Illumio Core®

Version 21.5

Events Administration Guide

November 2022

80000-100-21.5

Legal Notices

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.

Product Version

PCE Version: 21.5 (LTS Release)

For the complete list of Illumio Core components compatible with Core PCE, see the Illumio Support portal (login required).

For information on Illumio software support for Standard and LTS releases, see Versions and Releases on the Illumio Support portal.

Resources

Legal information, see https://www.illumio.com/legal-information

Trademarks statements, see https://www.illumio.com/trademarks

Patent statements, see https://www.illumio.com/patents

License statements, see https://www.illumio.com/eula

Open source software utilized by the Illumio Core and their licenses, see Open Source Licensing Disclosures

Contact Information

To contact Illumio, go to https://www.illumio.com/contact-us

To contact the Illumio legal team, email us at legal@illumio.com

To contact the Illumio documentation team, email us at doc-feedback@illumio.com

illumio

Contents

Chapter 1

Overview of Events Administration

This chapter contains the following topics:

This section describes how to do typical administration tasks related to PCE events.

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

Before Reading This Guide

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

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

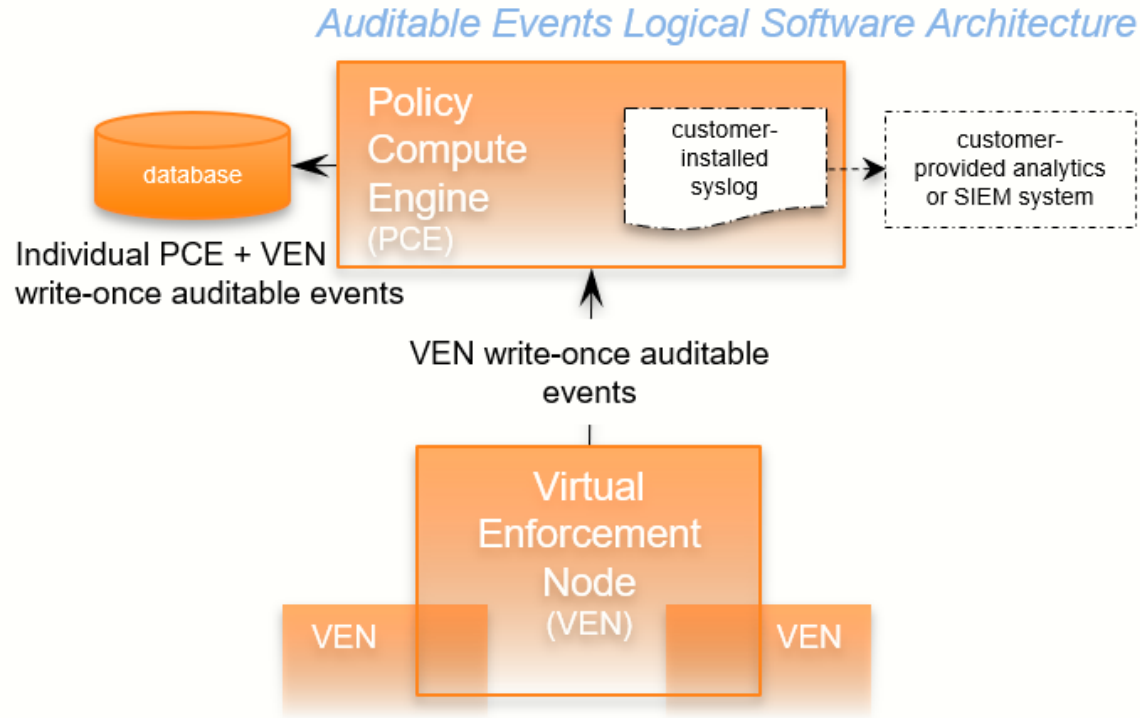
The Illumio events framework provides an information-rich, deep foundation for actionable insights into the operations of Illumio Core.

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
Resource Lifecycle Tracking	All information necessary to track a resource through creation, modification, and deletion.	Events Lifecycle for Resources
Operations	Trace of recent changes to resources.	Events Lifecycle for Resources
Security	Evidence to show which changes failed, such as incorrect user permissions or failed authentication.	User Password Update Failed (JSON)

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 intregration
  - 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.

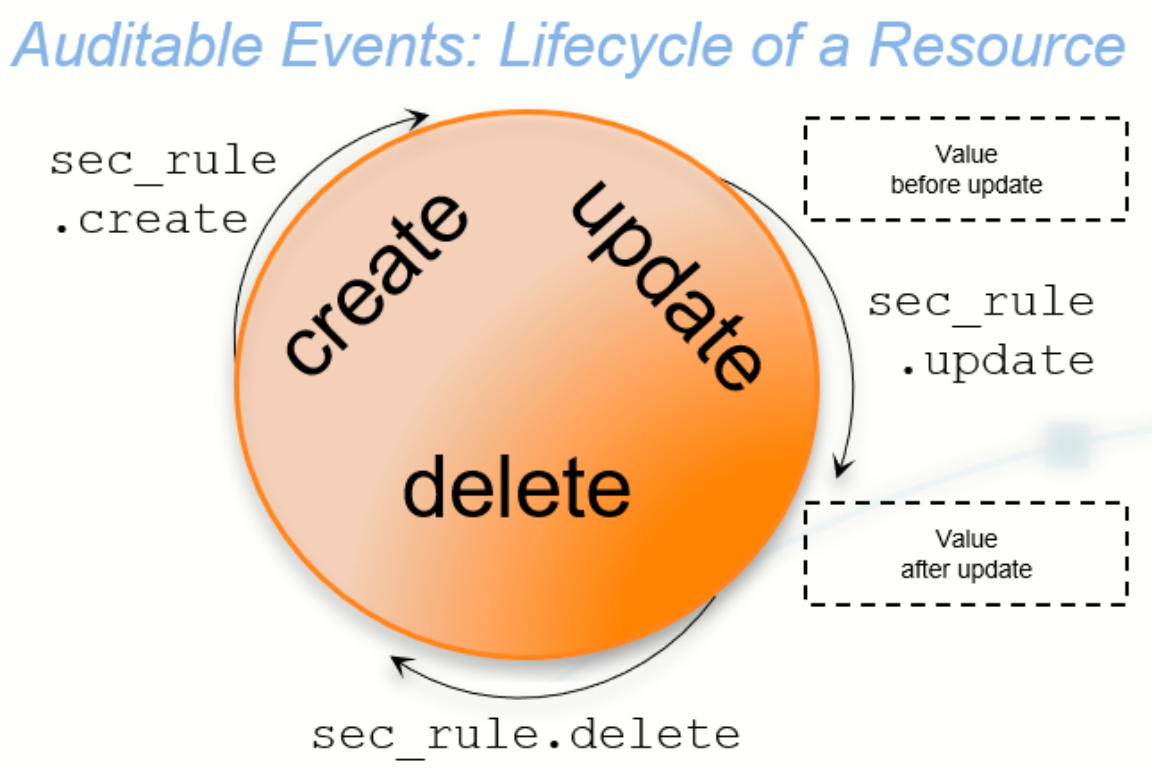
Events Lifecycle for Resources

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`



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`

Chapter 2

Events Described

This chapter contains the following topics:

This chapter describes 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	• VEN identified by hostname and agent href • User identified by username and href • PCE system identified by “system”
What	The action that triggered the event, including the following data: • Resource type + operation + success or failure • Application Request ID

Type of information	Description

	• Status of successful events and failed events:
	  ◦ 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	The target resource of the action, composed of the following data:
	• Identifier of the target resource (primary field).
	• Friendly name for the target resource. For example:
	  ◦ workload/VEN: `hostname`
	  ◦ 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 *not* 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
`href`	Unique event identifier; contains a UUID.
`timestamp`	Exact time that the event occurred in RFC 3339 format with fractional seconds.
`pce_fqdn`	The fully qualified domain name of the PCE; especially useful for Super-cluster deployments or if there are multiple PCEs sending data to the SIEM server.

Field Name	Description
`created_by`	Identifies creator of the event; could be a user, the system, or a workload.
`event_type`	Name of the event; for more information, see the List of Event Types table.
`status`	"Success" or "failure;" if the status is null, the event is for information only and doesn't indicate success or failure.
`severity`	"Informational," "warning," or "error" indicating the severity of the event.
`version`	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.

JSON Event Type	Description
`access_restriction.create`	Access restriction created
`access_restriction.delete`	Access restriction deleted
`access_restriction.update`	Access restriction updated
`agent.activate`	Agent paired
`agent.activate_clone`	Agent clone activated
`agent.clone_detected`	Agent clone detected
`agent.deactivate`	Agent unpaired
`agent.goodbye`	Agent disconnected
`agent.machine_identifier`	Agent machine identifiers updated
`agent.refresh_token`	Agent refreshed token
`agent.refresh_policy`	Success or failure to apply policy on VEN
`agent.request_upgrade`	VEN upgrade request sent
`agent.service_not_available`	Agent reported a service not running
`agent.suspend`	Agent suspended
`agent.tampering`	Agent firewall tampered
`agent.unsuspend`	Agent unsuspended
`agent.update`	Agent properties updated.
`agent.update_interactive_users`	Agent interactive users updated
`agent.update_iptables_href`	Agent updated existing iptables href
`agent.update_running_cont ainers`	Agent updated existing containers
`agent.upload_existing_ip_table_rules`	Agent existing IP tables uploaded

JSON Event Type	Description
agent.upload_support_report	Agent support report uploaded
agent_support_report_request.create	Agent support report request created
agent_support_report_request.delete	Agent support report request deleted
agents.clear_conditions	Condition cleared from a list of VENs
agents.unpair	Multiple agents unpaired
api_key.create	API key created
api_key.delete	API key deleted
api_key.update	API key updated
auth_security_principal.create	RBAC auth security principal created
auth_security_principal.delete	RBAC auth security principal deleted
auth_security_principal.update	RBAC auth security principal updated
authentication_settings.update	Authentication settings updated
cluster.create	PCE cluster created
cluster.delete	PCE cluster deleted
cluster.update	PCE cluster updated
container_workload.update	Container workload updated
container_cluster.create	Container cluster created
container_cluster.delete	Container cluster deleted
container_cluster.update	Container cluster updated
container_cluster.update_services	Container cluster services updated as Kubelink
container_workload_profile.create	Container workload profile created
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

JSON Event Type	Description
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
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
lost_agent.found	Lost agent found

JSON Event Type	Description
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
network_endpoint.create	Network endpoint created
network_endpoint.delete	Network endpoint deleted
network_endpoint.update	Network endpoint updated
network_enforcement_node.activate	Network enforcement node activated
network_enforcement_node.clear_conditions	Network enforcement node conditions cleared
network_enforcement_node.deactivate	Network enforcement node deactivated
network_enforcement_node.degraded	Network enforcement node failed or primary lost connectivity to secondary
network_enforcement_node.missed_heartbeats	Network enforcement node did not heartbeat for more than 15 minutes
network_enforcement_node.missed_heartbeats_check	Network enforcement node missed heartbeats check
network_enforcement_node.network_devices_network_endpoints_workloads	Workload added to network endpoint
network_enforcement_node.policy_ack	Network enforcement node acknowledgment of policy
network_enforcement_node.request_policy	Network enforcement node policy requested
network_enforcement_node.update_status	Network enforcement node reports when switches are not reachable
network_enforcement_nodes.clear_conditions	A condition was cleared from a list of network enforcement nodes

JSON Event Type	Description
nfc.activate	Network function controller created
nfc.delete	Network function controller deleted
nfc.update_discovered_virtual_servers	Network function controller virtual servers discovered
nfc.update_policy_status	Network function controller policy status
nfc.update_slb_state	Network function controller SLB state updated
org.create	Organization created
org.recalc_rules	Rules for organization recalculated
org.update	Organization information updated
pairing_profile.create	Pairing profile created
pairing_profile.create_pairing_key	Pairing profile pairing key created
pairing_profile.delete	Pairing profile deleted
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
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

JSON Event Type	Description
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
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
services.delete	Services deleted
settings.update	Explorer settings updated

JSON Event Type	Description
slb.create	Server load balancer created
slb.delete	Server load balancer deleted
slb.update	Server load balancer updated
support_report.upload	Support report uploaded
syslog_destination.create	syslog remote destination created
syslog_destination.delete	syslog remote destination deleted
syslog_destination.update	syslog remote destination updated
system_task.agent_missed_heartbeats_check	Agent missed heartbeats
system_task.agent_offline_check	Agents marked offline
system_task.prune_old_log_events	Event pruning completed
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_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

JSON Event Type	Description
ven_settings.update	VEN settings updated
ven_software.upgrade	VEN software release upgraded
ven_software_release.create	VEN software release created
ven_software_release.delete	VEN software release deleted
ven_software_release.deploy	VEN software release deployed
ven_software_release.update	VEN software release updated
ven_software_releases.set_default_version	Default VEN software version set
virtual_server.create	Virtual server created
virtual_server.delete	Virtual server created
virtual_server.update	Virtual server updated
virtual_service.create	Virtual service created
virtual_service.delete	Virtual service deleted
virtual_service.update	Virtual service updated
virtual_services.bulk_create	Virtual services created in bulk
virtual_services.bulk_update	Virtual services updated in bulk
vulnerability.create	Vulnerability record created
vulnerability.delete	Vulnerability record deleted
vulnerability.update	Vulnerability record updated
vulnerability_report.delete	Vulnerability report deleted
vulnerability_report.update	Vulnerability report updated
workload.create	Workload created
workload.delete	Workload deleted
workload.online	Workload online
workload.recalc_rules	Workload policy recalculated
workload.redetect_network	Workload network redetected
workload.undelete	Workload undeleted
workload.update	Workload settings updated
workload.upgrade	Workload upgraded
workload_interface.create	Workload interface created
workload_interface.delete	Workload interface deleted
workload_interface.update	Workload interface updated
workload_interfaces.update	Workload interfaces updated For example, IP address changes, new inter-

JSON Event Type	Description
	face added, and interface shut down.
workload_service_report.update	Workload service report updated
workload_settings.update	Workload settings updated
workloads.apply_policy	Workloads policies applied
workloads.bulk_create	Workloads created in bulk
workloads.bulk_delete	Workloads deleted in bulk
workloads.bulk_update	Workloads updated in bulk
workloads.remove_labels	Workloads labels removed
workloads.set_flow_reporting_frequency	Workload flow reporting frequency changed
workloads.set_labels	Workload labels applied
workloads.unpair	Workloads unpaired
workloads.update	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
pce.application_started	PCE application started
pce.application_stopped	PCE application stopped
remote_syslog.reachable	Remote syslog destination reachable
remote_syslog.unreachable	Remote syslog destination not reachable
tls_channel.establish	TLS channel established
tls_channel.terminate	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

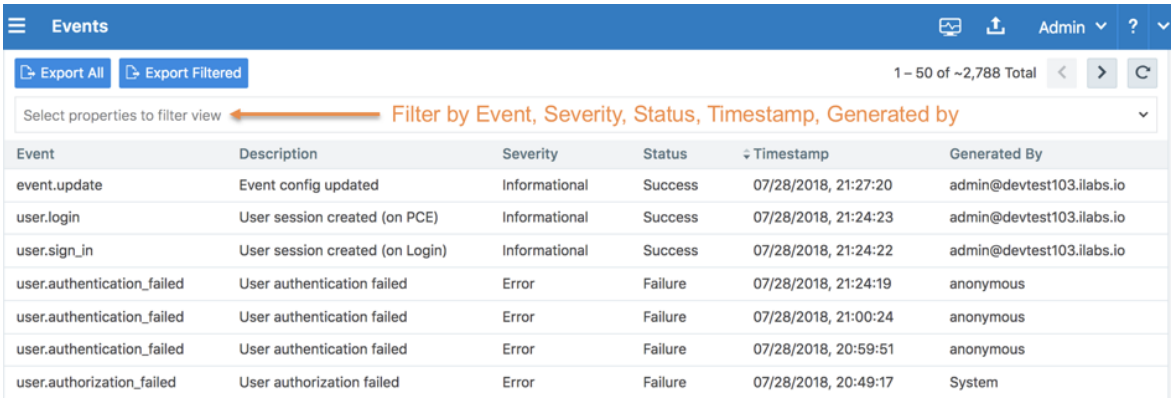
By default, the PCE web console shows events that occur in your organization, such as when a workload is paired, if a pairing failed, when a user logs in or logs out, when a user fails to authenticate, and so on.

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.



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`

VEN Events not shown in PCE Web Console	
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	

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

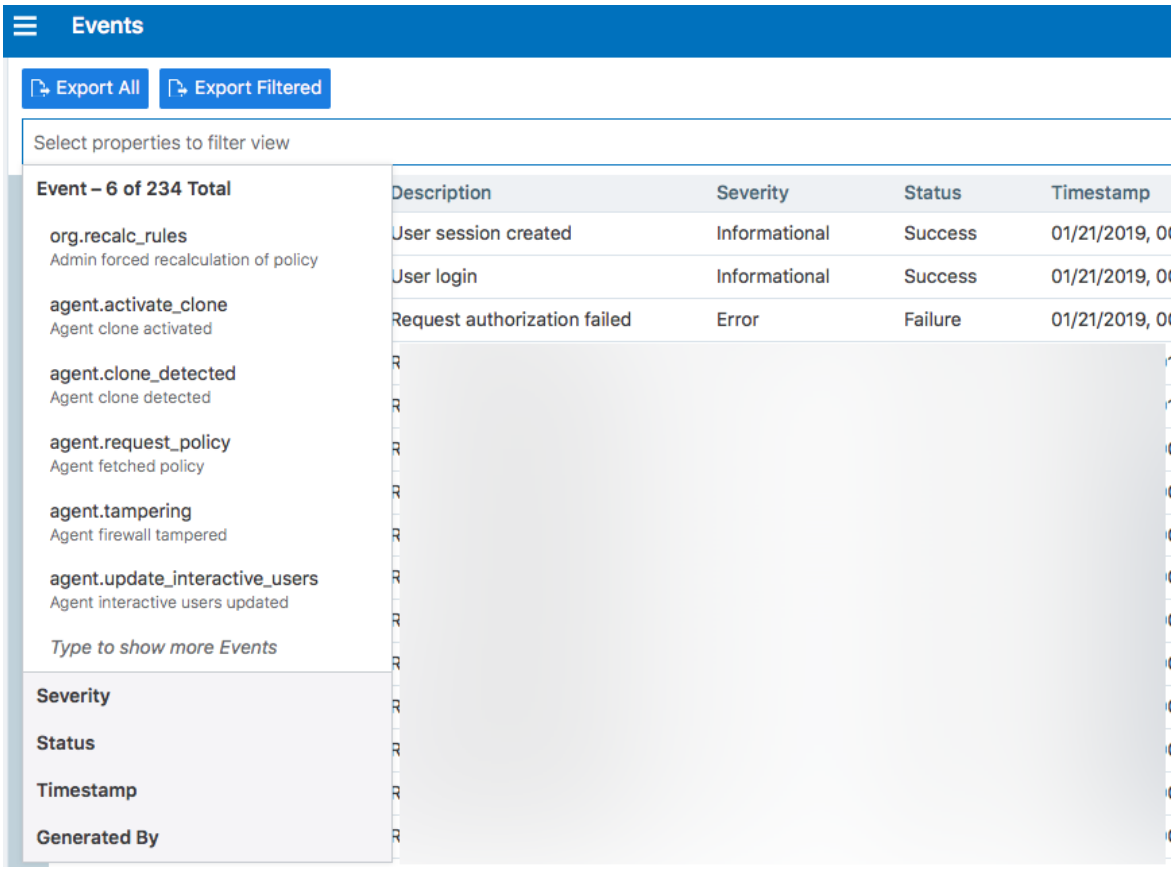
You can export all Organization events, or export a filtered list organization events to a CSV file.

To export events:

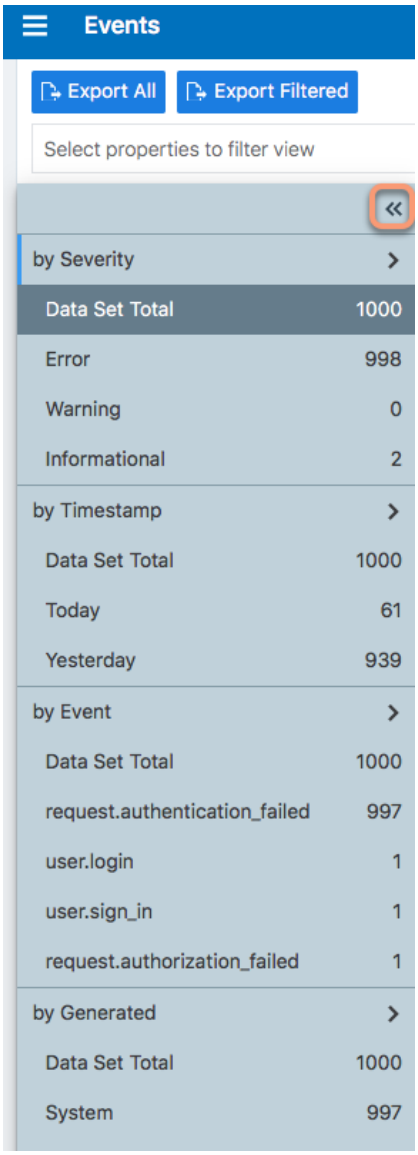
1. From the PCE web console menu, choose **Troubleshooting** > **Events**.

   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:



5. For a faster filtering via the browser, use the following field:



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/xxxxxxxx-39bd-43f1-a680-cc17c6984925",
        "timestamp": "2018-08-29T22:07:00.978Z",
        "pce_fqdn": "pce1.bigco.com",
        "created_by": {
               "system": {}
        },
        "event_type": "user.update_password",
        "status": "failure",
        "severity": "info",
        "action": {
               "uuid": "xxxxxxxx-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": "xxxxxxxx-7b8e-4205-a62a-1f070d8a0ee2",
               "notification_type": "user.pw_complexity_not_met",
               "info": null
        }, {
               "uuid": "xxxxxxxx-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/xxxxxxxx-8033-4f1a-83e9-fde57c425807",
"timestamp": "2018-08-29T22:04:04.733Z",
"pce_fqdn": "pce1.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":xxxxxxxxx,"mask_addr":someMask}},
"changes":{"address":{"before":null,"after":
{"family":2,"addr":xxxxxxxxx,"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 activation_failure	agent.activate
deactivation_success deactivation_failure	agent.deactivate

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 recommendations you monitor the following events at a minimum.

Events	Description
Program name = `Illumio_pce/system_health` Severity = Warning, Error, or Fatal	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. For more information about the metrics and thresholds, see the PCE Administration Guide.

Events	Description
	Recommendation: Monitor `system_health` messages with a severity of warning or higher and correlate the event with other operational monitoring tools to determine if administrative intervention is required.
`event_type="lost_agent.found"`	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. **Recommendation:** Monitor `lost_agent.found` events and send alerts in case you need to pair the workloads' VENs with the PCE again.
`event_type="system_task.agent_missed_heartbeats_check"`	Lists the VENs that missed three heartbeats (usually 15 minutes). Typically, this event precedes the PCE taking the VENs offline to perform internal maintenance. **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).
`event_type="system_task.agent_offline_check"`	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. **Recommendation:** Monitor these events for high-value workloads because they indicate change in the affected workloads' security posture.
`event_type-e="agent.suspend"`	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. **Recommendation:** Monitor these events for high-value workloads.
`event_type-e="agent.tampering"`	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.

Events	Description
	Recommendation: Monitor these events for high-value workloads.
`event_type-e="agent.update"`	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: • Processes not running • Policy deployment failure **Recommendation:** Monitor `agent.update` events that include notifications because they indicate workloads that might require administrative intervention.

`event_type="rule_set.create"`
`event_type="rule_set.update"`
`event_type="rule_sets.delete”`
	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.
	Recommendation: Monitor these events to pinpoint ruleset scopes that are unintentionally overly broad.

`event_type="sec_rule.create"`
`event_type="sec_rule.update"`
`event_type="sec_rule.delete"`
	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.
	Recommendation: Monitor these events for high-value labels.

`event_type="sec_policy.create"`	**[NEW in Illumio Core 19.3.0]** Contains the `workloads_affected` 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.

Events	Description
	Recommendation: Monitor the `workloads_affected` field for a high number of affect workloads. If the number exceeds an acceptable threshold, investigate the associated the policy.
`event_type-e="agent.clone_detec-ted"`	The PCE detects cloned VENs based on clone token mis-match. 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. **Recommendation:** If severity is 1 or 'error', some intervention may be needed.

Chapter 3

Events Setup

This chapter contains the following topics:

This chapter 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 information about the default events data retention period, database dumps with and without events data, disk compacting, and more, see Manage Data and Disk Capacity in the *PCE Administration Guide* in the Illumio Core.

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
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 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, for example 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	• If the organization's record retention is more than	As per your

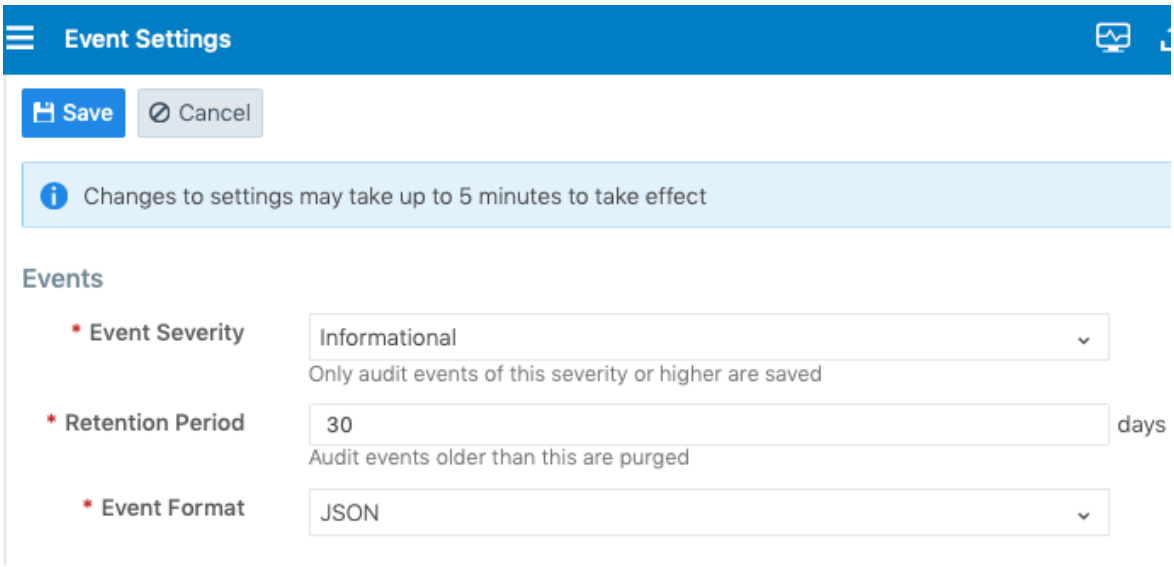
SIEM	Consideration	Value
	30 days • If disk monitoring is not set up, it is required to set up disk monitoring	record retention policy 200 days (maximum)
Not applicable	If events data is not needed for reporting or troubleshooting	1 day (minimum)

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. For more details, see "PCE Default Object Limits" in the *PCE Administration Guide*.

- 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 Micro Focus ArcSight®.
- Log Event Extended Format (LEEF), needed for IBM QRadar®.

Illumio Tools for SIEM Integration

Illumio offers other tools for SIEM integration.

Illumio App for Splunk:

- Software: Technical Add-on for Illumio and Illumio App for Splunk
- Documentation: Illumio App for Splunk Guide 3.2.0

Illumio App for ServiceNow:

- Software: Illumio App for CMDB
- Documentation: Illumio App for ServiceNow 1.4.0

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/'
```

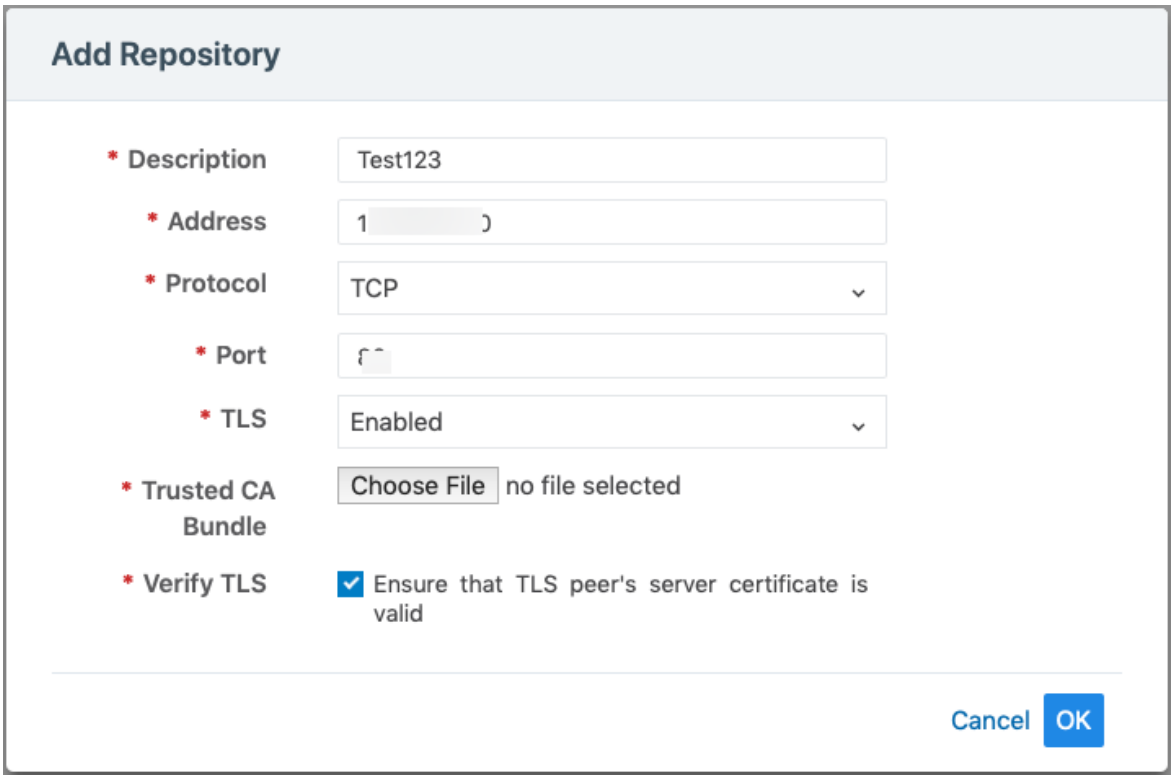
Forward Events to External Syslog Server

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**.



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

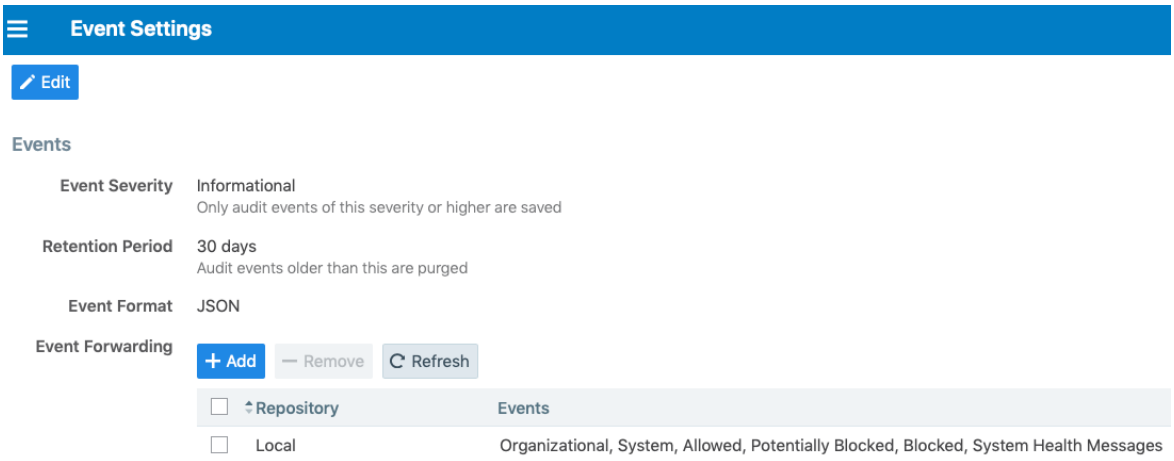
PCE system health messages are useful for PCE operations and monitoring. You can choose to forward them if they are needed on the remote destination.

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.

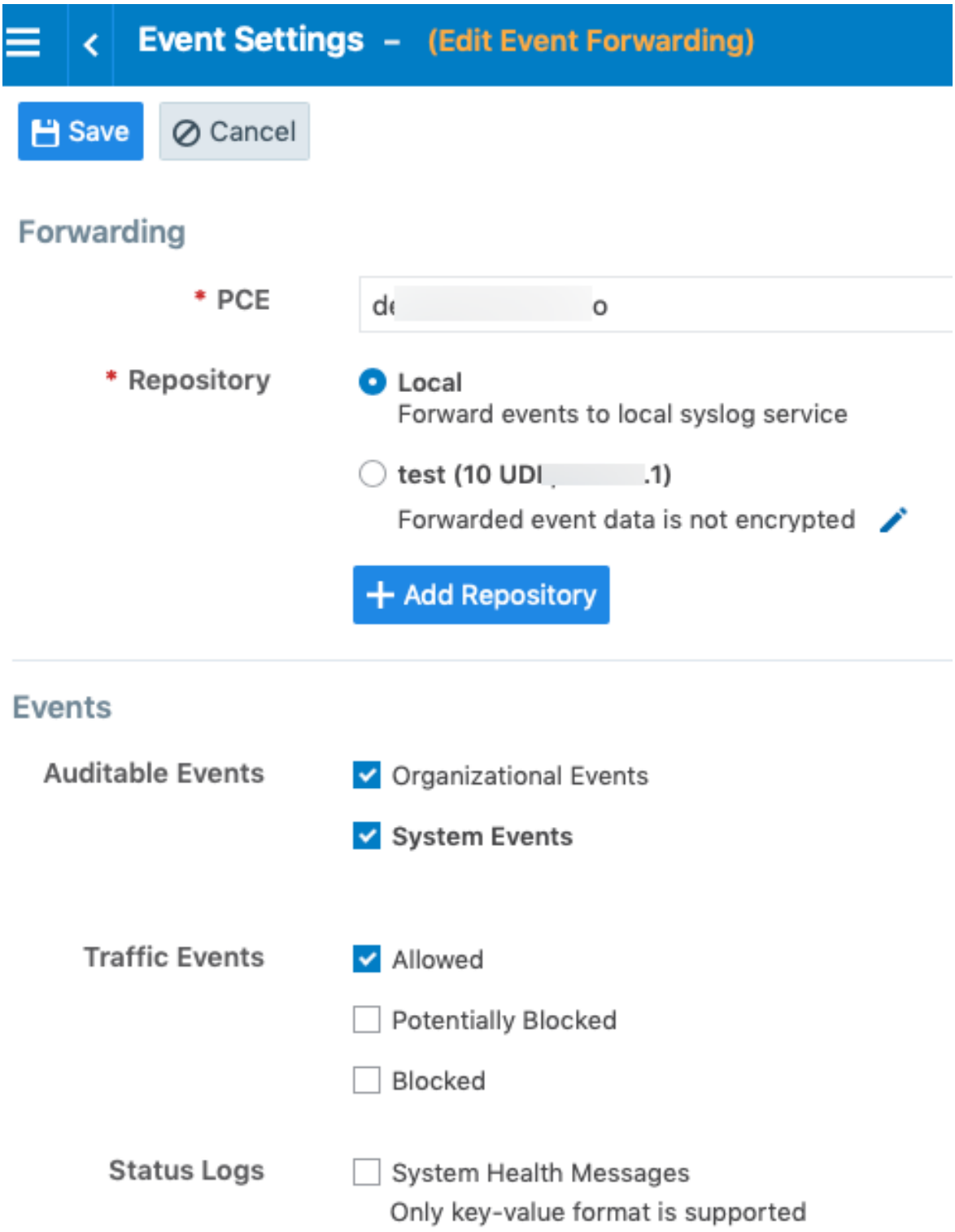
The PCE system health messages are only provided in key/value syslog format. They are not translatable into CEF, LEEF, or JSON formats. If your SIEM does not support processing key/value messages in syslog format, do not forward system health messages to those SIEMs. For example, IBM QRadar and Micro 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.



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
* 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.

Chapter 4

Traffic Flow Summaries

This chapter contains the following topics:

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 workload policy state. Events have attributes that can be allowed, potentially blocked, or blocked and might not appear in the traffic flow summary.

Workload Policy State

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.

Workload Policy State	Logged in Traffic Flow Summary
Build	All traffic logged and categorized as Allowed
Test	All traffic logged and categorized as Allowed or Potentially Blocked
Enforced - Low Detail	Only Blocked traffic logged
Enforced - High Detail	All traffic logged and categorized as Allowed and Blocked traffic
Enforced - No Detail	Nothing logged

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`	✓	✓	✓	✓
`interval_sec`	✓	✓	✓	✓
`timestamp`	✓	✓	✓	✓
`dir`	✓	✓	✓	✓
`src_ip`	✓	✓	✓	✓
`dst_ip`	✓	✓	✓	✓
`proto`	✓	✓	✓	✓
`dst_prt`	✓	✓	✓	✓
`state`	✓	✓	✓	✓
`pd`	✓	✓	✓	✓
`code*`	✓	✓	✓	✓

Event Attributes	Allowed (pd=0)	Potentially Blocked (pd=1)	Blocked (pd=2)	Unknown (pd=3)
type*	✓	✓	✓	✓
dst_vulns*	✓	✓	✓	✓
fqdn*	✓	✓	✓	✓
un*	✓	✓	X	✓
pn*	✓	✓	X	✓
sn*	✓	✓	X	✓
src_labels*	✓	✓	✓	✓
dst_labels*	✓	✓	✓	✓
src_host-name*	✓	✓	✓	✓
dst_host-name*	✓	✓	✓	✓
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 (`dst_tbo`): Number of bytes transferred out of provider.

Destination Total Bytes In (`dst_tbi`): Number of bytes transferred in to provider.

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	Required	Possible Values
`version`	Version of the flow summary schema.	Integer	Yes	4
`timestamp`	Indicates the time (RFC3339) when the first flow in the summary was created, represented in UTC. Format: `yyyy-MM-dd'T'HH:mm:ss.SSSSSSZ`	String	Yes	
`interval_sec`	Sample duration for the flows in the summary. Default is approx-	Integer	Yes	

Property	Description	Type	Required	Possible Values
	imately 600 seconds (10 minutes), depending on the VEN's ability to report traffic and PCE's current load.			
`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). 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. 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).	Integer	No	Minimum=0 Maximum=255

Property	Description	Type	Required	Possible Values
	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. Example: 1 for “Destination host unreachable.”			
`dst_port`	Destination port. This value exists only if protocol is not TCP (6) or UDP (17).	Integer	Yes	Minimum=0 Maximum=65535
`pd`	Policy decision value, which indicates if the flow was allowed, potentially blocked (but allowed), blocked, or unknown. Possible values: • 0 – Allowed traffic • 1 – Allowed traffic but will be blocked after policy enforcement • 2 – Blocked traffic • 3 - Unknown	Integer	Yes	Minimum=0 Maximum=3

Property	Description	Type	Required	Possible Values
	NOTE: Policy decision is "unknown" in the following cases: • Flows uploaded using existing bulk API (`/orgs/<org_id>/agents/bulk_traffic_flows`). • Flows uploaded using Network Flow Ingest Application (`/orgs/<org_id>/traffic_data`). • Traffic reported by idle VENs and specifically those that have been reported with "s" state (snapshot).			
`count`	Count of the number of flows in the flow summary.	Integer	Yes	
`state`	Session state for the traffic flows in the flow summaries. Possible values: • **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.	String	No	A, C, T, S, N

Property	Description	Type	Required	Possible Values
	• **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.			
pn	Program name associated with the first flow in the summary. It is supported on inbound flows for Linux and Windows VEN and on outbound flows for only Windows VEN. This information might not be available on short-lived processes. Currently flows are aggregated, so this value might represent only the first process that was	String	No	

Property	Description	Type	Required	Possible Values
	detected across all aggregated flows.			
un	User name associated with the first flow in the summary. It is supported on inbound flows for Linux and Windows VEN and on outbound flows for only Linux VEN. On Windows, it can include the username of the user account that initiated the connection. NOTE: This information might not be available on short-lived processes.	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	

Property	Description	Type	Required	Possible Values
	NOTE: The `src_hostname`, `src_href`, and `src_labels` values are not be 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.			
`dst_hostname`	Hostname of the destination workload that reported the flow.	String	No	
`dst_href`	HREF of the destination workload that reported the flow.	String	No	
`dst_labels`	Labels applied to the destination workload. NOTE: The `dst_hostname`, `dst_href`, and `dst_labels` 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.	Object	No	
dst_vulns	Information about the vulnerabilities on the destination of the traffic flow with the specific	Object	No	

Property	Description	Type	Required	Possible Values
	port and protocol. See Sub-properties for dst_vulns propertyfor information about the sub-properties. NOTE: • 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.			
`fqdn`	Fully qualified domain name	String	No	

Sub-properties for `dst_vulns` property

Sub-property	Description	Type	Required
`count`	The total number of existing vulnerabilities on the destination port and protocol.	Integer	No
`max_score`	The maximum of all the scores for the vul-	Number	No

Sub-property	Description	Type	Required
	nerabilities on the destination port and protocol.		
`cve_ids`	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

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 dbo (delta bytes out) / delta_duration_ms, or dbi / 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 tbo (total bytes out) / total_duration_ms, or tbo / total_duration_ms. It also enables you to calculate the average volume of data in a connection between two applications. The formula is tbo (total bytes out) / count (number of flows in an aggregate), or tbi / 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-
35a1abe45838","dst_labels":
```

{"app":"AppName","env":"Development","loc":"Cloud2","role":"Web"},"dst_hostname":"dev-ubuntu-1","dst_href":"/orgs/1/workloads/773f3e81-5779-4753-b879-35a1abe45838","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":"corp-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_hostname":"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/a20eb1b5-10a4-419e-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 cn1=120 cn1Label=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 cn1=31 cn1Label=interval_sec cs2=S cs2Label=state
```

```
dhost=workload1 cs6=/orgs/1/workloads/a20eb1b5-10a4-419e-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
```