

After starting the installation program, follow the leading prompts.

A successful installation ends with the "Installation Successfully Completed" message and the help text for the CLI Tool is displayed.

Upgrade Windows CLI Tool

The CLI Tool cannot be directly upgraded from an existing CLI Tool installation.

If you have already installed a previous version of the CLI Tool, manually uninstall it with the Windows Control Panel's Add/Remove Programs.

After uninstalling the previous version of the CLI Tool, install the new version of the CLI Tool as described in [Install Windows CLI Tool \[228\]](#).

Uninstall Windows CLI Tool

Log into your local Windows computer as an administrator, and from the Windows Control Panel, launch Add/Remove Programs.

Select Illumio CLI from the list and click the **Uninstall** button.

Authenticate with the PCE

When using the CLI Tool, you can authenticate to your PCE in the following ways:

- **With an API key and key secret:**

This is the easiest way. Before you create the API key and secret, you need to log in to authenticate to the PCE. After creating and using the key, you do not have to specify your username and password again.

- **With the explicit command to log in:**

This always requires a username and password.

This method also requires you to log out with a user ID displayed at login. The explicit login times out after ten minutes of inactivity, after which you must log in again.

For both authentication mechanisms, on the command line, you always need to specify the FQDN and port of your PCE. The default port for the PCE is 8443. However, your system administrator can change this default. Check with your system administrator to verify the port you need.

Authenticate with an API Key

To authenticate to the PCE with an API key, you must first explicitly log into the PCE, create the API key, and then use the key to authenticate.

1. Authenticate via explicit login:

```
ilo login --server yourPCEfqdn:itsPort
```

2. Create the API key:

```
ilo api_key create --name someLabel
```

someLabel is an identifier for the key.

3. Use the API key to authenticate:

```
ilo use_api_key --server yourOwnPCEandPort --key-id yourOwnKeyId --org-id --key-secret yourOwnKeySecret
```

Create an API Key

On Linux, for later ease of use, with the `api_key --create-env-output` option, you can store the API key, API secret, and the PCE server name and port as environment variables in a file that you source in future Linux sessions.

Linux Example

This example creates the API key and secret and stores them as environment variables in a file named `ilo_key_MY_SESSION_KEY`.

```
# ilo api_key create --name MY_SESSION_KEY --create-env-output
# Created file ilo_key_MY_SESSION_KEY with the following contents:

export ILO_API_KEY_ID=14ea453b6f8b4d509
export ILO_API_KEY_SECRET=elfa1262461ca2859fcf9d91a0546478d10a1bcc4c579d888
a4e1cace71f9787
export ILO_SERVER=myPCE.BigCo.com:8443
export ILO_ORG_ID=1

# To export these variables:
# $ source ilo_key_MY_SESSION_KEY
```

Log Into the PCE

Without an API key, you must explicitly log into the PCE.

For on-premises PCE deployments, the login syntax is the FQDN and port of the PCE:

```
ilo login --server yourPCEfqdn:itsPort
```

For `yourPCEfqdn:itsPort`, do not specify a URL instead of the PCE's FQDN and port. If you do, an error message is displayed.

For the Illumio Secure Cloud customers, the login syntax is:

```
ilo login --server URL_or_bare_PCEfqdn:itsPort --login-server
login.illum.io:443
```

See the explanation above about the argument to the `--server` option.

- After login, the output of the command shows a user ID value. Make a note of this value. You need it when you log out.
- The session with the PCE remains in effect as long as you keep using the CLI Tool. After 10 minutes of inactivity, the session times out, and you must log in again.

Example

In this example, the user ID is 6.

```
C:\Users\marie.curie> ilo login --server myPCE.BigCo.com:8443
Enter User Name: albert.einstein@BigCo.com
```

```

Enter Password: Welcome Albert!
User ID = 6
Last Login Time 2018-08-10T-09:58:07.000Z from someIPaddress
Access to Orgs:
Albert: (2)
Roles: [3]
Capabilities: {"basic"=>["read", "write"], "org_user_roles"=>["read",
"write"]}
User Time Zone: America/Los_Angeles
Server Time: 2018-08-12T17:58:07.522Z
Product Version: 16.09.0-1635
Internal Version: 48.0.0-255d6983962db54dc7ca627534b9f24b94429bd5
Fri Aug 6 16:11:50 2018 -0800
Done

```

Log Out of the PCE

To end a session with the PCE, use the following command:

```
ilo user logout --id valueOfUserIdFromLogin
```

Where:

- `valueOfUserIdFromLogin` is the user ID from your login. See [Log Into the PCE \[230\]](#) for information.

Example

In this example, the user ID is 6.

```
ilo user logout --id 6
```

CLI Tool Commands for Resources

This section describes how to use the CLI Tool with various PCE resources.

View Workload Rules

You can view a specific workload's rules with the following command:

```
ilo workload rule_view --workload-id UUID
```

Where:

- `UUID` is the workload's UUID. See [About the Workload UUID \[236\]](#) for information.

In the example below, the workload's UUID is as follows:

```
2ca0715a-b7e3-40e3-ade0-79f2c7adced0
```

Example View Workload Rules

```
ilo workload rule_view --workload-id 2ca0715a-b7e3-40e3-ade0-79f2c7adced0
+-----+-----+
| Attribute | Value |
+-----+-----+
| providing | [] |
+-----+-----+
Using
+-----+
+-----+
+-----+
| Ports And Protocols |
Rulesets
+-----+
| Name | Href |
+-----+
+-----+
+-----+
| [[-1, -1, nil]] | [{"href"=>"/api/v2/orgs/28/sec_policy/8/rule_sets/1909", "name"=>"Default", "secure_connect"=>false, "peers"=>[{"type"=>"ip_list", "href"=>"/api/v2/orgs/28/sec_policy/8/ip_lists/188", "name"=>"Any (0.0.0.0/0)", "ip_ranges"=>[{"from_ip"=>"0.0.0.0/0"}]}]}] | /api/v2/orgs/28/sec_policy/8/services/1153 | All Services |
+-----+
+-----+
+-----+
200, OK
```

View Report of Workload Services or Processes

The following command lists all running services or processes on a workload:

```
ilo workload service_reports_latest --workload-id UUID
```

Where:

- UUID is the workload's UUID. See [About the Workload UUID \[236\]](#).

In the example, the workload's UUID is as follows:

```
2ca0715a-b7e3-40e3-ade0-79f2c7adced0
```

Example Workload Service Report

```
ilo workload service_reports_latest --workload-id 2ca0715a-b7e3-40e3-ade0-79f2c7adced0
+-----+-----+
| Attribute | Value |
+-----+-----+
| uptime_seconds | 1491 |
| created_at | 2015-10-20T15:13:00.681Z |
+-----+-----+
```



```

+-----+-----+
Open Service Ports
+-----+-----+-----+-----+-----+
+-----+
| Protocol | Address | Port | Process Name | User
| Package | Win Service Name |
+-----+-----+-----+-----+-----+
+-----+
| udp      | 0.0.0.0 | 5355 | svchost.exe | NETWORK
SERVICE |         | Dnscache
...
| tcp      | 0.0.0.0 | 135  | svchost.exe | NETWORK
SERVICE |         | RpcSs
+-----+-----+-----+-----+-----+
+-----+
200, OK

```

View Host and System Inventory

You can use the following commands to get a quick source of information for troubleshooting or when working with Illumio Customer Support. Using these commands is a quicker and less detailed alternative to running a PCE support report.

To show host inventory for the "local" node:

```
$ illumio-pce-env show host-inventory
```

To show system inventory for the PCE:

```
$ illumio-pce-env show system-inventory
```

To show host inventory for all PCE nodes and also the PCE system inventory:

```
$ illumio-pce-env show inventory
```

Use the list Option for Resources

Many resources take the `list` option. This section details some of its uses.

Default List of All Fields

The default `list` command displays all fields associated with the resource:

```
ilo resource list
```

List Only Specific Fields

With the `--field` option, specify the fields to display:

```
ilo resource list --field CSV_list_of_fieldnames
```

For example, to display a list of labels with only the href, key, and value fields, use the `--field` option with those fields as comma-separated arguments.

Example List with Selected Fields

```
ilo label list --fields href,key,value
```

Href	Key	Value
/api/v2/2/labels/1	role	Web
/api/v2/2/labels/2	role	Database
...		
/api/v2/2/labels/48	loc	Asia

Nested Resource Fields and Wildcards

Some resources have hierarchical, nested fields. For example, the workload resource includes the following hierarchy for the agent field:

```
agent/config/log_traffic
```

- A field named `agent`
 - That has a field named `config`
 - That has a field named `log_traffic`

To list nested fields, separate the hierarchy of the field names with a slash to the depth of the desired field.

To see all nested fields of one of a resource's fields, use the asterisk (*) wildcard.

Examples

The following example displays all fields under the `agent/config` field.

Example of All Nested Fields with Wildcard (*)

```
ilo workload list --field agent/config/*
```

Log Traffic	Visibility Level	Mode
false	flow_summary	illuminated
false	flow_summary	idle

You can combine individual field names, nested field names, and the * wildcard.

Example Combination of Individual fields, Nested fields, and Wildcard

```
ilo workload list --fields href,hostname,agent/config/*,agent/status/uid,agent/status/status
```

```

+-----+-----+-----+
| Href                                     |
| Hostname                               | Log Traffic | Visibility
Level | Mode                               | Uid                                     | Status |
+-----+-----+-----+
+-----+-----+-----+
| /api/v2/1/workloads/527b8aca-97aa-43b9-82e1-29b17a947cdd
| hrm-web.webscaleone.info | false      | flow_summary
| illuminated | 0ffd2290-e26a-4ec6-b241-9e2205c0b730 | active |
| /api/v2/1/workloads/4a8743a4-14ee-40d0-9ed2-990fe3f0ffb1
| hrm-db.webscaleone.info | false      | flow_summary
| illuminated | 145a3cc8-01a8-4a52-97b8-74264ad690e4 | active |
+-----+-----+-----+
+-----+-----+-----+
...

```

Linux: Save Fields for Reuse

On Linux, for ease of reuse of specific fields, create a display configuration file in YAML format and set the environment variable `ILO_DISPLAY_CONFIG` to point to that file. Thereafter, you no longer need to specify specific fields on the list command line.

Examples

Configure the workloads list command to display only the href, hostname, all agent configuration fields, and agent version:

Example Command to Save to List Configuration File

```
ilo workload list --fields href,hostname,agent/config/*,agent/status/agent_version
```

Add the field names to a display configuration file in the following YAML format:

Example YAML Layout of Display Configuration File

```

workload:
  fields:
    - href
    - hostname
  agent:
    config:
      fields:
        - '*'
    status:
      fields:
        - agent_version

```

Set the Linux environment variable `ILO_DISPLAY_CONFIG` to the path to the YAML file:

Example `ILO_DISPLAY_CONFIG` environment variable

```
$ export ILO_DISPLAY_CONFIG=~/.ilo_display/display_config.yaml
```

List of All Workloads

To view all details for all workloads, use the following command:

```
ilo workload list
```

About the Workload UUID

To view an individual workload, you need the workload's identifier, called the UUID, or Universal Unique Identifier.

The UUID is shown in the list of all workloads described in [List of All Workloads \[236\]](#). The UUID is the last word of the value of the workload's href field, as shown in bold in the following example:

```
/api/v2/orgs/28/workloads/2ca0715a-b7e3-40e3-ade0-79f2c7adced0
```

View Individual Workload

To see the details about an individual workload, use the following command:

```
ilo workload read --workload-id UUID
```

Where:

- UUID is the workload's UUID. See [About the Workload UUID \[236\]](#) for information.

The details of an individual workload are grouped under major headings:

- Workload > Interfaces
- Workload > Labels
- Workload > Services
- Services > Open Service Ports
- Agent > Status

Example List of Individual Workload

```
ilo workload read --workload-id 2ca0715a-b7e3-40e3-ade0-79f2c7adced0
+-----+
+-----+
+-----+
| Attribute          |
+-----+
Value
+-----+
+-----+
+-----+
| href               | /orgs/1/workloads/2ca0715a-b7e3-40e3-
ade0-79f2c7adced0
| deleted            |
false
...
Workload -> Interfaces
```

```

+-----+-----+-----+-----+
+-----+-----+-----+-----+
| Name | Address | Cidr Block | Default Gateway Address | Link
State | Network Id | Network Detection Mode
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| eth0 | 10.0.0.16 | 8 | 10.0.0.1 |
up | 1 | single_private_brn
...
Workload -> Labels
+-----+
| Href |
+-----+
| /orgs/1/labels/37 |
...
Workload -> Services
+-----+-----+
| Attribute | Value |
+-----+-----+
| uptime_seconds | 69016553 |
...
Services -> Open Service Ports
+-----+-----+-----+-----+-----+-----+
+-----+
| Protocol | Address | Port | Process Name | User | Package | Win Service
Name |
+-----+-----+-----+-----+-----+-----+
+-----+
| 17 | 0.0.0.0 | 123 | ntpd | root |
|
...
Workload -> Agent
+-----+
+-----+
+-----+
| Attribute |
Value
|
+-----+
+-----+
+-----+
| config | {"log_traffic"=>true, "visibility_level"=>"flow_summary",
"mode"=>"enforced"} |
| href | /orgs/1/agents/
16 |
...
Agent -> Status
+-----+-----+
| Attribute | Value |
+-----+-----+
| uid | db482b06-41c6-4297-a60c-396de13576ad |
| last_heartbeat_on | 2016-12-07T04:07:03.756Z |
...
200, OK

```

List Draft or Active Version of Rulesets

A security policy item consists of ruleset, IP lists, label groups, services, and security settings. Before changes to these items take effect, the policy must be provisioned on the managed workload by setting its state to active with the CLI Tool or provisioning it with the PCE web console.

To view a ruleset and provisioning state use the following command:

```
ilo rule_set list --pversion state
```

Where `state` is one of the following values:

- Draft: Any policy item that has not yet been provisioned.
- Active: All policy items that have been provisioned and are enabled on workloads.

The provisioning states are listed in the Enabled column:

- True: The policy is provisioned.
- Empty: The policy is a draft.

Example Draft Versions of Rulesets

```
ilo rule_set list --pversion draft
+-----+
+-----+-----+-----+-----+
| Href                                     |
| Created By                             | Name | Description | Enabled |
+-----+-----+-----+-----+
| /api/v2/orgs/28/sec_policy/draft/rule_sets/2387
| {"href"=>"/api/v2/users/74"} | fool |           | true
| /api/v2/orgs/28/sec_policy/draft/rule_sets/1909
| {"href"=>"/api/v2/users/0"} | Default |         | true ...
200, OK
```

The state of the policy is stored in the `agent/status/status` field. See [Nested Resource Fields and Wildcards \[234\]](#) for information.

Import and Export Security Policy

Using the CLI Tool, you can export and import security policy to and from the PCE. Importing and exporting security policy is particularly useful for moving policy from one PCE to another so you can avoid recreating policy from scratch on the target PCE. For example:

- You can test policy on a staging PCE and then move it to your production PCE.
- You can move policy from a proof-of-concept PCE deployment to your production PCE.

Export and Import Policy Objects

You can use the CLI Tool to export or import the following objects in the PCE:

- Labels: `labels`
- Label groups: `label_groups`
- Pairing profiles: `pairing_profiles`
- IP lists: `ip_lists`
- Services: `services`
- Rulesets and rules: `rule_sets`

About Exporting Rules

You can export rules for workloads, virtual services, or virtual servers.

For flexibility, Illumio recommends that you base your security policy rules on labels. Do not tie the rules to specific individual workloads, virtual services, or virtual servers.

Virtual servers and virtual services are not exported.

The CLI Tool policy export does not include such references. When you have rules that are tied to individual workloads, virtual services, or virtual servers, a warning is displayed on export. Attempts to import such rules fail and display the reason for the failure.

Example Failed Attempt to Export Rules for Workload

```
WARNING: rule /orgs/1/sec_policy/active/rule_sets/3/sec_rules/39
contains non-transferrable providers: workload /orgs/1/workloads/
a51ae67d-472a-44c3-984e-d518a8e95aee
Unable to proceed, please verify input
```

Workflow for Security Policy Export/Import

- Authenticate to the source PCE. See [Authenticate with the PCE \[229\]](#) for information.
- Export the policy to a file. Syntax summary:

```
ilo sec_policy export --file someExportFilename
```

- Authenticate to the target PCE. See [Authenticate with the PCE \[229\]](#) for information.
- Import the saved policy. Syntax summary:

```
ilo sec_policy import --file someImportFilename
```

Output Options, Format, and Contents

All exported policy is written to standard output. To write to a file, use the `--file` option.

Exported policy is in JSON format.

By default, all supported policy objects are exported. You can export a subset of policy by specifying one or more resource types with the `-resource` option (`labels`, `label_groups`, `pairing_profiles`, `ip_lists`, `services`, or `rule_sets`).

When a subset of policy items is exported (such as only labels), all referenced resources are also exported.

See also [About Exporting Rules \[239\]](#) for information.

Exported Rulesets

With the `-- rule_set` option, you can export multiple rulesets.

By default, only the most recently provisioned, active policy is exported. To export the current draft policy or a previous policy, use the `--pversion` state option. See [List Draft or Active Version of Rulesets \[238\]](#) for information.

For a single ruleset, make sure the `--pversion` state you specify matches the provisioned state of the ruleset. In the following example, the state is draft:

```
ilo sec_policy export --pversion draft --rule_set /orgs/1/sec_policy/draft/  
rule_sets/1
```

Effects of Policy Import

All imported policy is read from standard input, unless you import from a file with the `--file` option.

You can import policy file multiple times. Each import affects only a single copy of a resource.

All imported policy is set to the draft provisioned state. After the import, you must explicitly provision the active state.

Non-transferrable policy rules (that is, rules tied to specific workloads, virtual servers, and bound services), the import aborts with a warning. See [About Exporting Rules \[239\]](#) for information.

Policy items already on the target PCE are updated by imported resources whose names match the already existing resources' names. Services do not have to have the same names. Services match if they have the same set of ports and protocols.

Resources are not deleted by an import. For example, if you export policy from PCE-1 to PCE-2, delete a resource "R" from PCE 1, and then export and import again, resource "R" is still present on PCE 2. You must explicitly delete resource "R" from PCE2.

Upload Vulnerability Data

This section describes how to use the `ilo` commands to upload vulnerability data to the PCE for analysis in Illumination.

After uploading the data, you can use Vulnerability Maps in the PCE web console to gain insights into the exposure of vulnerabilities and attack paths across your applications running in data centers and clouds. See the "Vulnerability Maps" topic in the Visualization Guide for information.

Add the License for Vulnerability Data Upload

An Illumio Core Vulnerability Maps license is required to upload vulnerability data into the Illumio PCE. For information about obtaining the license, contact Illumio Customer Support.

You are provided with a license file named `license.json`. After you have obtained your license key, store it in a secure location.



NOTE

Before adding the license, you must first authenticate to the PCE. See [Authenticate with the PCE \[229\]](#) for information.

To add the license, you must be the organization owner or a be a user who has owner privileges.

Use the following command to inform the PCE of your valid license:

```
ilo license create --license-file "path_to_license_file/license.json" --
feature "feature_name" [debug [v | verbose] trace]
```

Where:

What	Required?	Description
"path_to_license_file/license.json"	Yes	The quoted path to the <code>license.json</code> file from Illumio Example: <code>"~/secretDir/license.json"</code>
"feature_name"	Yes	The quoted string <code>"vulnerability_maps"</code> , which specifies the feature name the license enables
debug	No	Enable debugging
v verbose	No	For verbose logging
trace	No	Enable API trace

Vulnerability Data Upload Process

On upload, the CLI Tool associates a workload's IP addresses with corresponding vulnerabilities identified for that workload.

Using API to Download Vulnerability Data

In release CLI 1.3, Tenable IO and tenable SC have been supporting both manual and API download of vulnerability data while Qualys tool was only available for manual download.



IMPORTANT

Starting from the release CLI 1.4, Qualys supports also API download, with some minor differences in options.

For the release CLI 1.4.1, it is suggested that users use an API key instead of a login session while using Qualys API download.

For the release CLI 1.4.2 for Tenable, the most reliable way to provide authentication is through API keys instead of username/password. If customers observe any authentication issues while using Tenable SC API upload, they are advised to use API keys for authentication.

There are 2 ENV variables to set up the Tenable SC API keys which are used for authentication:

`TSC_ACCESS_KEY`

`TSC_SECRET_KEY`

The API connects directly to the cloud instance of Tenable or Qualys and the vulnerability tool then scans new vulnerabilities and downloads them into the PCE.

Users can also set up cron jobs that run in the desired intervals and check the state of the vulnerability scanner.

Qualys and Tenable scanners work in a similar way, using the username and password and similar options.

Automating Vulnerability Imports from Tenable-SC

Users of Illumio vulnerability maps can automate the import of vulnerabilities from tenable-sc using a script.

Illumio CLI supports the API username and password as environment variables or a cmd line switch (such as `--api-password`).

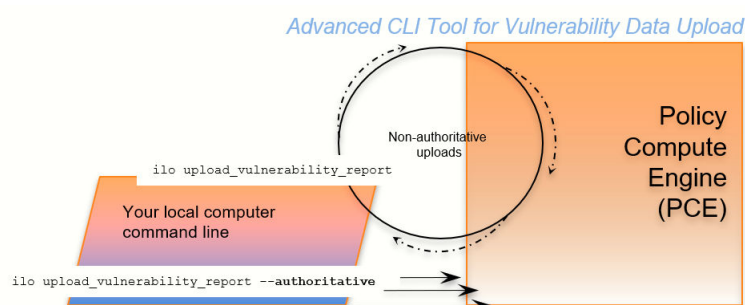
The ILO-CLI tool was updated to add a switch for `--api-user`.

Kinds of Vulnerability Data Uploads

There are two kinds of upload: non-authoritative and authoritative.

- **Non-authoritative:** This is the default. A non-authoritative upload:
 - Appends incoming data to any previously loaded records
 - Accumulates records for the same workloads without regard to duplicates.

You can repeat the non-authoritative upload as many times as you like until you are satisfied with the results.



- **Authoritative:** You indicate authoritative data with the `-authoritative` option. An authoritative upload:
 - Overwrites any previously uploaded records for workloads matched to the incoming records.
 - Eliminates duplicate records.
 - Adds new records not previously written by other uploads.

You can repeat the authoritative upload as many times as you like until you are satisfied with the results.

After either kind of upload, you can examine the uploaded data with the CLI Tool or the PCE web console. See “Vulnerability Maps” in the Visualization Guide for information.

Supported Vulnerability Data Sources

The CLI Tool works with vulnerability data from the following sources.

- Nessus Professional™
- Qualys®
- Tenable Security Center
- Tenable.io
- Rapid7©



NOTE

Before uploading Rapid7 data to the PCE, export the data from Rapid7 to Qualys format with Qualys XML Export.

Vulnerability Data Formats

In the CLI 1.4.0, 1.4.1 and 1.4.2 releases, Illumio supports the following report formats:

- For `tenable-io`: API, CSV
- For `tenable-sc`: API, CSV
- For `nessus-pro`: XML
- For `qualys`: API, XML

Common Vulnerabilities and Exposures (CVE)

Vulnerabilities are defined by Common Vulnerabilities and Exposures (CVE), with identifiers and descriptive names from the U.S. Department of Homeland Security [National Cybersecurity Center](#).

Vulnerability Scores

Illumio computes a vulnerability score, which is a measure of the vulnerability of your entire organization. The score is displayed by the `ilo vulnerability list` command for all vulnerabilities or individual vulnerability via the vulnerability identifier.

Vulnerability Identifier

A uploaded vulnerability has an identifier as shown in the example below. The vulnerability identifier is tied to a specific CVE. You use this identifier with `--reference-id` option to

examine specific uploaded vulnerabilities. See [Example – List Single Uploaded Vulnerability \[248\]](#) for information.

The following are examples of vulnerability identifiers.

- Nessus Professional: nessus-65432
- Qualys: qualys-23456
- Rapid7: qualys-98765. Because Rapid7 data is first exported from Rapid7 in Qualys format, it is given a Qualys identifier when uploaded to the PCE.

Vulnerabilities for Unmanaged Workloads

You can upload vulnerabilities for unmanaged workloads. However, unmanaged workloads do not have any vulnerability score or associated CVE. If the unmanaged workload is later changed to managed, this information becomes available.

Prerequisites for Vulnerability Data Upload

Before uploading vulnerability data, ensure that you are ready with the following requirements.

- An Illumio Vulnerability Maps license is required to upload vulnerability data to the PCE. See [Add the License for Vulnerability Data Upload \[240\]](#) for information.
- XML-formatted vulnerability data files from one of the supported sources.
- Authenticated CLI-tool access to the target PCE. See [Authenticate with the PCE \[229\]](#) for information.
- Authenticated access and necessary permissions in the PCE web console for working with vulnerability maps. See [Authenticate with the PCE \[229\]](#) for information.

Vulnerability Data Upload CLI Tool Syntax

The key argument and option for uploading vulnerability data are as follows. For readability, this syntax is broken across several lines.

```
ilo upload_vulnerability_report
--input-file path_to_datafile.xml [path_to_datafile.xml]...
--source-scanner [nessus-pro|qualys|tenable-sc|tenable-io]
--format xml
[--authoritative]
[ --api-user ApiServerUserName --api-server SourceApiServer:port ]
```

Where:

What	Required	Description
--input-file path_to_datafile.xml [path_to_data- file.xml]...	Yes	Location of one or more data files to upload. The path to the data file can be either an absolute path or a relative path. If more than one data file is listed (bulk upload), separate the file names with space characters.
--debug	No	Enable debugging

What	Required	Description
<code>--authoritative</code>	No	For uploading authoritative vulnerability data. The default command is without the <code>--authoritative</code> option. See Kinds of Vulnerability Data Uploads [242] for information.
<code>--workload-cache</code> <code>FILE</code>	No	DEBUGGING ONLY: Workload Cache file - use this if available
<code>--source-scanner</code> <code>[nessus-pro qualys </code> <code>tenable-sc]</code>	Yes	Indicates the source of the scan. Note for rapid data: <ul style="list-style-type: none"> Vulnerability data from Rapid must have been exported from Rapid in Qualys XML format. To load the Rapid data, use the 'qualys' argument
<code>--format</code> <code>REPORT_FORMAT</code>	Yes	Report format. Allowed values are: <p>xml</p> <ul style="list-style-type: none"> <code>--source-scanner nessus-pro</code> <code>--source-scanner qualys</code> <p>csv</p> <ul style="list-style-type: none"> <code>--source-scanner tenable-sc</code> <code>--source-scanner tenable-io</code> <p>api</p> <ul style="list-style-type: none"> <code>--source-scanner tenable-sc</code> <code>--source-scanner qualys</code> <code>--source-scanner nessus-pro</code> <p>See also <code>--api-server</code> and <code>--api-user</code>.</p>
<code>--api-server</code> <code>SourceApiServer:port</code> <code>SERVER_FQDN</code>	Yes for Tenable with <code>--format</code> <code>api</code>	API server FQDN. Allowed formats are <code>HOST</code> or <code>HOST:PORT</code>
<code>--api-user</code> <code>ApiServerUserName</code> <code>USERNAME</code>	Yes for source API server au- thentication	The user name for authenticating to the SourceApiServer. You are always prompted to enter your password.
<code>--api-page-size</code> <code>PAGE_SIZE</code>	Yes for Qualys and Tenable	Appropriate page size if API supports pagination. The default page is 1000.
<code>--skip-cert-verifi- cation</code>	Yes for Qualys and Tenable	Disable certificate verification for API.
<code>--on-premise</code>	Yes only for Tenable io	Tenable IO deployment is on premise.
<code>--mitigated</code>	Yes only for Tenable sc	Tenable SC input is exported from the mitigated vulnerabilities analysis view.

What	Required	Description
--scanned-after SCANNED_AFTER	Yes for Qualys	Qualys users can select scan data to process after a certain date, in ISO 8601 format. When the optional <code>scanned-after</code> option is not provided, the system will pull all the historical vulnerability records from your Qualys account. If your account has historical records, it may take a very long time for the first time. With the <code>scanned-after</code> option, vulnerability data scanned after a certain date will be extracted and uploaded. It is recommended to include a certain scanned-after time if you use Qualys API upload option for the first time.
--severities SEVERITIES	No	Qualys API users can select vulnerabilities with defined severity levels to include in their report. Users can filter based on severity and avoid severity levels 1 and 2, which are often very informational and noisy. Example: <code>--only-include-severity=3,4,5</code> For Windows, be sure to include quotes around the severity levels: Example: <code>--only-include-severity="3,4,5"</code> NOTE: This option was added in Release 1.4.1
-v, --verbose	No	Verbose logging mode
--trace	No	Enable API trace mode

Using the ILO Command with Windows Systems

Windows systems take a maximum of four options with the ILO command for the vulnerability data upload. Users who choose to use more optional parameters need to set `api-server`, `username`, and `password` as the environmental variables to use other options in the command.

Work with Vulnerability Maps in Illumination

See "Vulnerability Maps" in the Visualization Guide for information.

Vulnerability Data Examples

Example - Upload Non-Authoritative Vulnerability Data

In this example, the `--source-scanner nessus-pro` option indicates that the data comes from Nessus Professional. On Windows, provide the absolute path to the data file. This Windows example is broken across several lines with the PowerShell line continuation character (```).

```
C:\Users\donald.knuth> ilo upload_vulnerability_report `
--input-file C:\Users\donald.knuth\Desktop\vuln_reports\nessus3.xml `
--source-scanner nessus-pro --format xml

Elapsed Time [0.05 (total : 0.05)] - Data parsing is done.
Elapsed Time [1.08 (total : 1.13)] - Got workloads. Workload count: 5.
Elapsed Time [0.0 (total : 1.13)] - Built workload interface mapping. Total
```

```

interfaces : 11.
Elapsed Time [4.57 (total : 5.7)] - Imported Vulnerabilities..
Elapsed Time [0.0 (total : 5.7)] - Detected Vulnerabilities are associated
with vulnerability and workload data..
Elapsed Time [0.83 (total : 6.53)] - Report Imported.

Summary:
Processed the report with the following details :
Report meta data =>
Name           : Generic
Report Type    : nessus
Authoritative  : false
Scanned IPs    : ["10.1.0.74", "10.1.0.223", "10.1.0.232", "10.1.0.221",
"10.1.0.11", "10.1.0.82", "10.1.0.43", "10.1.0.91", "10.1.0.8",
"10.1.1.250"]

Stats :
  Number of vulnerabilities           => 19
  Number of detected vulnerabilities => 31

Done.

```

Example - Upload of Rapid7 Vulnerability Data

The syntax for uploading vulnerability data from Rapid7 is identical to the syntax for uploading vulnerability data from Qualys. On Windows, you use the `--format qualys` option and the absolute path to the data file. This Windows example is broken across several lines with the PowerShell line continuation character (```).

Rapid7 data exported in Qualys format

Before uploading to the PCE, Rapid7 vulnerability data must have been exported in Qualys format from Rapid7 with Qualys XML Export.

```

C:\Users\edward.teller> ilo upload_vulnerability_report `
--input-file C:\Users\edward.teller\Desktop\vuln_reports\rapid7.xml `
--source-scanner qualys --format xml
...
Done.

```

Example - Upload Authoritative Vulnerability Data

In this example, the prompt shows this is an authoritative upload.

To proceed, you must enter the word YES in all capital letters.

```

C:\Users\jrobert.oppenheimer> ilo upload_vulnerability_report --input-file
dataDir/authoritativedata.xml --authoritative --source-scanner qualys --
format xml

Using /home/centos/.rvm/gems/ruby-2.4.1
Authoritative scan overwrites the previous entries for all the ips within
this scan. There is no ROLLBACK
Are you sure this is an authoritative scan? (YES | NO)
YES

```

```

Elapsed Time [11.86 (total : 11.86] - Data parsing is done.
Elapsed Time [0.27 (total : 12.13] - Got workloads. Workload count: 3.
Elapsed Time [0.0 (total : 12.13] - Built workload interface mapping. Total
interfaces : 6.
Elapsed Time [3.02 (total : 15.15] - Imported Vulnerabilities..
Elapsed Time [0.0 (total : 15.15] - Detected Vulnerabilities are associated
with vulnerability and workload data..
Elapsed Time [0.84 (total : 16.0] - Report Imported.
Summary:
Processed the report with the following stats -
    Number of vulnerabilities          => 14
    Number of detected vulnerabilities => 48
Done.

```

Example - List Single Uploaded Vulnerability

This example uses a single Qualys vulnerability identifier to show the associated vulnerability. The value passed to the `--reference-id` option is shown as `qualys-38173`. See [Vulnerability Identifier \[243\]](#) for information.

```

$ ilo vulnerability read --xorg-id=1 --reference-id=qualys-38173
...

| Attribute | Value |
+-----+
+-----+
| href | /orgs/1/vulnerabilities/qualys-38173 |
| name | SSL Certificate - Signature Verification Failed Vulnerability
| score | 39 |
| cve_ids | [] |
| created_at | 2018-11-05T18:16:56.846Z |
...

```

Example - List All Uploaded Vulnerabilities

This example highlights the vulnerability identifier, the CVE identifiers, and the description of the CVE. See [Common Vulnerabilities and Exposures \(CVE\) \[243\]](#) and [Vulnerability Identifier \[243\]](#) for information. The layout of the output is the same for all supported vulnerability data sources.

Nessus Professional

```

C:\Users\werner.heisenberg> ilo vulnerability list --xorg-id=1
...
| Href | Name | Score | Description | Cve Ids | Created At | Updated At |
Created By | Updated By |
+-----+
+-----+
| /orgs/1/vulnerabilities/nessus-18405 | Microsoft Windows Remote
Desktop Protocol Server Man-in-the-Middle Weakness | 51 |
| ["CVE-2005-1794"] | 2018-11-07T03:15:39.410Z |
2018-11-07T03:15:39.410Z | {"href"=>"/users/1"} | {"href"=>"/users/1"} |
...

```

Qualys


```
C:\Users\isaac.newton> ilo vulnerability list --xorg-id=1
...
| Href | Name | Score | Description | Cve Ids | Created At | Updated At |
Created By | Updated By |
-----+-----+-----+-----+-----+-----+-----+-----+
| /orgs/1/vulnerabilities/qualys-38657 | Birthday attacks against
TLS ciphers with 64bit block size vulnerability (Sweet32)
| 69 | | ["CVE-2016-2183"] | 2018-07-27T18:16:57.166Z |
2018-08-08T22:30:32.421Z | {"href"=>"/users/1"} | {"href"=>"/users/16"} |
...
```

Rapid7

Because Rapid7 vulnerability data must be in Qualys format before upload, the output is the same as for Qualys data, including the vulnerability identifier (qualys-38657 in the example above) and CVE. See [Common Vulnerabilities and Exposures \(CVE\) \[243\]](#) and [Vulnerability Identifier \[243\]](#) for information.

Example - View Vulnerability Report

The Report Type column identifies the source of the scan; in this example, Qualys.

```
C:\Users\gracemurry.hopper> ilo vulnerability_report list --xorg-id=1
...
| Href | Report Type | Name | Created At | Updated At | Num Vulnerabilities |
Created By | Updated By |
-----+-----+-----+-----+-----+-----+-----+-----+
| /orgs/1/vulnerability_reports/scan_1502310096_09344 | qualys |
NewAuthoritativeScan | 2018-08-08T22:30:34.877Z | 2018-08-08T22:30:34.877Z
| 62 | {"href"=>"/users/16"} | {"href"=>"/users/16"} |
...
```

Example - Upload a Qualys Report Using API

```
upload_vulnerability_report --source-scanner qualys --format api
--api-server qualysguard.qg3.apps.qualys.com --api-user um3sg
--scanned-after 2021-09-20
```

CLI Tool Tutorials

This section provides several hands-on exercises that demonstrate step-by-step how to perform common tasks using the CLI Tool.

How to Import Traffic Flow Summaries

Static Illumination provides “moment-in-time” visibility of inter-workload traffic. This visibility is useful to model policies, to look for specious traffic flows, and to ensure that metadata for labels is accurate.

Goal

Load workload and traffic data needed for analysis with static Illumination.

Setup

This tutorial relies on the following data to import.

- 1,000 workloads defined in the file `bulkworkloads-1000.csv`, which has the following columns:

```
hostname,ips,os_type
10.14.59.8.netstat,10.14.59.8,linux
10.4.78.178.netstat,10.4.78.178,linux
10.37.134.179.netstat,10.37.134.179,linux
...
```

- 1,000,000 traffic flows defined in the CSV file `traffic.clean-1m.csv`, which has the following columns:

```
src_ip,dst_ip,dst_port,proto
10.40.113.86,10.14.59.8,10050,6
10.14.59.8,10.8.251.138,8080,6
10.40.113.124,10.14.59.8,22,6
...
```

Steps

The workflow is authenticate to the PCE and run two `ilo bulk_upload_csv` commands.

1. Authenticate to the PCE via API key or explicit login. See [Authenticate with the PCE \[229\]](#) for information.
2. Load the workload data:

```
ilo workload bulk_upload_csv --file bulkworkloads-1000.csv
```

3. Load the traffic flow data:

```
ilo traffic bulk_upload_csv --file traffic.clean-1m.csv
```

Results

The data from the CSV files are uploaded.

How to Create Kerberos-Authenticated Workloads

This tutorial describes how to create workloads that use Kerberos for authentication. The tutorial makes the following assumptions:

- This tutorial assumes that you already have your Kerberos implementation in place.
- As required by Kerberos, the Kerberos realm name is shown in all capital letters as `MYR-EALM`.
- VEN environment variables must be set *before* VEN installation. Environment variables for Linux are detailed in the VEN Installation and Upgrade Guide.

Goals

- Create two workloads on Linux that are authenticated by Kerberos.
- Set the workloads' modes to idle and illuminated.
- Run the kinit command to get Kerberos tickets for the workloads.

Setup

The key data for using the `ilo` command to create these workloads are the name of the Kerberos realm and the Service Principle Name (SPN).

Steps

The workflow is authenticate, run two `workload create` commands that set the workloads' modes, set the VEN environment variables, install the VEN, and run two Kerberos `kinit` commands to get Kerberos tickets for the workloads.

1. Authenticate to the PCE via API key or explicit login. See [Authenticate with the PCE \[229\]](#) for information.
2. Create Kerberos-authenticated `myWorkload1` and set its mode to `idle`:

```
ilo workload create --hostname myPCE.BigCo.com --name myWorkload1
--service-principal-name host/myKerberosTicketGrantingServer@MYREALM --
agent/config/mode idle
```

For information about how the mode is a nested field, see [Nested Resource Fields and Wildcards \[234\]](#).

3. Create Kerberos-authenticated `myWorkload2` and set its mode to `illuminated`:

```
ilo workload create --hostname myPCE.BigCo.com --name myWorkload2
--service-principal-name host/myKerberosTicketGrantingServer@MYREALM --
agent/config/mode illuminated
```

4. Before installation, set VEN environment variables:

```
# Activate on installation
VEN_INSTALL_ACTION=activate
# FQDN and port PCE to pair with
VEN_MANAGEMENT_SERVER=myPCE.BigCo.com:8443
# Kerberos Service Principal Name
VEN_KERBEROS_MANAGEMENT_SERVER_SPN=host/myKerberosTicketGrantingServer
# Path to Kerberos shared object library
VEN_KERBEROS_LIBRARY_PATH=/usr/lib/libgssapi_krb5.so
```

5. Install the Linux VEN:

```
rpm -ivh illumio-ven*.rpm
```

6. Run `kinit` to get a Kerberos ticket for `myWorkload1`:

```
kinit -k -t /etc/krb5.keytab host/myWorkload1.BigCo.com@MYREALM
```

7. Run `kinit` to get a Kerberos ticket for `myWorkload2`:

```
kinit -k -t /etc/krb5.keytab host/myWorkload2.BigCo.com@MYREALM
```

Results

The Kerberos-authenticated workloads are created, set in the desired modes, and given a Kerberos ticket.

How to Work with Large Datasets

The `--async` option is for working with large sets of data without having to wait for the results. The option works like “batch job.”

The option can be used with any resource. The workflow is as follows:

1. You issue the desired `ilo` command with the `--async` option, which displays a job ID.
2. You take note of the job ID.
3. Your session is freed up while the job runs.
4. The job creates a data file, which you then view with `datafile --read --job-id jobID`.

Goal

Get a report of a large workload data set.

Steps

1. Issue the `--async` request for a workload list. Take note of job ID which is the final word of the href displayed on the Location line.

```
[kurt.goedel~]$ ilo workload list --async
Using /home/kurt.goedel/.rvm/gems/ruby-2.2.1
Location: /orgs/1/jobs/fe8a1c2b-1674-4b83-8967-eb56c4ffale3
202, Accepted
```

2. Check to see if the job completed. Use the job ID from the Location output in previous command:

```
[sigmund.freud~]$ ilo job read --job-id fe8a1c2b-1674-4b83-8967-eb56c4ffale
Using /home/sigmund.freud/.rvm/gems/ruby-2.2.1
```

3. Download the resulting data file, specifying the job ID with `-uuid jobID`:

```
[bill.gates ~]$ ilo datafile read --uuid 1e1c1540-8a01-0136-ec14-02f4d6c1190c
Using /home/ bill.gates /.rvm/gems/ruby-2.2.1
+-----+
+-----+
... Many lines not shown
+-----+
+-----+
| Href
| Deleted | Name | Description | Hostname
| Service Principal Name | Public Ip
| Distinguished Name | External Data Set | External Data Reference
| Interfaces | Ignored Interface Names | Service Provider | Data Center
| Data Center Zone | Os
Id | Os Detail | Online | Labels | Services | Agent
| Created At
Created By | Updated At | Updated By
+-----+
+-----+
... More lines not shown
+-----+
| /orgs/1/workloads/50ce441e-75ac-4be8-9201-96169545019c
```

```
| false | | 10.14.59.8.netstat
...
... Many lines not shown
...
```

How to Upload Vulnerability Data

This example tutorial shows how to upload vulnerability data to the PCE. For more information, see [Upload Vulnerability Data \[240\]](#). The source of the vulnerability data in this example comes from Qualys®.

Goal

Upload authoritative vulnerability data for analysis in Illumination.

Steps

1. Do a non-authoritative upload of vulnerability data for examination:

```
ilo upload_vulnerability_report --input-file C:\Users\albert-
einstein0.xml --source-scanner qualys --format xml
```

2. Examine a single uploaded vulnerability record identified by its vulnerability identifier, qualys-38173. See [Vulnerability Identifier \[243\]](#) for information.

```
ilo vulnerability read --xorg-id=1 --reference-id=qualys-38173
```

3. Do another non-authoritative upload of vulnerability data.

```
ilo upload_vulnerability_report --input-file C:\Users\albert-
einstein99.xml --source-scanner qualys --format xml
```

4. Do an authoritative upload of vulnerability data, overwriting any previously uploaded records and adding any new vulnerability records.

```
ilo upload_vulnerability_report --input-file C:
\Users\albert.einstein_FINAL.xml --authoritative --source-scanner qualys
--format xml
```

Results

The authoritative vulnerability data has been uploaded and is ready for use in Illumination.

New Document Locations

Welcome to the new and improved Illumio documentation library. These tables provide links to the new documentation locations. Remember to update your bookmarks.

Use the new search (powered by Coveo) to search for version specific documentation. You can filter search results by product, version, and content type.

- [Core \[255\]](#)
- [Cloud \[257\]](#)
- [Edge, Xpress, MSP \[258\]](#)
- [Integrations \[258\]](#)

The screenshot shows the Illumio Technical Documentation website. At the top, there is a navigation bar with links for Home, Cases, Community, Knowledge Base, and Training. Below the navigation bar is a large section titled "Explore Illumio Documentation" with a search bar. Underneath this is a large orange banner for "Illumio Zero Trust Segmentation Platform" with a description. Below the banner are four colored buttons for "ILLUMIO CORE", "ILLUMIO CLOUDSECURE", "ILLUMIO ENDPOINT", and "CONTAINERS". Below these are two buttons for "AI/ML" and "Other Products". The "Integrations" section follows, listing various integrations: IBM QRadar, Sentinel, Splunk, Netskope, ServiceNow CMDB, and Terraform. At the bottom, there is a dark footer bar with copyright information and links for About Support, EULA, and Privacy Policy.

TECHNICAL DOCUMENTATION

Home Cases Community Knowledge Base Training

Explore Illumio Documentation

Search...

Illumio Zero Trust Segmentation Platform

Discover Illumio's ZTS Platform, including getting started guides and user documentation.

ILLUMIO CORE ILLUMIO CLOUDSECURE ILLUMIO ENDPOINT CONTAINERS

AI/ML > Other Products >

Integrations

- > IBM QRadar
- > Sentinel
- > Splunk
- > Netskope
- > ServiceNow CMDB
- > Terraform

Copyright © 2024 | About Support | EULA | Privacy Policy

Core

Table 3. New Locations for the Illumio Documentation: Core

Top-Level Category/Topics	New Location for Category/Topics	Second Level Topics
Get Started	Application Ringfencing Tutorial	
	Glossary	
Install and Upgrade	Upgrading Illumio Core: Why and How	
	VEN Installation and Upgrade Guide	Prepare for VEN Installation Set Up PCE for VEN Installation VEN Installation and Upgrade VEN Installation and Upgrade with VEN CTL VEN Reference
	Endpoint Concepts Guide	NLA Support for Endpoints
	Endpoint Installation and User Guide	
	LW-VEN Installation and Configuration Guide	LW-VEN Requirements and Limitations Install and Configure the Illumio LW-VEN Service Manage and Troubleshoot the LW-VEN
	Illumio Core for Kubernetes and Openshift	
Release Notes	What's New and Release Notes for 24.3 What's New and Release Notes for 24.2.10 Kubernetes What's New and Release Notes for 5.2, 5.1, 5.0, 4.3.0	
Use Core	Security Policy Guide	Security Policy Objects Workloads Create Security Policy Policy Enforcement Secure Workload Connections

Top-Level Category/Topics	New Location for Category/Topics	Second Level Topics
	Visualization Guide	Visualization Tools Dashboards Vulnerability Map
Administer	PCE Administration Guide	Overview of PCE Administration Connectivity Configuration for PCE Access Configuration for PCE PCE Troubleshooting
	VEN Administration Guide	Overview of VEN Administration VEN State VEN Deactivation and Unpairing Monitor and Diagnose VEN Status
	Events Administration Guide	Overview of Events Administration Events Described Events Setup Traffic Flow Summaries
	PCE CLI Tool Guide	Overview of the CLI Tool Installation and Authentication CLI Tool Commands for Resources CLI Tool Tutorials
Develop	REST API Developer Guide	REST API Reference
	REST API Public Schemas 24.3 (Zipped File), REST API Public Schemas 24.2.10 (Zipped File)	
	24.3 OpenAPI Specification (JSON) 24.2.10 OpenAPI Specification (JSON)	

Top-Level Category/Topics	New Location for Category/Topics	Second Level Topics
	<p>Illumio Core REST API Getting Started Guide</p> <p>This content is retired and no longer available.</p>	
Connect	Flowlink Configuration and Usage Guide	<p>Flowlink Configuration</p> <p>Flowlink Usage</p>
	NEN Installation and Usage Guide	<p>NEN Installation and Configuration</p> <p>Load Balancers and Virtual Servers for the NEN</p> <p>NEN Integration with Switches</p>
Support	Knowledge Base	
	Training	
	Community	
	Contact Support	
	Documentation Archives	
	Legal Notices	
	Open Source Licensing Disclosure	
	Illumio 24.2 Documentation Library	
Archived Documentation	Log in to view archived documentation on Support.	

Cloud

Table 4. New Locations for the Illumio Documentation: Cloud

Top-Level Category/Topics	New Location for Category/Topics
Get Started	Getting Started
Release Notes	Current Release Notes
Visualize	Visualize
Define	Define Deployments and Applications
Policy	Policy Model

Top-Level Category/Topics	New Location for Category/Topics
Administer	User Management
Reference	Onboarding AWS
Support	Legal Notices
	Knowledge Base
	Training
	Community
	Contact Support

Other Products: Edge, Xpress, MSP

Table 5. New Locations for the Illumio Documentation: Edge, Xpress, MSP

Top-Level Category/Topics	New Location for Category/Topics
Other Products	Edge 22.31
	Xpress
	MSP

Integrations

Table 6. New Locations for the Illumio Documentation: Integrations

Integration	Description	New Location for Documentation and Link to App	Validated Compatibility
Ansible	Ansible modules for <ul style="list-style-type: none"> • VEN and C-VEN pairing • Label creation/update/removal 	0.2.6 Ansible Website	Ansible 2.12+PCE 22.5, 22.2, 21.5, 21.2, SaaS
IBM QRadar (SIEM)	Connector and Dashboards to view Illumio flow and event data	1.4 1.4 Integration Guide: PDF 1.3	QRadar 7.4.3+ PCE 24.1 (SaaS), 23.5, 23.2, 22.5, and 21.5 QRadar 7.4.1+ PCE 21.2, 19.3, SaaS

Integra- tion	Description	New Location for Documentation and Link to App	Validated Compatibil- ity
IBM QRadar (SOAR)	Provides a selective port-block- ing playbook	1.0 User Guide: PDF	PCE 21.2+, SaaS
Netskope Cloud Ex- change	Ensures dynamic access con- trols and security across hybrid and multi-cloud environments	1.0.0 Integration Guide: PDF	
Palo Alto Cortex (SOAR)	Provides a selective port-block- ing playbook	1.0.1 Configuration Guide Port Blocking Playbook Guide	Cortex 6.0 (6.2, 6.5, 6.8, and master), PCE 22.2, 21.5, 21.2, SaaS
Python SDK	Python REST client for Illumio PCE APIs	1.1.3 User Guide	PCE 21.2+, SaaS
Sentinel	Azure function Apps for data ingestion, Analytics rules	3.2.2 Integration Guide : PDF	PCE SaaS
ServiceNow (CMDB)	Uses ServiceNow as the source of truth for labeling PCE work- loads with R/A/E/L labels	2.1.0 Installation and Configura- tion Guide: PDF	Vancouver, Washington DC, Xanadu PCE 22.5, 23.2.30, 23.5.20, 24.2.10, or SaaS
Splunk (SIEM)	Connector and Dashboards to view Illumio flow and event data	TA-Illumio 3.2.3 Illumio App for Splunk User Guide v3.2.3 (PDF) EULA TA-Illumio 4.0.2 Illumio App for Splunk 4.0.1 Integration Guide 4.0: PDF	For 3.2.3: Splunk 9.1, 9.0, 8.2, 8.1 + PCE 21.2, 21.5, 22.2, 22.5, and SaaS For 4.0.2: Splunk 9.3, 9.2, 9.1, 9.0, 8.2, 8.1 + PCE 21.5, 22.2, 22.5, 23.2, 23.5, and SaaS
Terraform	Terraform HCL scripts to man- age PCE policy and policy ob- jects	1.1.4 User Guide	Terraform 1.4+ PCE 22.5, 22.2, 21.5, 21.2, SaaS

PDF Library

Download PDFs for version 24.4. If you need a PDF that's not listed in this library, send a request to [Illumio Documentation](#).



NOTE

Documentation versions 21.2 and earlier are archived and available as PDFs from the [Documentation Archives](#) library. You must log in to get access.

PDFs for Core 24.4

PDF	Description
What's New and Release Notes	
What's New and Release Notes for 24.4	Provides a list of new and updated features in version 24.4. Describes resolved issues and known issues and applicable workarounds.
What's New and Release Notes in 24.2.x	Provides a list of new and updated features in version 24.2.11, 24.2.10, and 24.2.0. Describes resolved issues and known issues and applicable workarounds.
What's New and Release Notes in 23.5	Provides a list of new and updated features in version 23.5. Describes resolved issues and known issues and their workarounds for the Illumio Core 23.5.x release.
Illumio Core for Kubernetes and OpenShift 5.1.x	Describes the resolved issues and related information for several Illumio Core for Kubernetes releases, formerly known as Illumio Containerized VEN, or C-VEN. Illumio Core for Kubernetes also includes the related required component, Kubelink. Because of this heritage, many references to this product as "C-VEN" are still used throughout the documentation.
NEN Release Notes, versions 2.6.x through 2.0.0	<p>Describes resolved issues and known issues and their workarounds for the Illumio Network Enforcement Node (NEN).</p> <ul style="list-style-type: none"> • 2.6.x • 2.5.x, • 2.4.x • 2.3.x • 2.1.1 • 2.0.0
Install, Configure, and Upgrade Guides	
24.4 Install, Configure, Upgrade (NEN, VEN, LW-VEN, Kubernetes and Openshift)	A combined installation guide for 24.4 NEN, VEN, Legacy Windows VEN (LW-VEN), Kubernetes and Openshift.
VEN Installation and Upgrade Guide 24.2.10	Provides installation and upgrade information for VENs on the hosts in your environment.

PDF	Description
NEN Installation and Usage Guide 24.2.10	Learn how to install the Illumio Network Enforcement Node (NEN), configure switches to work with it, and use the NEN to secure workloads that are attached to network switches.
LW-VEN Installation and Configuration Guide 24.2.10	Learn how to install and use the Legacy Windows VEN (LW-VEN) with the Illumio Core PCE to enforce security policies on computers running the Windows Server 2003 SP1 and SP2 or Windows Server 2008 SP1 and SP2 operating system.
Administration Guide	
24.4 Administration Guide	A combined administration guide for 24.4 NEN, VEN, Legacy Windows VEN (LW-VEN), and Kubernetes and Openshift.
Events Administration Guide	Learn how to control the behavior of the PCE as it records events and how to change event-related settings in the PCE web console.
PCE Administration Guide	Learn how to maintain and operate the Policy Compute Engine (PCE). This guide also includes other important tasks required to manage your PCE deployment.
VEN Administration Guide	Learn how to manage the VENs that you have installed on the hosts in your environment. This guide provides information about VEN functionality and explains how to troubleshoot issues with the VENs in your environment.
REST API Developer Guide	
REST API Developer Guide 24.4	Learn about the Illumio Core REST APIs.
REST API Developer Guide 24.2.10	Learn about the Illumio Core REST APIs.
User Guides	
Visualization Guide 24.4	Describes the Illumio Core Visualization tools, the problems they solve, some use cases, and examples for 24.4.
Visualization Guide 24.2.10	Describes the Illumio Core Visualization tools, the problems they solve, some use cases, and examples.
Security Policy Guide 24.4	Learn about new and updated features in the 24.4 version of the security policy including the policy objects.
Security Policy Guide 24.2.10	Learn about the Illumio Core security policy including the policy objects. Get guidance about designing a label schema and learn about recommended approaches for Illumio's security policy design including how to create rulesets and rules.
Flowlink Configuration and Usage Guide	Learn about Flowlink, an Illumio-provided standalone application to collect network flow data from different network sources, and its configuration and known limitations.
Application Ringfencing	The Application Ringfencing tutorial is divided into a series of lessons. The lessons correspond to the major phases of creating an application ringfence in your environment and are organized according to the workflow for creating an application ringfence.
Using XPress User Guide	Describes how to use the Xpress features to onboard servers and endpoints.
Edge User Guide 22.31	Describes the new features, enhancements, and platform support for the Illumio Edge 22.31.

PDF	Description
Managed Services Portal User Guide	Describes how to use MSP to onboard your customers in to Illumio Core, Illumio Xpress, and Illumio Edge in the Illumio Cloud and then manage and administer those Illumio products on their behalf.

PDFs for Older Releases

Guide	Description
CLI Tool Release Notes and Containerized VEN Release Notes	
Illumio Core CLI Tool Release Notes 1.4.2	These release notes describe the new features and enhancements for the Illumio Core Advanced Command-line Interface Tool 1.4.2 release. For more information about the CLI, see the Illumio Core PCE CLI Tool Guide, which describes the installation, setup, usage, and tutorials for the CLI tool.
Illumio Core PCE CLI Tool Guide 1.4.2	This guide provides an overview of the CLI Tool, describes how to install and authenticate it, and provides CLI Tools commands for resources.
Illumio Containerized VEN Release Notes 21.5.15	These release notes describe the resolved issues and known issues for the Illumio Containerized VEN 21.5.15 release.
Kubernetes and OpenShift Release Notes and User Guides	
Illumio Core for Kubernetes Release Notes 3.0.0	This document describes the resolved issues and related information for the 3.0.0 release of Illumio Core for Kubernetes, formerly known as Illumio Containerized VEN, or C-VEN.
Illumio Core for Kubernetes Release Notes 3.1.0	This document describes the resolved issues and related information for the 3.1.0 release of Illumio Core for Kubernetes, formerly known as Illumio Containerized VEN, or C-VEN.
Illumio Core for Kubernetes Release Notes 4.0.0	This document describes the resolved issues and related information for the 4.0.0 release of Illumio Core for Kubernetes, formerly known as Illumio Containerized VEN, or C-VEN.
Illumio Core for Kubernetes Release Notes 4.1.0	This document describes the resolved issues and related information for the 4.1.0 release of Illumio Core for Kubernetes, formerly known as Illumio Containerized VEN, or C-VEN.
Illumio Core for Kubernetes Release Notes 4.2.0	This document describes the resolved issues and related information for the 4.2.0 release of Illumio Core for Kubernetes, formerly known as Illumio Containerized VEN, or C-VEN.
Illumio Core for Kubernetes Release Notes 5.2	These release notes describe the resolved issues, known issues, and related information for the 5.2.x releases of Illumio Core for Kubernetes, formerly known as Illumio Containerized VEN, or C-VEN.
Illumio Core for Kubernetes and OpenShift Guide 4.1	This guide explains how deploy the Illumio Core with Kubernetes or OpenShift on your distributed, on-premises and cloud systems.
Illumio Core for Kubernetes and OpenShift Guide 4.2	This guide explains how deploy the Illumio Core with Kubernetes or OpenShift on your distributed, on-premises and cloud systems.
Kubelink	
Illumio Kubelink Release Notes 2.0.2	These release notes describe the enhancements, resolved, and known issues for the Illumio Kubelink 2.0.2 release.

Guide	Description
Illumio Kubelink Release Notes 2.1.1	These release notes describe the enhancements, resolved, and known issues for the Illumio Kubelink 2.1.1 release and earlier releases.
Flowlink	
Illumio Flowlink Release Notes 1.2.2	These release notes describe the enhancements, resolved, and known issues for the Illumio FlowLink 1.2.2 release.
Illumio FlowLink Release Notes 1.3.0	These release notes describe the enhancements, resolved, and known issues for the Illumio FlowLink 1.3.0 release.
NEN and LW-VEN Installation and Configuration PDFs	
Illumio NEN Installation and Usage Guide 2.3.10	This guide introduces the Illumio Network Enforcement Node and describes how to install and configure it and how to integrate the NEN with load balancers and switches.
Illumio NEN Installation and Usage Guide 2.4.10	This guide introduces the Illumio Network Enforcement Node and describes how to install and configure it and how to integrate the NEN with load balancers and switches.
Illumio NEN Installation and Usage Guide 2.5.2	This guide introduces the Illumio Network Enforcement Node and describes how to install and configure it and how to integrate the NEN with load balancers and switches.
Illumio NEN Installation and Usage Guide 2.6.0	This guide introduces the Illumio Network Enforcement Node and describes how to install and configure it and how to integrate the NEN with load balancers and switches.
Illumio NEN Installation and Usage Guide 2.6.10	This guide introduces the Illumio Network Enforcement Node and describes how to install and configure it and how to integrate the NEN with load balancers and switches.
Illumio NEN Installation and Usage Guide 2.6.30	This guide introduces the Illumio Network Enforcement Node and describes how to install and configure it and how to integrate the NEN with load balancers and switches.
Illumio LW-VEN Installation and Configuration Guide 1.0.10	This guide describes the Illumio LW-VEN requirements and how to install and configure the service.
Illumio LW-VEN Installation and Configuration Guide 1.1.0	This guide describes the Illumio LW-VEN requirements and how to install and configure the service.

Legal Notice

Copyright © 2024 Illumio 920 De Guigne Drive, Sunnyvale, CA 94085. All rights reserved.

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

Resources

- [Legal information](#)
- [Trademarks statements](#)
- [Patent statements](#)
- [License statements](#)

Contact Information

- [Contact Illumio](#)
- [Contact Illumio Legal](#)
- [Contact Illumio Documentation](#)