Illumio® Adaptive Security Platform® 18.2 Auditable Events and SIEM Integration Guide

09/06/2018

Table of Contents

Product Version

Illumio Adaptive Security Platform PCE Version: 18.2.0 (Standard release)
Illumio Adaptive Security Platform VEN Version: 18.2.0 (Standard release)

About Illumio

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

Illumio Professional Services for Deployment

To ensure optimal deployment of the Illumio Adaptive Security Platform you should work with Illumio Professional Services. Contact your Illumio representative.

Preview Features Only for Evaluation Before General Availability

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

> ⚠ **Do not deploy preview features in a production environment**
> Be sure to install these preview features only on a non-production system. To avoid inadvertently impacting your current operations, do not install the preview features on production systems. The purpose of preview features is to 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** tabs.

Illumio Adaptive Security Platform Support

If you cannot find what you are looking for in this document or the 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.
- *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) Supercluster Reference Implementation*: comparing designs of network architectures for the PCE Supercluster with the F5 Global Traffic Manager (GTM).
- *Policy Compute Engine (PCE) REST API Guide*: web-programming Illumio® Adaptive Security Platform®.
- *Policy Compute Engine (PCE) Advanced Command-line Tool Guide*: using the CLI tool on your own local computer for management of PCE resource objects, including importing vulnerability data for analysis in Illumination®.
- *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 a nalytics 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
  ...
  ```
- Section titles in this guide are in double quotation marks. Example: See "Basic Theory of Operation".
- Reference to other guides n the Illumio library are *italicized*. Example: See the *PCE Web Console User Guide*.

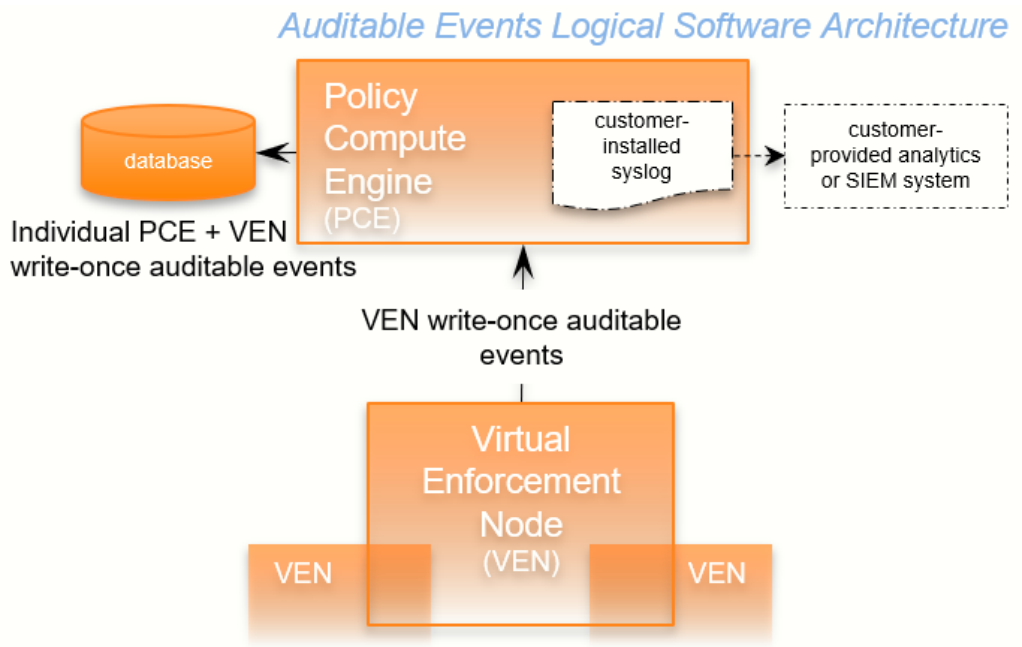
How To Use This Guide

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 standard for auditing.

Benefits of Auditable Events Framework and Problems It Solves

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

Take Action to Move to New Auditable Events

Old events continue to be generated and streamed in 18.2.0. However, be aware of the following planned changes.

Old events are no longer available via API or the PCE web console and will be removed completely in the next release. The old API does not send any new events in the old event format but the old events will continue to be streamed over syslog. In addition, the old API returns events only if they saved to the database. Old events saved to the database will be removed as they age over 90 days and will then no longer be available via the API.

If you have alerts based on old events sent to syslog, you should migrate to the new event types.

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.

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

VEN Events not shown in PCE Web Console	
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	

Possible Future Changes

This release of Auditable Events is public experimental. The release and the events are designed with the goal of getting early feedback from the Illumio customer community about API desirability and design before the product general availability. As a result of your feedback, the information in this guide and the auditable events themselves might change in a future release. Illumio encourages your feedback, comments, suggestions, and ideas. To send feedback, contact Illumio Customer Support.

Will Not Change in Future Releases	Might Change in Future Releases
Events in release 18.2.0 will not be removed.	New events might be added.
Fields inside events for release 18.2.0 will not be removed.	New fields inside events might be added.
	Values of fields (such as event_type) will change. Note: 20% to 40% of events types will change in release 18.2.1.

General Auditing Needs Satisfied by the Auditable Events Framework

Need	Description	See...
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.	Resource update before and after values
Security	Evidence to show which changes failed, such as incorrect user permissions or failed authentication.	User authentication failure for security audit

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"

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.

Type of information	Description

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.

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®.

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, 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 is estimated as an average 1,500 bytes per event. Thus, 25 million events requires approximately 38GB of disk.

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 in PCE Web Console

Use the PCE web console to change event-related settings:

- Event severity level.
- Event data retention.
- Event message format.

Set Event Severity Level

Set the severity level of events to record. Only messages at this level are recorded.

- Error.
- Warning.
- Informational (default).

To change the event severity level:

1. Log into the PCE web console.
2. Navigate to **Settings > Events**.
3. Click **Edit**.
4. For **Event Severity**, select from the following:
    - Error
    - Warning
    - Informational (default)
5. Click **Save**.

Set Event Data Retention

By default, the system retains event records for 90 days.

Acceptable values are 1 day to 200 days.

To set the default retention setting:

1. Log into the PCE web console.
2. Navigate to **Settings > Events**.
3. Click **Edit**.
4. In **Retention Period**, enter the number of days you want to retain data.
5. Click **Save**.

Set Desired syslog Message Format -- JSON, CEF, or LEEF

Set the message output to one of the following formats. This 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), default.
- Common Event Format (CEF).
- Log Event Extended Format (LEEF).

To set the event output format:

1. Log into the PCE web console.
2. Navigate to **Settings > Events**.
3. Click **Edit**.
4. For **Event Format**, select JSON, CEF or LEEF.

5. Click **Save**.

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

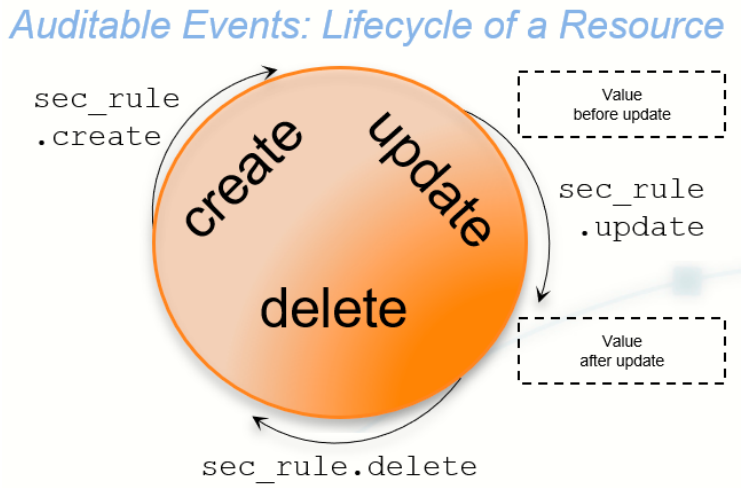
The following unanticipated occurrences on the PCE cannot be recorded as auditable events:

- 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.

Preview – PCE internal syslog

This release of the Illumio Adaptive Security Platform comes with a preview: the PCE internal syslog. The PCE internal syslog is to help companies implement syslog without having to install it themselves.

For documentation for the PCE internal syslog preview, contact Illumio Customer Support.

Auditable Events Syslog Message Size – 8K Bytes

Ensure that your syslog configuration is set for 8K message size. The PCE ensures that the size of an auditable event record does not exceed 8K bytes. However, many implementations of syslog have a default message size of 4K bytes.

Messages are usually less than 8K but any data that exceeds 8K is truncated.

Changing the receiving end's syslog message size depends on your implementation of syslog. Consult your vendor documentation for details.

Secure Syslog Data Transport and Storage

Enabling Transport Layer Security (TLS) with the syslog protocol allows you to secure the communication to your syslog service with public CA certificates or with TLS certificates from your own CA.

On the remote syslog server, you should ensure restricted access to the data by relying on the OS-level user access mechanisms. In addition, you should limit the number of users allowed access to the syslog storage itself. If possible, rely on an enterprise-class log management system for post-processing the event data.

Templates for rsyslog and syslog-ng, with Log Rotation and Regular Expressions

The PCE comes with syslog templates for transporting JSON, CEF, and LEEF-formatted data to your SIEM system. The templates include guidance for configuring audit log forward JSON, CEF, LEEF.

The syslog templates are delivered with the PCE in the following directory:

```
install_root/Illumio/config/templates
```

Included are templates for rsyslog, syslog-ng, a template for log rotation, and an example of the parameters for syslog in the `runtime_env.yml` file.

Exporting Traffic Summaries to Syslog

Configuring Export of Traffic Summaries

To enable traffic flow summary export to syslog, you must configure the PCE `runtime_env.yml` parameter `export_flow_summaries_to_syslog` and specify the type of flow summaries to include: allowed, blocked, or potentially blocked.

The `export_flow_summaries_to_syslog` parameter is public experimental.

For example, to export traffic summaries for allowed, potentially blocked and/or blocked flow summaries, edit the following parameter in your PCE `runtime_env.yml` file:

```
export_flow_summaries_to_syslog:
 - accepted
 - potentially_blocked
 - blocked
```

If you remove one of the options, that type of flow information is not logged.

Specifying Traffic Summary syslog Export Format

By default, the PCE exports traffic summaries JSON. To export traffic summaries in either CEF or LEEF formats, configure the following PCE `runtime_env.yml` parameter:

`syslog_event_export_format: cef` or `leef`

You can only specify only one export format.

If you specify CEF or LEEF, you continue also receive auditable events in JSON.

VEN Traffic Summaries

Once a Workload gets a VEN installed and is paired with the PCE, the VEN observes 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 be present:

1. timestamp
2. source hostname
3. source href
4. source labels
5. destinatin hostname
6. destination href
7. destination labels
8. program name
9. user name
10. service name
11. total bytes in
12. 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

Notes on Specific Event Resources

- The comment column shows **General** for some event types. These events types are useful for general auditing. Other event types without this comment are more specific, some of which are particular to the Illumio Adaptive Security Platform.
- Event types matching the pattern `agent.*` are triggered by a VEN.
- Resources categorized as `local_profile.*` relate to the database of user information maintained on the PCE itself, rather than an external-to-the-PCE database.
- Resources categorized as `api_key.*` and `request.*` represent resources related to the Illumio Adaptive Security Platform REST API.

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
`admin.recalc_rules`	Admin forced recalculation of policy	`admin.recalc_rules.success`	`admin.recalc_rules.failure`
`compatibility_report.update`	Agent compatibility check report updated	`compatibility_report.update.success`	`compatibility_report.update.failure`
`interface_status.update`	Agent interfaces updated	`interface_status.update.success`	`interface_status.update.failure`
`service_report.create`	Agent service report updated	`service_report.create.success`	`service_report.create.failure`
`agent_support_report_request.create`	Agent support report request created	`agent_support_report_request.create.success`	`agent_support_report_request.create.failure`

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
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
agent.activate	Agent paired	agent.activate.success	agent.activate.failure
agent.activate_clone	Agent clone activated	agent.activate_clone.success	agent.activate_clone.failure
agent.deactivate	Agent unpaired	agent.deactivate.success	agent.deactivate.failure
agent.dev_alert_logs	Agent uploaded dev-alert logs	agent.dev_alert_logs.success	agent.dev_alert_logs.failure
agent.firewall_config	Agent fetched policy	agent.firewall_config.success	agent.firewall_config.failure
agent.goodbye	Workload shutdown	agent.goodbye.success	agent.goodbye.failure
agent.interactive_users	Agent interactive users updated	agent.interactive_users.success	agent.interactive_users.failure
agent.machine_identifier	Agent machine identifiers updated	agent.machine_identifier.success	agent.machine_identifier.failure
agent.ops_alert_logs	Agent uploaded ops-alert logs”	agent.ops_alert_logs.success	agent.ops_alert_logs.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
agent.put_from_agent	Success or Failure to apply policy on VEN	agent.put_from_agent.success	agent.put_from_agent.failure
agent.refresh_token	Agent refreshed token	agent.refresh_token.success	agent.refresh_token.failure
agent.service_not_available	Agent reported a service not running	agent.service_not_available.success	agent.service_not_available.failure
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_iptables_href	Agent updated existing iptables href	agent.update_iptables_href.success	agent.update_iptables_href.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.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_setting.update	Authentication settings updated	authentication_setting.update.success	authentication_setting.update.failure
blocked_traffic.delete	Blocked traffic event deleted	blocked_traffic.delete.success	blocked_traffic.delete.failure
cluster.create	Cluster created	cluster.create.success	cluster.create.failure
cluster.delete	Cluster deleted	cluster.delete.success	cluster.delete.failure
cluster.update	Cluster updated	cluster.update.success	cluster.update.failure
container_workload.update	Container workload updated	container_workload.update.success	container_workload.update.failure
destination.create	Syslog destination created	destination.create.success	destination.create.failure
destination.delete	Syslog destination deleted	destination.delete.success	destination.delete.failure
destination.update	Syslog destination updated	destination.update.success	destination.update.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
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
firewall_setting.update	Global policy settings updated	firewall_setting.update.success	firewall_setting.update.failure
ignored_interface.update	Ignored interfaces list updated	ignored_interface.update.success	ignored_interface.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_tables_rule.create	IP tables rules created	ip_tables_rule.create.success	ip_tables_rule.create.failure
ip_tables_rule.delete	IP tables rule delete	ip_tables_rule.delete.success	ip_tables_rule.delete.failure
ip_tables_rule.update	IP tables rule updated	ip_tables_rule.update.success	ip_tables_rule.update.failure
label_group.create	Label group created	label_group.create.success	label_group.create.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
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
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
license.delete	License deleted	license.delete.success	license.delete.failure
license.update	License updated	license.update.success	license.update.failure
local_profile.create	Local user profile created	local_profile.create.success	local_profile.create.failure
local_profile.delete	Local user profile deleted	local_profile.delete.success	local_profile.delete.failure
local_profile.password	Local user password changed	local_profile.password.success	local_profile.password.failure
local_profile.reinvite	Local user reinvited	local_profile.reinvite.success	local_profile.reinvite.failure
login_proxy_auth_setting.update	Authentication settings updated	login_proxy_auth_setting.update.success	login_proxy_auth_setting.update.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
login_proxy_password_policy.update	Password policy updated	login_proxy_password_policy.update.success	login_proxy_password_policy.update.failure
login_proxy_radius_config.create	RADIUS configurations created	login_proxy_radius_config.create.success	login_proxy_radius_config.create.failure
login_proxy_radius_config.delete	RADIUS configuration deleted	login_proxy_radius_config.delete.success	login_proxy_radius_config.delete.failure
login_proxy_radius_config.update	RADIUS configuration updated	login_proxy_radius_config.update.success	login_proxy_radius_config.update.failure
login_proxy_radius_config.verify_shared_secret	RADIUS config shared secret verified	login_proxy_radius_config.verify_shared_secret.success	login_proxy_radius_config.verify_shared_secret.failure
login_proxy_saml_config.update	SAML configuration updated	login_proxy_saml_config.update.success	login_proxy_saml_config.update.failure
login_proxy_user.accept_invitation	User accepted invitation	login_proxy_user.accept_invitation.success	login_proxy_user.accept_invitation.failure
login_proxy_user.invite	User invited	login_proxy_user.invite.success	login_proxy_user.invite.failure
login_proxy_user.reset_password	User reset password	login_proxy_user.reset_password.success	login_proxy_user.reset_password.failure
login_proxy_user.update	User updated	login_proxy_user.update.success	login_proxy_user.update.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
login_user.authenticate	Local user authenticated	login_user.authenticate.success	login_user.authenticate.failure
login_user.password	Local user password changed	login_user.password.success	login_user.password.failure
lost_agent.update	Lost agent updated	lost_agent.update.success	lost_agent.update.failure
network.create	Networks 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
discovered_virtual_servers.update	Network function controller list of discovered virtual servers updated	discovered_virtual_servers.update.success	discovered_virtual_servers.update.failure
nfc.policy_status	Network function controller policy status update	nfc.policy_status.success	nfc.policy_status.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
nfc.slbs_state	Network function controller SLB state updated	nfc.slbs_state.success	nfc.slbs_state.failure
event.update	Organization setting updated	event.update.success	event.update.failure
org.update	Organization information updated	org.update.success	org.update.failure
pairing_profile.create	Pairing profile created	pairing_profile.create.success	pairing_profile.create.failure
pairing_profile.delete	Pairing profile deleted	pairing_profile.delete.success	pairing_profile.delete.failure
pairing_profile.delete	Pairing profiles deleted	pairing_profile.delete.success	pairing_profile.delete.failure
pairing_profile.pairing_key	Pairing profile pairing key generated	pairing_profile.pairing_key.success	pairing_profile.pairing_key.failure
pairing_profile.update	Pairing profile updated	pairing_profile.update.success	pairing_profile.update.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

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
password_policy.update	Password policy updated	password_policy.update.success	password_policy.update.failure
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_config.create	RADIUS configurations created	radius_config.create.success	radius_config.create.failure
radius_config.delete	RADIUS configuration deleted	radius_config.delete.success	radius_config.delete.failure
radius_config.update	RADIUS configuration 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

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
radius.auth_challenge	RADIUS auth challenge issued	radius.auth_challenge.success	radius.auth_challenge.failure
release.create	VEN release created	release.create.success	release.create.failure
release.delete	VEN release deleted	release.delete.success	release.delete.failure
release.deploy	VEN release deloyed	release.deploy.success	release.deploy.failure
release.update	VEN release updated	release.update.success	release.update.failure
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

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
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
rule_set.delete	Rule set deleted	rule_set.delete.success	rule_set.delete.failure
rule_set.projected_ves	Rule set projected vulnerability exposure score updated	rule_set.projected_ves.success	rule_set.projected_ves.failure
rule_set.update	Rule set updated	rule_set.update.success	rule_set.update.failure
running_container.update	Workload running containers updated	running_container.update.success	running_container.update.failure
running_container.update	Running container updated	running_container.update.success	running_container.update.failure
saml_acs.update	SAML assertion consumer services updated	saml_acs.update.success	saml_acs.update.failure
saml_acs.update	SAML assertion consumer service updated	saml_acs.update.success	saml_acs.update.failure
saml_config.create	SAML configuration created	saml_config.create.success	saml_config.create.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
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
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 policies created	sec_policy.create.success	sec_policy.create.failure
sec_policy.delete	Security policies deleted	sec_policy.delete.success	sec_policy.delete.failure
sec_policy.restore	Security policy restored	sec_policy.restore.success	sec_policy.restore.failure
sec_rule.create	Security policy rules created	sec_rule.create.success	sec_rule.create.failure
sec_rule.delete	Security policy rule deleted	sec_rule.delete.success	sec_rule.delete.failure
sec_rule.update	Security policy rule 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	Secure connect gateway deleted	secure_connect_gateway.create.success	secure_connect_gateway.create.failure
secure_connect_gateway.delete	Secure connect gateway updated	secure_connect_gateway.delete.success	secure_connect_gateway.delete.failure
secure_connect_gateway.update	Secure connect gateways created	secure_connect_gateway.update.success	secure_connect_gateway.update.failure
security_principal.bulk_create	RBAC security principals bulk created	security_principal.bulk_create.success	security_principal.bulk_create.failure
security_principal.create	RBAC security principals created	security_principal.create.success	security_principal.create.failure
security_principal.delete	RBAC security principal deleted	security_principal.delete.success	security_principal.delete.failure
security_principal.update	RBAC security principal updated	security_principal.update.success	security_principal.update.failure
service_binding.create	Service binding created	service_binding.create.success	service_binding.create.failure
service_binding.delete	Service binding deleted	service_binding.delete.success	service_binding.delete.failure
service.create	Service created	service.create.success	service.create.failure
service.delete	Service deleted	service.delete.success	service.delete.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
service.update	Service updated	service.update.success	service.update.failure
slb.create	Server load balancers 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
system_admin.create	System administrator deleted	system_admin.create.success	system_admin.create.failure
system_admin.delete	System administrators created	system_admin.delete.success	system_admin.delete.failure
system_task.agent_missed_heartbeats_check	Agent missed a few 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

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
tls_channel.terminate	TLS channel terminated	tls_channel.terminate.success	tls_channel.terminate.failure
upgrade.update	Upgrade started	upgrade.update.success	upgrade.update.failure
user.accept_invitation	User accepted invitation	user.accept_invitation.success	user.accept_invitation.failure
user.authentication_failed	User failed authentication	user.authentication_failed.success	user.authentication_failed.failure
user.authorization_failed	User failed authorization	user.authorization_failed.success	user.authorization_failed.failure
user.create	User created	user.create.success	user.create.failure
user.create_first_user_for_domain_from_jwt	First user created	user.create_first_user_for_domain_from_jwt.success	user.create_first_user_for_domain_from_jwt.failure
user.delete	User deleted	user.delete.success	user.delete.failure
user.login	User login	user.login.success	user.login.failure
user.logout	User logout	user.logout.success	user.logout.failure
user.logout_from_jwt	User logout from JWT	user.logout_from_jwt.success	user.logout_from_jwt.failure
user.sign_in	User session created	user.sign_in.success	user.sign_in.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
user.sign_out	User session terminated	user.sign_out.success	user.sign_out.failure
user.update	User 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 expired password used	user.use_expired_password.success	user.use_expired_password.failure
virtual_server.create	Virtual servers created	virtual_server.create.success	virtual_server.create.failure
virtual_server.delete	Virtual server deleted	virtual_server.delete.success	virtual_server.delete.failure
virtual_server.update	Virtual server updated	virtual_server.update.success	virtual_server.update.failure
virtual_service.bulk_create	Virtual Service bulk created	virtual_service.bulk_create.success	virtual_service.bulk_create.failure
virtual_service.bulk_update	Virtual Service bulk updated	virtual_service.bulk_update.success	virtual_service.bulk_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

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
virtual_service.update	Virtual Service updated	virtual_service.update.success	virtual_service.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
vulnerability.delete	Vulnerability deleted	vulnerability.delete.success	vulnerability.delete.failure
vulnerability.update	Vulnerability updated	vulnerability.update.success	vulnerability.update.failure
interface.create	Workload interfaces created	interface.create.success	interface.create.failure
interface.delete	Workload interface deleted	interface.delete.success	interface.delete.failure
interface.network	Workload interface network created	interface.network.success	interface.network.failure
workload.update	Workload settings updated	workload.update.success	workload.update.failure
workload.apply_policy	Workload apply pending policy	workload.apply_policy.success	workload.apply_policy.failure
workload.bulk_create	Workloads bulk created	workload.bulk_create.success	workload.bulk_create.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
workload.bulk_delete	Workload bulk deleted	workload.bulk_delete.success	workload.bulk_delete.failure
workload.bulk_update	Workload bulk updated	workload.bulk_update.success	workload.bulk_update.failure
workload.create	Workload created	workload.create.success	workload.create.failure
workload.delete	Workload deleted	workload.delete.success	workload.delete.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
workload.remove_labels	Workloads labels removed	workload.remove_labels.success	workload.remove_labels.failure
workload.service_reports	Workload service reports updated	workload.service_reports.success	workload.service_reports.failure
workload.set_flow_reporting_frequency	Workload flow reporting frequency changed	workload.set_flow_reporting_frequency.success	workload.set_flow_reporting_frequency.failure
workload.set_labels	Workload labels applied	workload.set_labels.success	workload.set_labels.failure
workload.soft_delete	Workload soft deleted	workload.soft_delete.success	workload.soft_delete.failure

JSON Event Type	Description	CEF/LEEF Success Event	CEF/LEEF Failure Event
workload.undelete	Workload undeleted	workload.undelete.success	workload.undelete.failure
workload.unpair	Workloads unpaired	workload.unpair.success	workload.unpair.failure
workload.update	Workload updated	workload.update.success	workload.update.failure
workload.update	Workloads updated	workload.update.success	workload.update.failure
workload.upgrade	Workload upgraded	workload.upgrade.success	workload.upgrade.failure

Deprecated – Pre-18.2 Organizational Events

With this release, the older, pre-version 18.2 form of events, known as "organizational events," is deprecated. Support for the older organization events will be discontinued in a future release.

Revision History

Illumio Adaptive Security Platform ASP Auditable Events and SIEM Integration Guide

Date	Description
2018-09-06	• General availability release of Auditable Events with Illumio Adaptive Security Platform version 18.2. • Start of revision history.