Release Notes 18.2.1

01/24/2019

14000-100-18.2.1

Table of Contents

Welcome

These release notes describe the new features, enhancements, platform support, and new and modified APIs for the Illumio Adaptive Security Platform (ASP) 18.2.1 release.

Document Last Revised: January 2019

Product Version

Current PCE Version: 18.2.1

Current VEN Version: 18.2.1

Note: 18.2.1 has not been designated as a Long Term Support (LTS) release. In the future an 18.2.x LTS release will be designated.

Release Types and Numbering

Illumio ASP release numbering uses the following format: "a.b.c-d+e"

- “a.b": Standard or LTS release number, e.g. "17.1"
- “c”: Maintenance release number
- “-d”: Optional descriptor for pre-release versions, e.g. “preview2"
- “+e”: Hot Fix release descriptor, e.g, “+H1”, “+H2”, “+H3”.

Information about Illumio software support for Standard and LTS releases can be found here: Illumio Versions and Releases.

About Illumio

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

Preview Features Only for Evaluation Before General Availability

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

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

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

Contact Us

Illumio Adaptive Security Platform Training

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

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

Search Knowledge Base and Documentation

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

Illumio Adaptive Security Platform Support

If you cannot find what you are looking for in this document or in support Knowledge Base and Documentation, contact us at:

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

General Advisories

The information in this section is general advisories about important aspects of this release. To ensure proper operation of the system after upgrade, you might need to to take action on these advisories.

Before Upgrade, Review All Changes from Current Version to version 18.2.1

To ensure readiness, Illumio strongly encourages you to review the prior release notes, from your currently installed version of Illumio Adaptive Security Platform to version 18.2.1. To view the release notes for each version, go to the Documentation page and select the version from the pulldown menu.

PCE Capacity Sizing: Recommendation for Additional Storage Device For Explorer Data

PCE and Supercluster PCE storage capacity requirements now include the recommendation of a separate storage device for traffic flow data used by Explorer. Also included is a storage layout scheme for the PCE installed directories.

Use these guidelines and requirements to estimate host system capacity based on typical usage patterns.

Exact requirements vary on a large number of factors, including, but not limited to:

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

Recommended vs minimum sizes

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

There are two configurations for data nodes:

1. A single storage device shared between the data nodes.
2. A dedicated storage device for each data node. This configuration is to accommodate growth in traffic data, which is used by the Explorer. See also "PCE Storage Device Partitions".

MNC Type + Workloads/ VENs[1]	Cores/Clock Speed[2]	RAM per Node[3]	Storage Device Size[4] and IOPS[5]	
			Core Nodes	Data Nodes

2X2
• 2,500 VENs
• 12,500 workloads
	• Four cores per node.
	• Intel® Xeon(R) CPU E5-2695 v4 at 2.10GHz or equivalent.
		32 GB	• 1 x 100 GB
			• 100 IOPS
				• Recommended:
				  • 2 x 250 GB
				  • 600 IOPS per device
				• Minimum:
				  • 1 x 250 GB
				  • 600 IOPS

2X2
• 10,000 VENs
• 50,000 workloads
	• 16 cores per node
	• Intel® Xeon(R) CPU E5-2695 v4 at 2.10GHz or equivalent.
		• Recommended: 128 GB
		• Minimum: 64 GB
			• 1 x 200 GB
			• 100 IOPS
				• Recommended:
				  • 2 x 1 TB
				  • 1,800 IOPS per device
				• Minimum:
				  • 1 x 1 TB
				  • 1,800 IOPS

4X2 • 25,000 VENs • 125,000 workloads	• 16 cores per node • Intel® Xeon(R) CPU E5-2695 v4 at 2.10GHz or equivalent.	128 GB	• 1 x 200 GB • 100 IOPS	• 2 x 1 TB • 5,000 IOPS per device

Footnotes

[1] Number of VENs/workloads is the sum of both the number of managed VENs and number of unmanaged workloads.

[2] CPUs:

- The recommended number of cores is based only on physical cores from allocated CPUs, irrespective of hyper-threading or virtual cores. For example, in AWS one vCPU is only a single hyperthread running on a physical core. that is. half a core. So 16 physical cores equates to 32 vCPUs in AWS.
- Full reservations for vCPU. No overcommit.

[3] Full reservations for vRAM. No overcommit.

[4] Storage requirements for network traffic data can increase rapidly as the amount of network traffic increases. Allocating a separate, large storage device for traffic data can accommodate these rapid changes without potentially interrupting service.

[5] Input/output operations per second (IOPS) are based on 8K random write operations. IOPS specified for an average of 300 flow summaries (80% unique src_ip, dest_ip, dest_port, proto) per workload every 10 minutes. Different traffic profiles might require higher IOPS.

For more than 100 IOPS, either mixed-use Solid-State Disk (SSD) or Storage Area Network (SAN) is required. Locally attached, spinning hard disk drives (HDD) are not sufficient.

For more information, see the *PCE Deployment Guide* or *PCE Supercluster Deployment and Usage Guide*.

New Features in 18.2.1

The following section describes the new features in the Illumio ASP 18.2.1 release.

PCE

Unless otherwise noted, the minimum VEN version for all new PCE features is 17.1.x VEN.

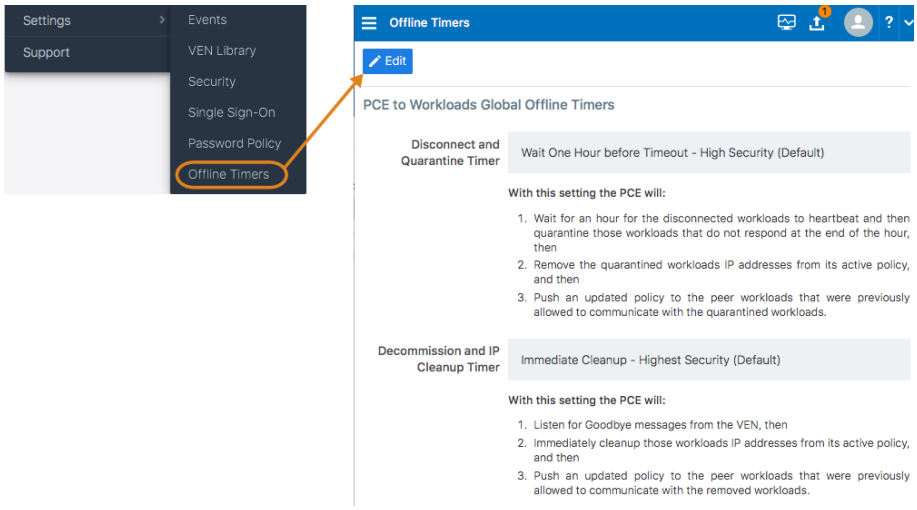
Offline Timers

You can configure Offline Timers in the PCE web console by navigating to **Settings > Offline Timers** and selecting appropriate settings for your workloads.

- **Disconnect and Quarantine:** This timer sets the time period to wait with no heartbeat before a managed workload is marked offline. The default setting is '*Wait One Hour before Timeout*'.
- **Decommission and IP Cleanup:** This timer sets the time period to wait after a managed workload has gracefully shutdown to mark it offline. The default setting is '*Immediate Cleanup*'.

PCE runtime parameters for VEN disconnect no longer valid
The former `runtime_env.yml` file parameters for VEN disconnection settings, `ven_disconnected_timeout_seconds` and `ven_goodbye_delay_seconds`, are no longer valid. These values are now stored in the database and should be set via the PCE web console. Setting these parameters in the `runtime_env.yml` file might not take effect, and these parameters will be removed in a future release.

See the *PCE Web Console User Guide* for the new steps to configure the time limit for VEN disconnect.



PCE internal syslog now generally available

Previously a preview feature, the PCE internal syslog is now generally available. This feature eliminates the need to manage syslog and log rotation on the PCE by yourself.

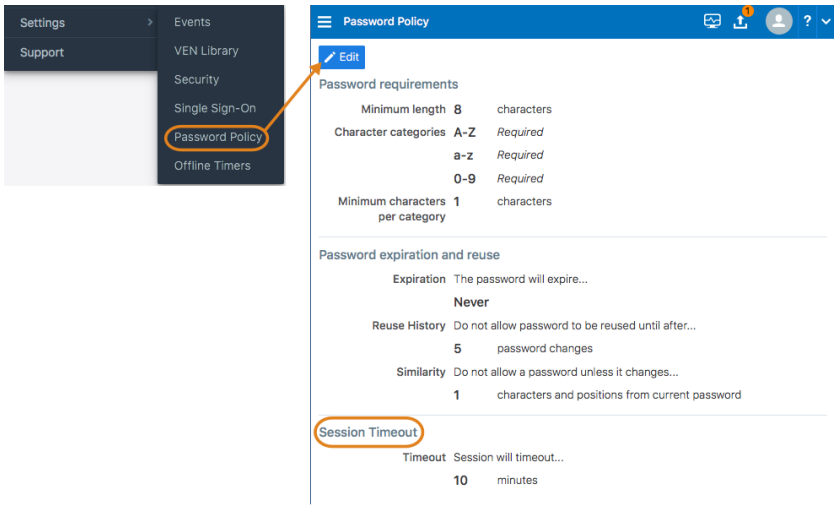
- With the PCE internal syslog, you use the PCE web console to control and configure the relaying of audit events, flow summaries, and system health messages from the PCE to one or more remote syslog destinations.
- Smooth transition from existing system syslog configuration is achieved by a default setting called "Local". Via this setting, the PCE internal syslog relays messages to the existing system syslog. After configuring the internal syslog to rely to a remote destination, you can chose to disable the "Local" setting.
- With the internal syslog, PCE application logs are managed internally and no longer sent to the existing system syslog. All PCE application logs are written to the 'log_dir' directory specified in `runtime_env.yml` (typically `/var/log/illumio-pce`).

See the *PCE Deployment Guide* and the *PCE Web Console User Guide*.

Session Timeout

A global organization owner can now configure the session timeout for their Illumio ASP users in the PCE web console by navigating to **Settings > Password Policy** and setting the desired value.

- The session timeout default value is 10 minutes.
- You can set it between 3 minutes and 30 minutes.
- The changed value does not affect the existing browser session.



VEN

VEN Support for Windows Server Core 1803

The VEN is now supported on Windows Server Core version 1803.

VEN Components Optimized

Formerly, the VEN relied on its components EventSync to send VEN events to the PCE and AgentLogManager to send VEN logs to the PCE. For optimized performance, these two functions have been moved into the PlatformHandler and AgentManager components.

EventSync and AgentLogManager are no longer part of the VEN software architecture.

Customers who whitelist the EventSync and AgentLogManager services or processes should modify their whitelisting to exclude these retired components. Below are the default locations of the executables. If the VEN has been installed in different directories, verify those directory paths.

OS	EventSync Removed	AgentLogManager Removed
Linux	`/opt/illumio_ven/bin/venEventSync`	`/opt/illumio_ven/bin/venAgentLogMgr`
Windows	`C:\Program Files\Illumio\bin\venEventSync.exe`	`C:\Program Files\Illumio\bin\venAgentLogMgr.exe`

Support for Kerberos-based VEN Authentication on Linux and Windows

The PCE and the Linux or Windows VEN can be configured to rely on authentication by a preconfigured Kerberos-based system, such as Microsoft Active Directory. See the *VEN Deployment Guide*.

Modified Features in 18.2.1

The following section describes the features that have been modified or enhanced in this release.

PCE

Improvements in Auditable Events

The following are improvements to Auditable events.

- Event type names have been updated for clarity and consistency.
- The `sec_policy.create` includes the href of the policy that is created. This href can be used to obtain by an alerting system to obtain more information about the policy change.
- Optionally in `runtime_env.yml`, you can enable startup and shutdown events of the Policy Compute Engine (PCE). These are events `pce.application_started` and `pce.application.stopped`.
- Optionally in `runtime_env.yml`, established and dropped connections to remote syslog servers can be recorded as the events `remote_syslog.reachable` and `remote_syslog.unreachable`.

Increase in PCE soft and hard limits for label groups and label group members

The soft and hard limits for Labels and Label Group objects have been significantly increased.

- Soft limit: 8,000 objects
- Hard limit: 10,000 objects

Explorer now supports two storage devices

Explorer data can now be stored on a dedicated storage device. See "General Advisories".

Supercluster

Logs now preserved by illumio-pce-ctl reset command

Formerly, the Supercluster command `illumio-pce-ctl reset` truncated system logs. Now by default the logs are preserved.

Restoring a PCE requires runlevel to be set to 2

Restoring a single PCE in the Supercluster or the entire Supercluster requires that the runlevel of each PCE is set to 2.

Illumio ASP REST API 18.2.1

These new REST API documents have been added to the Illumio ASP documentation library:

- PREVIEW: Illumio ASP 18.2.1 v2 REST API Reference – Available from the public Illumio ASP Documentation Center and from the Illumio Support site (login required).
- PREVIEW: Illumio ASP 18.2.1 OpenAPI3 (Swagger3) Specification – Available from the Illumio Support site (login required).

Note: The parameter tables and code examples in the Illumio ASP 18.2.1 REST API Guide typically describe the v1 APIs, which in many cases are the same or very similar to the v2 APIs. For v2 API parameter tables and code examples, see the Illumio ASP 18.2.1 v2 REST API Reference.

ASP REST API Updates from 18.2.0 v1 to 18.2.1 v1

New Public Experimental REST API Endpoints Added to ASP 18.2.1 v1

- `GET /orgs/:xorg_id/settings/syslog/destinations`

- `POST /orgs/:xorg_id/settings/syslog/destinations`
- `GET /orgs/:xorg_id/settings/syslog/destinations/:syslog_destination_id`
- `PUT /orgs/:xorg_id/settings/syslog/destinations/:syslog_destination_id`
- `DELETE /orgs/:xorg_id/settings/syslog/destinations/:syslog_destination_id`
- `GET /orgs/:xorg_id/settings/events`
- `PUT /orgs/:xorg_id/settings/events`
- `GET /orgs/:xorg_id/settings/workloads`
- `PUT /orgs/:xorg_id/settings/workloads`

ASP REST API Updates from 18.2.0 v2 to 18.2.1 v2

New Public Experimental REST API Endpoints Added to ASP 18.2.1 v2

- `GET /orgs/:xorg_id/settings/syslog/destinations`

- `POST /orgs/:xorg_id/settings/syslog/destinations`
- `GET /orgs/:xorg_id/settings/syslog/destinations/:syslog_destination_id`
- `PUT /orgs/:xorg_id/settings/syslog/destinations/:syslog_destination_id`
- `DELETE /orgs/:xorg_id/settings/syslog/destinations/:syslog_destination_id`
- `GET /orgs/:xorg_id/settings/events`
- `PUT /orgs/:xorg_id/settings/events`
- `GET /orgs/:xorg_id/settings/workloads`
- `PUT /orgs/:xorg_id/settings/workloads`

Exposure Changes from Public Experimental to Public Stable in ASP 18.2.1 v2 REST API Endpoints

- `GET /orgs/:xorg_id/labels`
- `GET /orgs/:xorg_id/labels/:label_id`
- `GET /orgs/:xorg_id/sec_policy/:pversion/services`
- `POST /orgs/:xorg_id/sec_policy/:pversion/services`
- `GET /orgs/:xorg_id/sec_policy/:pversion/services/:service_id`
- `PUT /orgs/:xorg_id/sec_policy/:pversion/services/:service_id`
- `GET /orgs/:xorg_id/sec_policy/:pversion/rule_sets`
- `POST /orgs/:xorg_id/sec_policy/:pversion/rule_sets`
- `GET /orgs/:xorg_id/sec_policy/:pversion/rule_sets/:rule_set_id`
- `PUT /orgs/:xorg_id/sec_policy/:pversion/rule_sets/:rule_set_id`
- `GET /orgs/:xorg_id/sec_policy/:pversion/rule_sets/:rule_set_id/sec_rules`
- `POST /orgs/:xorg_id/sec_policy/:pversion/rule_sets/:rule_set_id/sec_rules`
- `GET /orgs/:xorg_id/sec_policy/:pversion/rule_sets/:rule_set_id/sec_rules/:sec_rule_id`
- `PUT /orgs/:xorg_id/sec_policy/:pversion/rule_sets/:rule_set_id/sec_rules/:sec_rule_id`

Query Parameter Change in an ASP 18.2.1 v2 REST API Endpoint

The "protocol" query parameter was changed to "proto" for this endpoint:

- `GET /orgs/:xorg_id/sec_policy/:pversion/services`

Changed APIs (Modified or Removed)

Deprecated: GET Provisioning Dependencies

The following Public Experimental API was deprecated and was no longer available after the Illumio ASP 18.2.0 release.

API	Description	Exposure
`GET [api_version]/ sec_policy/dependencies`	This method gets a list of all non-modified security policy objects that will also get provisioned when you provision all of modified ("draft") security items. List also includes modified items.	Public Experimental

The above deprecated API endpoint was replaced by an improved API that allows you to check provisioning dependencies more efficiently.

API	Description	Exposure
`POST [api_version]/ sec_policy/draft/ dependencies`	This method allows you to determine if a specific set of objects can be provisioned, or if they are dependent on other objects that need to be provisioned as well.	Public Experimental

Resolved Issues in 18.2.1

PCE Resolved Issues

- **Virtual servers shown multiple times in Illumination** (E-50082)
  Formerly, when a virtual was manged, then unmanaged, and the managed again, it would appear twice in Illumination. This issue has been resolved.
- **Blocked traffic page not displayed after PCE upgrade** (E-49854)
  Formerly, after a PCE was upgraded to version 18.2.0, the erroneous message "Blocked traffic feature is disabled on this PCE" was displayed and the blocked traffic page in the PCE web console did not display any data. This issue has been resolved.

- **SecureConnect rules with non-SecureConnect rules in the opposite-direction need additional rule to allow communication** (E-48780)
  When two workloads have a SecureConnect rule between a provider and a consumer in one direction and a non-SecureConnect rule in the opposite direction, customers had to add an additional rule allowing UDP port 500 from the provider to the consumer to enable non-SecureConnect traffic. This issue is resolved.
- **Change to IP List on Consumer side was not reflected in new policy rules** (E-52178)
  When a rule that had only an IP list on the consumer side was edited to replace the existing IP list with a different IP list, the rule change was not sent to the VEN when provisioned. This issue is resolved.
- **Some workloads and traffic flows were not displayed** (E-50029)
  Some workloads in an application and traffic flows connecting those workloads were not displayed in Illumination due to an error in the UI. This issue is resolved and all workloads and traffic flows are now displayed.
- **Empty page could appear when editing the Password Policy for the PCE** (E-49081)
  An empty page could appear if you clicked the browser's back button while editing the Password Policy for the PCE. This issue is resolved. Clicking the browser's back button while editing password policy returns you to the Password Policy Settings page.
- **GET /events REST API command could timeout without the max_results parameter** (E-49404)
  The max_results parameter wasn't required with the GET /events REST API; however, when you didn't specify it, the GET /events REST API could timeout when your environment had a large number of event records. This issue is resolved. The GET /events REST API no longer times out without the max_results parameter.
- **Querying PCE events could take longer than 10 seconds to receive a response** (E-47224)
  Querying PCE events using the Illumio REST API or filtering events in the PCE web console could take longer than 10 seconds when your environment had a large number of event records. This issue is resolved.
- **Read-only users without explicit permissions could receive an error message in the PCE web console** (E-49507)
  When read-only users accessed the PCE web console without explicit permissions, they could receive error messages. SAML users especially encountered this issue. This issue is resolved. Read-only users without explicit permissions can view the PCE web console without encountering error messages.
- **Duplicated rulesets did not include notes** (E-49911)
  Duplicating a ruleset did not copy the rule notes to the new ruleset. This issue is resolved. In this release, duplicated rulesets include the notes from the original rules.
- **Slow load of Label Groups list page in PCE web console** (E-51245)
  The Label Groups list page in the PCE web console could take a significant time to load when a large number of groups were loaded. This issue is resolved.
- **Provisioning large number of rules caused rendering problems in PCE web console** (E-51198)
  Formerly, provisioning a large number of rules caused rendering problems for the final rows in the PCE web console. This issue is resolved.
- **Workloads edit page in PCE web console did not display new labels** (E-50677)
  Formerly, when new labels were created, they did not appear on the Workloads page in the PCE web console and thus could not be applied to workloads. This issue is resolved.
- **Process-based rules created by using Policy Generator could be incorrect** (E-49197)
  When you have a PCE Supercluster deployed and you use Policy Generator to generate policy, Policy Generator in certain cases could suggest port-based rules instead of process-based rules. This issue is resolved.

- **For auditable events, type of CEF field suser was not human-readable** (E-49525)
  Formerly the data type of the `suser` field in CEF-format messages for auditable events was not human-readable (data type hash). It is now human-readable (data type string). This issue has been resolved.
- **Rules using services with port ranges could not sync** (E-49881)
  VENs could get stuck in the "Active (Syncing)" state indefinitely when the following conditions occurred:
    - You added a service with a port range to a rule
    - Enabled SercureConnect for that rule
    - Provisioned the updated policy

  This issue is resolved. In this release, the VENs sync and generate system events alerting you that adding services with port ranges and enabling SecureConnect is not supported.

- **VEN Library page appeared in the PCE web console when you had not loaded the VEN Library file** (E-48730)
  When you had not configured the PCE web console to install VENs on workloads, the PCE still displayed an empty VEN Library page (Settings > VEN Library). This issue is resolved. The PCE web console only displays a VEN Library menu option under Settings when you have loaded the VEN Library file into the PCE.
- **PCE returned 500 errors when VENs uploaded Support reports** (E-49411)
  When a VEN uploaded a Support report, it could receive a 500 error from the PCE. The PCE updated the Support report correctly before returning the 500 error. Therefore, the VEN did not generate a system event due to the 500 error or try to re-upload the file. This issue is resolved. The PCE no longer returns 500 errors when VENs upload Support reports.
- **PCE displayed an empty page when you clicked the browser's Back button while editing the Password Policy** (E-48331)
  When you edited the PCE Password Policy (Settings > Password Policy > Edit button) and clicked the browser's Back button before changing or saving the settings, the PCE displayed an empty page. This issue is resolved. Clicking the Back button now returns you to the Password Policy page in view mode.
- **Peer invalidation was missing or incorrect for virtual services with IP overrides** (E-50983)
  IP overrides and the ports defined by virtual services were not received by service consumers when the virtual services were bound to workloads and used as rule providers. Additionally, the service consumers' ports were not overridden. This issue is resolved.
- **PCE didn't send IP overrides to consumers when the virtual services weren't bound to workloads** (E-51044)
  Outbound rules for consumers allowing access to IP overrides weren't configured until the virtual services were bound to workloads. This issue is resolved. In 18.2.1, the PCE allows consumers to access the IP addresses of IP overrides even when the virtual services aren't bound to workloads.
- **PCE didn't configure the correct IP address and port for a workload** (E-48251)
  When a workload was bound to multiple virtual services with IP overrides, the PCE configured an incorrect IP address and port for the service consumer. This issue is resolved.
- **Deleted local user could not be re-invited as a local user** (E-44563)
  If you deleted a local user and attempted to re-invite the same local user, the operation would fail with a message 'This user already exists'. The is caused because the PCE converts deleted local users to external users instead of deleting the user account. This issue is resolved and you can now re-invite a previously deleted local user.
- **TCP/UDP port 0 could not be used in policy writing** (E-47245)
  Previously, you could not write policy covering port 0. This issue is resolved and you can now specify TCP/UDP port 0 in a service, use it in policy writing, and also see traffic from/to TCP/UDP port 0 in

Explorer. The Policy Generator will also generate rules that cover port 0. You can also see the rule-coverage in Illumination for multiple services including port 0.

- **Explorer displayed inconsistent results** (E-52394, E-52578)
  Explorer displayed traffic as "potentially blocked" even though there was a rule to allow the traffic. The traffic was not displayed on the "blocked traffic" page. This issue is resolved and the traffic flows are displayed correctly.

PCE Supercluster Resolved Issues

- **Restoring a PCE Supercluster Leader could fail** (E-50482, E-49905)
  An issue prevented the restore of the Supercluster Leader from successfully completing. This issue is resolved. Restoring a PCE Supercluster Leader completes successfully in this release.
- **Unable to retry a failed supercluster-join command** (E-50746)
  When joining a member PCE to a Supercluster fails, rerunning the supercluster-join command continues to fail and returns exit code 1. This issue is resolved. After a member PCE fails to join a Supercluster, you can now rerun the supercluster-join command without the command automatically failing.

VEN Resolved Issues

- **AIX unsatisfied symlink caused infinite loop in VEN** (E-49886)
  Formerly, if the AIX VEN was not started from the `/opt/illumio_ven` directory, the VEN went into an infinite loop trying to traverse an unsatisfied symlink. This issue has been resolved.
- **OEL VEN conntrack timeout not set correctly** (E-49665)
  Formerly, the installation of the VEN on OEL 5.x did not set the conntrack timeout to eight hours. This issue is resolved.
- **Firewall tampering events generated in error** (E-49115)
  On platforms with SELinux policy enabled, a temporary file could not be written by VEN. This caused a firewall tampering event to be generated erroneously. This issue has been resolved.
- **Idle mode on Linux VEN did not restore previous firewall** (E-51195)
  Formerly, when the mode of a Linux VEN was changed to idle, the previous firewall state was not restored. This issue has been resolved.
- **Setting value of VEN_KERBEROS_WORKLOAD_SPN during VEN upgrade did not take effect** (E-49563)
  Formerly, during update of a Kerberos-authenticated VEN, setting the environment variable `VEN_KERBEROS_WORKLOAD_SPN` did not take effect. This issue has been resolved.
- **Version 16.04 of Ubuntu was unpaired during upgrade to version 18.2.0** (E-51246)
  Formerly, when an Ubuntu workload running VEN version 16.04 was upgraded to VEN version 18.2.0, the VEN was unpaired. This issue has been resolved.
- **Suspending VEN on Debian 9.5 did not consistently take effect** (E-51274)
  Formerly, suspending the Debian 9.5 VEN did not consistently take effect. This issue has been resolved.
- **VEN-to-PCE SSL/TLS session was not resumed** (E-50331)
  Formerly, the VEN did not properly resume its SSL/TLS session with the PCE, causing renegotiations (handshakes). This issue has been resolved.
- **VEN restart did not reload SecureConnect configuration** (E-50631)
  Formerly, when a VEN configured for SecureConnect was restarted in certain ways, the SecureConnect configuration was not reloaded. On Windows, if policy rules were removed and the VEN restarted, the

configuration was not reloaded. On Linux, if the StrongSwan service was stopped and the VEN restarted, the configuration was not reloaded. This issue has been resolved.

- **Windows VEN PlatformHandler crashed on certain older CPU architectures** (E-50558)
  On Windows 7 2008 R2 32-bit, when IPsec was enabled, the PlatformHandler component of the VEN would crash on some older CPU architectures. This issue has been resolved.
- **Upload of VEN support report used erroneous URL** (E-51239, E-49552)
  Formerly, when the VEN uploaded its support report to the PCE, the VEN used an invalid URL and a URL with non-standard field names was written to the VEN log. This issue has been resolved.
- **Windows VEN did not write events to system log** (E-49368)
  Formerly, the VEN on Windows did not write events to its system log. This issue has been resolved.

Known Issues in 18.2.1

PCE Known Issues

- **Rules tab can display a 500 Internal Server error** (E-53518)
  When a rule contains a provider that is a virtual service, displaying the Rules tab for consumer workloads impacted by that rule can display a 500 Internal Server error.
- **Provisioning a Static Scope that contains a label group displays a 500 internal server error** (E-53416)
  Adding a new, un-provisioned label group to a Static Policy causes the PCE to display a 500 Internal Server Error when you save the policy update. Go to **Settings** > **Edit** > **Manage Policy Update** > **Add**. Select an un-provisioned label group to add to the Static Policy Scopes and Labels field.
  Workaround: Provision new label groups before you add them to Static Policy.
- **Updating the Repository in Event Settings fails unless you re-upload the TLS CA certificate bundle** (E-53414)
  When you update the Repository configured to use a remote syslog server, you must re-upload the TLS CA certificate bundle or the PCE web console will return a TLS peer verification failure error. If you don't re-upload the certificate bundle, the PCE overwrites the existing bundle with a null value.
- **API requests with misspelled endpoint succeed** (E-53411)
  The workload/settings API provides a flexible request format, and does not strictly validate the request. Flexible request validation is required for adding future settings because it allows the REST API to ignore incorrect or invalid objects passed in the request.
- **Events viewer incorrectly suggests filtering events by notification types** (E-53038)
  The Events viewer includes suggestions to filter events by `event_types` and `notification_types`. The Event Type filter should only include `event_types` in the suggested list. You can safely ignore the suggestion to filter events by `notification_types`.
- **Can't merge rules in Policy Generator when the rules have a common provider and service** (E-53329)
  In the Rule Construction field of the Policy Generator, selecting the option **Merge rules with common Provider and Service** does not work.
- **Deleting the Policy Sync: Suspended filter in the Workloads list page displays an error** (E-53158)
  Selecting the Policy Sync filter with the Suspended option, then deleting that option, displays the text "Policy Sync (0)" in the filter options. You can safely ignore this text.
- **Policy Generator shows different number of connections for IP Lists** (E-52539)
  Policy Generator might show one set of connection numbers in the initial page and a different number of connections in the subsequent pages while writing policy for IPLists.

- **CEF message for agent.activate.success event shows suser field as null** (E-51784)
  The CEF-format message for the agent.activate.success event shows the `suser` field as null.
- **Port 0 not displayed in Windows Service page of PCE web console** (E-51689)
  A Windows Service created with 0 TCP and 0 UDP ports is displayed in the Windows Services page with only the protocol but without port 0.
- **On upload of workload support report, action_log_event not logged** (E-51506)
  When the agent support report is uploaded to the PCE, the event does not contain action details.
- **Cannot use port 0 to override port ranges for virtual services** (E-51275)
  In defining a rule for virtual services with port range 2700-2710 TCP, port 0 cannot be used to override that range.
- **Field "workloads_affected" for logged event sec_policy.create shows 0** (E-50862)
  The logged event sec_rule.create shows 0 for the workloads_affected field. Workaround: The proper value for workloads affected is shown for the event in the PCE web console and by the REST API.
- **Event logged for user.authauthorization failure does not include IP address of VEN that caused failure** (E-50415)
  The event for user.authorization failures does not include the IP address of the VEN that triggered the event.
- **Event workload.update before and after timer values of 0 not displayed correctly in PCE Web Console** (E-50248)
  When the workload.update event has a timer before and after values of 0, the event is not displayed correctly in the PCE web console.
- **Offline workload erroneously shows "Active (Syncing)" in PCE Web Console** (E-52367)
  When a workload is offline (for example, the workload was destroyed without first unpairing) the PCE web console erroneously shows "Active (Syncing)" for that workload.
- **Resource change in event type rule_set.update does not correctly represent scope of change** (E-52732)
  When a rule set is changed, the event type rule_set.update incorrectly represents the scope of the change as individual scope objects, instead of as an array of those scope objects.
- **Virtual services rule with mix of port overrides and and non-port-overrides does not contain all necessary port overrides** (E-52380)
  For a virtual service, when a rule includes port overrides and non-port overrides, the resulting rule does not include all the ports specified in the port overrides.
- **Event logged for permission.create for user with "Global Read Only" shows "before" value as null for some fields** (E-50293)
  When a user is given "Global Read Only" permission, the permission.create event fields role_id and org_scope_id show a "before" value of null.
- **Failure of creating a remote syslog destination shows un-parsed error message on PCE web console Events page** (E-49960)
  When an attempt to create a remote syslog destination via the PCE web console fails because of invalid input, the Events page shows the error message as "Unable to connect to remote syslog server: %s".
- **Inactivity timeout from PCE web console logs erroneous user.sign_out failure event** (E-49907)
  When a user session in the PCE web console is terminated due to inactivity, an erroneous user.sign_out event is recorded.
- **Browser pre-fetching of pages after user logout can cause multiple erroneous events** (E-49778, E-49797)
  After a user has logged out of the PCE web console and tries to access the previous page (with the back arrow, for example), browser pre-fetching of that page when the user is no longer authenticated results in multiple, erroneous user.authorization_failure and user.authentication_failure events. This is an infrequent problem.

- **Workloads page may display an error message after pairing for 'Read Only' users** (E-49539)
  When you pair a VEN and then open the Workloads page, the UI may display an error message even if the pairing is successful. Workaround: Refresh the Workloads page.
- **External users can create API keys** (E-49234)
  API keys are not supported for use by external users. External users can create API keys but they aren't usable.
- **Pairing a VEN on a workload that has multiple IP addresses per interface generates multiple events** (E-49120)
  When a VEN is installed on a workload that has multiple IP addresses on an interface (for example, both IPv4 and IPv6 addresses), the PCE generates interface status update messages for each IP address. In the second message, the IPv4 address is converted to an IPv6 address.
- **The rule-coverage bar doesn't always appear in the App Groups List page** (E-49049)
  Go to App Groups → App Groups List. The rule-coverage bar in the Coverage column can be missing for some App Groups with connections.
  Workaround: Click the Refresh icon in the Coverage column to display the bar.
- **Blocked Traffic page can report blocked IP addresses that do not exist on the workloads** (E-48181)
  In the PCE web console, the Blocked Traffic pages (list and details) can report blocked IP addresses that do not exist on the providing workloads. This issue occurs when traffic is directed at network broadcast addresses or global broadcast addresses. The PCE associates these addresses with the reporting workloads. You can safely ignore these non-existent IP addresses.
- **Workloads in Idle policy state report traffic as allowed** (E-47883)
  When a workload's policy state is set to Idle, the PCE web console won't report any traffic as potentially blocked for that workload on the Blocked Traffic page (Troubleshooting > Block Traffic from the menu), on the workload's Blocked Traffic tab, or on the workload's Vulnerabilities tab. The PCE logs the traffic in the Event log and Explorer. Workaround: To view potentially blocked traffic for a workload, change the workload's policy state from Idle to Test or view the Event logs.
- **Events page or Events API can take 10 seconds to respond** (E-47598)
  When the Events functionality hasn't been accessed for over 5 minutes (300 seconds) by any Illumio user, the Events page in the web console or the Events API are slow to respond. The web console page can take 10 seconds to load and the API can take 10 seconds to return a response. When the Events functionality is frequently accessed (multiple times within 5 minutes), only the first access is slow to respond. All subsequent access responds quickly.
- **Read-only users can see a confusing message in the PCE web console pages** (E-47029)
  When you have read-only access to the PCE web console, the details pages (such as the Service Details page) can display the following message:
  "You are editing the draft version". Read-only users do not have permission to modify security policy configured in the PCE; therefore, this message does not apply. You can safely ignore it.
- **PCE uptime value can be wrong in the PCE Health page** (E-45143)
  Temporary, expected PCE service restarts can reset the PCE uptime values displayed in the web console's PCE Health page so that it is not consistent with the uptime values displayed by "illumio-pce-ctl start".
- **Delay in displaying 'Service' attached to Bound Service in the Bound Service Summary page** (E-40892)
  If you create a new Bound Service, 'Service' attached to the Bound Service does not initially appear in Bound Service Summary page. After a few more seconds, it does appear. (In 18.2, Bound Services are now called Virtual Services.)
- **Saving a change to "My Profile" sends user to other pages** (E-40873, E-29658)
  If you make and save a change to your user profile (User menu → My Profile), when you click save, you are returned to a different page, instead of your profile. For example, in some cases when a user clicked Save, the PCE web console displayed the Illumination map. The changes are saved, however.

- **Illumination displays incorrect traffic coverage for some Workload types** (E-30142)
  In some cases where Rules involving IP Lists or the "Any" Label are expected to match unmanaged Workloads, the Illumination map incorrectly displays traffic lines as red in the Draft View. This is because traffic lines between managed and unmanaged Workloads are shown in green only when there are Rules to allow both on the outbound and inbound entities. To avoid this issue, we recommend using the Reported View to verify traffic.
- **PCE web console does not provide a warning when using entities in Rules that are not in Scope** (E-29502)
  You are incorrectly allowed to select a Workload as a Provider for a Rule, even if the Provider's Labels do not match the Labels of the specified Scope.
- **Http(s) proxy is redirecting invites from MNC to null** (E-26007)
  When an invite is sent to a user, the invite is redirected due to a proxy configured on PCE host and the invited user receives a 500 error when trying to access the page.

PCE Supercluster Known Issues

- **During rolling upgrade, some columns in workloads view in PCE web console are not translated to English** (E-48623)
  During a rolling upgrade, some columns of the workloads view are not translated to English.

VEN Known Issues

All Platforms

- **Unpairing a workload doesn't succeed when using API without accepted values** (E-52043)
  When using the unpair workloads API, the request body must include the property `ip_table_restore` with the following accepted values: `saved`, `default`, `disable`
- **Depending on amount of data and number of support reports already created, VEN support report can sometimes fail** (E-49537)
  In some rare cases, the VEN support report might fail due to the amount of data and the number of support reports that have been previously generated.
- **Upgrading the VEN on a Workload can cause the Illumio REST API to generate an HTTP 406 NOT ACCEPTABLE** (E-40132)
  This API error occurs when the API version is incompatible with the VEN. Every 24 hours the VEN retrieves a new master configuration file, which will correct the API version incompatibility. In most cases, this issue corrects itself within a few minutes. If it does not, wait for the VEN to retrieve a new master configuration file or restart the VEN to force it to update the file.
- **Installing or upgrading the VEN on Windows fails when Wireshark Network Analyzer is running** (E-38953)
  When installing or upgrading the VEN using the MSI installer, installation or upgrade fails when Wireshark Network Analyzer is running. To workaround this issue, stop the Wireshark Network Analyzer application before installing or upgrading the VEN.

AIX VEN Known Issues

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

Solaris VEN Known Issues

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

End of Support Announcements, Deprecations, On-premises Upgrade Paths, Compatibility

For more information on PCE and VEN version compatibility, visit the Illumio Support site and select Software → Upgrade Path.

Supported Upgrade Type for PCE version 18.1 to 18.2.1

Version-dependent upgrade paths
If you plan on upgrading from Supercluster version 18.1 to version 18.2.1, use the simple upgrade. Do *not* use the rolling upgrade.
Rolling upgrade is supported from version 18.2.0 forward.

End of Support

- **External VEN repo no longer supported**
  The external VEN repo is no longer supported for VEN versions 18.2 and higher. Customers must migrate to using the new PCE-based VEN deployment or install VEN packages directly on workloads.
- **System events for OVA no longer supported** (E-48119)
  Events 2.0 system events are no longer supported on the Open Virtual Appliance (OVA).

Old "organization events" no longer supported

With this release, the older form of events, known as "audit or organization events", is no longer supported or available.

> Any versions of the former *SIEM Integration Guide* that are earlier than version 18.2.1 are valid only for their corresponding versions, not version 18.2.1 or later.

Customers should upgrade to the latest version of Illumio Adaptive Security and take advantage of the newly designed auditable events. See the *Auditable Events and SIEM Integration Guide*.

Deprecations in This Release

Deprecated – Illumio ASP REST API Version 1

Illumio ASP REST API Version 1 (v1) is deprecated as of this release. These are the endpoints beginning with `/api/v1`.

REST API v1 is deprecated as of ASP 18.2.1 and will stay deprecated until it is removed from ASP 19.2.0. ASP 19.2.0 will only have v2 APIs, the v1 APIs will be removed and will no longer be available in 19.2.0 or post-19.2.0. Therefore, consider planning to migrate from v1 to v2 APIs in your ETL tools, dashboards, portals, and so forth that interact with the PCE.

A detailed FAQ on the REST API v1 deprecation is available on Illumio support site.

PCE Supported OSs

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

PCE Virtual Appliance

VMware ESXi 5.0, 5.1, 5.5, 6.0, or 6.5.

VEN Supported OSs

There is no change in the VEN supported operating systems from 18.2.0 to 18.2.1. For the detailed list, see the Illumio support site.

Documentation Updates for 18.2.1

In addition to general updates to documentation for Illumio ASP version 18.2.1, these new REST API documents have been added to the Illumio ASP documentation library:

- PREVIEW: Illumio ASP 18.2.1 v2 REST API Reference – Available from the public Illumio ASP Documentation Center and from the Illumio Support site (login required).
- PREVIEW: Illumio ASP 18.2.1 OpenAPI3 (Swagger3) Specification – Available from the Illumio Support site (login required).