

Events Administration and REST APIs

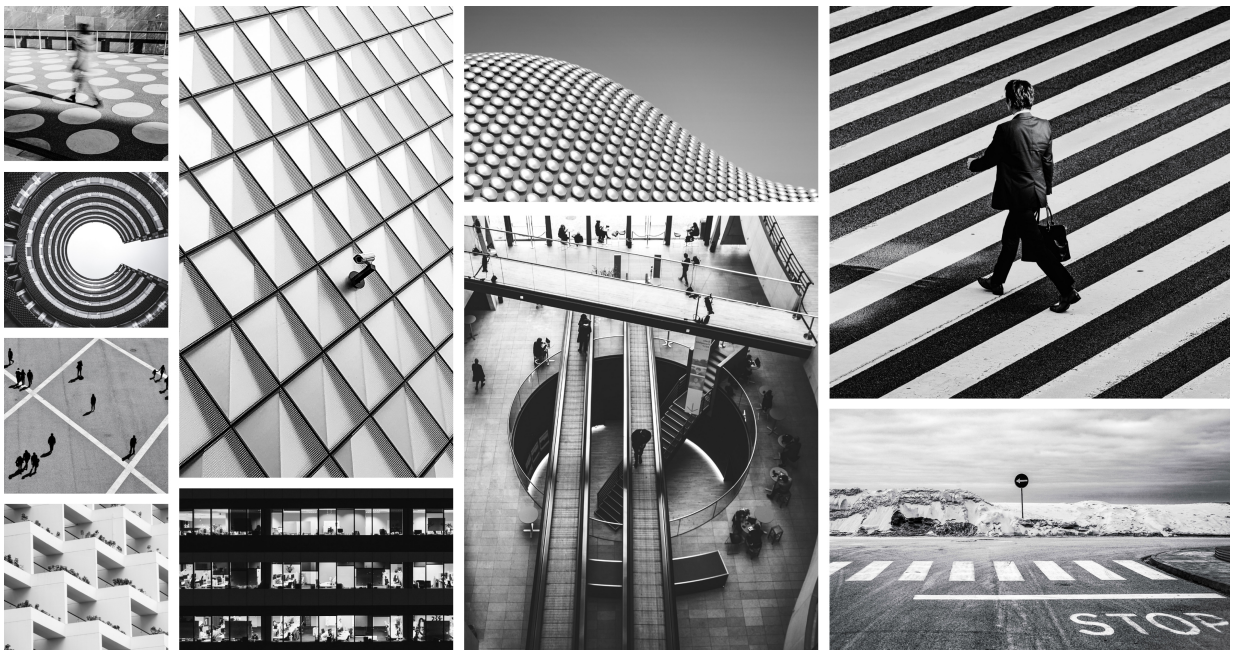


Table of Contents

Overview of Events Administration	4
Before You Begin	4
About This Guide	4
Notational Conventions in This Guide	4
Events Framework	5
Overview of the Framework	5
Auditing Needs Satisfied by Framework	5
Benefits of Events Framework	6
Events Lifecycle for Resources	6
About the Lifecycle	6
Other Resource Lifecycles	7
Events Described	8
Event Types, Syntax, and Record Format	8
Types of Events	8
Anonymized Database Dumps	8
REST API Events Schema	8
Event Syntax	8
Events Record Information	9
Event Record Structure	9
Events Displayed in PCE Web Console	10
Cross-Site Request Forgery Protection	10
List of Event Types	11
Notification Messages in Events	21
Common Criteria Only Events	22
View and Export Events	23
View Events in PCE Web Console	23
View Events Using PCE Command Line	24
Export Events Using PCE Web Console	25
Examples of Events	26
User Password Update Failed (JSON)	27
Resource Updated (JSON)	27
Security Rule Created (JSON)	29
User Logged In (JSON)	30
User Logged Out (JSON)	32
Login Failed — Incorrect Username (JSON)	33
Login Failed — Incorrect Password (JSON)	34
User Log Out (CEF)	35
Workload Security Policy Updated (LEEF)	35
Differences from Previous Releases	36
Changed VEN Event Names	36
Events Monitoring Best Practices	36
Monitoring Operational Practices	37
Recommended Events to Monitor	37
Events Setup	40
Requirements for Events Framework	40
Database Sizing for Events	40
Data and Disk Capacity for Events	40
Events Preview Runtime Setting	40
Events Settings	41
Events Are Always Enabled	41
Event Settings in PCE Web Console	41
Configure Events Settings in PCE Web Console	43
SIEM Integration for Events	45

About SIEM Integration	45
.....	45
Syslog Forwarding	45
Identify Events in Syslog Stream	45
Forward Events to External Syslog Server	45
Disable Health Check Forwarding	46
Traffic Flow Summaries	49
Traffic Flow Types and Properties	49
Visibility Settings	49
Event Types	49
Show Amount of Data Transfer	51
Manage Traffic Flows Using REST API	51
Export Traffic Flow Summaries	56
Export to Syslog	57
Export to Fluentd	58
Flow Duration Attributes	58
Traffic Flow Summary Examples	58
JSON	58
Syslog	59
CEF	61
LEEF	61

Overview of Events Administration

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

Before You Begin

Illumio recommends that you be familiar with the following technology:

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

About This Guide

This guide provides the following information to administer your PCE deployment:

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

See also the following related documentation:

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

Notational Conventions in This Guide

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

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

Events Framework

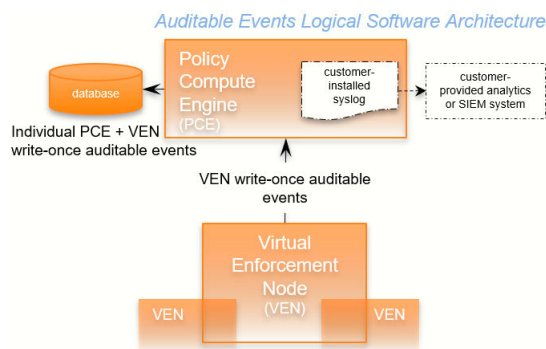
The Illumio events framework provides an information-rich, deep foundation for actionable insights into the operations of Illumio Core.

Overview of the Framework

Auditable events are records of transactions collected from the following management interfaces:

- PCE web console
- REST API
- PCE command-line tools
- VEN command-line tools

All actions that change the configuration of the PCE, security policy, and the VENs are recorded, including workload firewall tampering.



As required by auditing standards, every recorded change includes a reference to the program that made the change, the change's timestamp, and other fields. After recording, the auditable events are read-only.

Auditable events comply with the [Common Criteria Class FAU Security Audit requirements](#) standard for auditing.

Auditing Needs Satisfied by Framework

Need	Description	See topic...
Audit and Compliance	Evidence to show that resources are managed according to rules and regulatory standards.	Events Record Information [9]
Resource Lifecycle Tracking	All information necessary to track a resource through creation, modification, and deletion.	Events Lifecycle for Resources [6]
Operations	Trace of recent changes to resources.	Events Lifecycle for Resources [6]

Need	Description	See topic...
Security	Evidence to show which changes failed, such as incorrect user permissions or failed authentication.	User Password Update Failed (JSON) [27]

Benefits of Events Framework

The events framework in the Illumio Core provides the following benefits:

- Exceeds industry standards
- Delivers complete content
 - Comprehensive set of event types
 - Includes more than 200 events
 - Additional notable system events are generated
- Easily accessible interfaces to capture events:
 - Event Viewer in the PCE web console
 - REST API with filtering
 - SIEM integration
 - Events are the same across all interfaces
- Designed for customer ease of use
 - Flattened, common structure for all events
 - Eliminates former duplicate or multiple events for single actions
 - Streamed via syslog in JSON, CEF, or LEEF format
 - Create/Update/Delete REST APIs recorded as events
 - Read APIs/GET requests are not recorded, because they do not change the Illumio Core.

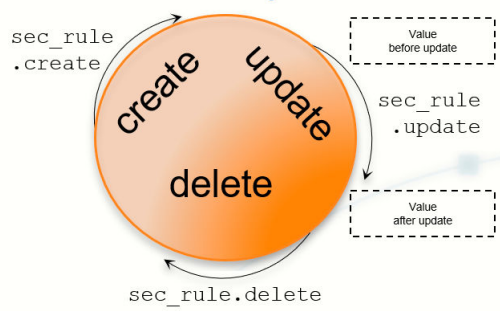
Events Lifecycle for Resources

Illumio resources progress through the lifecycle stages (creation, updating, deletion) and Illumio Core records them with the appropriate event types.

About the Lifecycle

Many resources have a lifecycle from creation through update to deletion. For example, the events related to a security policy rule (identified by the resource name `sec_rule`) are recorded with the following event types.

- `sec_rule.create`
- `sec_rule.update`: Update events record with the values of the resource object both before and after the event for a lifecycle audit trail.
- `sec_rule.delete`

Auditable Events: Lifecycle of a Resource**Other Resource Lifecycles**

Some resources have unique characteristics and do not follow the create-update-delete pattern. For example, workloads have the following event types:

- `workload.update`
- `workload.upgrade`
- `workload.redetect_network`
- `workload.recalc_rules`
- `workload.soft_delete`
- `workload.delete`
- `workload.undelete`

Events Described

This section describes the concepts and types of PCE events.

Event Types, Syntax, and Record Format

When working with events, it is important to recognize their type, REST API schema, syntax, and record information.

Types of Events

The Illumio Core includes the following general categories of auditable events:

- Organizational events: Organizational events are further grouped by their source:
 - API-related events: Events occurring from a use of the REST API, including the PCE web console
 - System-related events: Events caused by some system-related occurrence
- Traffic events

Anonymized Database Dumps

To troubleshoot customer-reported issues, Illumio Customer Support sometimes requests that you supply an anonymized dump of the PCE database.

To safeguard your organization's privacy, the event information is not included in the anonymized database dump.

REST API Events Schema

The Events schema in JSON is downloadable from this documentation portal in the zipfile of the REST API schemas. From the documentation portal Home page, go to the **Develop** category > **REST API Public Schemas (Archive File)**.

Event Syntax

The names of recorded auditable events in have the following general syntax:

```
resource.verb[.success_or_failure]
```

Where:

- **resource** is a PCE and VEN object, such as PCE `user` or VEN `agent` component.
- **verb** describes the action of the event on that resource.

- In CEF and LEEF formats, the success or failure of the verb is included in the recorded event type. This indicator is not needed in the JSON format.

Events Record Information

The following information is included in a event record, which answers the who, what, where, how, and when:

Type of information	Description
Who	<ul style="list-style-type: none"> • VEN identified by hostname and agent href, and after Release 22.3, VEN href • User identified by username and href • PCE system identified by "system"
What	<p>The action that triggered the event, including the following data:</p> <ul style="list-style-type: none"> • Resource type + operation + success or failure • Application Request ID • Status of successful events and failed events: <ul style="list-style-type: none"> • In case of failure, exception type and exception message. • All failures related to security, such as authentication and authorization. • Severity as INFO, WARNING, ERROR. • The pre-change and post-change values of the affected resources.
Where	<p>The target resource of the action, composed of the following data:</p> <ul style="list-style-type: none"> • Identifier of the target resource (primary field). • Friendly name for the target resource. For example: <ul style="list-style-type: none"> • workload/VEN: <code>hostname</code> • user: <code>username</code> • ruleset, label, service, etc: <code>name, key/value</code>
How	API endpoint, method, HTTP status code, and source IP address of the request.
When	Timestamp of the event's occurrence. This timestamp is <i>not</i> the time the event was recorded.

Event Record Structure

Regardless of export format (JSON, CEF, or LEEF), the records and fields for all events share a common structure. This common structure of composite events makes post-processing of event data easier.

Bulk change operations on many resources simultaneously are recorded as individual operations on the resource within a single composite event. Failed attempts to change a configuration, such as incorrect authentication, are also collected.

Common Fields

Field Name	Description
<code>href</code>	Unique event identifier; contains a UUID.
<code>timestamp</code>	Exact time that the event occurred in RFC 3339 format with fractional seconds.
<code>pce_fqdn</code>	The fully qualified domain name of the PCE; especially useful for Supercluster deployments or if there are multiple PCEs sending data to the SIEM server.
<code>created_by</code>	Identifies creator of the event; could be a user, the system, or a workload.
<code>event_type</code>	Name of the event; for more information, see the List of Event Types [1] table.
<code>status</code>	“Success” or “failure;” if the status is null, the event is for information only and doesn’t indicate success or failure.
<code>severity</code>	“Informational,” “warning,” or “error” indicating the severity of the event.
<code>version</code>	Schema version for events.

Events Displayed in PCE Web Console

The PCE web console provides an ongoing log of all Organization events that occur in the PCE. For example, Organization events capture actions such as users logging in and logging out, and failed login attempts; when a system object is created, modified, deleted, or provisioned; when a workload is paired or unpaired; and so on.

From the platform and API perspective, Organization events are referred to internally as `auditable_events` and are generated by the `auditable_events_service`.

You can use the filter at the top of the page to search for events by type of event, event severity level, and when the event occurred.

Cross-Site Request Forgery Protection

A cross-site request forgery (CSRF) is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is an application functionality using predictable URL or form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a website has for a user.

For more details on this attack, see the [CSRF article](#) on the Web Application Security Consortium website.

Illumio Core can notify you of this type of attack in the following ways:

- The PCE web console logs the attack as an Organization Event called “CSRF token validation failure.”

- The event is logged in the Illumio Core REST API as `authz_csrf_validation_failure` in the `audit_log_events_get.schema`.
- The event `authz_csrf_validation_failure` appears in the PCE syslog output if you have deployed the PCE as a software.



IMPORTANT

When you see this event occur, you should immediately investigate the issue because the request might not have originated from a valid user.

List of Event Types

The following table provides the types of JSON events generated and their description. For each of these events, the CEF/LEEF success or failure events generated are the event name followed by `.success` or `.failure`.

For example, the CEF/LEEF success event for `agent.activate` is `agent.activate.success` and the failure event is `agent.activate.failure`.

Each event can generate a variety of notification messages. See [Notification Messages in Events \[21\]](#).

JSON Event Type	Description
<code>access_restriction.create</code>	Access restriction created
<code>access_restriction.delete</code>	Access restriction deleted
<code>access_restriction.update</code>	Access restriction updated
<code>agent.activate</code>	Agent paired
<code>agent.activate_clone</code>	Agent clone activated
<code>agent.clone_detected</code>	Agent clone detected
<code>agent.deactivate</code>	Agent unpaired
<code>agent.generate_maintenance_token</code>	Generate maintenance token for any agent
<code>agent.goodbye</code>	Agent disconnected
<code>agent.machine_identifier</code>	Agent machine identifiers updated
<code>agent.refresh_token</code>	Agent refreshed token
<code>agent.request_policy</code>	Policy request sent
<code>agent.request_upgrade</code>	VEN upgrade request sent

JSON Event Type	Description
<code>agent.service_not_available</code>	Agent reported a service not running
<code>agent.suspend</code>	Agent suspended
<code>agent.tampering</code>	Agent firewall tampered
<code>agent.unsuspend</code>	Agent unsuspended
<code>agent.update</code>	Agent properties updated.
<code>agent.update_interactive_users</code>	Agent interactive users updated
<code>agent.update_iptables_href</code>	Agent updated existing iptables href
<code>agent.update_running_containers</code>	Agent updated existing containers
<code>agent.upload_existing_ip_table_rules</code>	Agent existing IP tables uploaded
<code>agent.upload_support_report</code>	Agent support report uploaded
<code>agent_support_report_request.create</code>	Agent support report request created
<code>agent_support_report_request.delete</code>	Agent support report request deleted
<code>agents.clear_conditions</code>	Condition cleared from a list of VENS
<code>agents.unpair</code>	Multiple agents unpaired
<code>api_key.create</code>	API key created
<code>api_key.delete</code>	API key deleted
<code>api_key.update</code>	API key updated
<code>auth_security_principal.create</code>	RBAC auth security principal created
<code>auth_security_principal.delete</code>	RBAC auth security principal deleted
<code>auth_security_principal.update</code>	RBAC auth security principal updated
<code>authentication_settings.update</code>	Authentication settings updated
<code>cluster.create</code>	PCE cluster created
<code>cluster.delete</code>	PCE cluster deleted
<code>cluster.update</code>	PCE cluster updated
<code>container_workload.update</code>	Container workload updated
<code>container_cluster.create</code>	Container cluster created
<code>container_cluster.delete</code>	Container cluster deleted
<code>container_cluster.update</code>	Container cluster updated

JSON Event Type	Description
<code>container_cluster.update_label_map</code>	Container cluster label mappings updated all at once
<code>container_cluster.update_services</code>	Container cluster services updated, created, or deleted by Kubelink
<code>container_workload_profile.create</code>	Container workload profile created
<code>container_workload_profile.delete</code>	Container workload profile deleted
<code>container_workload_profile.update</code>	Container workload profile updated
<code>database.temp_table_autocleanup_started</code>	DB temp table cleanup started
<code>database.temp_table_autocleanup_completed</code>	DB temp table cleanup completed
<code>domain.create</code>	Domain created
<code>domain.delete</code>	Domain deleted
<code>domain.update</code>	Domain updated
<code>enforcement_boundary.create</code>	Enforcement boundary created
<code>enforcement_boundary.delete</code>	Enforcement boundary deleted
<code>enforcement_boundary.update</code>	Enforcement boundary updated
<code>event_settings.update</code>	Event settings updated
<code>firewall_settings.update</code>	Global policy settings updated
<code>group.create</code>	Group created
<code>group.update</code>	Group updated
<code>ip_list.create</code>	IP list created
<code>ip_list.delete</code>	IP list deleted
<code>ip_list.update</code>	IP list updated
<code>ip_lists.delete</code>	IP lists deleted
<code>ip_tables_rule.create</code>	IP tables rules created
<code>ip_tables_rule.delete</code>	IP tables rules deleted
<code>ip_tables_rule.update</code>	IP tables rules updated
<code>job.delete</code>	Job deleted
<code>label.create</code>	Label created
<code>label.delete</code>	Label deleted

JSON Event Type	Description
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
login_proxy_msp_tenants.create	New MSP tenant created
login_proxy_msp_tenants.delete	MSP tenant deleted
login_proxy_msp_tenants.update	MSP tenant updated
login_proxy_orgs.create	New managed organization created
login_proxy_orgs.delete	Managed organization deleted
login_proxy_orgs.update	Managed organization updated
lost_agent.found	Lost agent found
network.create	Network created
network.delete	Network deleted
network.update	Network updated
network_device.ack_enforcement_instructions_applied	Enforcement instruction applied to a network device
network_device.assign_workload	Existing or new unmanaged workload assigned to a network device

JSON Event Type	Description
<code>network_device.create</code>	Network device created
<code>network_device.delete</code>	Network device deleted
<code>network_device.update</code>	Network device updated
<code>network_devices.ack_multi_enforcement_instructions_applied</code>	Enforcement instructions applied to multiple network devices
<code>network_endpoint.create</code>	Network endpoint created
<code>network_endpoint.delete</code>	Network endpoint deleted
<code>network_endpoint.update</code>	Network endpoint updated
<code>network_enforcement_node.activate</code>	Network enforcement node activated
<code>network_enforcement_node.clear_conditions</code>	Network enforcement node conditions cleared
<code>network_enforcement_node.deactivate</code>	Network enforcement node deactivated
<code>network_enforcement_node.degraded</code>	Network enforcement node failed or primary lost connectivity to secondary
<code>network_enforcement_node.missed_heartbeats</code>	Network enforcement node did not heartbeat for more than 15 minutes
<code>network_enforcement_node.missed_heartbeats_check</code>	Network enforcement node missed heartbeats check
<code>network_enforcement_node.network_devices_network_endpoints_workloads</code>	Workload added to network endpoint
<code>network_enforcement_node.policy_ack</code>	Network enforcement node acknowledgment of policy
<code>network_enforcement_node.request_policy</code>	Network enforcement node policy requested
<code>network_enforcement_node.update_status</code>	Network enforcement node reports when switches are not reachable
<code>network_enforcement_nodes.clear_conditions</code>	A condition was cleared from a list of network enforcement nodes
<code>nfc.activate</code>	Network function controller created
<code>nfc.delete</code>	Network function controller deleted
<code>nfc.update_discovered_virtual_servers</code>	Network function controller virtual servers discovered
<code>nfc.update_policy_status</code>	Network function controller policy status
<code>nfc.update_slb_state</code>	Network function controller SLB state updated
<code>org.create</code>	Organization created
<code>org.recalc_rules</code>	Rules for organization recalculated

JSON Event Type	Description
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
radius_config.create	Create domain RADIUS configuration
radius_config.delete	Delete domain RADIUS configuration
radius_config.update	Update domain RADIUS configuration
radius_config.verify_shared_secret	Verify RADIUS shared secret
request.authentication_failed	API request authentication failed
request.authorization_failed	API request authorization failed
request.internal_server_error	API request failed due to internal server error
request.service_unavailable	API request failed due to unavailable service
request.unknown_server_error	API request failed due to unknown server error
resource.create	Login resource created
resource.delete	Login resource deleted
resource.update	Login resource updated
rule_set.create	Rule set created
rule_set.delete	Rule set deleted
rule_set.update	Rule set updated

JSON Event Type	Description
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.pce_signing_cert	Generate a new cert for signing SAML AuthN requests
saml_config.update	SAML configuration updated
saml_sp_config.create	SAML Service Provider created
saml_sp_config.delete	SAML Service Provider deleted
saml_sp_config.update	SAML Service Provider updated
sec_policy.create	Security policy created
sec_policy_pending.delete	Pending security policy deleted
sec_policy.restore	Security policy restored
sec_rule.create	Security policy rules created
sec_rule.delete	Security policy rules deleted
sec_rule.update	Security policy rules updated
secure_connect_gateway.create	SecureConnect gateway created
secure_connect_gateway.delete	SecureConnect gateway deleted
secure_connect_gateway.update	SecureConnect gateway updated
security_principal.create	RBAC security principal created
security_principal.delete	RBAC security principal bulk deleted
security_principal.update	RBAC security principal bulk updated
security_principals.bulk_create	RBAC security principals bulk created
service.create	Service created
service.delete	Service deleted
service.update	Service updated
service_account.create	Service account created
service_account.delete	Service account deleted
service_account.update	Service account updated

JSON Event Type	Description
<code>service_binding.create</code>	Service binding created
<code>service_binding.delete</code>	Service binding created
<code>service_bindings.delete</code>	Service bindings deleted
<code>service_bindings.delete</code>	Service binding deleted
<code>services.delete</code>	Services deleted
<code>settings.update</code>	Explorer settings updated
<code>slb.create</code>	Server load balancer created
<code>slb.delete</code>	Server load balancer deleted
<code>slb.update</code>	Server load balancer updated
<code>support_report.upload</code>	Support report uploaded
<code>syslog_destination.create</code>	syslog remote destination created
<code>syslog_destination.delete</code>	syslog remote destination deleted
<code>syslog_destination.update</code>	syslog remote destination updated
<code>system_task.agent_missed_heartbeats_check</code>	Agent missed heartbeats
<code>system_task.agent_missing_heartbeats_after_upgrade</code>	VEN missing heartbeat after upgrade
<code>system_task.agent_offline_check</code>	Agents marked offline
<code>system_task.agent_self_signed_certs_check</code>	VEN self signed certificate housekeeping check
<code>system_task.agent_settings_invalidation_error_state_check</code>	VEN settings invalidation error state check
<code>system_task.agent_uninstall_timeout</code>	VEN uninstall timeout
<code>system_task.clear_auth_recover_condition</code>	Clear VEN authentication recovery condition
<code>system_task.compute_policy_for_unmanaged_workloads</code>	Compute policy for unmanaged workloads
<code>system_task.delete_expired_service_account_api_keys</code>	An expired service account api_key was successfully deleted
<code>system_task.delete_old_cached_perspectives</code>	Delete old cached perspectives
<code>system_task.endpoint_offline_check</code>	Endpoint marked offline
<code>system_task.provision_container_cluster_services</code>	Container cluster services provisioned

JSON Event Type	Description
<code>system_task.prune_old_log_events</code>	Event pruning completed
<code>system_task.remove_stale_zone_subsets</code>	Stale zone subnets removed
<code>system_task.set_server_sync_check</code>	Set server synced
<code>system_task.vacuum_deactivated_agent_and_deleted_workloads</code>	Deactivated and deleted workloads have been vacuumed
<code>traffic_collector_setting.create</code>	Traffic collector setting created
<code>traffic_collector_setting.delete</code>	Traffic collector setting deleted
<code>traffic_collector_setting.update</code>	Traffic collector setting updated
<code>trusted_proxy_ips.update</code>	Trusted proxy IPs created or updated
<code>user.accept_invitation</code>	User invitation accepted
<code>user.authenticate</code>	User authenticated
<code>user.create</code>	User created
<code>user.delete</code>	User deleted
<code>user.invite</code>	User invited
<code>user.login</code>	User logged in
<code>user.login_session_terminated</code>	User login session terminated
<code>user.logout</code>	User logged
<code>user.pce_session_terminated</code>	User session terminated
<code>user.reset_password</code>	User password reset
<code>user.sign_in</code>	User session created
<code>user.sign_out</code>	User session terminated
<code>user.update</code>	User information updated
<code>user.update_password</code>	User password updated
<code>user.use_expired_password</code>	User entered expired password
<code>user.verify_mfa</code>	User verified MFA
<code>users.auth_token</code>	Auth token returned for user authentication on PCE
<code>user_local_profile.create</code>	User local profile created
<code>user_local_profile.delete</code>	User local profile deleted
<code>user_local_profile.reinvite</code>	User local profile reinvited

JSON Event Type	Description
<code>user_local_profile.update_password</code>	User local password updated
<code>ven_settings.update</code>	VEN settings updated
<code>ven_software.upgrade</code>	VEN software release upgraded
<code>ven_software_release.create</code>	VEN software release created
<code>ven_software_release.delete</code>	VEN software release deleted
<code>ven_software_release.deploy</code>	VEN software release deployed
<code>ven_software_release.update</code>	VEN software release updated
<code>ven_software_releases.set_default_version</code>	Default VEN software version set
<code>virtual_server.create</code>	Virtual server created
<code>virtual_server.delete</code>	Virtual server created
<code>virtual_server.update</code>	Virtual server updated
<code>virtual_service.create</code>	Virtual service created
<code>virtual_service.delete</code>	Virtual service deleted
<code>virtual_service.update</code>	Virtual service updated
<code>virtual_services.bulk_create</code>	Virtual services created in bulk
<code>virtual_services.bulk_update</code>	Virtual services updated in bulk
<code>vulnerability.create</code>	Vulnerability record created
<code>vulnerability.delete</code>	Vulnerability record deleted
<code>vulnerability.update</code>	Vulnerability record updated
<code>vulnerability_report.delete</code>	Vulnerability report deleted
<code>vulnerability_report.update</code>	Vulnerability report updated
<code>workload.create</code>	Workload created
<code>workload.delete</code>	Workload deleted
<code>workload.online</code>	Workload online
<code>workload.recalc_rules</code>	Workload policy recalculated
<code>workload.redetect_network</code>	Workload network redetected
<code>workload.undelete</code>	Workload undeleted
<code>workload.update</code>	Workload settings updated

JSON Event Type	Description
<code>workload.upgrade</code>	Workload upgraded
<code>workload_interface.create</code>	Workload interface created
<code>workload_interface.delete</code>	Workload interface deleted
<code>workload_interface.update</code>	Workload interface updated
<code>workload_interfaces.update</code>	Workload interfaces updated
	For example, IP address changes, new interface added, and interface shut down.
<code>workload_service_report.update</code>	Workload service report updated
<code>workload_settings.update</code>	Workload settings updated
<code>workloads.apply_policy</code>	Workloads policies applied
<code>workloads.bulk_create</code>	Workloads created in bulk
<code>workloads.bulk_delete</code>	Workloads deleted in bulk
<code>workloads.bulk_update</code>	Workloads updated in bulk
<code>workloads.remove_labels</code>	Workloads labels removed
<code>workloads.set_flow_reporting_frequency</code>	Workload flow reporting frequency changed
<code>workloads.set_labels</code>	Workload labels applied
<code>workloads.unpair</code>	Workloads unpaired
<code>workloads.update</code>	Workloads updated

Notification Messages in Events

Events can generate a variety of notifications that are appended after the event type:

- `agent.clone_detected`
- `agent.fw_state_table_threshold_exceeded`
- `agent.missed_heartbeats`
- `agent.missing_heartbeats_after_upgrade`
- `agent.policy_deploy_failed`
- `agent.policy_deploy_succeeded`
- `agent.process_failed`
- `agent.service_not_available`
- `agent.upgrade_requested`
- `agent.upgrade_successful`
- `agent.upgrade_time_out`
- `container_cluster.duplicate_machine_id`
- `container_cluster.region_mismatch`

- `container_workload.invalid_pairing_config`
- `container_workload.not_created`
- `database.temp_table_autocleanup_completed`
- `database.temp_table_autocleanup_started`
- `hard_limit.exceeded`
- `pce.application_started`
- `pce.application_stopped`
- `remote_syslog.reachable`
- `remote_syslog.unreachable`
- `request.authentication_failed`
- `request.authorization_failed`
- `request.internal_server_error`
- `request.invalid`
- `request.service_unavailable`
- `request.unknown_server_error`
- `sec_policy.restore`
- `soft_limit.exceeded`
- `system_task.event_pruning_completed`
- `system_task.hard_limit_recovery_completed`
- `user.csrf_validation_failed`
- `user.login_failed`
- `user.login_failure_count_exceeded`
- `user.login_session_created`
- `user.login_session_terminated`
- `user.pce_session_created`
- `user.pce_session_terminated`
- `user.pw_change_failure`
- `user.pw_changed`
- `user.pw_complexity_not_met`
- `user.pw_reset_completed`
- `user.pw_reset_requested`
- `virtual_service.not_created`
- `workload.duplicate_interface_reported`
- `workload.nat_rules_present`
- `workload.offline_after_ven_goodbye`
- `workload.online`
- `workload.oob_policy_changes`
- `workload.partial_policy_delivered`
- `workload.update_mismatched_interfaces`
- `workloads.flow_reporting_frequency_updated`

Common Criteria Only Events

The following table lists the types of JSON events that are generated and their descriptions.

For each of these events, the CEF/LEEF success or failure events generated are the event name followed by `.success` or `.failure`.

For example, the CEF/LEEF success event for `agent.update` is `agent.update.success` and the failure event is `agent.update.failure`.

JSON Event Type	Description
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.

Event	Description	Severity	Status	Timestamp	Generated By
event.update	Event config updated	Informational	Success	07/28/2018, 21:27:20	admin@devtest103.ilabs.io
user.login	User session created (on PCE)	Informational	Success	07/28/2018, 21:24:23	admin@devtest103.ilabs.io
user.sign_in	User session created (on Login)	Informational	Success	07/28/2018, 21:24:22	admin@devtest103.ilabs.io
user.authentication_failed	User authentication failed	Error	Failure	07/28/2018, 21:24:19	anonymous
user.authentication_failed	User authentication failed	Error	Failure	07/28/2018, 21:00:24	anonymous
user.authentication_failed	User authentication failed	Error	Failure	07/28/2018, 20:59:51	anonymous
user.authorization_failed	User authorization failed	Error	Failure	07/28/2018, 20:49:17	System

**NOTE**

In the Events Viewer, the suggested values for the filters are generated from all possible values. For example, the “Generated By” filter shows all users on the system. However, the actual results displayed by that filter might not contain any data.

VEN Event Not Displayed in PCE Web Console

The following events related to VENs are not currently viewable in the PCE web console. This is a two-column list of event names.

VEN Events not shown in PCE Web Console	
fw_tampering_revert_failure	lost_agent
fw_tampering_reverted	missing_os_updates
fw_tampering_subsystem_failure	pce_incompat_api_version
invoke_powershell_failure	pce_incompat_version
ipsec_conn_state_change	pce_reachable
ipsec_conn_state_failure	pce_unreachable
ipsec_monitoring_failure	proc_config_failure
ipsec_monitoring_started	proc_envsetup_failure
ipsec_monitoring_stopped	proc_init_failure
ipsec_subsystem_failure	proc_malloc_failure
ipsec_subsystem_started	proc_restart_failure
ipsec_subsystem_stopped	proc_started
refresh_token_failure	proc_stopped
refresh_token_success	

VEN href Added to Events Information

After the 22.3.0 upgrade, all events created by a VEN includes the VEN href as well as the previously included Agent href. The VEN href can be used to query the VEN API, obtain the workload record, and execute various operations on the VEN from the PCE.

View Events Using PCE Command Line

Run this command at any runlevel to display:

- The total number of events
- The average number of events per day


```
$ sudo -u ilo-pce illumio-pce-db-management events-db events-db-show
```

Run this command at any runlevel to display:

- The amount of disk space used by events
- The total number of events

```
$ sudo -u ilo-pce illumio-pce-db-management events-db disk-usage-show
```

Export Events Using PCE Web Console

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

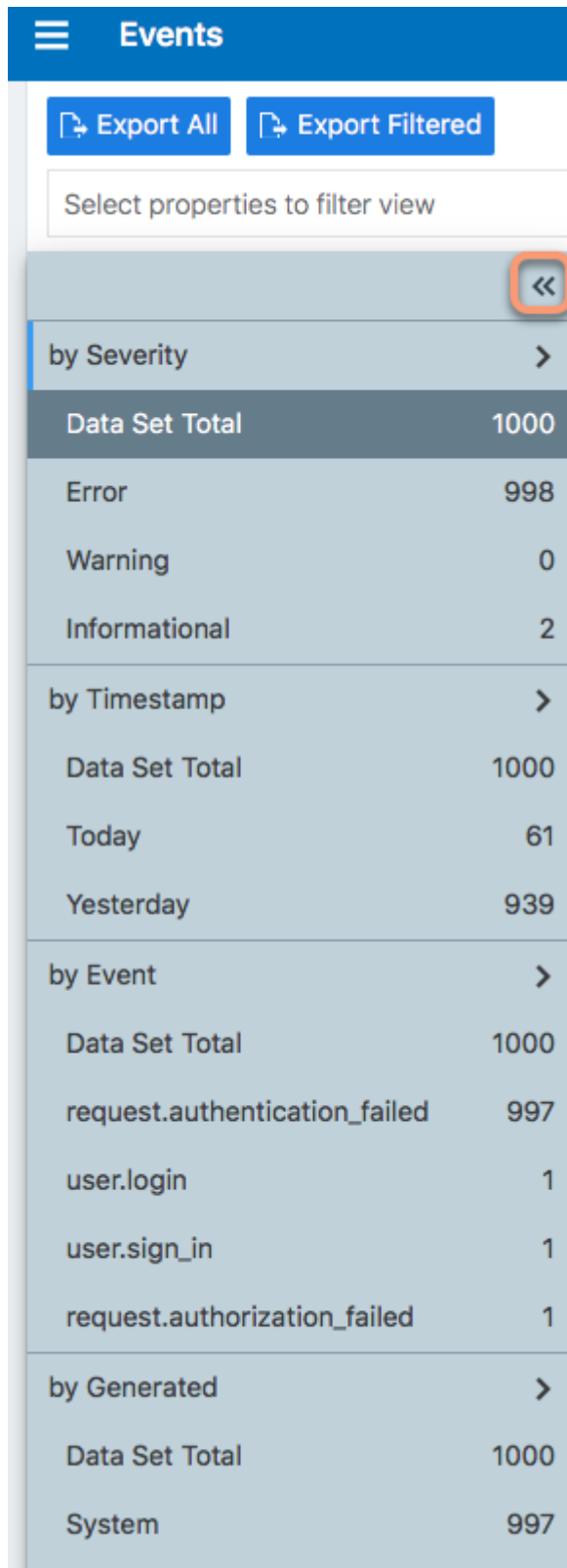
To export events:

1. From the PCE web console menu, choose **Troubleshooting > Events**.
You see a list of events based on the activities performed.
2. Click **Export > Export All** to export all Organization events.
3. To export a filtered list of a events, filter the list and then click **Export > Export Filtered** to export only the filtered view.
4. To search for events based on event type, severity, status, timestamp, and who generated them, use the search filter:

The screenshot shows the 'Events' page in the PCE web console. At the top, there's a blue header with a menu icon and the word 'Events'. Below the header, there are two buttons: 'Export All' and 'Export Filtered'. A search bar is present with the text 'Select properties to filter view'. The main area displays a list of events. On the left, there's a sidebar with a list of event types and a 'Severity' filter. The event list has columns for Description, Severity, Status, and Timestamp.

Event – 6 of 234 Total	Description	Severity	Status	Timestamp
org.recalc_rules Admin forced recalculation of policy	User session created	Informational	Success	01/21/2019, 01:00:00
agent.activate_clone Agent clone activated	User login	Informational	Success	01/21/2019, 01:00:00
agent.clone_detected Agent clone detected	Request authorization failed	Error	Failure	01/21/2019, 01:00:00
agent.request_policy Agent fetched policy				
agent.tampering Agent firewall tampered				
agent.update_interactive_users Agent interactive users updated				
Type to show more Events				

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



The screenshot shows the 'Events' administration interface. At the top, there are two buttons: 'Export All' and 'Export Filtered'. Below them is a text input field labeled 'Select properties to filter view'. To the right of this field is a collapse button, represented by two left-pointing chevrons ('<<'), which is highlighted with an orange square. The sidebar contains several expandable sections, each with a right-pointing chevron ('>'). The first section is 'by Severity', which is expanded to show a table of event counts by severity level. The second section is 'by Timestamp', also expanded, showing counts for 'Today' and 'Yesterday'. The third section is 'by Event', expanded, showing counts for specific event types. The fourth section is 'by Generated', expanded, showing counts for 'System' events.

by Severity	
Data Set Total	1000
Error	998
Warning	0
Informational	2

by Timestamp	
Data Set Total	1000
Today	61
Yesterday	939

by Event	
Data Set Total	1000
request.authentication_failed	997
user.login	1
user.sign_in	1
request.authorization_failed	1

by Generated	
Data Set Total	1000
System	997

Examples of Events

This section presents examples of recorded events in JSON, CEF, and LEEF for various auditing needs.

User Password Update Failed (JSON)

This example event shows a user password change that failed validation. Event type `user.update_password` shows `"status": "failure"`, and the notification shows that the user's attempted new password did not meet complexity requirements.

```
{
  "href": "/orgs/1/events/xxxxxxxx-39bd-43f1-a680-cc17c6984925",
  "timestamp": "2018-08-29T22:07:00.978Z",
  "pce_fqdn": "pcel.bigco.com",
  "created_by": {
    "system": {}
  },
  "event_type": "user.update_password",
  "status": "failure",
  "severity": "info",
  "action": {
    "uuid": "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": "pcel.bigco.com",
  "created_by": {
    "user": {
      "href": "/users/1",
      "username": "albert.einstein@bigco.com"
    }
  }
```

```

},
"event_type": "rule_set.update",
"status": "success",
"severity": "info",
"action": {
"uuid": "xxxxxxxx-7488-480b-9ef9-0cd2a8496004",
"api_endpoint": "/api/v2/orgs/1/sec_policy/draft/rule_sets/6",
"api_method": "PUT",
"http_status_code": 204,
"src_ip": "10.3.6.116"
},
"resource_changes": [{
"uuid": "xxxxxxxx-1d13-4e5e-8f0b-e0e8bccc44e0",
"resource": {
"rule_set": {
"href": "/orgs/1/sec_policy/draft/rule_sets/6",
"name": "rule_set_3",
"scopes": [
[{
"label": {
"href": "/orgs/1/labels/19",
"key": "app",
"value": "app2"
}
}, {
"label": {
"href": "/orgs/1/labels/20",
"key": "env",
"value": "env2"
}
}, {
"label": {
"href": "/orgs/1/labels/21",
"key": "loc",
"value": "loc2"
}
}
]
}
}
],
"changes": {
"name": {
"before": "rule_set_2",
"after": "rule_set_3"
}
},
"change_type": "update"
}],
"notifications": [],
"version": 2
}

```

Security Rule Created (JSON)

In this example of a successful `sec_rule` composite event, a new security rule is created. Because this is a creation event, the `before` values are `null`.

```
{ "href": "/orgs/1/events/xxxxxxx-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": "xxxxxxx-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":xxxxxxxxxx,"mask_addr":someMask}},
"changes":{"address":{"before":null,"after":
{"family":2,"addr":xxxxxxxxxx,"mask_addr":someMask}},
"cidr_block":{"before":null,"after":16},"default_gateway_address":
{"before":null,"after":
{"family":2,"addr":someGateway,"mask_addr":someMask}},
```

```

"link_state":{"before":"unknown","after":"up"},
"network":{"before":null,"after":{"href":"/orgs/7/networks/xx"}},
"network_detection_mode":{"before":null,"after":"single_private_brn"}},
{"resource":{"href":"/orgs/7/workloads/someUUID/interfaces/eth1",
"name":"eth1","address":
{"family":2,"addr":someAddress,"mask_addr":someMask}},
"changes":{"address":{"before":null,"after":{"family":2,"addr":someAddress,
"mask_addr":someMask}},
"cidr_block":{"before":null,"after":16},"link_state":
{"before":"unknown","after":"up"},
"network":{"before":null,"after":{"href":"/orgs/7/networks/xx"}},
"network_detection_mode":{"before":null,"after":"single_private_brn"}}}}},
"change_type":"update"}] notifications=[] event_href=/orgs/7/events/someUUID

```

Differences from Previous Releases

The following table indicates which event names changed in the Illumio Core 18.2 release. If you are upgrading from a release prior to 18.2, be sure to use the current event name in your alert monitoring system.

Changed VEN Event Names

This table lists the names of VEN-related events prior to the Illumio Core 18.2 release and the names they were changed to in the 18.2 release.

Old Name Prior to 18.2	New Name as of 18.2
fw_config_change	agent.firewall_config
activation_success	agent.activate
activation_failure	
deactivation_success	agent.deactivate
deactivation_failure	

Events Monitoring Best Practices

The Illumio Core generates a rich stream of structured messages that provide the following information:

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

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

Monitoring Operational Practices

In addition to setting up an automated system, Illumio recommends implementing the following operational practices:


1. Determine the normal quantity of events from the Illumio Core and monitor the trend for changes; investigate spikes or reductions in the event generation rate.
2. Implement good operational practices to troubleshoot and investigate alerts, and to recover from events.
3. Do not monitor Illumio Core events in isolation. Monitor them as part of your overall system. Understanding the events in the context of your overall system activity can provide as much information as the events themselves.

Recommended Events to Monitor

As a best practice, Illumio recommends you monitor the following events at a minimum.

Events	Description
Program name = <code>Illumio_pce/system_health</code> Severity = Warning, Error, or Fatal	<p>Provides multiple systems metrics, such as CPU and memory data, for each node in a PCE cluster. The PCE generates these events every minute. The Severity field is particularly important. When system metrics exceed thresholds, the severity changes to warning, error, or fatal.</p> <p>For more information about the metrics and thresholds, see the PCE Administration Guide.</p> <p>Recommendation: Monitor <code>system_health</code> messages with a severity of warning or higher and correlate the event with other operational monitoring tools to determine if administrative intervention is required.</p>
<code>event_type="lost_agent_found"</code>	<p>Contains the information necessary to identify workloads with lost agents. A lost agent occurs when the PCE deletes a workload from its database but that workload still has a VEN running on it.</p> <p>Recommendation: Monitor <code>lost_agent_found</code> events and send alerts in case you need to pair the workloads' VENs with the PCE again.</p>
<code>event_type="system_task.agent_missed_heartbeats_check"</code>	<p>Lists the VENs that missed three heartbeats (usually 15 minutes). Typically, this event precedes the PCE taking the VENs offline to perform internal maintenance.</p> <p>This event triggers an alert to be sent at 25% of the time configured in the offline timer. For example, if the offline timer is configured to 1 hour, an alert is sent after the VEN has not sent a heartbeat for 15 minutes; if the offline timer is configured to 4 hours, an alert is sent after the VEN hasn't sent a heartbeat for 1 hour.</p> <p>Recommendation: Monitor these events for high-value workloads because the PCE can take these workloads offline when the VENs miss 12 heartbeats (usually 60 minutes).</p>

Events	Description
<code>event_type="sys-tem_task.agent_offline_check"</code>	<p>Lists VENs that the PCE has marked offline, usually because they missed 12 heartbeats. The VENs on these workloads haven't communicated with the PCE for an hour and it removed the workloads from policy.</p> <p>Recommendation: Monitor these events for high-value workloads because they indicate change in the affected workloads' security posture.</p>
<code>event_type="agent.suspend"</code>	<p>Indicates that the VEN is suspended and no longer protecting the workload. If you did not intentionally run the VEN suspend command on the workload, this event can indicate the workload is under attack.</p> <p>Recommendation: Monitor these events for high-value workloads.</p>
<code>event_type="agent.tampering"</code>	<p>Indicates tampering of the workload's Illumio managed firewall and that the VEN recovered the firewall. Firewall tampering is one of the first signs that a workload is compromised. During a tampering attempt, the VEN and PCE continue to protect the workload; however, you should investigate the cause of the event.</p> <p>Recommendation: Monitor these events for high-value workloads.</p>
<code>event_type="agent.update"</code>	<p>Contains the state data that the VEN regularly sends to the PCE. Typically, these events contain routine information; however, the VEN can attach a notice indicating the following issues:</p> <ul style="list-style-type: none"> • Processes not running • Policy deployment failure <p>Recommendation: Monitor <code>agent.update</code> events that include notifications because they indicate workloads that might require administrative intervention.</p>
<code>event_type="rule_set.create"</code>	<p>Contains the labels indicating the scope of a draft ruleset. Illumio Core generates these events when you create, update, or delete a draft ruleset. When you include "All Applications," "All Environments," or "All Locations" in a ruleset scope, the PCE represents that label type as a null HREF. Ruleset scopes that are overly broad affect a large number of workloads. Draft rulesets do not take effect until they are provisioned.</p> <p>Recommendation: Monitor these events to pinpoint ruleset scopes that are unintentionally overly broad.</p>
<code>event_type="rule_set.update"</code>	
<code>event_type="rule_sets.delete"</code>	
<code>event_type="sec_rule.create"</code>	<p>Contains labels indicating when all workloads affected, all services, or a label/label-group are used as a rule provider or consumer. Illumio Core generates these events when you create, update, or delete a draft ruleset. The removed or added labels could represent high-value applications or environments.</p> <p>Recommendation: Monitor these events for high-value labels.</p>
<code>event_type="sec_rule.update"</code>	
<code>event_type="sec_rule.delete"</code>	
<code>event_type="sec_policy.create"</code>	<p>[NEW in Illumio Core 19.3.0] Contains the <code>workloads_affected</code> field, which includes the number of workloads affected by a policy. Illumio Core generates this event when you provision draft policy that updates the policy on affected workloads. The number of affected workloads could be high or a significant percentage of your managed workloads.</p> <p>Recommendation: Monitor the <code>workloads_affected</code> field for a high number of affect workloads. If the number exceeds an acceptable threshold, investigate the associated the policy.</p>

Events	Description
<code>event_type="agent.clone_detected"</code>	<p>The PCE detects cloned VENs based on clone token mismatch. This is a special alert from the Illumio Core release 19.3.2 onwards, as clones have become a higher priority. Volume of these events make the severity level important and not the fact that these events occurred.</p> <p>Recommendation: If severity is 1 or 'error', some intervention may be needed.</p> <div><p>NOTE Automatic Cloned VEN Remediation</p><p>For on-prem domain joined Windows workloads, cloned VENs support automatic clone remediation by detecting changes to the workload's domain Security identifier (SID). After the VEN reports such changes to the PCE, the PCE tells the clone to re-activate itself, after which the cloned VEN is remediated and becomes a distinct agent from the original VEN.</p></div>

Events Setup

This section describes PCE settings related to events and how to use them to configure PCE behavior.

Requirements for Events Framework

To use the events framework, ensure that you allocate enough disk space for event data, and be familiar with the disk capacity requirements.

Database Sizing for Events

Disk space for a single event is estimated at an average 1,500 bytes.



CAUTION

As the number of events increases, the increase in disk space is not a straight line. The projections below are rough estimates. Disk usage can vary in production and depends on the type of messages stored.

Number of Events	Disk Space
25 million	38GB
50 million	58GB

Data and Disk Capacity for Events

For Illumio Core Cloud customers, Illumio Operations manages all data and disk capacity requirements and configuration for events; including the default events data retention period, database dumps with and without events data, and disk compacting.

For more information, contact your Illumio Support representative.

Events Preview Runtime Setting

If you participated in the preview of Events in 18.1.0, the preview was enabled by configuring a setting in your PCE `runtime_env.yml` file.

**WARNING****Remove preview parameter from runtime_env.yml**

Before you upgrade to the latest release, you must remove `v2_auditable_events_recording_enabled: true` from `runtime_env.yml`. Otherwise, the upgrade does not succeed.

Removing this preview parameter does not affect the collection of “organization events” records, which continue to be recorded.

To remove the Events preview setting:

1. Edit the `runtime_env.yml` file and remove the line `v2_auditable_events_recording_enabled:`

```
v2_auditable_events_recording_enabled: true
```

If you are not participating in any other previews, you can also remove the line `enable_preview_features`.

2. Save your changes.

Events Settings

The following section describes how to configure the Events Settings in the PCE web console.

Events Are Always Enabled

Events are enabled by default in the PCE and cannot be disabled, in accordance with [Common Criteria compliance](#).

Use the PCE web console to change event-related settings and the PCE `runtime_env.yml` for traffic flow summaries.

Event Settings in PCE Web Console

From the PCE web console, you can change the following event-related settings:

- **Event Severity:** Sets the severity level of events to record. Only messages at the set severity level and higher are recorded. The default severity is “Informational.”
- **Retention Period:** The system retains event records for a specified number of days; from 1 day to 200 days with the default period being 30 days.
- **Event Pruning:** The system automatically prunes events based on disk usage and the age of events; events older than the retention period are pruned. When pruning is complete, the `system_task.prune_old_log_events` event is recorded.

- **Event Format:** Sets the message output to one of the three formats. The selected message output format only applies to messages that are sent over syslog to a SIEM. The REST API always returns events in JSON.
 - JavaScript Object Notation (JSON): The default; accepted by Splunk and QRadar SIEMs
 - Common Event Format (CEF): Accepted by ArcSight
 - Log Event Extended Format (LEEF): Accepted by QRadar

Event Severity Levels

Severity	Description
Emergency	System is unusable
Alert	Should be corrected immediately
Critical	Critical conditions
Error	Error conditions
Warning	Might indicate that an error will occur if action is not taken
Notice	Events that are unusual, but not error conditions
Informational	Normal operational messages that require no action
Debug	Information useful to developers for debugging the application

Output Format Change

The output format can be changed in the PCE web console:

- JSON (default)
- CEF
- LEEF

Records are in JSON format until you change to one of the other formats. Then, the new events are recorded in the new format; however, the earlier events are not changed to the selected format and they remain recorded in JSON.

Set Event Retention Values

You can set the event retention values depending on the specific conditions described below.

If you are using a SIEM, such as Splunk as the primary long-term storage for events and traffic in a dynamic environment, consider setting the event retention period to 7 days. On setting it to 7 days, you can use the PCE Troubleshooting or Events Viewer to quickly troubleshoot and diagnose events. The benefit of setting 7 days is that if an issue occurs on a Friday, it can still be diagnosed on the following Monday. A large number of events are generated in a dynamic environment, which increases the data stored (disk space used), backup size, and so on. The period of 7 days provides a good balance between disk usage and the ability to troubleshoot.

**NOTE**

A dynamic environment is when applications and infrastructure are subject to frequent changes; for example, usage of APIs, ETL, Containers, and so on.

If you are using a SIEM in a non-dynamic environment, consider setting the event retention period to 30 days. A smaller number of events are generated, and less disk space is used in a non-dynamic environment.

If you are not using a SIEM such as Splunk and the PCE is the primary storage for the events data used for reporting, diagnosis, and troubleshooting, set the event retention period as per the organization's record retention policy, such as 30 days. If you generate quarterly reporting using events, set the event retention period to 90 days.

SIEM	Consideration	Value
Yes: Primary storage for events	If primary storage of events is not on the PCE	7 days (PCE troubleshooting) 1 day (minimum)
No: Not primary storage for events	If primary storage of events is on the PCE, consider the organization's record retention policy as well as the available disk and event growth pattern	30 days (default)
No	<ul style="list-style-type: none"> If the organization's record retention is more than 30 days If disk monitoring is not set up, it is required to set up disk monitoring 	As per your record retention policy 200 days (maximum)
Not applicable	If events data is not needed for reporting or troubleshooting	1 day (minimum)

If disk space availability and event growth projections indicate that the desired retention period cannot be safely supported, consider using a SIEM because the PCE might not store events for the desired period.

**NOTE**

Running the `illumio-pce-db-management events-db` command provides an output of the average number of events and the storage used.

Configure Events Settings in PCE Web Console

1. From the PCE web console menu, choose **Settings** > **Event Settings** to view your current settings.
2. Click **Edit** to change the settings.
 - For Event Severity, select from the following options:
 - Error
 - Warning

- Informational
- For Retention Period, enter the number of days you want to retain data.
- For Event Format, select from the following options:
 - JSON
 - CEF
 - LEEF

3. Click **Save** once you're done.

Limits on Storage

From the Illumio Core 19.3.1 release onwards, the PCE will automatically limit the maximum number of events stored. The limits are set on the volume of events stored locally in the PCE database, so that the events recorded in the database do not fill up the disk. The limit is a percentage of the disk capacity, cumulative for all services that store events on the disk.



IMPORTANT

To change the default limits, contact Illumio Support.

The configuration limit includes both hard and soft limits.

- Soft limit: 20% of disk used by event storage

Aggressive pruning is triggered when the soft limit is reached. However, new events are still recorded while pruning. On the Events list page of the PCE Web Console, the `system_task.prune_old_log_events` event is displayed with the "Object creation soft limit exceeded" message and 'Severity: Informational'.

- Hard limit: 25% of disk used by event storage.

More aggressive pruning is triggered when the hard limit is reached. New events are not recorded while pruning. On the Events list page of the PCE Web Console, the `system_task.prune_old_log_events` event is displayed with the message "Object creation hard limit exceeded" message and 'Severity: Error'. The pruning continues until the soft limit level of 20% is reached. When this occurs, a `system_task.hard_limit_recovery_completed` event occurs, and the PCE starts to behave as it did for the soft limit conditions.

SIEM Integration for Events

For analysis or other needs, event data can be sent using syslog to your own analytics or SIEM systems.

About SIEM Integration

This guide also explains how to configure the PCE to securely transfer PCE event data in the following message formats to some associated SIEM systems:

- JavaScript Object Notation (JSON), needed for SIEM applications, such as Splunk®.
- Common Event Format (CEF), needed for SIEM applications, such as Micro Focus Arc-Sight®.
- Log Event Extended Format (LEEF), needed for SIEM applications, such as IBM QRadar®.

Syslog Forwarding

The PCE can export logs to syslog. You can also use the PCE's own internal syslog configuration.

Identify Events in Syslog Stream

Event records from the syslog stream are identified by the following string:

```
"version":2  
AND  
' "href":\s*" /orgs/[0-9]*/events' OR ' "href":\s*" /system_events/ '
```

Forward Events to External Syslog Server

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

To configure forwarding to an external syslog server:

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

The Event Settings - Add Event Forwarding page opens.

3. Click **Add Repository**.

4. In the Add Repository dialog:

- Description: Enter name of the syslog server.
- Address: Enter the IP address for the syslog server.
- Protocol: Select TCP or UDP. If you select UDP, you only need to enter the port number and click **OK** to save the configuration.
- Port: Enter port number for the syslog server.
- TLS: Select Disabled or Enabled. If you select Enabled, click “Choose File” and upload your organization’s “Trusted CA Bundle” file from the location it is stored on. The Trusted CA Bundle contains all the certificates that the PCE (internal syslog service) needs to trust the external syslog server. If you are using a self-signed certificate, that certificate is uploaded. If you are using an internal CA, the certificate of the internal CA must be uploaded as the “Trusted CA Bundle”.
- Verify TLS: Select the check-box to ensure that the TLS peer’s server certificate is valid.

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

After ensuring that the events are being forwarded as configured to the correct external syslog servers, you can choose to stop using the “Local” server by editing the local server setting and deselect all message types.



NOTE

You cannot delete the “Local” server.

Disable Health Check Forwarding

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

For example, IBM QRadar is usually used by security personnel, who might not need to monitor the PCE system health. The Illumio App for QRadar does not process the PCE system health messages.

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

To disable syslog forwarding of health check messages:

1. From the PCE web console menu, choose **Settings > Event Settings**.
2. Click the Event listed under the **Events** column.

Event Settings

[Edit](#)

Events

Event Severity Informational
Only audit events of this severity or higher are saved



Retention Period 30 days
Audit events older than this are purged



Event Format JSON

Event Forwarding [+ Add](#) [- Remove](#) [Refresh](#)

Repository	Events
<input type="checkbox"/> Local	<input type="checkbox"/> Organizational, System, Allowed, Potentially Blocked, Blocked, System Health Messages

3. Under the Events block, for the Status Logs entry, deselect **System Health Messages**. System health check is only available in key-value format. Selecting a new event format does not change the system health check format to CEF or LEEF.

 **Event Settings** – (Edit Event Forwarding)

 Save  Cancel

Forwarding

* PCE


de o


* Repository

☒ Local

Forward events to local syslog service

☐ test (10 UDI .1)

Forwarded event data is not encrypted 

 Add Repository

Auditable Events

☒ Organizational Events

☒ System Events

Traffic Events

☒ Allowed

☐ Potentially Blocked

☐ Blocked

Status Logs

☐ System Health Messages

Only key-value format is supported

4. Click **Save**.



NOTE

IBM QRadar and HP ArcSight do not support system health messages. If you are using either of these for SIEM, make sure that you do not select the System Health Messages checkbox.

Traffic Flow Summaries

This section describes traffic flow summaries.

After you install a VEN on a workload and pair the VEN with the PCE, the VEN monitors each workload's traffic flows and sends the traffic flow summaries to the PCE.

Traffic summaries can be exported to syslog or Fluentd. If traffic data is configured for export, the PCE processes the received traffic flow summaries from each VEN and immediately sends them to syslog or Fluentd.

Traffic Flow Types and Properties

The Illumio Core logs traffic flows based on the Visibility setting. Events have attributes that can be Allowed, Blocked, or Potentially Blocked and might not appear in the traffic flow summary.

Visibility Settings

The table below indicates whether or not a traffic summary is logged as Allowed, Potentially Blocked, or Blocked depending on a workload's policy state.

**NOTE**

Traffic from workloads in the "Idle" policy state is not exported to syslog from the PCE.

Visibility	Logged in Traffic Flow Summary
Off	VEN does not log traffic connection information
Blocked - Low Detail	VEN logs connection information for blocked and potentially blocked traffic only
Blocked + Allowed - High Detail	VEN logs connection information for allowed, blocked, and potentially blocked traffic
Enhanced Data Collection	VEN logs byte counts in addition to connection details for allowed, blocked, and potentially blocked traffic

Event Types

In a traffic flow summary, the event type is designated by Policy Decision (pd).

**NOTE**

An asterisk (*) indicates the attribute might not appear in the summary.

Event Attributes	Allowed (pd=0)	Potentially Blocked (pd=1)	Blocked (pd=2)	Unknown (pd=3)
version	✓	✓	✓	✓
count	✓	✓	✓	✓
interval_sec	✓	✓	✓	✓
timestamp	✓	✓	✓	✓
dir	✓	✓	✓	✓
src_ip	✓	✓	✓	✓
dst_ip	✓	✓	✓	✓
proto	✓	✓	✓	✓
dst_prt	✓	✓	✓	✓
state	✓	✓	✓	✓
pd	✓	✓	✓	✓
code*	✓	✓	✓	✓
type*	✓	✓	✓	✓
dst_vulns*	✓	✓	✓	✓
fqdn*	✓	✓	✓	✓
un*	✓	✓	✗	✓
pn*	✓	✓	✗	✓
sn*	✓	✓	✗	✓
src_labels*	✓	✓	✓	✓
dst_labels*	✓	✓	✓	✓
src_hostname*	✓	✓	✓	✓
dst_hostname*	✓	✓	✓	✓
src_href*	✓	✓	✓	✓
dst_href*	✓	✓	✓	✓

Show Amount of Data Transfer

The JSON, CEF, and LEEF for the accurate byte count work events are related to the 'Show Amount of Data Transfer' preview feature available with the Illumio Core 20.2.0 release.

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

The direction reported in flow summary is from the viewpoint of the provider of the flow:

Destination Total Bytes Out: Number of bytes transferred out of provider:

```
dst_tbo
```

Destination Total Bytes In: Number of bytes transferred in to provider.

```
dst_tbi
```

To activate the 'Show Amount of Data Transfer' capability on the PCE, contact your Illumio representative.

LEEF Mapping

- LEEF field `x` contains JSON field `y`
- `srcBytes` contains `dst_tbo`
- `dstBytes` contains `dst_tbi`
- `dbi` contains `dst_dbi`
- `dbo` contains `dst_dbo`

CEF Mapping

- CEF field `cn2` is `dst_dbi` with `cn2Label` is "dbi"
- CEF field `cn3` is `dst_dbo` with `cn3Label` is "dbo"
- CEF field "in" is `dst_tbi`
- CEF field "out" is `dst_tbo`

Manage Traffic Flows Using REST API

You can use the following properties to manage traffic flows using the REST API.



**NOTE**



You should ignore and *not* use any extra properties that are not described in this document, such as `tbi`, `tbo`, `dbi`, and `dbo`.



Property	Description	Type	Re-quired	Possible Values
<code>version</code>	The version of the flow summary schema.	Integer	Yes	4
<code>timestamp</code>	Indicates the time (RFC3339) when the first flow in the summary was created, represented in UTC. Format: <code>yyyy-MM-dd'T'HH:mm:ss.SSSSSSZ</code>	String	Yes	
<code>interval_sec</code>	Sample duration for the flows in the summary. Default is approximately 600 seconds (10 minutes), depending on the VEN's ability to report traffic and PCE's current load.	Integer	Yes	
<code>dir</code>	Direction of the first packet: in or out (I, O).	String	Yes	I, O
<code>src_ip</code>	Source IP of the flows.	String	Yes	
<code>dst_ip</code>	Destination IP of the flows.	String	Yes	
<code>proto</code>	Protocol number (0-255).	Integer	Yes	Minimum=0 Maximum=255
<code>type</code>	The ICMP message type associated with the first flow in the summary. This value exists only if protocol is ICMP (1).	Integer	No	Minimum=0 Maximum=255


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."

Property	Description	Type	Re-quired	Possible Values
code	<p>The ICMP message code (subtype) associated with the first flow in the summary. This value exists only if protocol is ICMP (1).</p> <div>  NOTE This information is included in blocked flows for VEN versions lower than 19.1.0. It is included in all flows for VEN version 19.1.0 and later. </div> <p>Example: 1 for "Destination host unreachable."</p>	Integer	No	Minimum=0 Maximum=255
dst_port	<p>Destination port.</p> <p>This value exists only if protocol is not TCP (6) or UDP (17).</p>	Integer	Yes	Minimum=0 Maximum=65535
pd	<p>Policy decision value, which indicates if the flow was allowed, potentially blocked (but allowed), blocked, or unknown.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • 0 - Allowed traffic • 1 - Allowed traffic but will be blocked after policy enforcement • 2 - Blocked traffic • 3 - Unknown <div>  NOTE Policy decision is "unknown" in the following cases: <ul style="list-style-type: none"> • 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). </div>	Integer	Yes	Minimum=0 Maximum=3
count	Count of the number of flows in the flow summary.	Integer	Yes	

Property	Description	Type	Re-quired	Possible Values
state	<p>Session state for the traffic flows in the flow summaries.</p> <p>Possible values:</p> <ul style="list-style-type: none"> • Active (A): Connection was still open at the time the flow summary was logged. Applies to allowed and potentially blocked flows. • Closed (C): (Linux only) Connection closed at the time the flow summary was logged. Applies to allowed and potentially blocked flows. • Timed out (T): Connection timed out at the time the flow summary was logged. Applies to allowed and potentially blocked flows. Due to a limitation of WFP, a Windows VEN will report "T" even when the connection is closed at the time the flow summary was logged. • Snapshot (S): Snapshot of current connections to and from the VEN, which applies only to workloads whose policy state is set to Idle. Applies to allowed and potentially blocked flows. • New connection (N): Dropped TCP packet contains a SYN and is associated with a new connection. Applies to blocked TCP flows. The value is empty for blocked UDP flows. 	String	No	A, C, T, S, N
pn	<p>The program name is associated with the first flow of the summary. It is supported on inbound flows for Linux and Windows VEN and on outbound flows for only Windows VEN.</p> <div>  NOTE This information might not be available on short-lived processes, which are Linux-specific. </div> <p>Currently, flows are aggregated, so this value might represent only the first process detected across all aggregated flows.</p> <p>If network communication is done by an OS component (or a driver), no process is associated with it.</p>	String	No	
un	<p>The username is associated with the first flow of the summary. It is supported on inbound flows for Linux and Windows VEN and on outbound flows for only Linux VEN.</p> <p>On Windows, it can include the username of the user account that initiated the connection.</p> <div>  NOTE This information might not be available on short-lived processes. </div>	String	No	

Property	Description	Type	Re-quired	Possible Values
sn	Service name associated with the first flow in the summary. It is supported only on inbound flows on Windows VEN.	String	No	
src_host-name	Hostname of the source workload that reported the flow.	String	No	
src_href	HREF of the source workload that reported the flow.	String	No	
src_labels	Labels applied to the source workload.	Object	No	
<div>  <p>NOTE</p> <p>The <code>src_hostname</code>, <code>src_href</code>, and <code>src_labels</code> values are not included in a traffic summary if the source of the flow is not an Illumio-labeled workload. For example, Internet traffic or a managed workload without any labels applied.</p> </div>				
dst_host-name	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.	Object	No	
<div>  <p>NOTE</p> <p>The <code>dst_hostname</code>, <code>dst_href</code>, and <code>dst_labels</code> values are not 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.</p> </div>				

Property	Description	Type	Re-quired	Possible Values
dst_vulns	Information about the vulnerabilities on the destination of the traffic flow with the specific port and protocol.	Object	No	
	<div>  NOTE <ul style="list-style-type: none"> Vulnerabilities are defined by Common Vulnerabilities and Exposures (CVE), with identifiers and descriptive names from the U.S. Department of Homeland Security National Cybersecurity Center. The vulnerability information is sent only when the Vulnerability Maps feature is turned on via a license and the information is imported into the PCE from a Vulnerability Scanner, such as Qualys. </div>			
fqdn	Fully qualified domain name	String	No	

The following table describes the sub-properties for the `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 vulnerabilities on the destination port and protocol.	Number	No
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](#). [41]



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 (δdms):** 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 (τdms):** 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
cni=120 cniLabel=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 cni=31 cniLabel=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=0 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
```