Illumio Adaptive Security Platform 18.2.1 Auditable Events and SIEM Integration Guide

01/24/2019

80000-100-18.2.1

Table of Contents

Product Version

Illumio® Adaptive Security Platform®

Current PCE Version: 18.2.1

Current VEN Version: 18.2.1

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

About Illumio

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

Illumio Professional Services for Deployment

To ensure optimal deployment of the Illumio Adaptive Security Platform, contact your Illumio Professional Services representative.

Preview Features Only for Evaluation Before General Availability

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

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

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

Illumio Adaptive Security Platform Training

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

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

Search Knowledge Base and Documentation

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

Illumio Adaptive Security Platform Support

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

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

Recommended Skills

Illumio recommends that you be familiar with the following:

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

Related Documentation

Illumio® Adaptive Security Platform® documentation is available from the Support portal.

- *Policy Compute Engine (PCE) Web Console Guide*: working with Illumination®, designing security policy, and provisioning and administering VENs.
- *Policy Compute Engine (PCE) Deployment Guide*: planning and installing the PCE.
- *Policy Compute Engine (PCE) Operations Guide:* common management tasks of the PCE.
- *Advanced Command-line Tool Interface Guide*: common PCE-related tasks to use on your local computer.
- *Policy Compute Engine (PCE) Supercluster Deployment and Usage Guide*: designing, deploying, and managing the PCE Supercluster of multiple, distributed standard PCE clusters.
- *Policy Compute Engine (PCE) REST API Guide*: web-programming Illumio Adaptive Security Platform.
- *Virtual Enforcement Node (VEN) Deployment Guide:* installing and activating the VEN, including PCE-based distribution of the VEN and on-worload installation and management
- *Virtual Enforcement Node (VEN) Operations Guide*: common management tasks of the VEN.

- *Auditable Events and SIEM Integration Guide*: analyzing significant events on the PCE and VEN and securely transferring event records to analytics or Security Information and Event (SIEM) systems.

- 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

- 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:
  ```
  ...
  some command or command output
  ...
  ```
- References to section titles in this guide are in double quotation marks. Example: See "Basic Theory of Operation".
- Reference to other guides in the Illumio library are *italicized*. Example: See the *PCE Web Console User Guide*.

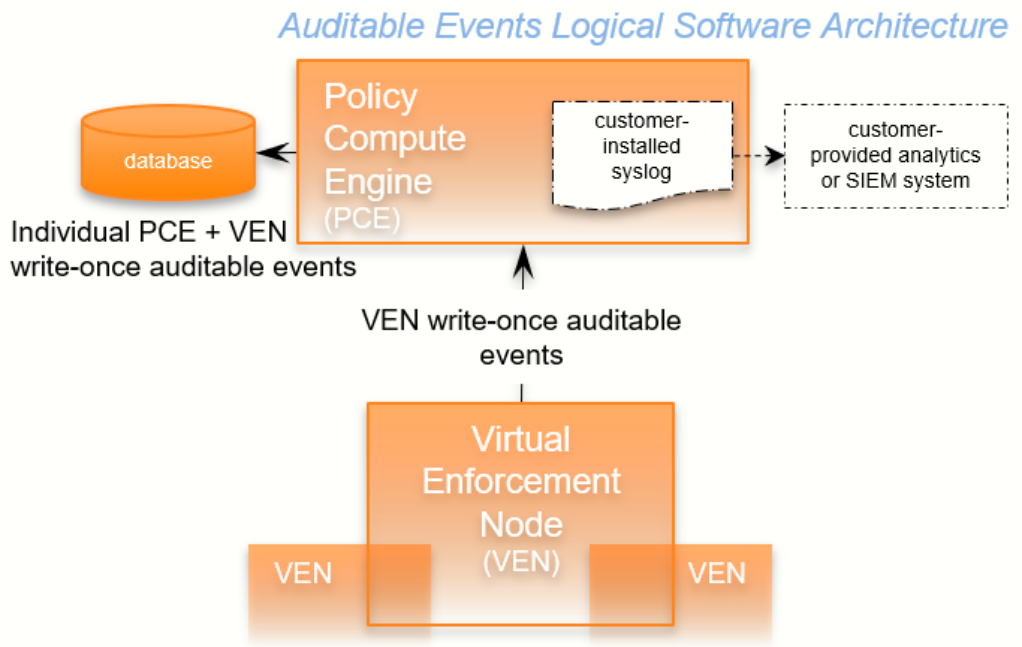
How To Use This Guide

The *Illumio Adaptive Security Platform Auditable Events and SIEM Integration* guide has several main divisions:

- Overview to Auditable Events and SIEM Integration.
- Auditable Events Setup Considerations.
- Event Record Formats, Types, and Common Fields.
- Event Types by Resource.
- Security Information and Event Management (SIEM) integration considerations and recommendations.

Overview to Auditable Events and SIEM Integration

The Auditable Events Framework is an information-rich, deep foundation for actionable insights into the operations of the Illumio Adaptive Security Platform. *Auditable events* are records of significant transactions collected from the Policy Compute Engine (PCE) and its paired Virtual Enforcement Nodes (VENs). All actions that change the configuration of the PCE, security policy, and the VENs are recorded, including workload firewall tampering.



Audit-worthy operations from any management interface are recorded:

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

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, auditable evnts are read-only.

Auditable Events comply with the Common Criteria Class FAU Security Audit requirements s tandard for auditing .

Benefits of Auditable Events Framework

The Auditable Events Framework is comprehensive set of auditable events with rich content that solves many problems with earlier events systems that made it difficult to use

- Designed for customer ease of use.
- Exceeds industry standards.
- Complete content.
    - Comprehensive set of event types.
    - Flattened, common structure for all events.
    - Eliminates former duplicate or multiple events for single action.

        - Additional notable system events are generated.
        - Create/Update/Delete REST APIs are recorded as events. (Read APIs/GET calls are not recorded, because they make no change.)
        - More than 200 events.
    - Improved interfaces:
        - New REST API with filtering.
        - New Event Viewer in the PCE web console. For more information on viewing events in the PCE web console, see the *PCE Web Console User Guide* .
        - New Settings in the PCE web console.
        - Auditable Events are the same across all interfaces.
        - Streamed via syslog in JSON, CEF or LEEF format

Effects of Change to New Auditable Events Framework

To migrate to the Auditable Events Framework, take into consideration the following important points.

Output Format Change

In this release, the desired 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. After the switch, new events are recorded in the new format, but the earlier events are not changed to the selected format remain recorded in JSON.

Changed VEN Event Names

The table below shows names of VEN-related events have changed in this release.

Old Name	New Name
fw_config_change	agent.firewall_config
activation_success activation_failure	agent.activate
deactivation_success deactivation_failure	agent.deactivate

VEN Event Types Not Shown the PCE Web Console

The following events related to VENs are not currently viewable in the PCE web console.

This a two-column alphabetical 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

VEN Events not shown in PCE Web Console	
refresh_token_success	

General Auditing Needs Satisfied by the Auditable Events Framework

Need	Description	See section...
Audit and Compliance	Evidence to show that resources are managed according to rules and regulatory standards.	"Who, What, When, Where, and How"
Resource lifecycle tracking	All information necessary to track a resource through creation, modification, and deletion.	"Lifecycle of resource events, with before and after values"
Operations	Trace of recent changes to resources.	"Lifecycle of resource events, with before and after values"
Security	Evidence to show which changes failed, such as incorrect user permissions or failed authentication.	"Example JSON event – Failed update of user password"

Who, What, When, Where, and How

The following information is included in an auditable event record. These data answer the questions who, what, where, how, and when.

Type of information	Description
Who	• VEN identified by hostname and agent href • User identified by username and href • PCE system identified by "system"

Type of information	Description

What	The action that triggered the event, including the following:
	• Resource type + operation + success or failure
	• Application Request ID
	• Status of successful events and failed events:
	  • In case of failure, exception type and exception message.
	  • All failures related to security, such as authentication and authorization.
	  • Severity as INFO, WARNING, ERROR.
	• The pre-change and post-change values of the affected resources.

Where	The target resource of the action, composed of the following:
	• Identifier of the target resource (primary field).
	• Friendly name for the target resource. For example:
	  • workload/VEN: `hostname`
	  • user.username
	  • ruleset, label, service, etc: name, key/value

How	API endpoint, method, HTTP status code, and source IP address of the request.
When	Timestamp of the event's occurrence. This timestamp is *not* the time the event was recorded.

Event Information Not Included in Anonymized Database Dumps

To troubleshoot customer-reported issues, Illumio Customer Support sometimes asks that the customer supply an anonymized dump of the PCE's database. To safeguard your organization's privacy, event information is not included in the anonymized database dump.

SIEM Integration

For analysis or other needs, auditable-event data can be extracted with regular expressions from the PCE logs and sent via syslog to your own analytics or other Security Information and Event Management (SIEM) system.

This guide also explains how to configure the PCE to securely transfer PCE auditable 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 HPE ArcSight®.
- Log Event Extended Format (LEEF), needed for IBM QRadar®.

Other Illumio Tools for SIEM Integration

Illumio offers other tools for SIEM integration:

- Illumio App for Splunk
  Software: Technical Add-on for Illumio and Illumio App for Splunk
  Documentation: Illumio Documentation Support Site.

Auditable Events Setup

This section describes the necessary setup for working with auditable events.

Before Upgrade, Remove Auditable Events Preview Runtime Flag

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

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 Auditable 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.

Database Sizing for Auditable Events

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

> ⚠ As the number of events increases, the increase in disk space is not a straight line. The projections below are based on Illumio's internal testing. Disk usage can vary in production and depending on the type of messages stored

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

Auditable Events are Always Enabled

Auditable Events are enabled by default in the PCE and cannot be disabled, in accordance with Common Criteria compliance.

Settings for Events

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

Configuring Events and syslog in the PCE Web Console

For details, including configuring remote syslog destinations, see the *PCE Web Console User Guide*, section "Settings > Events".

Other configuration settings related to remote syslog destinations

See "Optionally configure PCE internal syslog" in the *PCE Deployment Guide*.

Event Syntax, Types, Common Fields

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.

For a list of auditable events recorded by the system, see "Event Types by Resource".

These are the general categories of auditable events:

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

REST API Auditable Events Schema Available

The Auditable Events schema in JSON is downloadable from the Illumio Support Portal in the zipfile of the REST API schemas.

Composite Event Structure and Common Fields

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.

System Occurrences Not Recorded

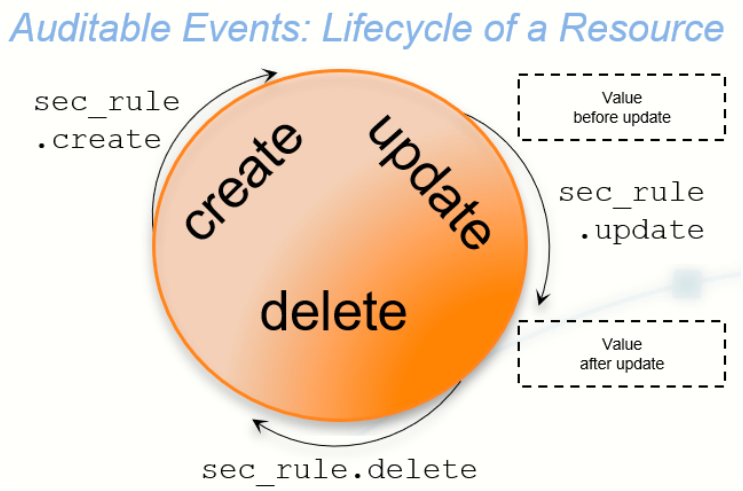
The following unanticipated occurrences on the PCE cannot be recorded as auditable events:

- PCE system crash due to software or hardware failure
- Failure of individual processes on the PCE due to out-of-memory condition or some other reason

Lifecycle of Resource Events with Before and After Values

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 the values of the resource object both before and after the event for a lifecycle audit trail.
- `sec_rule.delete`



Other Kinds of 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`

Regular Expression for Extracting Event Records from Log

The following regular expression extracts event records from a log file.

- This example relies on `grep` to write standard output to a file.
- It shows the log file as `/var/log/illumio-pce/agent` . Your log file might be in a different location. Check the `runtime_env.yml` parameter `log_dir`.

```
grep '"version":2' /var/log/illumio-pce/agent | grep someEventType > output_file
```

The syslog-ng templates delivered with the PCE always have the latest regular expression. See "Templates for rsyslog and syslog-ng, with Log Rotation and Regular Expressions".

Log Record of Auditable Events

Auditable event records from the log file are identified by the following string:

```
"version":2
```

The syslog-ng templates delivered with the PCE always have the latest regular expressions. See "Templates for rsyslog and syslog-ng, with Log Rotation and Regular Expressions".

Examples of Auditable Events

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

Example JSON event – Failed update of user password

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.

Example JSON event - password update failure


```
{
        "href": "/orgs/1/events/005342d3-39bd-43f1-a680-cc17c6984925",
        "timestamp": "2018-08-29T22:07:00.978Z",
        "pce_fqdn": "pce1.bigco.com",
        "created_by": {
               "system": {}
        },
        "event_type": "user.update_password",
        "status": "failure",
        "severity": "info",
        "action": {
               "uuid": "77af2348-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": "eef30f63-7b8e-4205-a62a-1f070d8a0ee2",
               "notification_type": "user.pw_complexity_not_met",
               "info": null
        }, {
               "uuid": "71872d1b-9721-4971-b613-d15aa67a4ee7",
               "notification_type": "user.pw_change_failure",
               "info": {
                       "reason": "Password must have minimum of 1 new character(s)"
               }
        }],
        "version": 2
}
```


Example JSON event - Successful resource update before and after values

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"`.

Example JSON event - resource update, before and after


```
{ "href": "/orgs/1/events/5d4ff30b-8033-4f1a-83e9-fde57c425807",
        "timestamp": "2018-08-29T22:04:04.733Z",
        "pce_fqdn": "pce1.bigco.com",
        "created_by": {
                "user": {
                        "href": "/users/1",
                        "username": "albert.einstein@bigco.com"
                }
        },
        "event_type": "rule_set.update",
        "status": "success",
        "severity": "info",
        "action": {
                "uuid": "20d3b926-7488-480b-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": "3b6d13ba-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
}
```


Example JSON event - Successful creation of security rule

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`.

Example JSON event - successful creation of security rule


```
{ "href": "/orgs/1/events/709dc474-6d29-4905-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": "54141cb0-165b-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
}
```


Example CEF event – Successful creation of draft security rule

Below is an example of an event record in CEF showing the before and after values of the successful creation of a draft security rule: CEF event type `sec_rule.create.success`. Because this is a creation event, the `before` value is `null`.

Key fields required by CEF include the following, as shown in the "CEF Key" field in the table below.

- `cs1`: Custom string.
- `cs1Label`: Custom label for `cs1`.
- `cn2`: Custom number.
- `cn2Label`: Custom label for `cn2`.

Example CEF event - successful creation of security rule

```
CEF:0|Illumio|PCE|18.2.0|sec_rule.create.success|Sec Rule Create Success|Low|src=someIP
rt=someDatetime dvchost=someHostname suid=/users/13 suser=albert.einstein
outcome=success
cat=audit_events request=/api/v2/orgs/7/sec_policy/draft/rule_sets/1088984/sec_rules
requestMethod=POST reason=201
cs2=[{"uuid":"someUUID",
"resource":{"sec_rule":{"href":"/orgs/7/sec_policy/draft/rule_sets/1088984/sec_rules/
someUUID"}},"changes":
{"rule_list":{"before":null,"after":{"href":"/orgs/7/sec_policy/draft/rule_sets/
someUUID"}},
"description":{"before":null,"after":"Rule #3"},
"type":{"before":null,"after":"SecRule"},"resolve_labels":
{"before":null,"after":"1010"},"providers":{"created":[{"provider":true,"label":
{"href":"/orgs/7/labels/387937"}}]},"consumers":
{"created":[{"provider":false,"label":{"href":"/orgs/7/labels/
387937"}}]},"ingress_services":
{"created":[{"href":"/orgs/7/sec_policy/draft/services/
775524","name":"Service_suspend_ven2ven"}]}},
"change_type":"create"}]
cs2Label=resource_changes
cs4=[] cs4Label=notifications
cn2=2 cn2Label=version
cs1Label=event_href cs1=/orgs/7/events/someUUID
```

Example LEEF event – Successful update of workload security policy

Below is an example of an event record in LEEF showing a successful update of security policy for a workload's Ethernet interfaces.

Example LEEF event - successful workload policy update

```
LEEF:2.0|Illumio|PCE|18.2.0|interface_status.update.success|src=66.151.147.220
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/133944/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/386183","key":"loc","value":"test_place_1"},
{"href":"/orgs/7/labels/386182","key":"env","value":"test_env_1"},
{"href":"/orgs/7/labels/386181","key":"app","value":"test_app_1"},
{"href":"/orgs/7/labels/386180","key":"role","value":"test_access_1"}]}},
"changes":{"workload_interfaces":
{"updated":[{"resource":
{"href":"/orgs/7/workloads/someUUID/interfaces/eth1","name":"eth0","
address":{"family":2,"addr":167911162,"mask_addr":someMask}},
"changes":{"address":{"before":null,"after":
{"family":2,"addr":167911162,"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/26"}},
"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/26"}},
"network_detection_mode":{"before":null,"after":"single_private_brn"}}}]}},
"change_type":"update"}] notifications=[] event_href=/orgs/7/events/someUUID
```

Configuring syslog Forwarding

The PCE can export logs to syslog. You must configure the rsyslog or syslog-ng service on each node in your cluster to forward these logs to a remote collector or SIEM system. You can also use the PCE's own internal syslog configuration.

For details on configuring the PCE internal syslog, see the *PCE Deployment Guide*.

Optional – 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.

To disable syslog forwarding of health check messages:

1. Log into the PCE web console.
2. Navigate to **Settings > Events**.
3. Configure the settings for forwarding events. For details, see the *PCE Deployment Guide*.
4. Under the **Events** block, for the **Status Logs** entry, uncheck **System Health Messages**.
5. Click **Save** to save the changes or **Cancel** to discard them.

VEN Traffic Summaries

Once a workload gets a VEN installed and is paired with the PCE, the VEN monitors each workloads network flows and begins sending traffic summaries to the PCE. A traffic summary is an aggregation of individual traffic flows over a ~10 minute period with the following common data attributes:

- Policy decision
- Source IP address
- Destination IP address
- Destination port
- Protocol
- IP Version
- Direction of first packet
- Session state
    - Allowed and potentially blocked traffic: active, closed, timed out, static snapshot
    - Blocked traffic: new connection, invalid connection

The following fields might not always be included:

1. source hostname
2. source href
3. source labels
4. destinatin hostname
5. destination href
6. destination labels
7. program name
8. user name
9. service name

10. total bytes in
11. total bytes out

There are three possible values for a 'policy decision' in a traffic summary:

- **Allowed** Field/value: pd=0. Traffic that your policy has allowed.
- **Potentially Blocked** Field/value: pd=1. Traffic that was allowed but will be blocked once you enforce your policy.
- **Blocked** Field/value: pd=2 Traffic that was blocked because it was not defined as permitted by your policy.

Traffic summaries can be exported to syslog or Fluentd. To export to Fluentd, set the `runtime_env.yml` parameter `export_flow_summaries_to_fluentd`. If traffic data is configured for export, the PCE processes the received traffic summaries from each VEN and immediately sends them to syslog or Fluentd within seconds of the post being received. There is no additional delay beyond the aggregation window on the VEN.

Workload Policy State and Traffic Summaries

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

Note: Traffic from Workloads in the "Idle" policy state is not exported to syslog from the PCE.

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

Changes to Traffic Summaries from Previous Releases – Vulnerabilities Data

The traffic summaries in this release include additional fields for vulnerabilities. These data are identified by the following object names:

- dst_vuln
- dst_label

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 .

Example JSON record for vulnerabilities


```
{
  "interval_sec": 600,
  "count": 1,
  "tbi": 73,
  "tbo": 0,
  "pn": "avahi-daemon",
  "un": "avahi",
  "src_ip": "someIPaddress",
  "dst_ip": "someIPaddress",
  "timestamp": "2018-05-23T16:07:12-07:00",
  "dir": "I",
  "proto": 17,
  "dst_port": 5353,
  "state": "T",
  "src_labels": {
    "app": "CRM",
    "env": "Development",
    "loc": "Azure",
    "role": "Web"
  },
  "src_hostname": "someHostName",
  "src_href": "/orgs/1/workloads/someID",
  "dst_labels": {
    "app": "CRM",
    "env": "Development",
    "loc": "Amazon",
    "role": "Database"
  },
  "dst_hostname": "someHostName",
  "dst_href": "/orgs/1/workloads/someID",
  "pd": 1,
  "dst_vulns": {
    "count": 8,
    "max_score": 8.5,
    "cve_ids": ["CVE-2016-2181", "CVE-2017-2241"]
```

```
    },
    "version" :  4
}
```

Example CEF record for vulnerabilities

```
 CEF:0|Illumio|PCE|2015.9.0|flow_potentially_blocked|Flow Potentially Blocked|3|
act=potentially_blocked cat=flow_summary deviceDirection=0 dpt=137
src=someIPaddress dst=someIPaddress  proto=udp cnt=1 in=1638 out=0 rt=Jun 14 2018
01:50:14 cn1=120 cn1Label=interval_sec cs2=T cs2Label=state dhost=someHostName
 cs6=/orgs/1/workloads/someID cs6Label=dst_href
cs4={"app":"CRM","env":"Development","loc":"Amazon","role":"Web"}
 cs4Label=dst_labels cs1={"count":1,"max_score":3.7,"cve_ids":
["CVE-2013-2566","CVE-2015-2808"]}
 cs1Label=dst_vulns dvchost=someDomainName
```

Example LEEF record for vulnerabilities

```
 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":"Azure","role":"Web"}
dstVulns={"count":2,"max_score":3.7,"cve_ids":["CVE-2013-2566","CVE-2015-2808"]}
```

Event Types by Resource

For formal syntax of events, see "Event Syntax, Types, Common Fields".

Complete List of Event Types

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
agent.activate	Agent paired	agent.activate.success	agent.activate.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
agent.activate_clone	Agent clone activated	agent.activate_clone.success	agent.activate_clone.failure
agent.clone_detected	Agent clone detected	agent.clone_detected.success	agent.clone_detected.failure
agent.deactivate	Agent unpaired	agent.deactivate.success	agent.deactivate.failure
agent.goodbye	Agent disconnected	agent.goodbye.success	agent.goodbye.failure
agent.machine_identifier	Agent machine identifiers updated	agent.machine_identifier.success	agent.machine_identifier.failure
agent.refresh_token	Agent refreshed token	agent.refresh_token.success	agent.refresh_token.failure
agent.request_policy	Success or Failure to apply policy on VEN	agent.request_policy.success	agent.request_policy.failure
agent.service_not_available	Agent reported a service not running	agent.service_not_available.success	agent.service_not_available.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
agent.suspend	Agent suspended	agent.suspend.success	agent.suspend.failure
agent.tampering	Agent firewall tampered	agent.tampering.success	agent.tampering.failure
agent.unsuspend	Agent unsuspended	agent.unsuspend.success	agent.unsuspend.failure
agent.update	Agent properties updated	agent.update.success	agent.update.failure
agent.update_interactive_users	Agent interactive users updated	agent.update_interactive_users.success	agent.update_interactive_users.failure
agent.update_iptables_href	Agent updated existing iptables href	agent.update_iptables_href.success	agent.update_iptables_href.failure
agent.upload_existing_ip_table_rules	Agent existing IP tables uploaded	agent.upload_existing_ip_table_rules.success	agent.upload_existing_ip_table_rules.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
agent.upload_support_report	Agent support report uploaded	agent.upload_support_report.success	agent.upload_support_report.failure
agent_support_report_request.create	Agent support report request created	agent_support_report_request.create.success	agent_support_report_request.create.failure
agent_support_report_request.delete	Agent support report request deleted	agent_support_report_request.delete.success	agent_support_report_request.delete.failure
agent_support_report_request.update	Agent support report request updated	agent_support_report_request.update.success	agent_support_report_request.update.failure
api_key.create	API key created	api_key.create.success	api_key.create.failure
api_key.delete	API key deleted	api_key.delete.success	api_key.delete.failure
api_key.update	API key updated	api_key.update.success	api_key.update.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
auth_security_principal.create	RBAC auth security principal created	auth_security_principal.create.success	auth_security_principal.create.failure
auth_security_principal.delete	RBAC auth security principal deleted	auth_security_principal.delete.success	auth_security_principal.delete.failure
auth_security_principal.update	RBAC auth security principal updated	auth_security_principal.update.success	auth_security_principal.update.failure
authentication_settings.update	Authentication settings updated	authentication_settings.update.success	authentication_settings.update.failure
cluster.create	PCE cluster created	cluster.create.success	cluster.create.failure
cluster.delete	PCE cluster deleted	cluster.delete.success	cluster.delete.failure
cluster.update	PCE cluster updated	cluster.update.success	cluster.update.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
container_workload.update	Container workload updated	container_workload.update.success	container_workload.update.failure
domain.create	Domain created	domain.create.success	domain.create.failure
domain.delete	Domain deleted	domain.delete.success	domain.delete.failure
domain.update	Domain updated	domain.update.success	domain.update.failure
event_settings.update	Event settings updated	event_settings.update.success	event_settings.update.failure
firewall_settings.update	Global policy settings updated	firewall_settings.update.success	firewall_settings.update.failure
ip_list.create	IP list created	ip_list.create.success	ip_list.create.failure
ip_list.delete	IP list deleted	ip_list.delete.success	ip_list.delete.failure
ip_list.update	IP list updated	ip_list.update.success	ip_list.update.failure
ip_lists.delete	IP lists deleted	ip_lists.delete.success	ip_lists.delete.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
ip_tables_rule.create	IP tables rules created	ip_tables_rule.create.success	ip_tables_rule.create.failure
ip_tables_rule.delete	IP tables rules deleted	ip_tables_rule.delete.success	ip_tables_rule.delete.failure
ip_tables_rule.update	IP tables rules updated	ip_tables_rule.update.success	ip_tables_rule.update.failure
label.create	Label created	label.create.success	label.create.failure
label.delete	Label deleted	label.delete.success	label.delete.failure
label.update	Label updated	label.update.success	label.update.failure
label_group.create	Label group created	label_group.create.success	label_group.create.failure
label_group.delete	Label group deleted	label_group.delete.success	label_group.delete.failure
label_group.update	Label group updated	label_group.update.success	label_group.update.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
labels.delete	Labels deleted	labels.delete.success	labels.delete.failure
license.delete	License deleted	license.delete.success	license.delete.failure
license.update	License updated	license.update.success	license.update.failure
lost_agent.found	Lost_agent.found	lost_agent.found.success	lost_agent.found.failure
network.create	Network created	network.create.success	network.create.failure
network.delete	Network deleted	network.delete.success	network.delete.failure
network.update	Network updated	network.update.success	network.update.failure
nfc.activate	Network function controller created	nfc.activate.success	nfc.activate.failure
nfc.delete	Network function controller deleted	nfc.delete.success	nfc.delete.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
nfc.update_discovered_virtual_servers	Network function controller virtual servers discovered	nfc.update_discovered_virtual_servers.success	nfc.update_discovered_virtual_servers.failure
nfc.update_policy_status	Network function controller policy status	nfc.update_policy_status.success	nfc.update_policy_status.failure
nfc.update_slb_state	Network function controller SLB state updated	nfc.update_slb_state.success	nfc.update_slb_state.failure
org.create	Organization created	org.create.success	org.create.failure
org.recalc_rules	Rules for organization recalculated	org.recalc_rules.success	org.recalc_rules.failure
org.update	Organization information updated	org.update.success	org.update.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
pairing_profile.create	Pairing profile created	pairing_profile.create.success	pairing_profile.create.failure
pairing_profile.create_pairing_key	Pairing profile pairing key created	pairing_profile.create_pairing_key.success	pairing_profile.create_pairing_key.failure
pairing_profile.delete	Pairing profile deleted	pairing_profile.delete.success	pairing_profile.delete.failure
pairing_profile.update	Pairing profile updated	pairing_profile.update.success	pairing_profile.update.failure
pairing_profiles.delete	Pairing profiles deleted	pairing_profiles.delete.success	pairing_profiles.delete.failure
password_policy.create	Password policy created	password_policy.create.success	password_policy.create.failure
password_policy.delete	Password policy deleted	password_policy.delete.success	password_policy.delete.failure
password_policy.update	Password policy updated	password_policy.update.success	password_policy.update.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
pce.application_started	PCE application started	pce.application_started.success	pce.application_started.failure
pce.application_stopped	PCE application stopped	pce.application_stopped.success	pce.application_stopped.failure
permission.create	RBAC permission created	permission.create.success	permission.create.failure
permission.delete	RBAC permission deleted	permission.delete.success	permission.delete.failure
permission.update	RBAC permission updated	permission.update.success	permission.update.failure
radius.auth_challenge	RADIUS auth challenge issued	radius.auth_challenge.success	radius.auth_challenge.failure
radius_config.create	RADIUS configurations created	radius_config.create.success	radius_config.create.failure
radius_config.delete	RADIUS configurations deleted	radius_config.delete.success	radius_config.delete.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
radius_config.update	RADIUS configurations updated	radius_config.update.success	radius_config.update.failure
radius_config.verify_shared_secret	RADIUS config shared secret verified	radius_config.verify_shared_secret.success	radius_config.verify_shared_secret.failure
remote_syslog.reachable	Remote syslog destination reachable	remote_syslog.reachable.success	remote_syslog.reachable.failure
remote_syslog.unreachable	Remote syslog destination not reachable	remote_syslog.unreachable.success	remote_syslog.unreachable.failure
request.authentication_failed	API request authentication failed	request.authentication_failed.success	request.authentication_failed.failure
request.authorization_failed	API request authorization failed	request.authorization_failed.success	request.authorization_failed.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
request.internal_server_error	API request failed due to internal server error	request.internal_server_error.success	request.internal_server_error.failure
request.service_unavailable	API request failed due to unavailable service	request.service_unavailable.success	request.service_unavailable.failure
request.unknown_server_error	API request failed due to unknown server error	request.unknown_server_error.success	request.unknown_server_error.failure
resource.create	Login resource created	resource.create.success	resource.create.failure
resource.delete	Login resource deleted	resource.delete.success	resource.delete.failure
resource.update	Login resource updated	resource.update.success	resource.update.failure
rule_set.create	Rule set created	rule_set.create.success	rule_set.create.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
rule_set.delete	Rule set deleted	rule_set.delete.success	rule_set.delete.failure
rule_set.update	Rule set updated	rule_set.update.success	rule_set.update.failure
rule_sets.delete	Rule sets deleted	rule_sets.delete.success	rule_sets.delete.failure
saml_acs.update	SAML assertion consumer services updated	saml_acs.update.success	saml_acs.update.failure
saml_config.create	SAML configuration created	saml_config.create.success	saml_config.create.failure
saml_config.delete	SAML configuration deleted	saml_config.delete.success	saml_config.delete.failure
saml_config.update	SAML configuration updated	saml_config.update.success	saml_config.update.failure
saml_sp_config.create	SAML Service Provider created	saml_sp_config.create.success	saml_sp_config.create.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
saml_sp_config.delete	SAML Service Provider deleted	saml_sp_config.delete.success	saml_sp_config.delete.failure
saml_sp_config.update	SAML Service Provider updated	saml_sp_config.update.success	saml_sp_config.update.failure
sec_policy.create	Security policy created	sec_policy.create.success	sec_policy.create.failure
sec_policy_pending.delete	Pending security policy deleted	sec_policy_pending.delete.success	sec_policy_pending.delete.failure
sec_rule.create	Security policy rules created	sec_rule.create.success	sec_rule.create.failure
sec_rule.delete	Security policy rules deleted	sec_rule.delete.success	sec_rule.delete.failure
sec_rule.update	Security policy rules updated	sec_rule.update.success	sec_rule.update.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
secure_connect_gateway.create	SecureConnect gateway created	secure_connect_gateway.create.success	secure_connect_gateway.create.failure
secure_connect_gateway.delete	SecureConnect gateway deleted	secure_connect_gateway.delete.success	secure_connect_gateway.delete.failure
secure_connect_gateway.update	SecureConnect gateway updated	secure_connect_gateway.update.success	secure_connect_gateway.update.failure
security_principal.create	RBAC security principal created	security_principal.create.success	security_principal.create.failure
security_principal.delete	RBAC security principal bulk deleted	security_principal.delete.success	security_principal.delete.failure
security_principal.update	RBAC security principal bulk updated	security_principal.update.success	security_principal.update.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
security_principals.bulk_create	RBAC security principals bulk created	security_principals.bulk_create.success	security_principals.bulk_create.failure
service.create	Service created	service.create.success	service.create.failure
service.delete	Service deleted	service.delete.success	service.delete.failure
service.update	Service updated	service.update.success	service.update.failure
service_binding.create	Service binding created	service_binding.create.success	service_binding.create.failure
service_binding.delete	Service binding created	service_binding.delete.success	service_binding.delete.failure
service_bindings.delete	Service binding deleted	service_bindings.delete.success	service_bindings.delete.failure
service.create	Service created	service.create.success	service.create.failure
service.delete	Service deleted	services.delete.success	services.delete.failure
service.updated	Service updated	service.update.success	service.update.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
slb.create	Server load balancer created	slb.create.success	slb.create.failure
slb.delete	Server load balancer deleted	slb.delete.success	slb.delete.failure
slb.update	Server load balancer updated	slb.update.success	slb.update.failure
syslog_destination.create	syslog remote destination created	syslog_destination.create.success	syslog_destination.create.failure
syslog_destination.delete	syslog remote destination deleted	syslog_destination.delete.success	syslog_destination.delete.failure
syslog_destination.update	syslog remote destination updated	syslog_destination.update.success	syslog_destination.update.failure
system_admin.create	System administrator created	system_admin.create.success	system_admin.create.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
system_admin.delete	System administrator deleted	system_admin.delete.success	system_admin.delete.failure
system_management.apply_ssl_certs	SSL/TLS certificates applied	system_management.apply_ssl_certs.success	system_management.apply_ssl_certs.failure
system_management.create_support_report_request	Creation of support report requested	system_management.create_support_report_request.success	system_management.create_support_report_request.failure
system_management.delete_network_interface	PCE system network interface deleted	system_management.delete_network_interface.success	system_management.delete_network_interface.failure
system_management.delete_software	PCE software deleted	system_management.delete_software.success	system_management.delete_software.failure
system_management.discard_ssl_certs	PCE system SSL/TLS certificates discarded	system_management.discard_ssl_certs.success	system_management.discard_ssl_certs.failure
system_management.restart_network_interfaces	PCE system network interfaces restarted	system_management.restart_network_interfaces.success	system_management.restart_network_interfaces.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
system_management.restart_system	PCE system restarted	system_management.restart_system.success	system_management.restart_system.failure
system_management.revert_network_interfaces	PCE network interfaces reverted	system_management.revert_network_interfaces.success	system_management.revert_network_interfaces.failure
system_management.shutdown_system	PCE system shutdown	system_management.shutdown_system.success	system_management.shutdown_system.failure
system_management.test_email	PCE system email tested	system_management.test_email.success	system_management.test_email.failure
system_management.update_console_password	PCE system web console password updated	system_management.update_console_password.success	system_management.update_console_password.failure
system_management.update_email_config	PCE system web email configuration updated	system_management.update_email_config.success	system_management.update_email_config.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
system_management.update_fluentd_config	PCE system fluentd component configuration updated	system_management.update_fluentd_config.success	system_management.update_fluentd_config.failure
system_management.update_network_interface	PCE system network interface updated	system_management.update_network_interface.success	system_management.update_network_interface.failure
system_management.update_syslog_config	PCE syslog configuration update	system_management.update_syslog_config.success	system_management.update_syslog_config.failure
system_management.update_system_config	PCE system configuration updated	system_management.update_system_config.success	system_management.update_system_config.failure
system_management.upgrade_software	PCE system software upgraded	system_management.upgrade_software.success	system_management.upgrade_software.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
system_management.upload_ssl_certs	PCE system SSL/TLS certificates uploaded	system_management.upload_ssl_certs.success	system_management.upload_ssl_certs.failure
system_management.verify_software	PCE system software verified	system_management.verify_software.success	system_management.verify_software.failure
system_task.agent_missed_heartbeats_check	Agent missed heartbeats	system_task.agent_missed_heartbeats_check.success	system_task.agent_missed_heartbeats_check.failure
system_task.agent_offline_check	Agents marked offline	system_task.agent_offline_check.success	system_task.agent_offline_check.failure
system_task.prune_old_log_events	Event pruning completed	system_task.prune_old_log_events.success	system_task.prune_old_log_events.failure
tls_channel.establish	TLS channel established	tls_channel.establish.success	tls_channel.establish.failure
tls_channel.terminate	TLS channel terminated	tls_channel.terminate.success	tls_channel.terminate.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
user.accept_invitation	User invitation accepted	user.accept_invitation.success	user.accept_invitation.failure
user.authenticate	User authenticated	user.authenticate.success	user.authenticate.failure
user.create	User created	user.create.success	user.create.failure
user.delete	User deleted	user.delete.success	user.delete.failure
user.invite	User invited	user.invite.success	user.invite.failure
user.login	User logged in	user.login.success	user.login.failure
user.login_session_terminated	User login session terminated	user.login_session_terminated.success	user.login_session_terminated.failure
user.logout	User logged	user.logout.success	user.logout.failure
user.pce_session_terminated	User session terminated	user.pce_session_terminated.success	user.pce_session_terminated.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
user.reset_password	User password reset	user.reset_password.success	user.reset_password.failure
user.sign_in	User session created	user.sign_in.success	user.sign_in.failure
user.sign_out	User session terminated	user.sign_out.success	user.sign_out.failure
user.update	User information updated	user.update.success	user.update.failure
user.update_password	User password updated	user.update_password.success	user.update_password.failure
user.use_expired_password	User entered expired password	user.use_expired_password.success	user.use_expired_password.failure
user_local_profile.create	User local profile created	user_local_profile.create.success	user_local_profile.create.failure
user_local_profile.delete	User local profile deleted	user_local_profile.delete.success	user_local_profile.delete.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
user_local_profile.reinvite	User local profile reinvited	user_local_profile.reinvite.success	user_local_profile.reinvite.failure
user_local_profile.update_password	User local password updated	user_local_profile.update_password.success	user_local_profile.update_password.failure
ven_software.upgrade	VEN software release upgraded	ven_software.upgrade.success	ven_software.upgrade.failure
ven_software_release.create	VEN software release created	ven_software_release.create.success	ven_software_release.create.failure
ven_software_release.delete	VEN software release deleted	ven_software_release.delete.success	ven_software_release.delete.failure
ven_software_release.deploy	VEN software release deployed	ven_software_release.deploy.success	ven_software_release.deploy.failure
ven_software_release.update	VEN software release updated	ven_software_release.update.success	ven_software_release.update.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
virtual_server.create	Virtual server created	virtual_server.create.success	virtual_server.create.failure
virtual_server.delete	Virtual server created	virtual_server.delete.success	virtual_server.delete.failure
virtual_server.update	Virtual server updated	virtual_server.update.success	virtual_server.update.failure
virtual_service.create	Virtual service created	virtual_service.create.success	virtual_service.create.failure
virtual_service.delete	Virtual service deleted	virtual_service.delete.success	virtual_service.delete.failure
virtual_service.update	Virtual service updated	virtual_service.update.success	virtual_service.update.failure
virtual_services.bulk_create	Virtual services created in bulk	virtual_services.bulk_create.success	virtual_services.bulk_create.failure
virtual_services.bulk_update	Virtual services updated in bulk	virtual_services.bulk_update.success	virtual_services.bulk_update.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
vulnerability.delete	Vulnerability deleted	vulnerability.delete.success	vulnerability.delete.failure
vulnerability.update	Vulnerability updated	vulnerability.update.success	vulnerability.update.failure
vulnerability_report.delete	Vulnerability report deleted	vulnerability_report.delete.success	vulnerability_report.delete.failure
vulnerability_report.update	Vulnerability report updated	vulnerability_report.update.success	vulnerability_report.update.failure
workload.create	Workload created	workload.create.success	workload.create.failure
workload.delete	Workload deleted	workload.delete.success	workload.delete.failure
workload.online	Workload online	workload.online.success	workload.online.failure
workload.recalc_rules	Workload policy recalculated	workload.recalc_rules.success	workload.recalc_rules.failure
workload.redetect_network	Workload network redetected	workload.redetect_network.success	workload.redetect_network.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
workload.soft_delete	Workload soft-deleted	workload.soft_delete.success	workload.soft_delete.failure
workload.undelete	Workload undeleted	workload.undelete.success	workload.undelete.failure
workload.update	Workload settings updated	workload.update.success	workload.update.failure
workload.upgrade	Workload upgraded	workload.upgrade.success	workload.upgrade.failure
workload_interface.create	Workload interface created	workload_interface.create.success	workload_interface.create.failure
workload_interface.delete	Workload interface deleted	workload_interface.delete.success	workload_interface.delete.failure
workload_interface.update	Workload interface updated	workload_interface.update.success	workload_interface.update.failure
workload_interfaces.update	Workload interfaces updated	workload_interfaces.update.success	workload_interfaces.update.failure
workload_service_report.update	Workload service report updated	workload_service_report.update.success	workload_service_report.update.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
workload_settings.update	Workload settings updated	workload_settings.update.success	workload_settings.update.failure
workloads.apply_policy	Workloads policies applied	workloads.apply_policy.success	workloads.apply_policy.failure
workloads.bulk_create	Workloads created in bulk	workloads.bulk_create.success	workloads.bulk_create.failure
workloads.bulk_delete	Workloads deleted in bulk	workloads.bulk_delete.success	workloads.bulk_delete.failure
workloads.bulk_update	Workloads updated in bulk	workloads.bulk_update.success	workloads.bulk_update.failure
workloads.remove_labels	Workloads labels removed	workloads.remove_labels.success	workloads.remove_labels.failure
workloads.set_flow_reporting_frequency	Workload flow reporting frequency changed	workloads.set_flow_reporting_frequency.success	workloads.set_flow_reporting_frequency.failure
workloads.set_labels	Workload labels applied	workloads.set_labels.success	workloads.set_labels.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
workloads.unpair	Workloads unpaired	workloads.unpair.success	workloads.unpair.failure
workloads.update	Workloads updated	workloads.update.success	workloads.update.failure

Name Changes of Event Types between Illumio ASP versions 18.1.0 and 18.2.1

Old event type from version 18.1 and earlier (Organization Events)	New event_type from 18.2.1 and later	Notes on new event type
activation_failure	agent.activate	With status "failure".
activation_success	agent.activate	With status "success".
agent_processes_down	agent.update with notification type agent.process_failed	Potentially can occur from multiple event_types.
agent_processes_up	agent.update with notification type agent.process_failed	Potentially can occur from multiple event_types.
api_key_created	api_key.create	
api_key_deleted	api_key.delete	
application_restarted	pce.application_stopped and pce.application_started	
application_started	pce.application_started	
application_stopped	pce.application_stopped	
authn_failure	request.authentication_failed	401 response.
authz_csrf_validation_failure	request.authentication_failed	

Old event type from version 18.1 and earlier (Organization Events)	New event_type from 18.2.1 and later	Notes on new event type
authz_failure	request.authorization_failed	403 response
dev_alert		Removed.
fw_tampering_revert_failure	agent.tampering	With notification workload.oob_policy_changes (revert_succeeded "false").
fw_tampering_reverted	agent.tampering	With notification workload.oob_policy_changes (revert_succeeded "true")
hard_limit_exceeded		Any event that creates resources with object limits (mostly POST/PUT API events) contains a notification: hard_limit.exceeded
pairing_key_created	pairing_profile.create_pairing_key	
pairing_profile_created	pairing_profile.create	
pairing_profile_deleted	pairing_profile.delete	
pairing_profile_modified	pairing_profile.update	
policy_deploy_failed	agent.update	Any event where an agent is updated
policy_deploy_succeeded	agent.update	Any event where an agent is updated
policy_provisioned	sec_policy.create	
refresh_token_failure	agent.refresh_token	With status "failure"
refresh_token_success	agent.refresh_token	With status "success"
server_added	agent.activate	With status "success"
server_already_unsuspended	agent.unsuspend	With status "failure", 406 response code, and already_unsuspended error message
server_clone_detected	agent.clone_detected	

Old event type from version 18.1 and earlier (Organization Events)	New event_type from 18.2.1 and later	Notes on new event type
server_cloned	agent.activate_clone	
server_delete_initiated	workload.unpair, agent.deactivate	
server_deleted	workload.unpair, agent.deactivate	
server_ip_change	workload_interface.update	Any event where workload_interfaces are updated
server_label_added	workload.update	With other events that correspond with adding workload_labels, such as workload.set_labels, workload.remove_labels, workload.bulk_update, workload.create, and workload.bulk_create
server_label_removed	workload.update	With other events that correspond with removing workload_labels, such as workload.set_labels, workload.remove_labels, workload.bulk_update.
server_offline	system_task.agent_offline_check	
server_online	workload.online	
server_oob_policy_changes	agent.tampering	With notification workload.oob_policy_changes (revert_succeeded "true")
server_oob_policy_changes_revert_failed	agent.tampering	With notification workload.oob_policy_changes (revert_succeeded "false").
server_pairing_failed	agent.activate	With status "failure".
server_state_change	workload.update	Whenever workload is updated to change any of the following attributes: mode, log_traffic, visibility_level.

Old event type from version 18.1 and earlier (Organization Events)	New event_type from 18.2.1 and later	Notes on new event type
server_suspended	agent.suspend	With status "success".
server_unreachable		system_task.agent_missed_heartbeats_check
server_unsuspended	agent.unsuspend	With status "success".
service_not_available	agent.service_not_available	
soft_limit_exceeded		Any event that creates resources with object limits (mostly POST/PUT API events) contains a notification: soft_limit.exceeded.
unpaired_server_detected	lost_agent.found	
user_admin_locked	user.update	Occurs whenever user is updated to be locked.
user_login	user.login	user.login or user.sign_in with status "success".
user_login_failed	user.login	user.login or user.sign_in with status "failure".
user_login_failure_count_exceeded	user.login with notification: user.login_failure_count_exceeded	
user_logout	user.logout	user.logout or user.sign_out.
user_permission_added	permission.create	Occurs whenever a permission is created.
user_permission_changed	permission.update	Occurs whenever a permission is updated.
user_permission_removed	permission.delete	Occurs whenever a permission is removed.
user_pw_reset_complete	user.update with user.pw_reset_completed notification	

Old event type from version 18.1 and earlier (Organization Events)	New event_type from 18.2.1 and later	Notes on new event type
user_pw_reset_request	user.reset_password	
user_unlocked	user.update	Occurs whenever user is updated to be unlocked.
workload_created	workload.create	Any event where a workload is created, for example workloads.bulk_create and on pairing (agent.activate).
workload_deleted	workload.delete	
workload_undeleted	workload.undelete	
workload_update_mismatched_interfaces		Any of the following events with workload.update_mismatched_interfaces notification: workload.create, workload.update, agent.activate, workload_interfaces.update, workloads.bulk_update.

Revision History

Illumio Adaptive Security Platform ASP Auditable Events and SIEM Integration Guide

Document ID: 80000-100-18.2.1

Date	Description
2019-01-23	Updated for Illumio Adaptive Security Platform version 18.2.1: • Event type names have been updated for clarity and consistency. • The `sec_policy.create` includes the href of the policy that is created. This href can be used to obtain by an alerting system to obtain more information about the policy change. • Optionally in `runtime_env.yml`, you can enable startup and shutdown events of the Policy Compute Engine (PCE). These are events `pce.application_started` and `pce.application.stopped`. Optionally in `runtime_env.yml`, established and dropped connections to remote syslog servers can be recorded as the events `remote_syslog.reachable` and `remote_syslog.unreachable`. • Included mapping of old organization events to new auditable events.
2018-09-06	• General availability release of Auditable Events with Illumio Adaptive Security Platform version 18.2. Formerly titled "SIEM Integration", which material is now included in this guide. • Start of revision history.