Illumio App for Splunk 3.2.0

Document History

Date	Changes
May 29, 2017	Initial draft
June 6, 2017	Added CIM information
October 18, 2017	Addition of new features with V1.1 of the App
December 12, 2017 - Jan 8 2018	Editing and style changes
May 5, 2018	Cosmetic prep for Illumio ASP 18.1
Sept 21, 2018	• Updates for Illumio ASP 18.1 and 18.2 • Illumio App for Splunk v2.0.0
Jan 3, 2019	• Cosmetic update to table of contents • Version stamp for Illumio ASP 18.2.1
July 22, 2019	• Added new configuration, dashboards for App version 2.2.0 • Added more Troubleshooting sections
Sept 9, 2019	Updated the guide version from 2.2.0 to 2.2.1 to match the shipping version of the Illumio Splunk App
Dec 16, 2019	Updated for version 2.3.0. Added the Alert Configuration screen, Alerts screen, updated screen shots, support for Illumio ASP 19.3 and API v2, drill down on Audit Events in Workload Investigation Dashboard, traffic flow timestamp = VEN timestamp, improved support for S3 data, example Splunk queries, added `ip_lists` and `services` to list of REST API endpoints called

February 21, 2020	Updated for version 3.0.0. Added: Splunk 8.0 is supported; app is compatible with Python 2/3; how to edit `summariesonly` macro for faster UI performance; after upgrade, rebuild data model and remove local customizations; new label filters in Workload Investigation dashboard; new Allowed option in Security Operations dashboard.
August 27, 2021	Correct instructions for configuring Splunk Add-on for AWS so that key prefix uses 'illumio' instead of <UUID>. Add clarification on quarantine workload using Enterprise Security Suite
October 28, 2021	Correct error in PCE Secure Cloud log description—all traffic flows are logged.
November 4, 2021	Updated for version 3.2.0. Added new events in CIM Mapping Table, and three new dashboards—PCE Authentication Events, Change Monitoring, and Traffic Explorer

Table of Contents

Architecture **1**
App Components 2
TA-Illumio (Technology Add-on for Illumio) **3**
Splunk Index, Source, and Source Types 4
Index 4
Sourcetype 5
Field Extractions 5
Purpose of TA-Illumio at Different Splunk Components 5
Data Model and Data Model Acceleration 6
CIM mapping 7
Illumio App for Splunk **8**
Dashboards 9
Security Operations Dashboard 9
PCE Operations Dashboard (On-Prem Only) 12
PCE Authentication Events Dashboard 14
Workload Operations Dashboard 14
Workload Investigation Dashboard 16
Traffic Explorer Dashboard 18
Alert Configuration Page 20
Alerts Page 20
Change Monitoring Dashboard 20
Installation **22**
Installation Prerequisites 22
Splunk Single Server Deployment 22
Splunk Distributed Deployment 22
Installing TA-Illumio 22
Application of TA-Illumio to Splunk Components 22
Installing Illumio App for Splunk in a Distributed Splunk Environment 23
Using Splunk Heavy Forwarder 24
Using Splunk Universal Forwarder 24
Splunk Cloud Instance Deployment 25
Installation Commands 25
Configuration **26**
Splunk App Configuration 27
On-Premise PCE Configuration 34

PCE runtime_env.yml Configuration 34
Illumio Cloud PCE Configuration 34
Configure Amazon S3 Bucket 35
Configure Splunk Add-on for AWS 39
Speeding Up UI Rendering 44
Configuring Alerts 45

Post-Installation Required Settings 50
Accelerate Data Model 50
Update Search Macros for Custom Index 51

Upgrade the App 51

Alerting Actions and Adaptive Response Framework 52
Quarantine Workload Using Splunk Core Alert Actions 53
Quarantine Workload using Enterprise Security Suite 53
Quarantine Workload from Illumio Splunk App 57
Access to Quarantine Workload Action 57

Example Splunk Queries 59

Troubleshooting 61
Data collection not working 61
Can’t use same port in new Data Input (Modular Input) 61
Data not available immediately after configuring data input (modular inputs) 62
Authentication failure on Data Input (Modular Input) page 62
Quarantine button is grayed out or does not work as expected 62
Invalid Certificate File error on Data Input (Modular input) page 63
PCE labels are not updated in Security Operations dashboard 63
Security Operations shows “Search is waiting for input” 64
Path for the custom certificate: invalid certificate file 64
Authentication Failed: Invalid PCE URL or API key id or API Secret 68
Sankey diagram is not displayed in Traffic Explorer dashboard 71
Label filters (i.e.App, Env and Loc) are not populated 72

Known Limitations 72

Compatibility Matrix 72

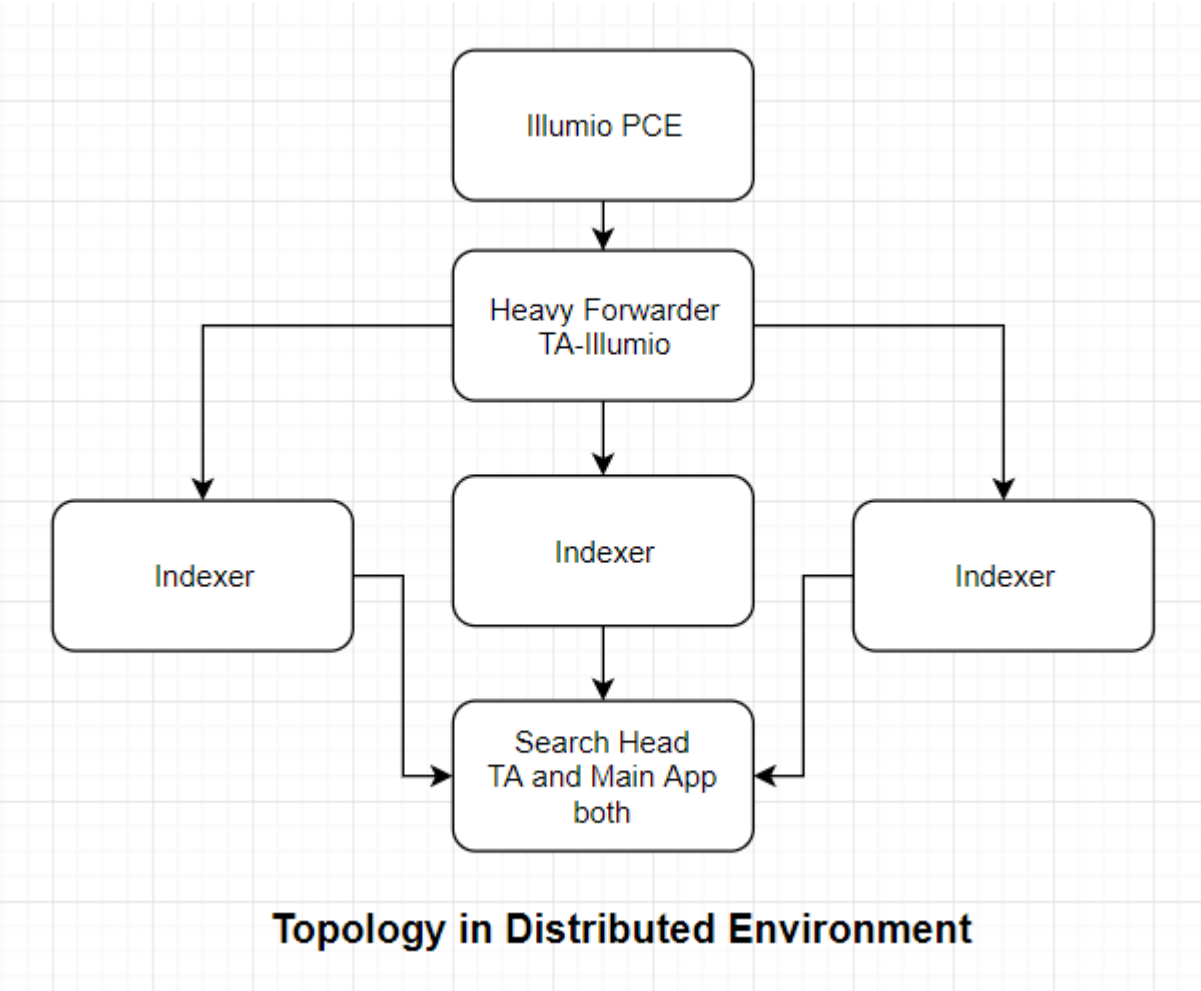
Architecture

The Illumio App for Splunk integrates Splunk with the Illumio Policy Compute Engine (PCE). Using the app, you can conveniently access PCE data through Splunk, and gain security and operational insights into your Illumio-secured data center.

The Technology Add-on for Illumio (TA-Illumio) performs data collection, data normalization, and data visualization using data that comes from the Illumio Policy Compute Engine (PCE) through REST API calls and syslog.

The following diagrams show a typical data collection architecture from PCE to Splunk in distributed and standalone environments.

Splunk Distributed Environment

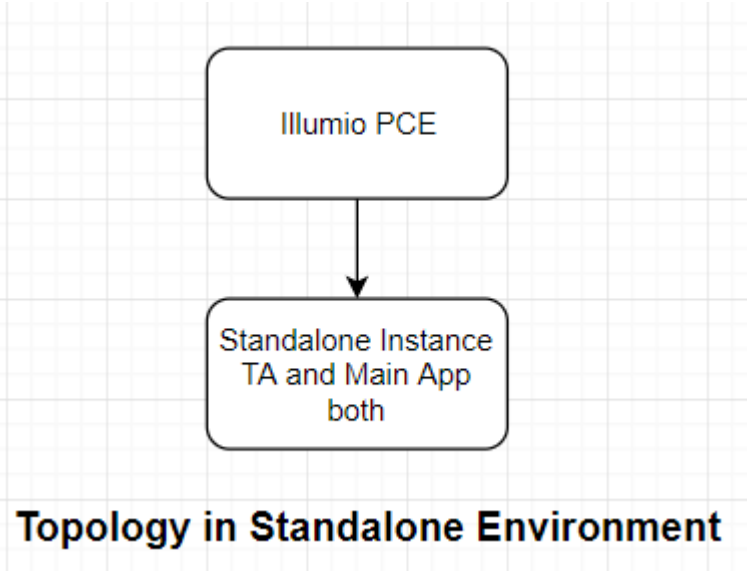


For information about how to install each component in a Splunk distributed environment, see "Application of TA-Illumio to Splunk Components."

If you use Splunk Universal Forwarder on a dedicated data collection node, see "Using Splunk Universal Forwarder."

Splunk Standalone Environment

In a standalone environment, the PCE forwards data directly to the Splunk instance. The Spunk heavy forwarder is not involved.



App Components

The Illumio app for Splunk is comprised of two parts:

- TA-Illumio (Technology Add-on for Illumio)
- Illumio App for Splunk

TA-Illumio and the Illumio App for Splunk are typically deployed together in the search head. TA-Illumio receives and transforms data, and enriches events with CIM fields; it can also be deployed at the indexer or forwarder. The Illumio App for Splunk uses the data enriched by TA-Illumio to display informational dashboards.

TA-Illumio (Technology Add-on for Illumio)

The Technology Add-on for Illumio (TA-Illumio) is a Splunk module that receives PCE data for Splunk and performs data normalization. TA-Illumio collects data from the PCE and enriches the data according to the Common Informational Model (CIM). CIM is the native data representation used by Splunk. Illumio data in CIM format can be used easily with Splunk applications such as Splunk Enterprise Security and Splunk App for PCI Compliance.

Data collection from the PCE is accomplished in two ways: through the Illumio ASP REST API and the Illumio PCE syslog.

The Adaptive Response Framework components that are used by Splunk Enterprise Security Suite are packaged with TA-Illumio.

Illumio ASP REST API

TA-Illumio pulls data using the Illumio ASP REST API. For data collection to work, you must set up the API configuration in TA-Illumio to use Data Input, also known as modular input. Data collected from API calls is used to create metadata for workloads, labels, and services. The API data is used to enrich syslog data, such as traffic flow summaries and auditable events.

The following Illumio ASP REST API endpoints are called:

- GET /api/v2/orgs/1/workloads/
- GET /api/v2/orgs/1/labels/
- GET /api/v2/orgs/1/health/
- GET /api/v2/product_version
- GET /api/v2/orgs/1/sec_policy/draft/ip_lists
- GET /api/v2/orgs/1/sec_policy/draft/services

Illumio PCE Syslog

TA-Illumio receives and processes messages directly from the PCE using the TCP port configured in Data Input (modular input). The types of messages are:

- Events, which are structured JSON messages representing auditing information.
- Traffic flow summaries, which are structured JSON messages representing enriched traffic flows. Traffic flow summaries contain flows, Illumio labels, and other data about the flow.
- PCE System Health messages in syslog format (key-value pairs).
- Other syslog messages.

Splunk Index, Source, and Source Types

Index and source type are default Splunk fields used to categorize and filter the indexed data to narrow down search results.

Index

In Splunk, raw syslog data is stored in indexes, classified by source type. With TA-Illumio, you can select an index while creating Data Input (modular input). Data collected from that modular input will be collected into the selected index.

If you chose the default index in Data Input, no further configuration is needed.

If you chose a non-default index, you must also update the search macros as follows to use the custom index. Otherwise, the dashboards will not display charts.

To modify the search macro:

1. In **Settings** > **Advanced Search** > **Search Macros** > **App: Illumio App for Splunk**, select Illumio_get_index.

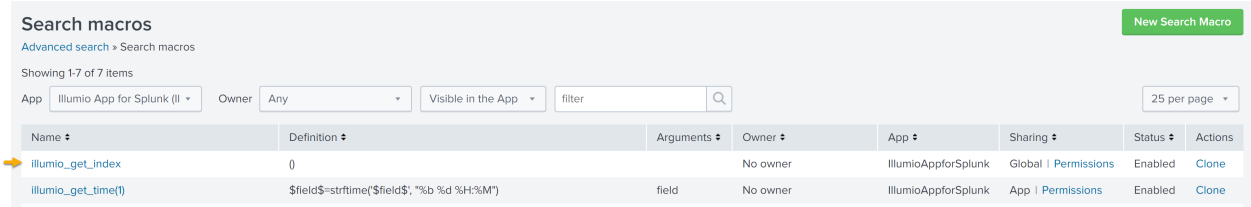
2. In **Definition**, do one of the following:

    - If you use the default index, enter open and close parentheses:

      ```
      ()
      ```

    - If you have created a custom index, enter the name of your index in parentheses:

      ```
      (index=custom_index_name)
      ```



Sourcetype

The following table shows how Illumio data is classified by source types.

Source type	Description
illumio:pce	Events collected from the Illumio PCE through syslog.
illumio:pce:metadata	Workloads, labels, iplists, and services collected from the PCE using REST API calls.
illumio:pce:collector	Traffic flow summaries collected from the Illumio PCE through syslog. Note: The time stamp for traffic flow summaries is the stamp in the message itself (as reported by the VEN), and is not the time when the message is received by the PCE or relayed to Splunk. Effectively, the timestamp of traffic flow summaries is the time when the traffic actually occurred.

Field Extractions

TA-Illumio extracts fields from various source types using regular expressions.

Purpose of TA-Illumio at Different Splunk Components

TA-Illumio has different purposes at different Splunk components

Heavy Forwarder: TA-Illumio at the Heavy Forwarder is used to do data collection. You configure the modular input as described in the Installation section below. Heavy forwarder does not have to be a separate component. It could be the same as an indexer or Search head.

Indexer: TA-Illumio may be installed at the indexer for the following purpose: sometimes the PCE sends invalid JSON data which is not supposed to be indexed. Logic to send such events to the null queue is implemented in TA. Users can choose to not install TA on the indexer if they are not worried about indexing additional events.

Search head: TA-Illumio at search head is used to do search time field extractions, which will be used by Illumio App for Splunk in visualizations.

Data Model and Data Model Acceleration

The app consists of one data model named "Illumio". The data model used in this application is not accelerated by default. If you wish to improve the responsiveness of the dashboards, you should enable data model acceleratation with a 1-week period. Accelerated data models help improve the performance of the dashboard, but also increase the disk usage on the indexer node.

To enable acceleration:

1. On the Splunk menu bar, click **Settings** > **Data models**.
2. From the list of data models, click **Edit** in the Action column of the row for the Illumio data model.
3. From the list of actions, select **Edit Acceleration**. The Edit Acceleration menu is displayed.
4. Check the **Accelerate** checkbox to enable data model acceleration.
5. Select the summary range and specify an acceleration period of 1 week.
6. Click **Save**.

If you don’t need to use the already indexed accelerated data model, the data model can be configured to rebuild from scratch for the specified acceleration period.

To rebuild the data model:

1. On the Splunk menu bar, click **Settings** > **Data models**.
2. From the list for Data models, expand the Illumio row by clicking the **>** arrow in the first column. Additional details appear.
3. From the Acceleration section, click **Rebuild**.

4. Monitor the status of Rebuild in the Status field of the Acceleration section. Reload the page to get the latest rebuild status.

CIM mapping

PCE events are mapped to multiple Common Information Model (CIM) data models as shown in the following table.

Event type	CIM data model	CIM field	Illumio field
sourcetype="illumio:pce" category = "auditable" event_type="user.sign_in" OR event_type="user.login"	Authentication	src	src_ip
		user	created_by.user.username
		app	“Illumio”
		action	“failure” OR "success"
sourcetype="illumio:pce" category = "auditable" event_type="agent.tampering" OR event_type="agent.firewall_config"	Network Changes	action	“modified”
		status	status
		vendor_product	“illumio:pce”
		change_type	change_type
		src	src_ip
		user	created_by.user.username
sourcetype="illumio:pce" category = "auditable" (event_type="*.create" OR event_type="*.delete" OR event_type="*.update") (event_type!="user.*")	Auditing Changes	action	"created" OR "deleted" OR "modified"
		src	src_ip
		status	status
		vendor_product	“illumio:pce”
		user	created_by.user.username
		change_type	change_type

sourcetype="illumio:pce" category = "auditable" event_type="user.create" OR event_type="user.update" OR event_type="user.delete"	Account Management Changes	action	"created" OR "deleted" OR "modified"
		src	src_ip
		status	status
		vendor_product	“illumio:pce”
		src_user	created_by.user.username
		change_type	change_type
		user	resources_changes.resource.username
sourcetype="illumio:pce:collector"	Network Traffic	action	pd
		bytes	tbi + tbo
		bytes_in	tbi
		bytes_out	tbo
		dest	dst_ip
		dest_ip	dst_ip
		dest_port	dst_port
		src	src_ip
		protocol	proto

Illumio App for Splunk

The Illumio App for Splunk integrates Splunk with the Illumio PCE to provide security and operational insights into your Illumio-secured data center. Multiple dashboards display an overview of your data center while monitoring the PCE and Illumio Virtual Enforcement Nodes (VENs) installed in your data center.

With improved visibility of east-west traffic, your Security Operations Center (SOC) staff can detect unauthorized activity and potential attacks from traffic blocked by Illumio segmentation policies on workloads in the "Enforced" policy state (policy is enforced). Additionally, the Illumio App for Splunk provides visibility into potentially blocked traffic for workloads in the "Test" policy state (policy is visualized but not enforced). This enables SOC staff to quickly pinpoint potential attacks and remedy those situations.

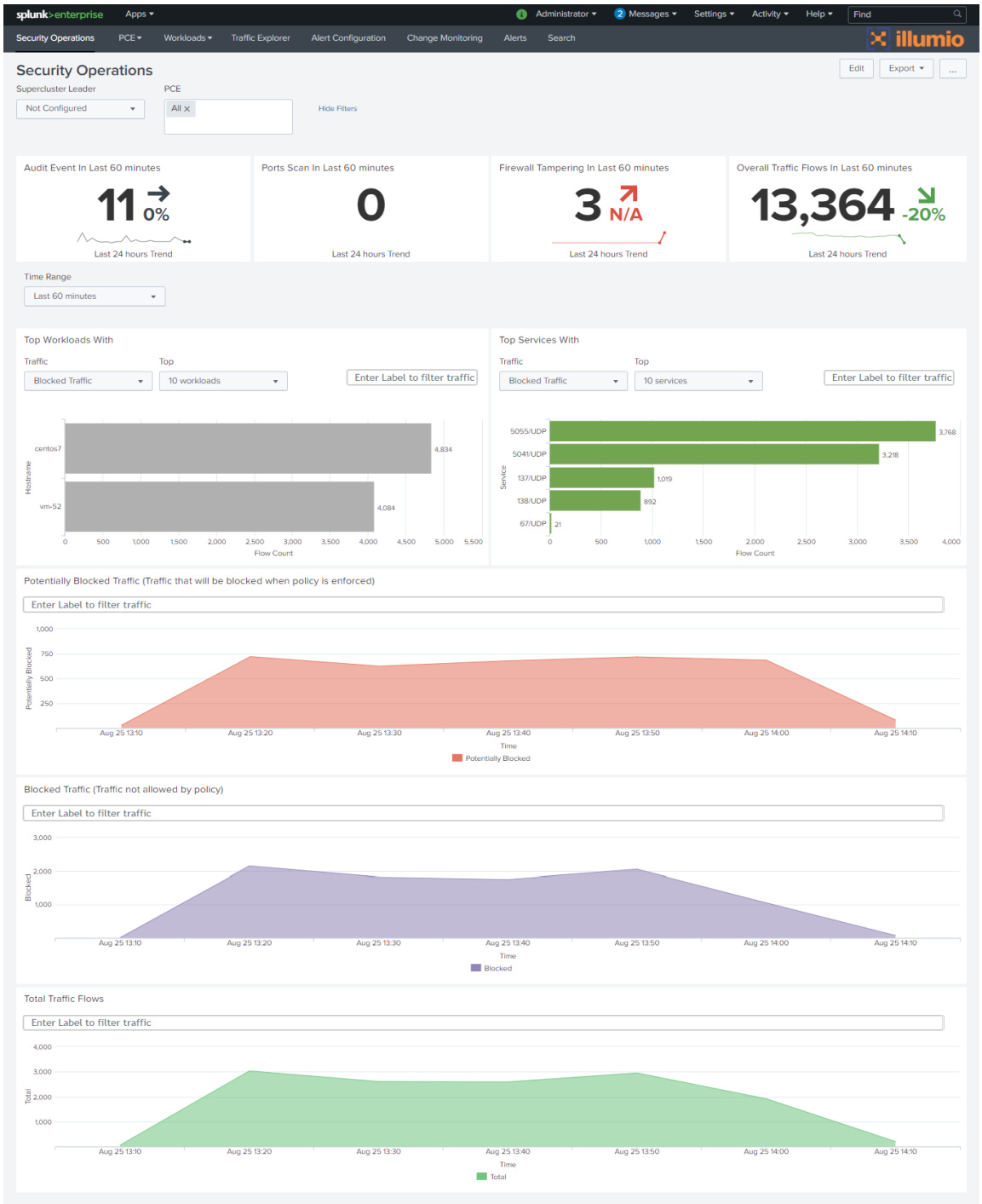
Dashboards

The Illumio App for Splunk has multiple dashboards to display system activities associated with the PCE instance. The following dashboards can be accessed from the top row of the app:

- Security Operations Dashboard
- PCE Operations (On-Prem Only) Dashboard
- PCE Authentication Events Dashboard
- Workload Operations Dashboard
- Workload Investigation Dashboard
- Traffic Explorer Dashboard
- Alert Configuration Page
- Change Monitoring Dashboard
- Alerts Page

Security Operations Dashboard

The Security Operations dashboard provides an overview which allows Splunk administrators to monitor the overall security state of the network, as determined from traffic flows reported by PCE instances. Top Blocked, Potentially Blocked, and Allowed traffic is displayed by host and by service. To see Allowed traffic, choose it in the dropdown list under Top Workloads With or Top Services With. In most panels, flows can be filtered using Illumio labels. You can also drill down to investigate notable events, such as Port Scans and Firewall Tampering.



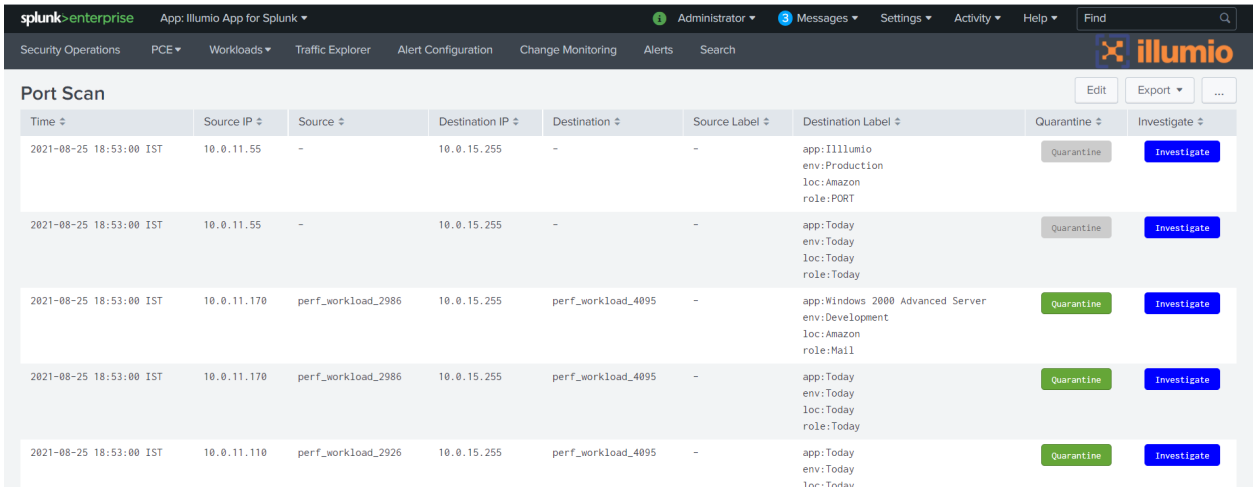
The Security Operations dashboard is built using data from the following sources:

- Traffic flow summaries
- REST API calls made to the PCE

- Events

Investigate Workload from Illumio Splunk App

When you are viewing a list of workloads, such as through the Port Scan or Firewall Tampering screens, you can click **Investigate** to view the Workload Investigation dashboard for the selected workload. For details, see "Workload Investigation Dashboard."



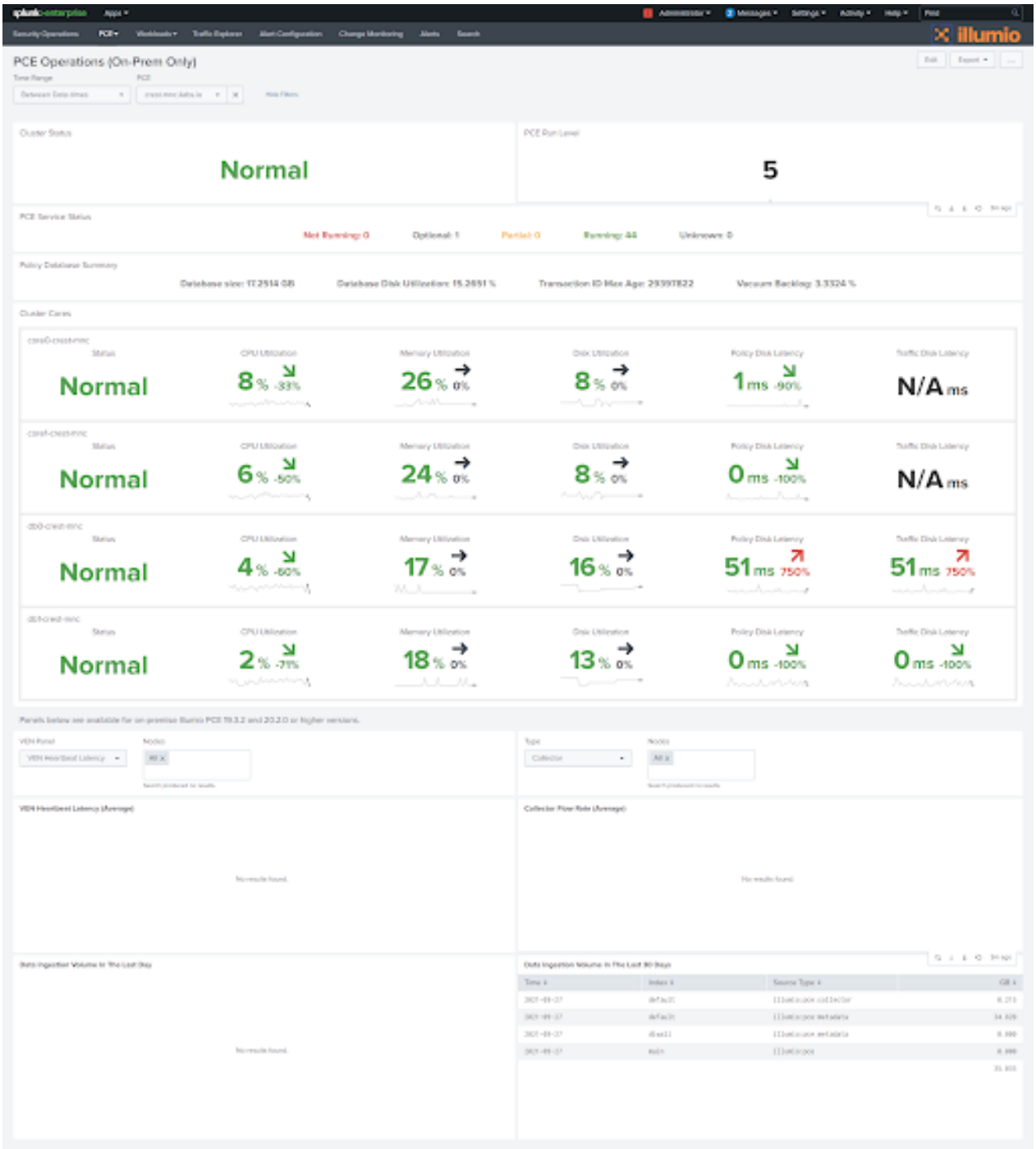
Depending on the results of the investigation, you might want to quarantine the workload.

PCE Operations Dashboard (On-Prem Only)

The PCE Operations dashboard enables Splunk administrators to monitor the health of multiple on-prem PCE instances from one Splunk server. This includes the overall PCE cluster status, service status summary, per-node service status, CPU, Memory and Disk utilization metrics. If multiple PCE instances are connected to Splunk, you can use the dropdown list at the top of the dashboard to choose which PCE to monitor.

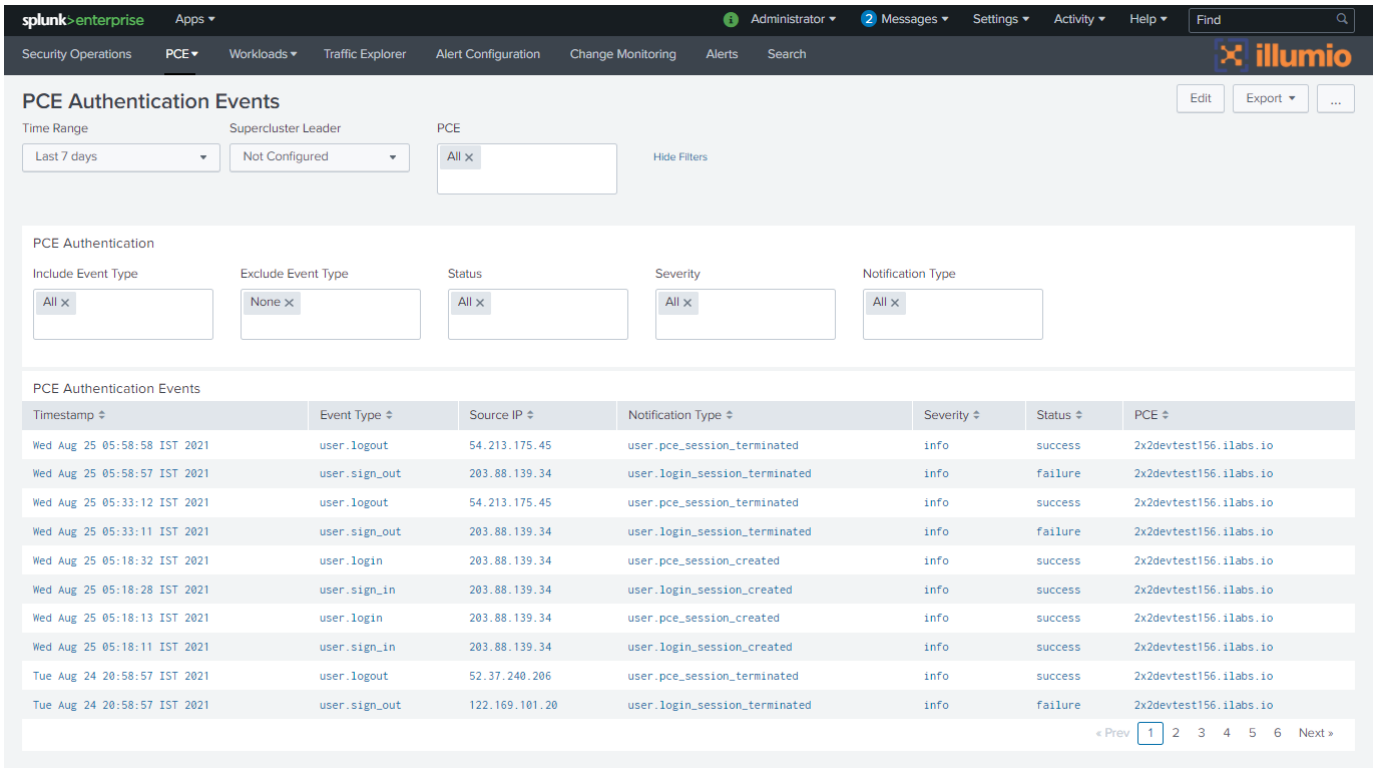
The PCE Operations dashboard is built using data from the following source:

- REST API calls made to the PCE (PCE 17.2 and later)


PCE Operations (On-Prem Only)
Normal
5
Normal
8 % -33%
26 % 0%
8 % 0%
1 ms -90%
N/A ms
Normal
6 % -50%
24 % 0%
8 % 0%
0 ms -100%
N/A ms
Normal
4 % -60%
17 % 0%
16 % 0%
51 ms 750%
51 ms 750%
Normal
2 % -71%
18 % 0%
13 % 0%
0 ms -100%
0 ms -100%

PCE Authentication Events Dashboard

The PCE Authentication Events dashboard enables Splunk administrators to search and filter types of user authentication data.

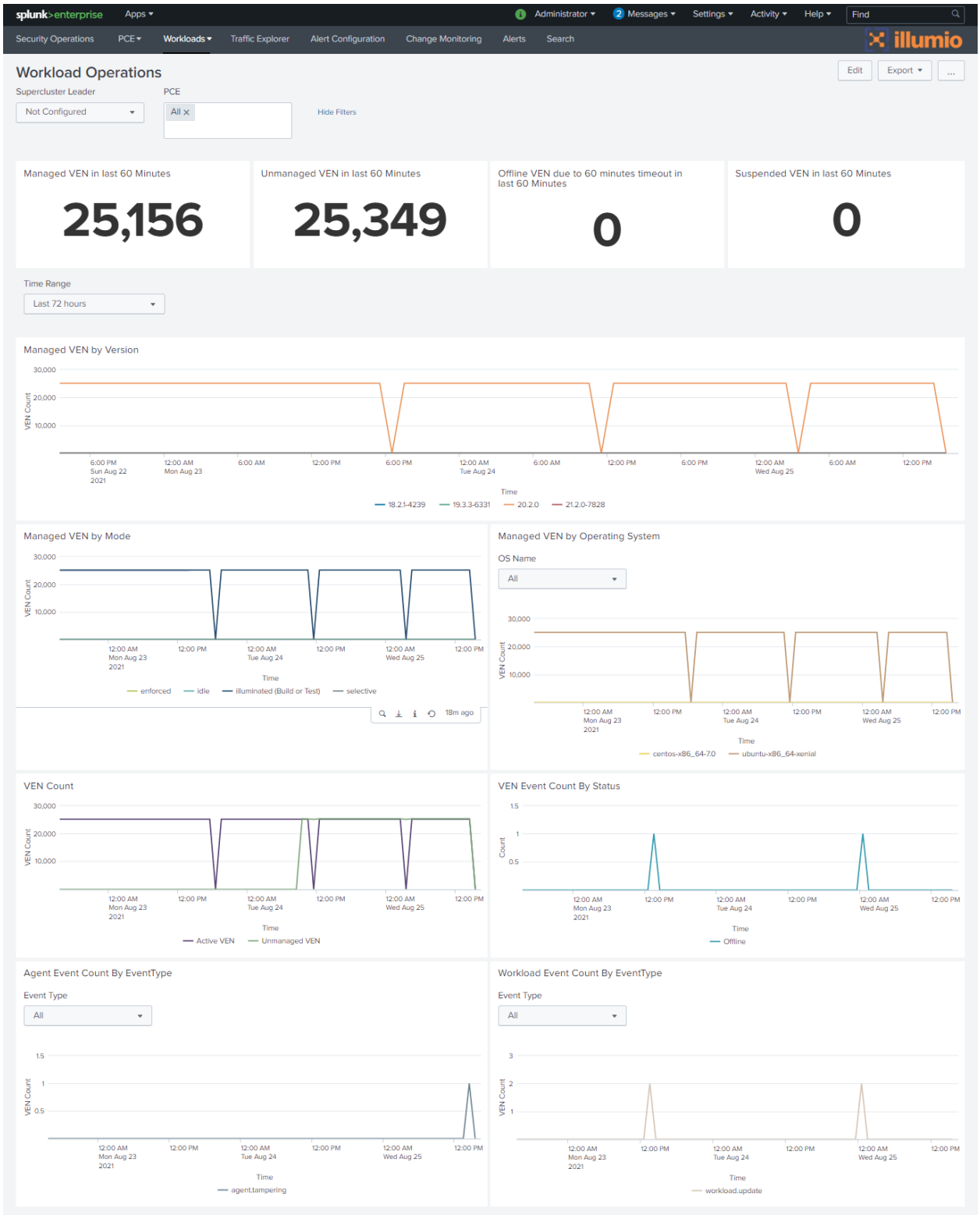


Workload Operations Dashboard

The Workload Operations dashboard enables Splunk administrators to monitor the Workloads managed by the PCE instances. The dashboard displays VEN deployment statistics as well as VEN-reported events. If multiple PCE instances are connected to Splunk, you can use the dropdown list at the top of the dashboard to choose which PCE to monitor.

The Workload Operations dashboard is built using data from the following sources:

- REST API calls made to the PCE
- Events


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Security Operations
PCE
Workloads
Traffic Explorer
Alert Configuration
Change Monitoring
Alerts
Search
illumio
Workload Operations
Edit
Export
Supercluster Leader
Not Configured
PCE
All
Hide Filters
Managed VEN in last 60 Minutes
25,156
Unmanaged VEN in last 60 Minutes
25,349
Offline VEN due to 60 minutes timeout in last 60 Minutes
0
Suspended VEN in last 60 Minutes
0
Time Range
Last 72 hours
Managed VEN by Version
VEN Count
Time
18.2.1-4239
19.3.3-6331
20.2.0
21.2.0-7828
Managed VEN by Mode
enforced
idle
illuminated (Build or Test)
selective
18m ago
Managed VEN by Operating System
OS Name
All
centos-x86_64-7.0
ubuntu-x86_64-xenial
VEN Count
Active VEN
Unmanaged VEN
VEN Event Count By Status
Count
Offline
Agent Event Count By EventType
Event Type
All
agent.tampering
Workload Event Count By EventType
workload.update

Workload Investigation Dashboard

The Workload Investigation dashboard enables Splunk administrators to search detailed information about one or more workloads. If multiple PCE instances are connected to Splunk, you can use the dropdown list to choose which PCE to monitor. You can use the Time Range dropdown list to filter the display. Wildcards or IP addresses can be used to select multiple workloads. Instead of using hostnames or IP addresses to select workloads, you can define a workload scope using the App Label, Env Label, and Loc Label dropdown lists.

The Workload Investigation dashboard has two panels:

- Workload Details – Hostname, IP, Operating System, Status of policy, PCE
- Audit Events – Events recorded for the workloads. You can click an event in the list to drill down for more details about the event.

splunk>enterprise Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Security Operations | PCE ▾ | Workloads ▾ | Traffic Explorer | Alert Configuration | Change Monitoring | Alerts | Search | illumio

Workload Investigations

Edit | Export ▾ | ...

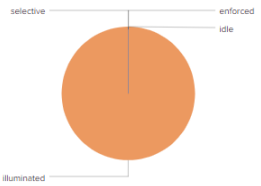
Time Range: Last 60 minutes | Supercluster Leader: Not Configured | PCE: All × | Hostname/IP: * | App Label: All | Env Label: All

Loc Label: All | Hide Filters

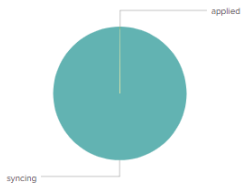
Please specify either hostname(s) or scope labels. If both hostname and scope labels are specified, then the filter uses AND condition.

Active VEN	Suspended VEN	Stopped VEN
25,241	0	22

Policy Enforcement State



Policy Synchronization Status



Workload Details

Workload	Host Name	Interfaces	IPs	OS Name	Workload labels - RAEL	Updated at	Online	Policy State	Status	Policy Sync	Policy applied at	Log Traffic	PCE
k8s-role-env-number	k8s-role-env-number	docker0 ens192	10.0.9.155 172.17.0.1	centos-x86_64-7.0	PORT Illlumio Production Amazon	Mon Aug 23 08:37:12 IST 2021	true	illuminated	active	applied	Mon Aug 23 12:07:32 IST 2021	false	2x2devtest156.ilabs.io
vm-157	vm-157	docker0 ens192	10.0.9.157 172.17.0.1	centos-x86_64-7.0	- CrestDastSystem ABCD Location	Thu Aug 12 11:17:35 IST 2021	true	illuminated	active	applied	Mon Aug 23 12:07:45 IST 2021	false	2x2devtest156.ilabs.io
vm-52	vm-52	docker0 ens192	10.0.9.52 172.17.0.1	centos-x86_64-7.0	Today Today Today Today	Thu Jul 29 13:45:02 IST 2021	true	enforced	active	applied	Mon Aug 23 12:10:57 IST 2021	true	2x2devtest151.ilabs.io
vm-new-45	vm-new-45	ens192	10.0.9.45 fe80::2780:9519:5c51:bbef fe80::808:af9f:5832:52bd fe80::9c84:2a8a:beac:a026	centos-x86_64-7.0	Today Today Today Today	Thu Jul 29 13:23:57 IST 2021	false	enforced	stopped	syncing	Thu Jul 29 12:30:10 IST 2021	false	crest-mnc.ilabs.io
vm-new-44	vm-new-44	ens192	10.0.9.44 fe80::2780:9519:5c51:bbef fe80::808:af9f:5832:52bd fe80::9c84:2a8a:beac:a026	centos-x86_64-7.0	- ABC - ABC	Thu Jul 29 13:23:57 IST 2021	false	enforced	stopped	syncing	Thu Jul 29 12:29:13 IST 2021	false	crest-mnc.ilabs.io

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

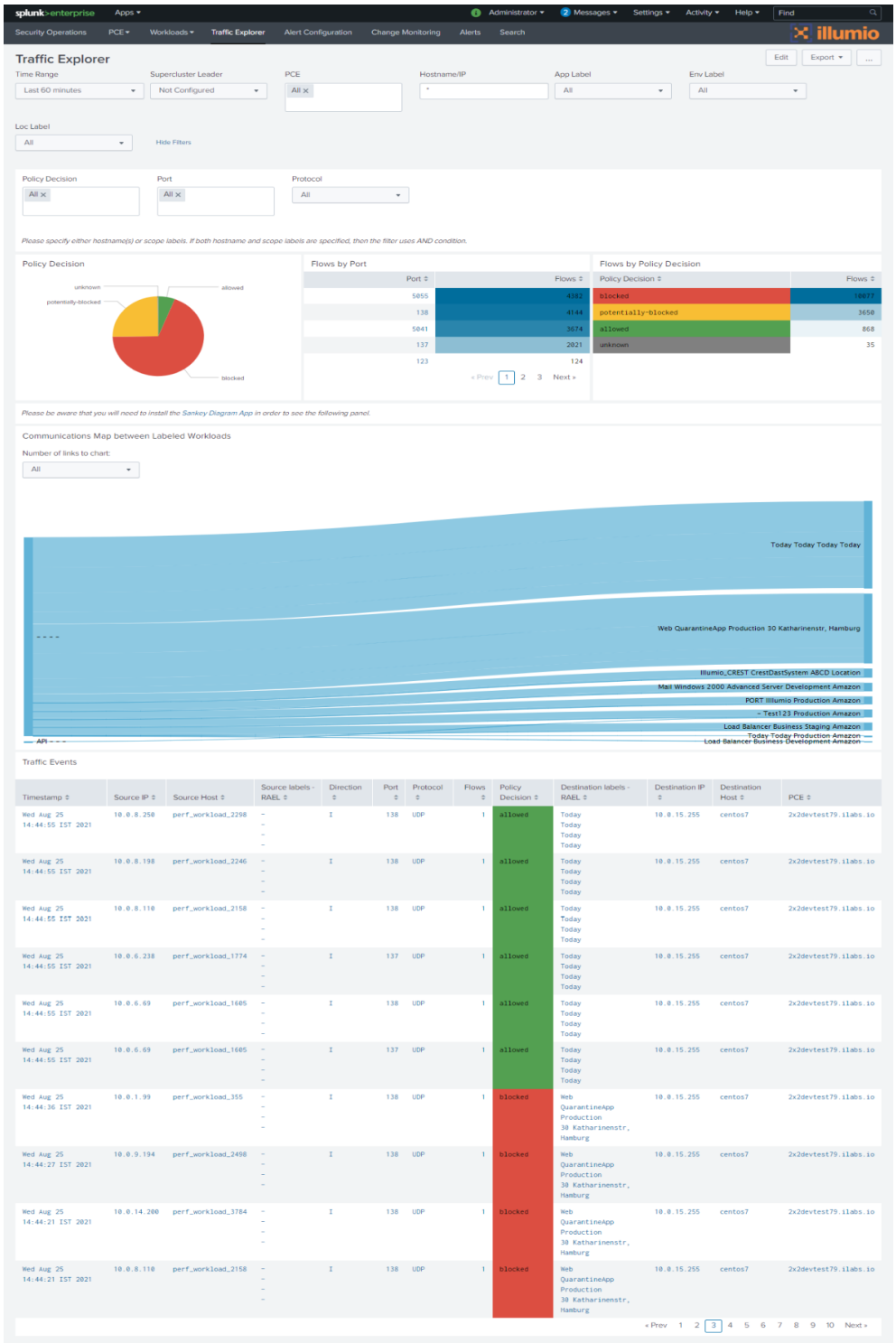
Audit Events

Include Event Type: All × | Exclude Event Type: None × | Status: All × | Severity: All × | Notification Type: All ×

Timestamp	Event Type	Host Name	Source IP	Notification Type	Severity	Status	PCE
Wed Aug 25 09:14:48 IST 2021	request.authentication_failed	-	122.169.101.20	request.authentication_failed	err	failure	2x2devtest79.ilabs.io
Wed Aug 25 09:14:48 IST 2021	request.authentication_failed	-	122.169.101.20	request.authentication_failed	err	failure	2x2devtest79.ilabs.io
Wed Aug 25 09:14:48 IST 2021	request.authentication_failed	-	122.169.101.20	request.authentication_failed	err	failure	2x2devtest79.ilabs.io
Wed Aug 25 09:14:46 IST 2021	request.authentication_failed	-	122.169.101.20	request.authentication_failed	err	failure	2x2devtest79.ilabs.io
Wed Aug 25 09:13:48 IST 2021	system_task.prune_old_log_events	-	52.42.94.101	system_task.event_pruning_completed	info	success	2x2devtest79.ilabs.io
Wed Aug 25 09:13:48 IST 2021	system_task.prune_old_log_events	-	52.42.94.101	system_task.event_pruning_completed	info	success	2x2devtest79.ilabs.io
Wed Aug 25 08:43:47 IST 2021	request.authorization_failed	-	203.88.139.34	request.authorization_failed	err	failure	2x2devtest151.ilabs.io
Wed Aug 25 08:43:47 IST 2021	request.authorization_failed	-	203.88.139.34	request.authorization_failed	err	failure	2x2devtest151.ilabs.io
Wed Aug 25 08:43:47 IST 2021	request.authorization_failed	-	203.88.139.34	request.authorization_failed	err	failure	2x2devtest151.ilabs.io

Traffic Explorer Dashboard

The Traffic Explorer Dashboard helps Splunk administrators to visualize traffic data which are coming from syslog, and enables them to search and filter traffic events.



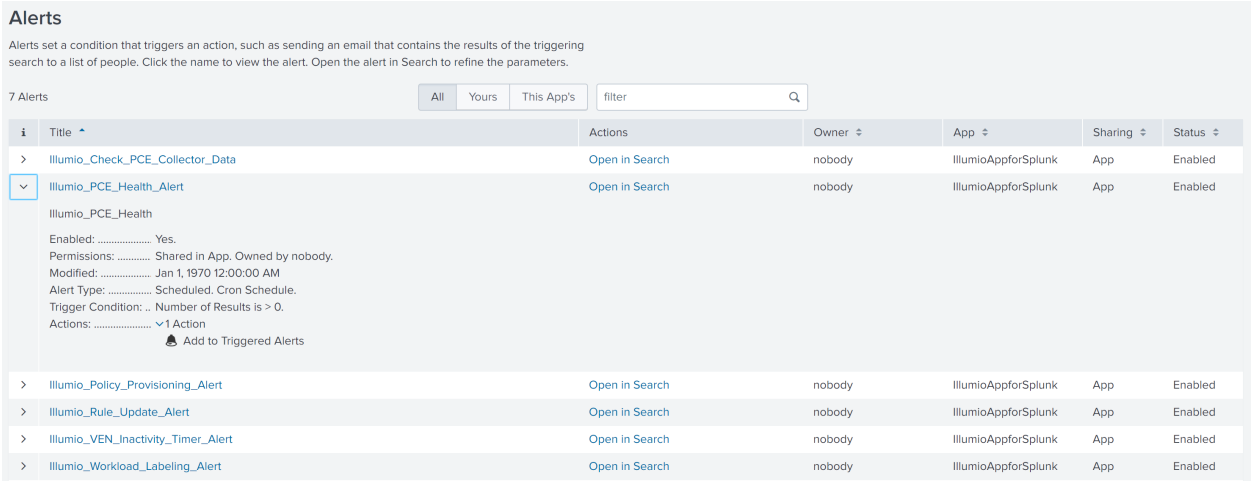
Note: This dashboard leverages the Splunk Sankey Diagram app for visualization. You will need to install this app .

Alert Configuration Page

See “Configuring Alerts” in the Configuration section later in this document.

Alerts Page

Click the Alerts link to view the Splunk Alerts Page. Use this page to view all alerts for the Illumio for Splunk app. Use the links in this page, such as Edit and Open in Search, to further work with the alerts. For example, using the Edit link, you can set up email notifications for alerts. See Splunk documentation for more information about this page.



Change Monitoring Dashboard

The Change Monitoring Dashboard helps Splunk administrators to search detailed level information of changes performed by users.

splunk>enterprise Apps ▾ Administrator ▾ 2 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Security Operations | PCE ▾ | Workloads ▾ | Traffic Explorer | Alert Configuration | Change Monitoring | Alerts | Search | illumio

Change Monitoring

Edit | Export ▾ | ...

Time Range: Last 7 days | Supercluster Leader: Not Configured | PCE: 2x2devtest156.ilabs.io ×

Hide Filters

Daily Changes	Daily Creates	Daily Updates	Daily Deletes
8 ↗ 8	2 ↗ 2	3 ↗ 3	1 ↗ 1

Changes by Object

Object Type	Count
syslog_destination	10
workload	5
workload_service_report	5
label	4
permission	2
labels	1

Changes by User

Actual User	Count
vatsal.halpara@crestdatasys.com	13
smit.belani@crestdatasys.com	12
kartavya.patel@crestdatasys.com	2

All Change Events

Timestamp	Actual User	Source IP	PCE	Object Type	Change Type	Resource Href	Change Details
Wed Aug 25 05:22:16 IST 2021	smit.belani@crestdatasys.com	203.88.139.34	2x2devtest156.ilabs.io	syslog_destination	update	-	{"node_status_included":{"before":false,"after":tr
Tue Aug 24 19:33:59 IST 2021	vatsal.halpara@crestdatasys.com	122.169.101.20	2x2devtest156.ilabs.io	labels	delete	-	null
Tue Aug 24 19:33:36 IST 2021	vatsal.halpara@crestdatasys.com	122.169.101.20	2x2devtest156.ilabs.io	workload_service_report	-	-	-
Tue Aug 24 19:33:35 IST 2021	vatsal.halpara@crestdatasys.com	122.169.101.20	2x2devtest156.ilabs.io	workload	update	/orgs/1/workloads/412e7465-986a-46cc-9b32-ac959e8487e0	{"labels":{"deleted": [{"href":"/orgs/1/labels/29","key":"role","value": [{"href":"/orgs/1/labels/30","key":"role","value":
Tue Aug 24 19:33:29 IST 2021	vatsal.halpara@crestdatasys.com	122.169.101.20	2x2devtest156.ilabs.io	label	create	/orgs/1/labels/30	{"key":{"before":null,"after":"role"},"value": {"before":null,"after":"Illumio_CREST"}}
Tue Aug 24 19:33:02 IST 2021	vatsal.halpara@crestdatasys.com	122.169.101.20	2x2devtest156.ilabs.io	workload_service_report	-	-	-
Tue Aug 24 19:33:01 IST 2021	vatsal.halpara@crestdatasys.com	122.169.101.20	2x2devtest156.ilabs.io	workload	update	/orgs/1/workloads/412e7465-986a-46cc-9b32-ac959e8487e0	{"labels":{"deleted": [{"href":"/orgs/1/labels/18","key":"role","value": [{"href":"/orgs/1/labels/29","key":"role","value":
Tue Aug 24 19:32:52 IST 2021	vatsal.halpara@crestdatasys.com	122.169.101.20	2x2devtest156.ilabs.io	label	create	/orgs/1/labels/29	{"key":{"before":null,"after":"role"},"value": {"before":null,"after":"Supercluster"}}
Mon Aug 23 08:37:13 IST 2021	smit.belani@crestdatasys.com	122.169.101.20	2x2devtest156.ilabs.io	workload_service_report	-	-	-
Mon Aug 23 08:37:12 IST 2021	smit.belani@crestdatasys.com	122.169.101.20	2x2devtest156.ilabs.io	workload	update	/orgs/1/workloads/8e000f52-2986-43d0-9268-9962f519c4ad	{"enforcement_mode":{"before":"idle","after":"visi
Mon Aug 23 08:35:35 IST 2021	smit.belani@crestdatasys.com	122.169.101.20	2x2devtest156.ilabs.io	label	create	/orgs/1/labels/28	{"key":{"before":null,"after":"role"},"value":{"be
Mon Aug 23 08:34:52 IST 2021	smit.belani@crestdatasys.com	122.169.101.20	2x2devtest156.ilabs.io	workload_service_report	-	-	-
Mon Aug 23 08:34:51 IST 2021	smit.belani@crestdatasys.com	122.169.101.20	2x2devtest156.ilabs.io	workload	update	/orgs/1/workloads/8e000f52-2986-43d0-9268-9962f519c4ad	{"labels":{"deleted": [{"href":"/orgs/1/labels/17","key":"app","value": [{"href":"/orgs/1/labels/15","key":"app","value":
Mon Aug 23 08:33:13 IST 2021	smit.belani@crestdatasys.com	122.169.101.20	2x2devtest156.ilabs.io	syslog_destination	create	-	{"pce_scope":{"before":null,"after":["2x2devtest1 {"before":null,"after":"RemoteSyslogDestination"}, {"before":null,"after":"cds.sb.9182"},"address": {"before":null,"after":"203.88.139.43"},"port": {"before":null,"after":9182},"protocol": {"before":null,"after":17},"tls_ca_bundle": {"before":null,"after":"FILTERED"},"tls_verify_cer {"before":null,"after":true},"node_status_includec {"before":null,"after":false}}
Mon Aug 23 07:38:29 IST 2021	kartavya.patel@crestdatasys.com	122.169.101.20	2x2devtest156.ilabs.io	permission	delete	/orgs/1/permissions/1c31c86b-8435-4f21-b6ce-74e6a1d36072	null
Mon Aug 23 07:38:29 IST 2021	kartavya.patel@crestdatasys.com	122.169.101.20	2x2devtest156.ilabs.io	permission	create	/orgs/1/permissions/826af3fa-0a68-4252-8e1b-27e93efd520e	{"role":{"before":null,"after": {"href":"/orgs/1/roles/owner"}},"auth_security_pri {"before":null,"after":{"href":"/orgs/1/auth_secur 3bca-4cc6-b288-a87d290f1ee9"}}}
Mon Aug 23 07:23:37 IST 2021	vatsal.halpara@crestdatasys.com	203.88.139.34 203.88.139.34	2x2devtest156.ilabs.io	syslog_destination	-	-	-
Mon Aug 23 07:22:49 IST 2021	vatsal.halpara@crestdatasys.com	203.88.139.34 203.88.139.34	2x2devtest156.ilabs.io	syslog_destination	-	-	-
Mon Aug 23 07:22:37 IST 2021	vatsal.halpara@crestdatasys.com	203.88.139.34 203.88.139.34	2x2devtest156.ilabs.io	syslog_destination	-	-	-
Mon Aug 23 07:10:18 IST 2021	smit.belani@crestdatasys.com	122.169.101.20 122.169.101.20	2x2devtest156.ilabs.io	syslog_destination	-	-	-

« Prev | 1 | 2 | Next »

Installation

This section tells how to install the Illumio App for Splunk and TA-Illumio.

Installation Prerequisites

- Environment variable SPLUNK_HOME set to the Splunk directory.
- Splunk Enterprise 7.3.x, 8.0.x, 8.1.x, or 8.2.x.
- Illumio PCE installed. For compatible PCE versions, see "Compatibility Matrix."

Splunk Single Server Deployment

In a single server deployment, a single instance of Splunk Enterprise works as a data collection node, indexer, and search head. In such scenarios, install both TA-Illumio and Illumio App for Splunk applications on this node. Then complete the setup of TA-Illumio to start data collection.

Splunk Distributed Deployment

In a distributed deployment, install Splunk Enterprise on at least on two instances. One node works as the search head, and the other node works as the indexer and data collection node. In a Splunk distributed deployment, the data collection node and indexer are deployed on separate servers. In this environment, install the Illumio App for Splunk application on each search head node and TA-Illumio on each indexer/forwarder and search head node.

Installing TA-Illumio

This section tells how to install the TA-Illumio add-on.

Application of TA-Illumio to Splunk Components

This section describes how TA-Illumio is applied to various Splunk components.

Splunk Heavy Forwarder: On the heavy forwarder, which is a Splunk Enterprise instance, TA-Illumio is used for data collection. TA-Illumio is required because the Illumio App for Splunk depends on both API and syslog data from Illumio. TA-Illumio provides both.

To make TA-Illumio data collection work, you must configure Data Input (modular input) as described in the "Installation" section of this document.

Depending on the Splunk deployment, the heavy forwarder might not be a separate component. It can be deployed on the same node as the indexer or search head.

Splunk Indexer: TA-Illumio has a special purpose on the indexer. The PCE might send invalid JSON data which does not need to be indexed. TA-Illumio filters out invalid JSON events. If invalid JSON events are not a concern, TA-Illumio does not need to be installed on the indexer. On the Splunk indexer, you can manually create the index in which the data is stored.

Splunk Search Head: TA-Illumio is used with the Splunk search head to extract time fields, which are then used by the Illumio App for Splunk in dashboard visualizations.

Installing Illumio App for Splunk in a Distributed Splunk Environment

The following table describes the apps to deploy when installing within a Splunk distributed environment.

App Name	Search Head	Indexer	Heavy Forwarder/Data Collection Node
Data Input (aka Modular Input or REST Modular Input)	Configure data input with API keys and data collection disabled (not checked)	Configure data input with API keys and data collection disabled (not checked)	Configure data input with API Keys and data collection enabled
Illumio App for Splunk	Yes	Not Applicable	Not Applicable

Illumio Technology Add-on (Illumio-TA) for Splunk	Yes	Optional (if filtering of invalid JSON is desired)	Yes

The deployment procedure varies depending on whether you are using Heavy Forwarder or Splunk Universal Forwarder.

Using Splunk Heavy Forwarder

In a distributed environment with Splunk Heavy Forwarder:

- On the search head, install the Illumio App for Splunk and the TA-Illumio add-on.
- On the Splunk Heavy Forwarder, install TA-Illumio.

Using Splunk Universal Forwarder

In a distributed environment with Splunk Universal Forwarder:

- Set up a data collection node with Splunk Universal Forwarder.
- Configure the PCE to forward data from all nodes to the Splunk Universal Forwarder.
- Configure the Splunk Universal Forwarder to send the data to Splunk Indexer or Splunk Heavy Forwarder.

The installation steps are as follows.

1. Configure the Splunk Universal Forwarder to collect data from the Illumio PCE.

   a. Create a TCP stanza in $SPLUNK_HOME/etc/system/local/inputs.conf file:

   ```
   [tcp://<PORT>]
   index=<INDEX-NAME>
   sourcetype=illumio:pce
   ```

   b. Configure the Splunk Universal Forwarder to send the data to the Splunk Indexer. Execute this command on the Splunk Universal Forwarder (for `<IP>:<PORT>`, fill in the Splunk Indexer IP and Listening Port):

   ```
   $SPLUNK_HOME/bin/splunk add forward-server <IP>:<PORT>
   ```

2. Configure the Splunk Indexer to receive data from SUF. Create the following stanza in the file $SPLUNK_HOME/etc/system/local/inputs.conf:

```
[splunktcp://<PORT>]
```

In a distributed environment:

- If you have a separate data collection node, be sure it is running a full Splunk Enterprise version.
- Complete the Data Input configuration on the data collection node (Heavy Forwarder) with API keys and data collection enabled.
- On all other nodes, configure the data input with the API keys and data collection disabled.
- In setups where a non-default index is used, it may be necessary to configure the search macro Illumio_get_index with a definition of “index=Illumio”. Use the steps in “Splunk Index, Source, and Source Types.”

Splunk Cloud Instance Deployment

In the Splunk Cloud, data indexing takes place in a cloud instance. The data collection can take place in an on-premise Splunk instance in your environment that will work as heavy forwarder.

Installation Commands

The Illumio App for Splunk and TA-Illumio can be installed either through a command line or from the Splunk UI.

Use these commands for a fresh installation. If you are upgrading from a previous version, see “Upgrade the App.”

- To install from the UI, log in to Splunk. Go to **App** > **Manage Apps** and click **Install app from a file**. Then choose the SPL file to install and click **Upload the SPL**.
- To install from the command window, go to the folder $SPLUNK_HOME/bin and execute the following command. For the XXs, substitute the rest of the actual file name.

```
./splunk install app TA-Illumio-XX-XXXX-XX.spl
./splunk install app IllumioAppForSplunk-XX-XXXX-XX.spl
```

Configuration

This section describes how to configure the following after installing the Illumio App for Splunk:

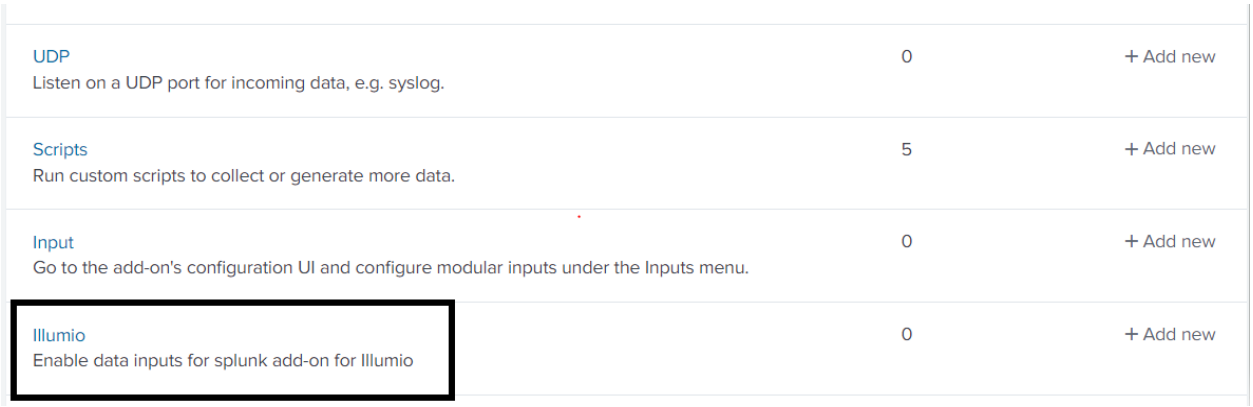
- The Splunk app itself
- Your on-premise or cloud PCE
- Alerts

You may also view video instructions at https://support.illumio.com/knowledge-base/articles/How-to-Configure-Illumio-to-Send-Event-logs-to-Splunk.html

Splunk App Configuration

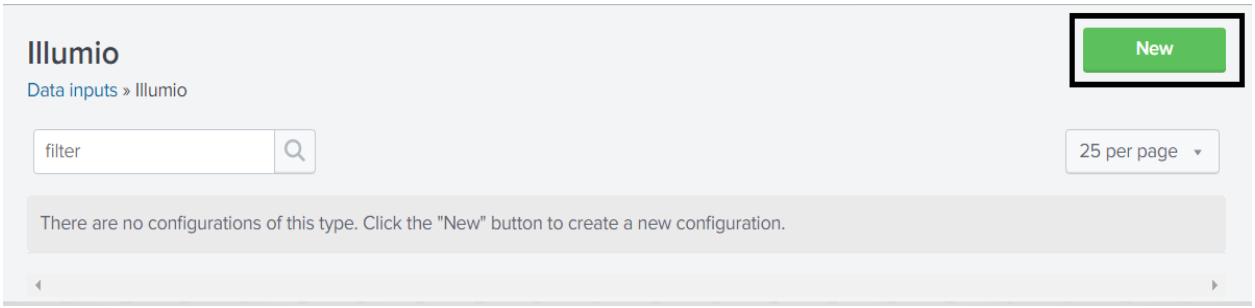
Once the installation of TA-Illumio has completed successfully, follow the steps below to configure Splunk to receive the data from the Illumio PCE syslog and to get workload and label information indexed into the Splunk App using the Illumio ASP REST API.

1. Log in to the Splunk web app.
2. Go to **Settings** > **Data inputs**.
3. Locate “Illumio” and click it.



4. Click **New** to create Data Input (Modular Input) for ingesting data from Illumio PCE to Illumio App for Splunk.

   NOTE: If you have multiple PCEs sending data to a single Splunk, then a different Data Input with different TCP ports is needed for each PCE.



5. In the Modular Input page, enter the configuration details using the following table:

Input Parameter	Mandatory or Optional	Description
Name	Mandatory	Identifying name of the Illumio PCE.
Supercluster Leader/ PCE URL	Mandatory	Enter the PCE URL including HTTPS and the port number.(Make sure that if the provided PCE is part of the supercluster then it must be the leader of the supercluster) For example: https://illumiopce.company.com:443/
API Authentication Username	Mandatory	API Authentication Username used to authenticate with the Illumio PCE. To generate the API key, log in to the Illumio PCE web console, then click **Username** > **My API Keys** > **Add New**. For example: api_16175f6af766fcd7b If API Username and Secret are not specified, the PCE Operations and Workload Operations dashboards will not work.
API Authentication Secret	Mandatory	The API Secret is the password for an API Key that is used to authenticate with the PCE. The API Secret is generated by the API key. For example: 4ed8ff8a5c40201dc52c89a59936f7b1003b950e0027204b2aaaa633ba040d22

Input Parameter	Mandatory or Optional	Description
TCP Port Number for incoming syslog from PCE	Optional	Splunk server port on which the Splunk App should listen for syslog messages from the PCE. The PCE in turn should be configured to forward syslog to this port on the Splunk server. If creating multiple Data Inputs, use a different TCP port for each PCE. For example: 5014
Port Scan configuration: Scan interval in seconds	Mandatory	Minimum time duration of connections between two workloads to determine a port scan. For example: If two workloads show flows between 10 unique ports within 60 seconds, then a port scan is registered. Default: 60 seconds.
Port Scan Configuration: Unique ports threshold	Mandatory	Minimum threshold of unique ports between two workloads to determine a port scan. For example: If two workloads show flows between 10 unique ports within 60 seconds, then a port scan is registered. Default: 10 ports.
Labels to quarantine Workloads	Optional	Comma-separated list of labels of type App, Environment, and Location. In the comma-separated list, whitespace is not allowed. Labels must be supplied in the exact order Application,Environment,Location. These labels should exist on the PCE with

Input Parameter	Mandatory or Optional	Description
		appropriate policy to quarantine workloads. These labels will be applied while quarantining the workloads using the App or AR action.
Organization ID	Optional	For Illumio Data Center (on-premise) customers, the organization ID is 1. For Illumio Cloud customers, the organization ID can vary. The administrator can determine the organization ID from the Illumio PCE Web Console by logging in, clicking the administrator's name at the top right, and clicking **My API keys** > **Add New**. The Create New API dialog shows the Organization ID.
IP addresses of PCE Nodes	Optional	Comma-separated IP addresses (private, public) of all the nodes managed by this PCE instance. All IP addresses must be provided. Use only commas. Do not add space characters.
Data Collection	Mandatory	When enabled, the TA will collect data on this instance. If using a Splunk Cluster, this should be enabled on indexer node but disabled on search head nodes. Default: enabled. Note: When invoking "Quarantine Workload" with Splunk Cluster, the search head node TA needs to be configured with data

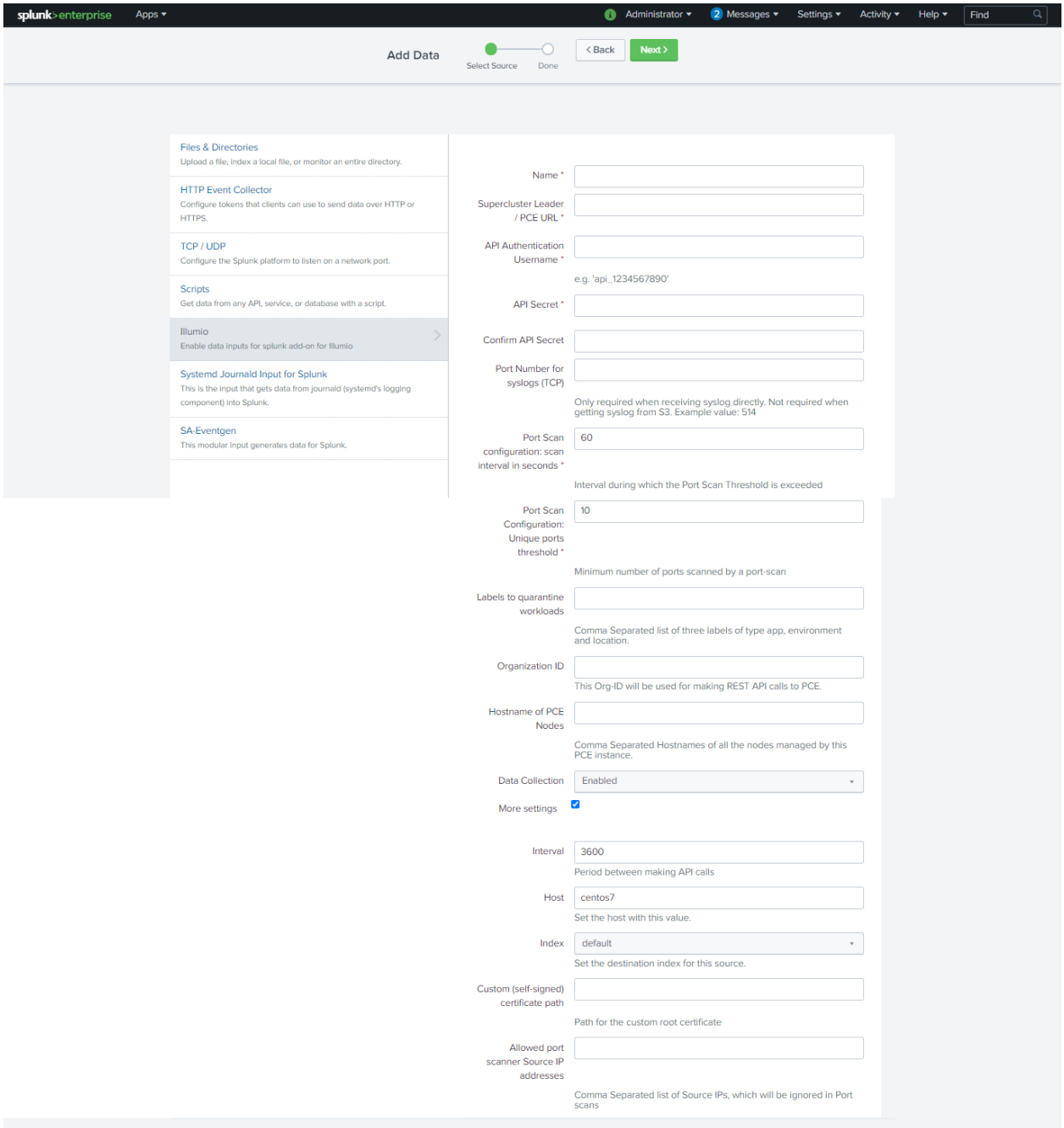
Input Parameter	Mandatory or Optional	Description
		collection disabled (and indexer node TA data collection enabled).

6. Make any desired additional settings from the following table:

Input Parameter	Mandatory or Optional	Description
Interval	Optional	Interval between REST API calls made by the Splunk App to refresh data from PCE. The minimum value is 3600 seconds. Default: 3600.
Host	Optional	Host information added into events to be indexed by Splunk. Illumio recommends using the FQDN of the Splunk server.
Index	Optional	For use by advanced Splunk users. Change the index name under which received events are categorized. If you use a non-default (custom) index such as "Illumio", the index should be created manually, and the search macros modified to return "index=illumio". See "Splunk Index, Source, and Source Types."
Custom (Self-Signed or Local CA Authority) Certificate Path	Optional	When a local CA Authority issued SSL certificate or a self-signed SSL certificate is used with the PCE, its SSL Certificate needs to be uploaded onto the Splunk Server and the full path to the directory

Input Parameter	Mandatory or Optional	Description
		containing the certificate should be provided here. For correct SSL operation, the Splunk server must be able to fully trust the PCE's certificate. If using a local CA Authority or a certificate issued by a secondary CA, the Splunk server CA trust chain must be updated to verify the certificate presented by the PCE. For example, on Linux, use the update-ca-trust tool.
Allowed port scanner IP addresses	Optional	White-list IP addresses of known port scanners, such as Qualys hosts. These addresses are excluded when determining port scans, which avoids false positives in the Port Scans panels.

For example:



7. Click **Next** after adding each value for data input (modular input).
8. Look for a success message displayed as a header in the setup page. This indicates correct credentials and validation passed. For incorrect credentials or errors in validation, a failure message is displayed. For more information, see "Troubleshooting."

On-Premise PCE Configuration

You must make configuration changes on the PCE so that data is forwarded to the Splunk server.

Syslog Configuration

Follow the steps in "Configure Events Forwarding to External Syslog Server" in the *Illumio ASP Web Console User Guide*.

PCE Runtime Configuration

(For PCE versions before 18.2.1. If you have PCE 18.2.1 or later, skip this section.)

To generate and send traffic flow summaries to the PCE syslog and forward to Splunk, you need to make the following changes to the PCE Runtime Environment file runtime_env.yml. Changes must be made to the runtime_env.yml file on all PCE nodes in the cluster, and the PCE must be restarted to put the changes into effect.

PCE runtime_env.yml Configuration

```
 export_flow_summaries_to_syslog:

- accepted

- potentially_blocked

- blocked
```

For more information about runtime_env.yml and the setting `export_flow_summaries_to_syslog`, see the *Illumio ASP PCE Deployment Guide*.

Illumio Cloud PCE Configuration

If you are using Illumio Secure Cloud, follow these steps:

1. Perform the configuration steps from “On-Premise PCE Configuration”.

2. In addition, two components are needed so your PCE data can be relayed to the Illumio App for Splunk:

    - Amazon S3 bucket, which permits reliably storing events from Illumio Cloud.
    - Splunk Add-on for AWS, which permits reading events from an Amazon S3 bucket.

Illumio PCE Secure Cloud logs all traffic flows, including allowed traffic, blocked traffic, potentially blocked traffic, and auditable events to your Amazon S3 bucket. You may choose to disable specific types of events in Illumio Cloud by filing a support ticket. The Splunk Add-on for AWS reads the data from Amazon S3, enriches the data with source type, and enables data to be processed by TA-Illumio. The data is then visualized with the Illumio App for Splunk.

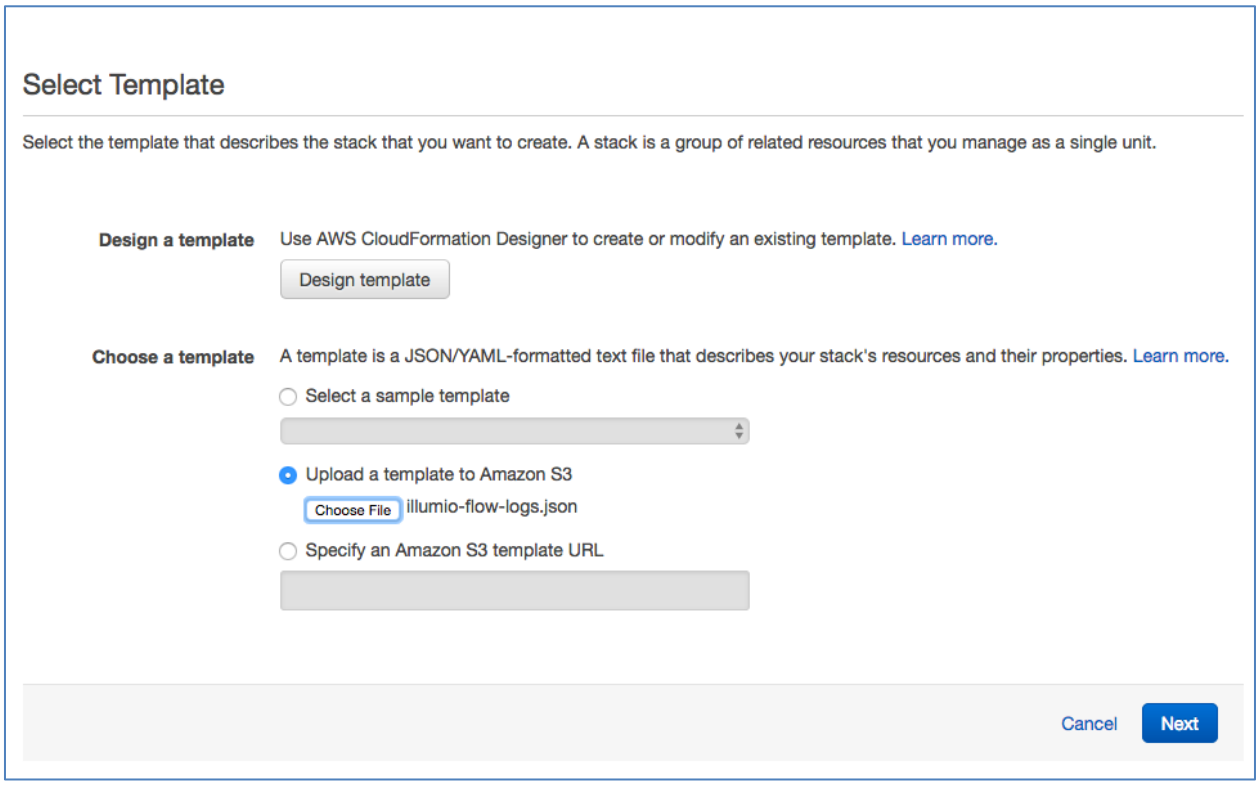
Starting with the Illumio App for Splunk 2.3.0, the consumption of data from S3 is more robust than in earlier versions.

Configure Amazon S3 Bucket

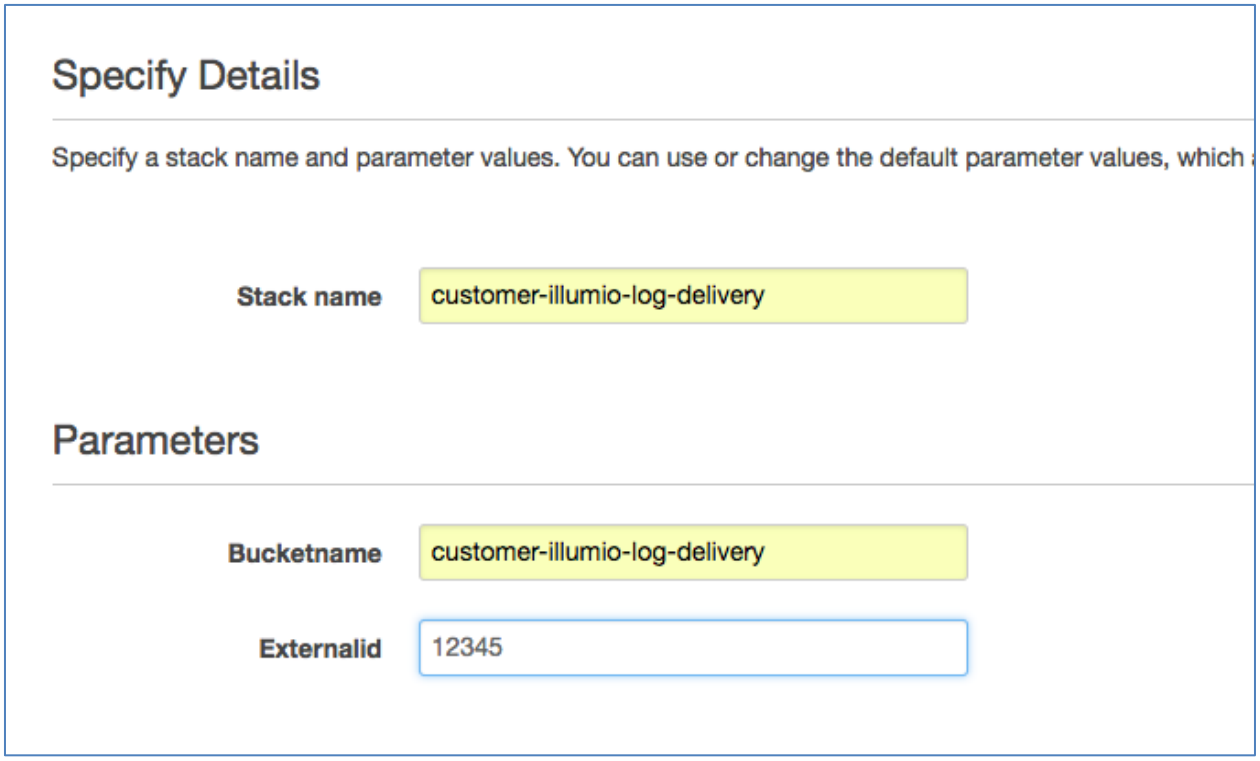
To implement the Illumio App for Splunk with your Illumio PCE Secure Cloud, you must provide an AWS S3 bucket. The S3 bucket can be created and configured using an Illumio-provided CloudFormation template, which you can get from Flow Logs for Illumio Secure Cloud PCE in the Illumio Knowledge Base.

Load the template into CloudFormation as follows:

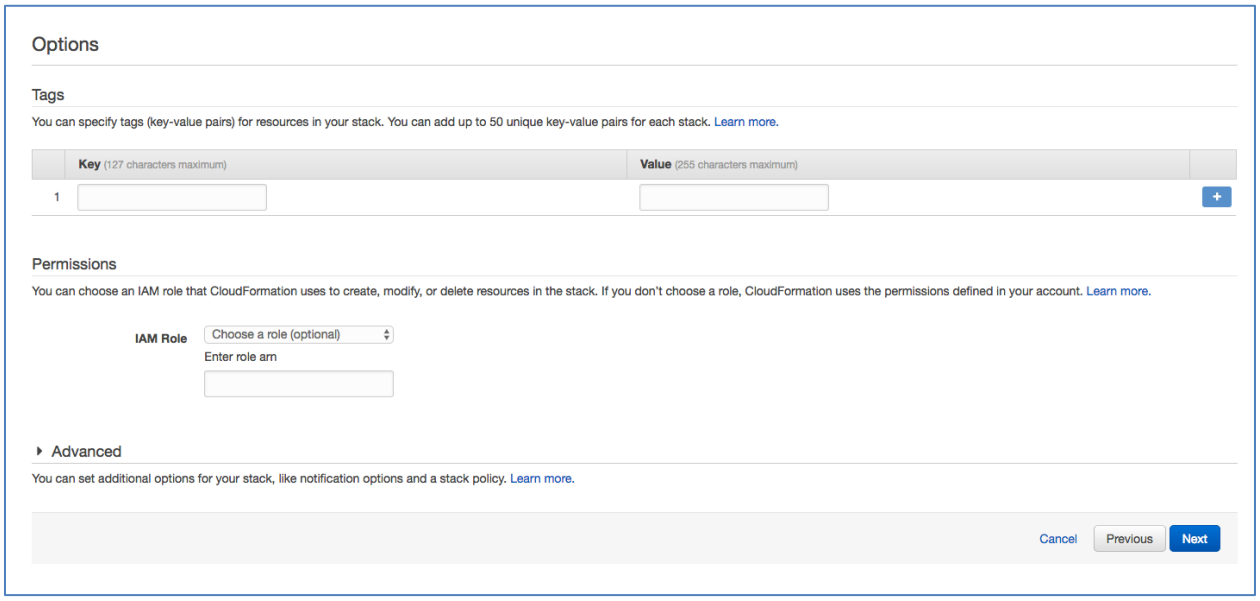
1. Select a template.



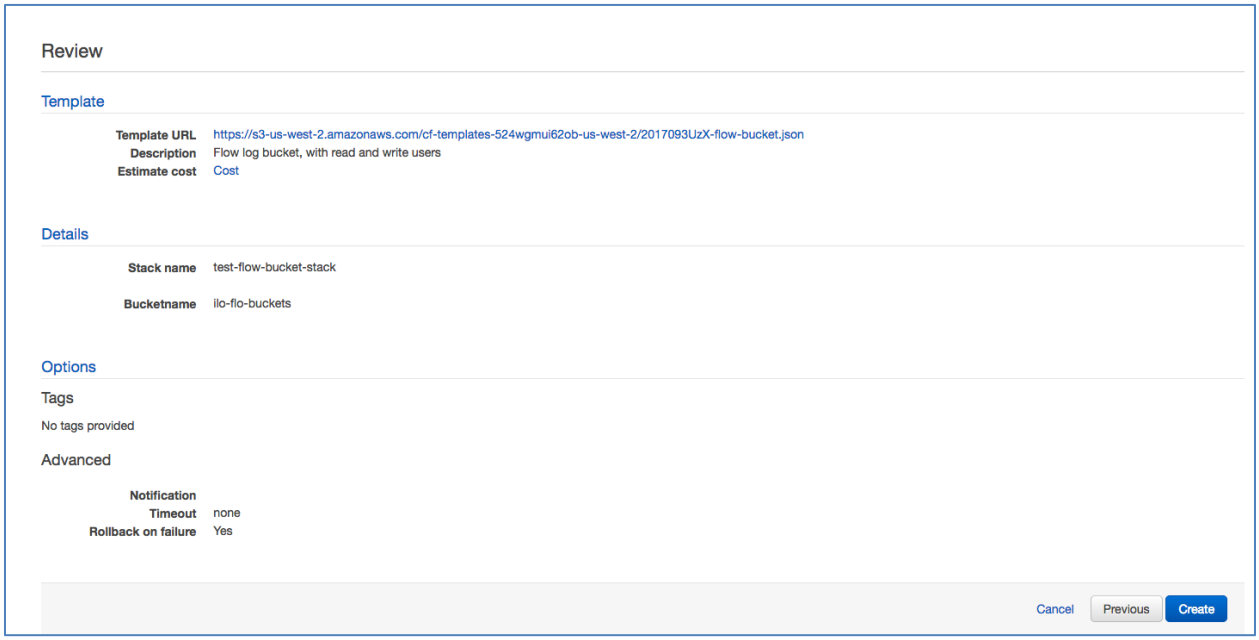
2. Specify the details. The value of **Stack name** can be any label you like; it is for convenience and display only.



3. Specify options.



4. Review the configuration.
5. Click Create.



The above example contains the Illumio AWS account ID. “Externalid” is an extra password to ensure that root access to the Illumio production account is not enough to access your S3 bucket, to prevent a poorly functioning third-party service. For more information, see How to Use External ID When Granting Access to Your AWS Resources in the Amazon Blog.

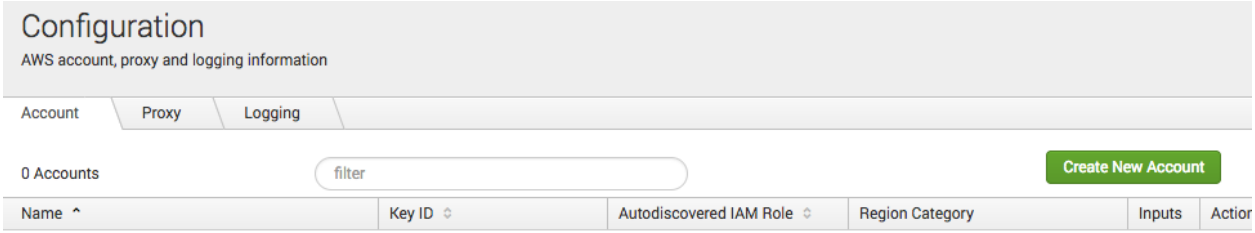
Provide the following information to Illumio:

- The AWS S3 bucket name that you have chosen.
- Your AWS account ID. This is available under "My Account", or https://console.aws.amazon.com/billing/home?#/account in the AWS console.

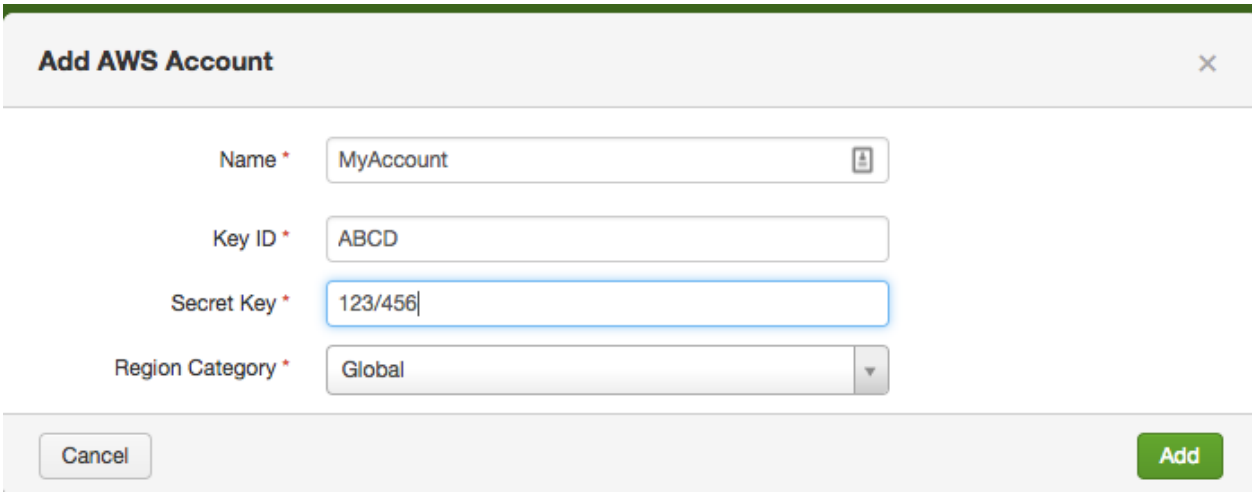
Configure Splunk Add-on for AWS

Install the Splunk Add-On for AWS. This is not to be confused with the Splunk App for AWS, which is an entirely different app.

1. Enter your account into the Splunk Add-On for AWS App:

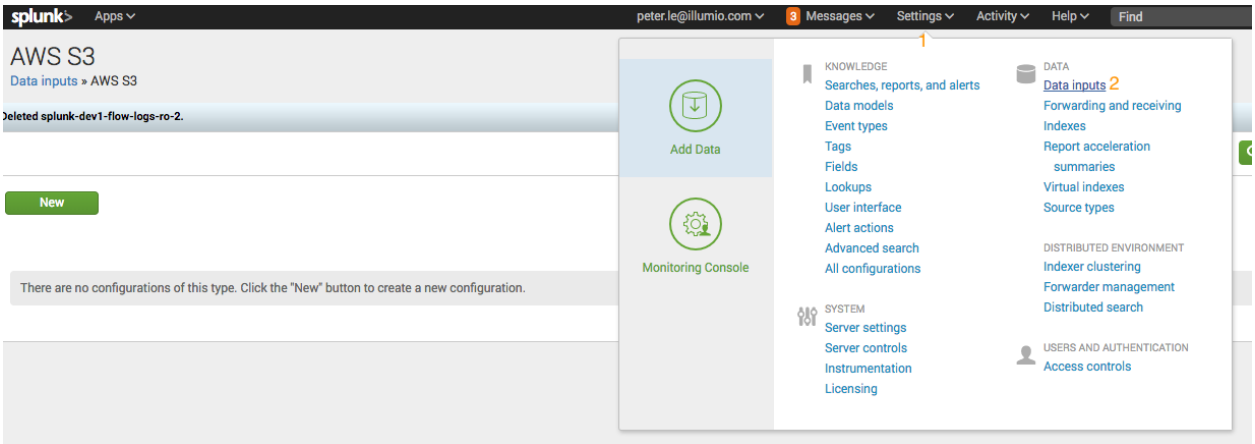


2. Enter Name, KeyID, Secret Key, and select the "global" Region Category:



3. Be sure to create an IAM S3 Bucket Policy that allows for Splunk to access the S3 Bucket. For instructions, see "Configure S3 permissions " in the Splunk documentation.

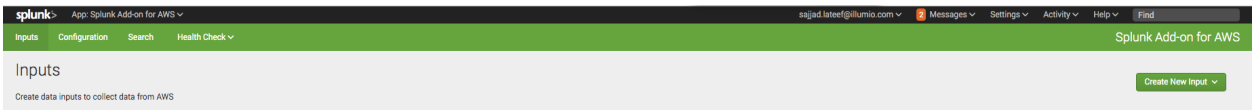
4. Choose **Settings** > **Data inputs**:



Next, you will create two data inputs for AWS S3:

- One data input for events, with source type set to Illumio:pce.
- One data input for traffic flow summaries, with source type set to Illumio:pce:collector.

5. Find AWS S3, then click **Add New**:



6. Add configuration data for Events. Fill in the following:

- Name
- AWS Account
- S3 Bucket name
- Polling interval (1800 seconds, optional)
- Key prefix: Illumio/auditable_events

You can accept the defaults for everything else on this screen.

Select Source — Done

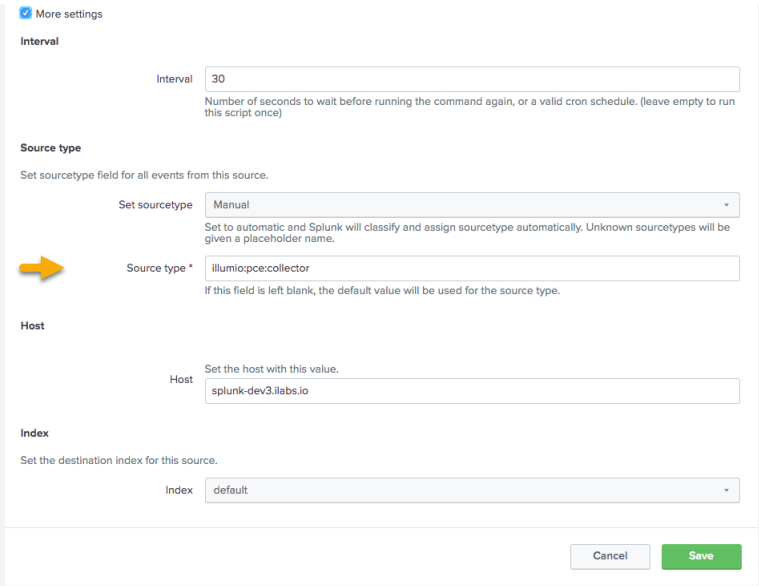
< Back | Next >

Collect and index log files stored in AWS S3.

Name *	Unique data input name Illumio Auditable Events
Secure S3 connection	True
S3 host name	For example: s3-ap-south-east-1.awsamazon.com s3.amazonaws.com
AWS Account *	corp-aws-splunk
Bucket Name *	audit-data
Polling interval	1800
Key prefix	illumio/auditable_events/
For folder keys	-1
Start datetime	Only S3 keys which have been modified after this datetime will be considered default
End datetime	Only S3 keys which have been modified before this datetime will be considered
Max trackable items	100000
Max number of retry attempts to stream incomplete items	3
Whitelist Regex	S3 key names which match this regex will be indexed
Blacklist Regex	S3 key names which match this regex will be ignored, but whitelist dominates
The encoding used in your S3 files	auto
Blacklist for CloudTrail Describe events	Only valid when manually set sourcetype=aws:cloudtrail. PCRE regex for specifying event names to be excluded. Leave blank to use the default set of read-only event names ^$
index for the excluded CloudTrail events	
Assume Role	
More settings	☐

7. Click the More Settings checkbox. Fill in the following:

    - Source type (illumio:pce)
    - You can accept the defaults for everything else.



8. Click **Save**.
9. Add configuration data for traffic flow summaries. Fill in the following:

    - Name
    - AWS Account
    - S3 Bucket name
    - Polling interval (1800 seconds, optional)
    - Key prefix: Illumio/summaries
    - Source type (illumio:pce:collector) – click More Settings to access this field

You can accept the defaults for everything else.

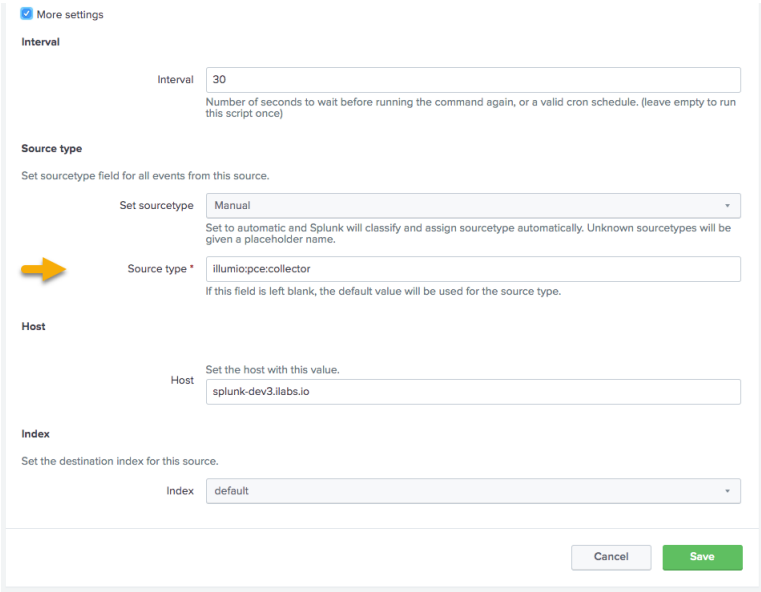
Select Source — Done

< Back | Next >

Collect and index log files stored in AWS S3.

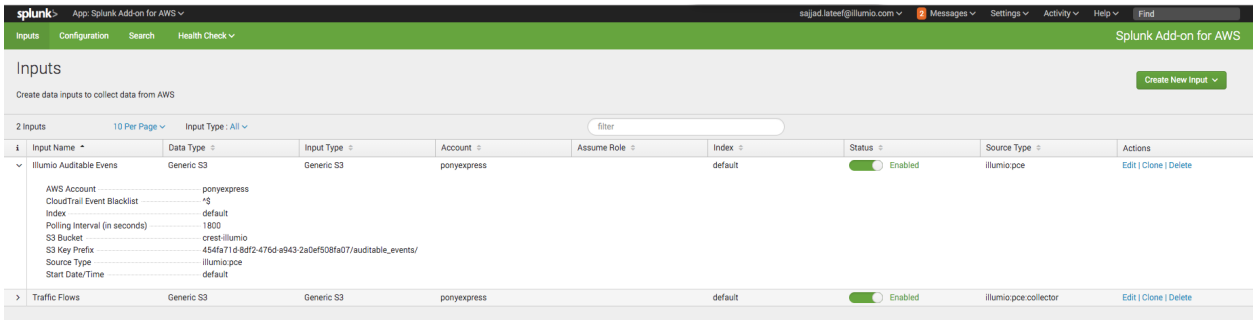
Name *	Unique data input name Traffic Flows
Secure S3 connection	True
S3 host name	For example: s3-ap-south-east-1.awsamazon.com s3.amazonaws.com
AWS Account *	corp-splunk
Bucket Name *	traffic
Polling interval	1800
Key prefix	illumio/summaries
For folder keys	-1
Start datetime	Only S3 keys which have been modified after this datetime will be considered default
End datetime	Only S3 keys which have been modified before this datetime will be considered
Max trackable items	100000
Max number of retry attempts to stream incomplete items	3
Whitelist Regex	S3 key names which match this regex will be indexed
Blacklist Regex	S3 key names which match this regex will be ignored, but whitelist dominates
The encoding used in your S3 files	auto
Blacklist for CloudTrail Describe events	Only valid when manually set sourcetype=aws:cloudtrail. PCRE regex for specifying event names to be excluded. Leave blank to use the default set of read-only event names ^$
index for the excluded CloudTrail events	
Assume Role	
More settings	☐

After clicking More settings, fill in the source type:



10. Click **Save**.

Back in the Inputs screen, you should now see your two new inputs. Click the arrow next to the input name to see some details about the input:



You should now have access to your VEN flow data and auditable event logs. See "Example Splunk Queries" for examples of how to access the data. Illumio can provide additional sample Splunk queries if needed. Contact Illumio Technical Support for assistance.

Speeding Up UI Rendering

If most of your searches will cover a time period of 7 days or less, you can make the panels in the app respond more quickly by modifying the `summariesonly` macro.

1. Choose Settings > Advanced Search > Search Macros.
2. Click the `summariesonly` macro. The macro editor is displayed.
3. Change the definition of the macro to `"summariesonly=true"`.

Configuring Alerts

If you have administrator privileges on the Illumio App for Splunk, you can create or update alert configurations using the Alert Configuration page. By using alert configurations, you can watch for events that are of interest related to a variety of Illumio PCE entities such as rules and workloads.

To display the Alert Configuration page, click Alert Configuration in the top-level navigation menu. This link only appears if your user account has the “admin” role.

After creating alert configurations, use the Alerts page to set up the usage of the alerts, such as sending emails whenever an alert is triggered. See Splunk documentation for details about alert configuration and the Alerts page.

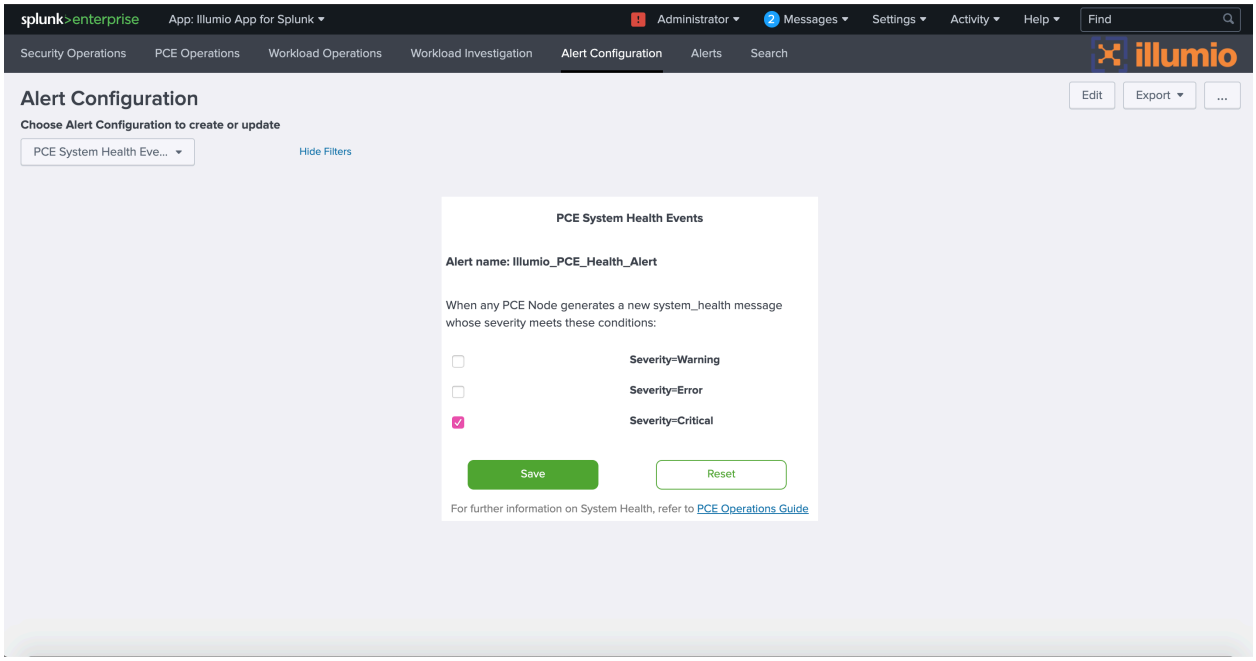
In the Illumio App for Splunk, you can configure five different types of alerts. Choose the desired alert type in the dropdown list on the Alert Configuration screen.

The options in the dropdown are:

- PCE System Health Events
- Rule Set Writing/Update
- Rule Writing Update
- Policy Provisioning
- Workload Labeling

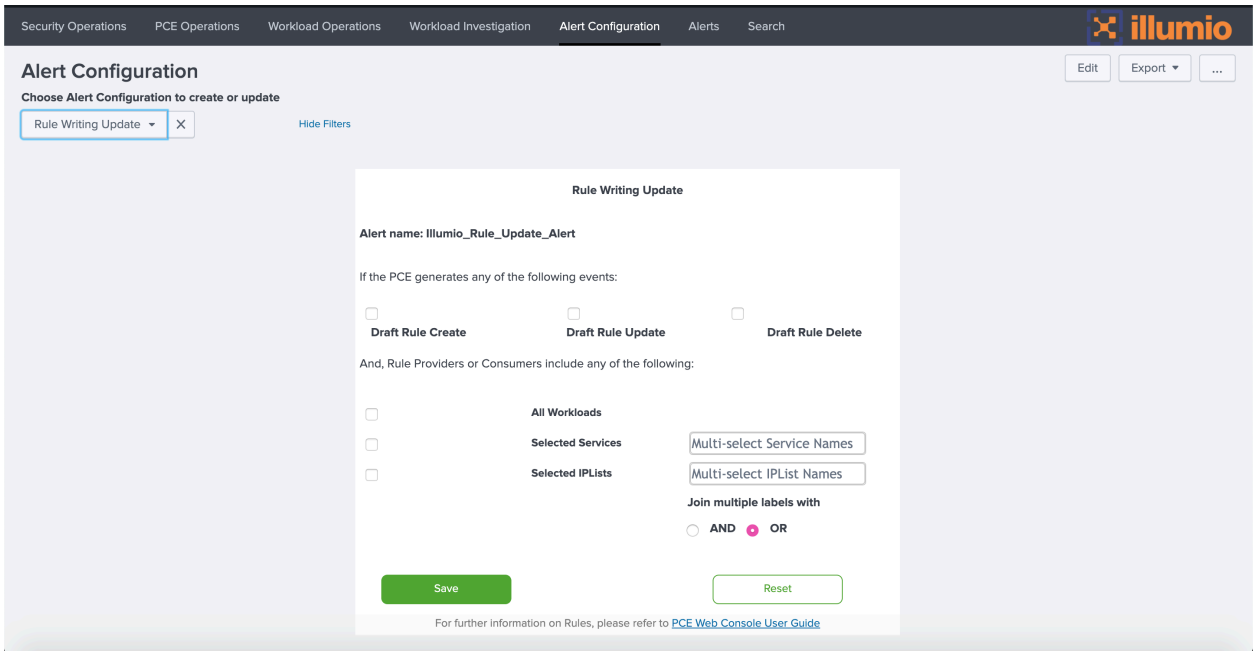
To configure alerts about system health events, choose PCE System Health Events from the dropdown, then choose which level of event severity (warning, error, or critical) to include. For details on conditions that trigger severity of warning or above, see PCE

Operations Guide's section on PCE Health Monitoring with Syslog in the *PCE Operations Guide*.



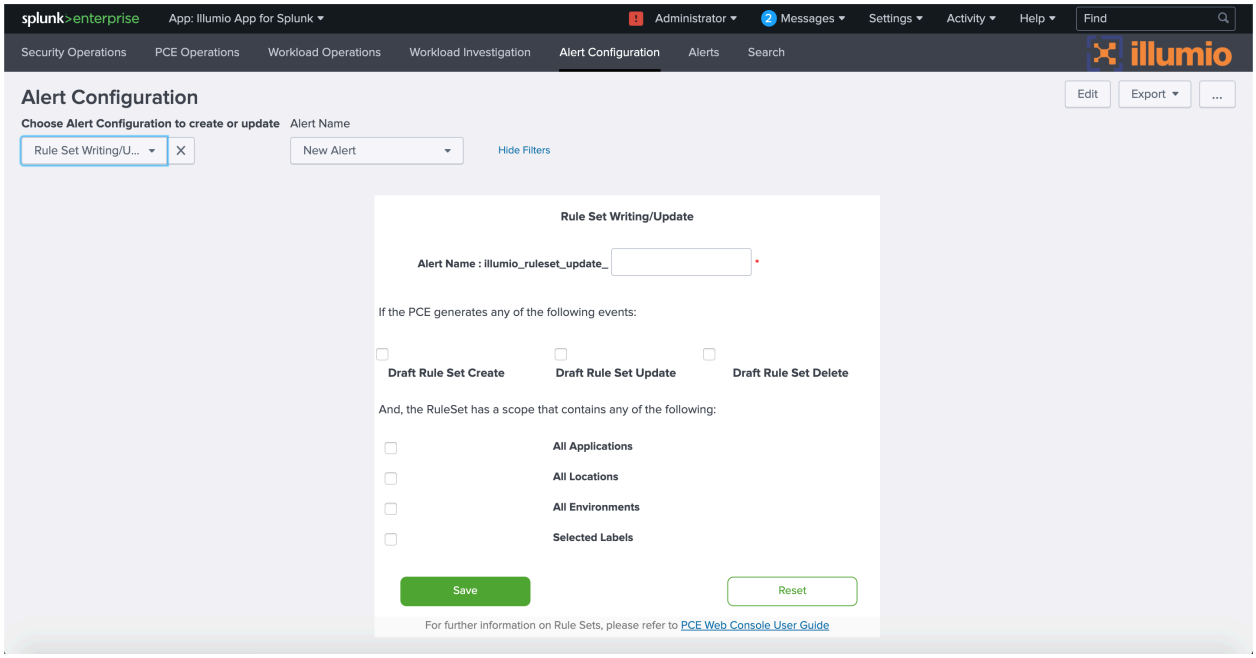
You can configure alerts about changes to rules on the PCE. For example, a draft rule might be created that affects all workloads. Since this is a very wide-ranging effect, which might have been unintentional, you might want to be alerted so you can confirm the rule is correct.

To configure alerts about changes to draft rules, choose Rule Writing Update in the dropdown, then choose which type of rule change to include (create new rule, update a rule, or delete a rule, or any combination) and which rule providers or consumers to include (all workloads, or a subset based on service names or IP lists). Choose the AND operator if all the selected rule providers/consumers must be matched. Choose the OR operator to match any one provider/consumer from the selected list.



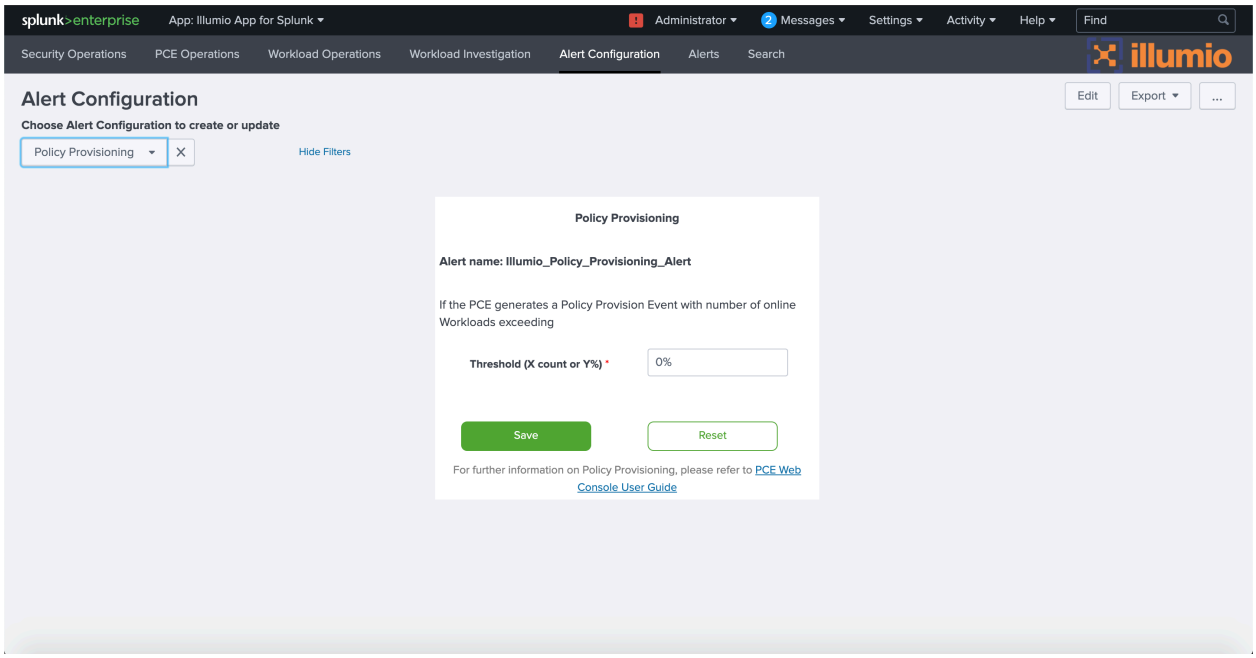
Similarly to rules, you can configure alerts about changes to draft rulesets on the PCE. For example, a draft ruleset might be created that has a broad scope. When provisioned, the ruleset might affect too many workloads unintentionally. It is useful to be alerted so you can confirm the ruleset's scope is correct.

To configure alerts about new, changed, or deleted rulesets, choose Rule Set Writing/Update from the dropdown. In the Alert Name dropdown, choose New Alert if you are setting up a new alert, or choose the name of an existing alert if you want to make changes to its configuration. If you are creating a new alert, give it a name in the Alert Name field. Choose which type of ruleset change to include (create new ruleset, update a ruleset, or delete a ruleset) and which ruleset scopes to include (based on applications, locations, environments, or labels).



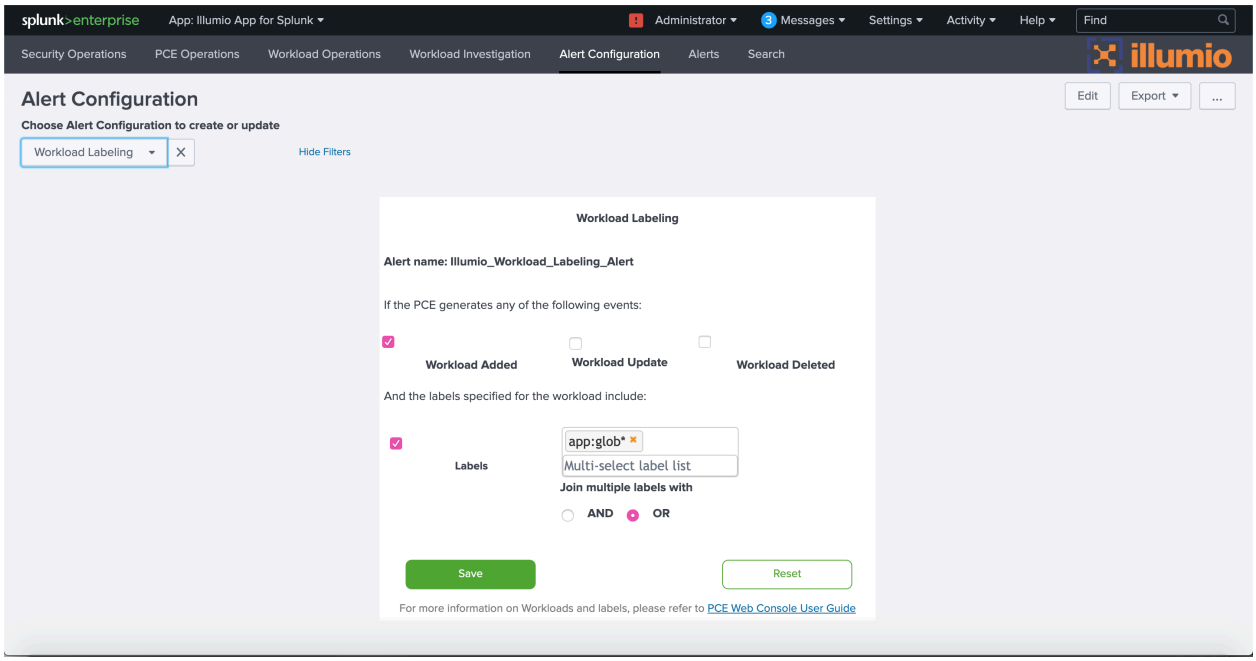
In PCE 19.1.0 and later, you can configure alerts to be triggered when new policies are provisioned. For example, you might want to know if a new policy is being provisioned to a large number of workloads.

To configure alerts about provisioning of new policies, choose Policy Provisioning from the dropdown, then set the minimum number of workloads that must receive the provisioning. The number can be specified as an absolute number, such as 100, or a percentage, such as 10% of the workloads. To trigger the alert no matter how many workloads are involved, set the threshold to 0.



You can configure alerts about changes to workload labels. For example, it might be a reason for concern if a workload label is changed in a way that reduces the workload's security posture, such as changing from "Production Top Secret" to "Internal Testing."

To configure alerts about changes to workload labels, choose Workload Labeling from the dropdown, then choose which type of change to include (add, update, or delete label) and which labels the workload must have. Choose the AND operator if a workload must have all the selected labels. Choose the OR operator to match any one label from the selected list.



Post-Installation Required Settings

After installing and configuring the Illumio App for Splunk, make the following settings.

Accelerate Data Model

The Illumio App for Splunk ships with the Illumio data model acceleration disabled, as required for Splunk App Certification. After installation, you must enable the acceleration of the data model, which is used for visualizations in the dashboards. Use the steps in "Data Model and Data Model Acceleration."

Update Search Macros for Custom Index

If you choose a non-default index, you must update the search macros to use the custom index. Use the steps in "Index, Source, and Source Types."

Upgrade the App

You can upgrade the Illumio App and TA using the CLI or UI.

Upgrade through the CLI:

1. Download the tarball of App or TA from Splunk base.
2. Stop the Splunk server.
3. Run this command:

```
$SPLUNK_HOME/bin/splunk install app APP_NAME.tgz -update 1
-auth username:password
```

4. Start the Splunk Server.
5. If you are upgrading to Splunk 3.0 from a previous version of the app, rebuild the data model after you install the app. See "Data Model and Data Model Acceleration."
6. If you are upgrading to Splunk 3.0 from a previous version of the app, remove any customizations you have made to the app in the `local` directory.

Upgrade through the UI:

1. Click **Manage Apps**.
2. Find the Illumio app and TA entry from the list.
3. If a newer version is available, an entry "Update to …" is displayed.
4. Click the link of the newer version under the version column.
5. If you are upgrading to Splunk 3.0 from a previous version of the app, rebuild the data model after you install the app. See "Data Model and Data Model Acceleration."
6. If you are upgrading to Splunk 3.0 from a previous version of the app, remove any customizations you have made to the app in the `local` directory.

Upgrade by installing files:

1. Click **Manage Apps**.
2. Click **Install App from File**.

3. In the dialog, upload the SPL file corresponding to the newer version of TA or App.
4. Select the **Upgrade App** check box.
5. Click **Upload**.
6. Restart Splunk after uploading both the TA and app.
7. If you are upgrading to Splunk 3.0 from a previous version of the app, rebuild the data model after you install the app. See "Data Model and Data Model Acceleration."
8. If you are upgrading to Splunk 3.0 from a previous version of the app, remove any customizations you have made to the app in the `local` directory.

Alerting Actions and Adaptive Response Framework

This section tells how the Alerting Actions and Adaptive Response Framework work with the Illumio App for Splunk. This section covers features where the Splunk App takes action by invoking update APIs on the Illumio PCE.

There are two types of quarantine provided by Illumio:

- A custom alert action provided for Splunk Enterprise, also called Splunk Core, the base Splunk product. See Using custom alert actions in the Splunk documentation.
- An adaptive response action provided for Splunk Enterprise Security (ES), which is different from the Splunk core product. See Set up adaptive response actions in Splunk Enterprise Security in the Splunk documentation.

The Splunk core already provides standard alert actions such as sending emails, notable events, and calling a Webhook URL. Modular actions on top of standard alert actions are nothing but custom alert actions. These custom alert actions let you invoke Python scripts that use APIs external to Splunk.

The Enterprise Security Suite app provides support for Correlation/Saved Searches with notable actions. When a Splunk Enterprise Security Correlation/Saved Search (with notable event mapped) is executed and gets at least one event in the results, notable events will be created through a standard notable action. These notable events are visible in the Incident Review dashboard of Splunk Enterprise Security App. No other alert action (other than the notable action) is executed automatically, because none are mapped.

Splunk provides the Adaptive Response Framework in the Enterprise Security Suite by leveraging the modular action functionality provided in Splunk_SA_CIM.

Using Splunk Enterprise Security's Adaptive Response Framework, Illumio PCE administrators can quarantine workloads managed by the PCE directly from Splunk Apps whenever the events are detected in Splunk, based on data sent by any source of alerts in Enterprise Security.

There are two ways to invoke actions on the workloads:

- Quarantine workloads using Splunk Core Alert Actions.
- Quarantine workloads using Splunk Enterprise Security Suite's Adaptive Response Framework.

Quarantine Workload Using Splunk Core Alert Actions

If Splunk Enterprise Security Suite (ESS) is not installed in your Splunk infrastructure, the Illumio App for Splunk offers a way to monitor and take action on the events reported by analytics on Illumio PCE logs.

To achieve this, the Illumio Add-on for Splunk leverages the custom alert action to quarantine the workload. These actions are available on the drill downs from the main dashboards.

Quarantine Workload using Enterprise Security Suite

Splunk provides the Splunk Enterprise Security Suite (ESS), which leverages Splunk's Adaptive Response Framework and allows administrators to monitor and manage threats and incidents directly from Splunk apps. It has rich dashboards that help monitor incidents and take actions on these incidents.

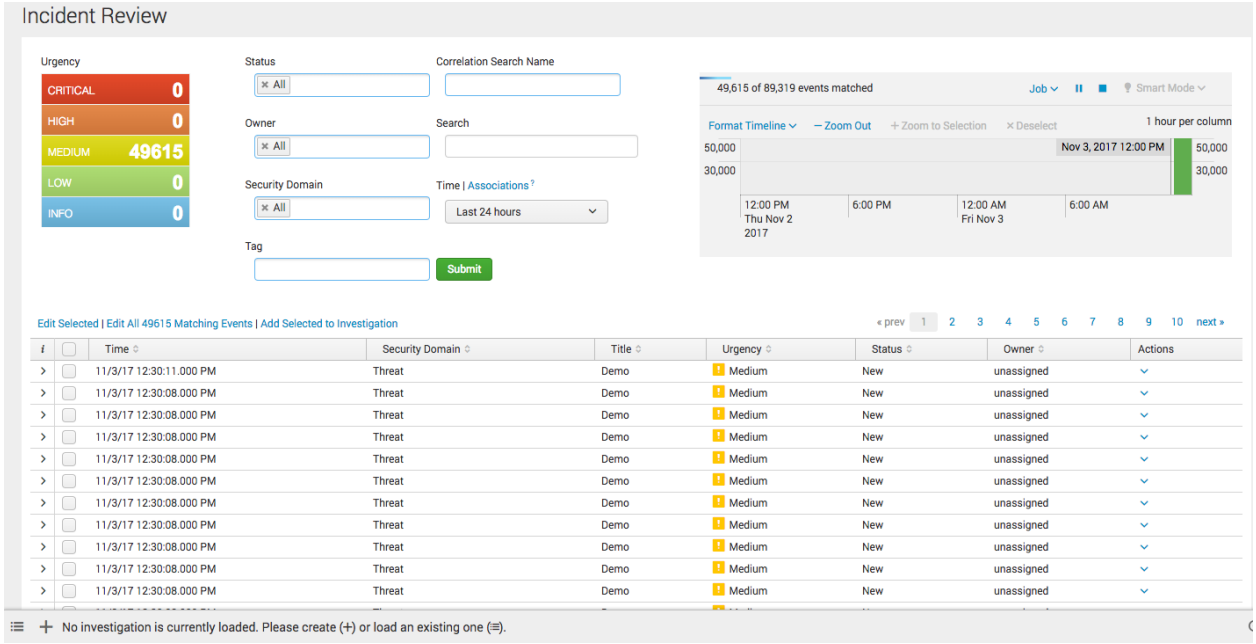
Splunk Enterprise Security Suite is extendable by adding a compatible Module App (Adaptive Response Add-ons) for a particular domain or technology. The Suite detects configurations in these Adaptive Response Add-ons and helps monitor and take actions on the incidents reported by these Add-ons.

The Illumio Add-on for Splunk (TA-Illumio) is one such module for Splunk Enterprise Security Suite. It leverages Splunk Adaptive Response Framework and empowers

System Administrators to monitor and take actions on incidents reported by analytics on Illumio PCE events or logs from the Splunk Enterprise Security Suite dashboards.

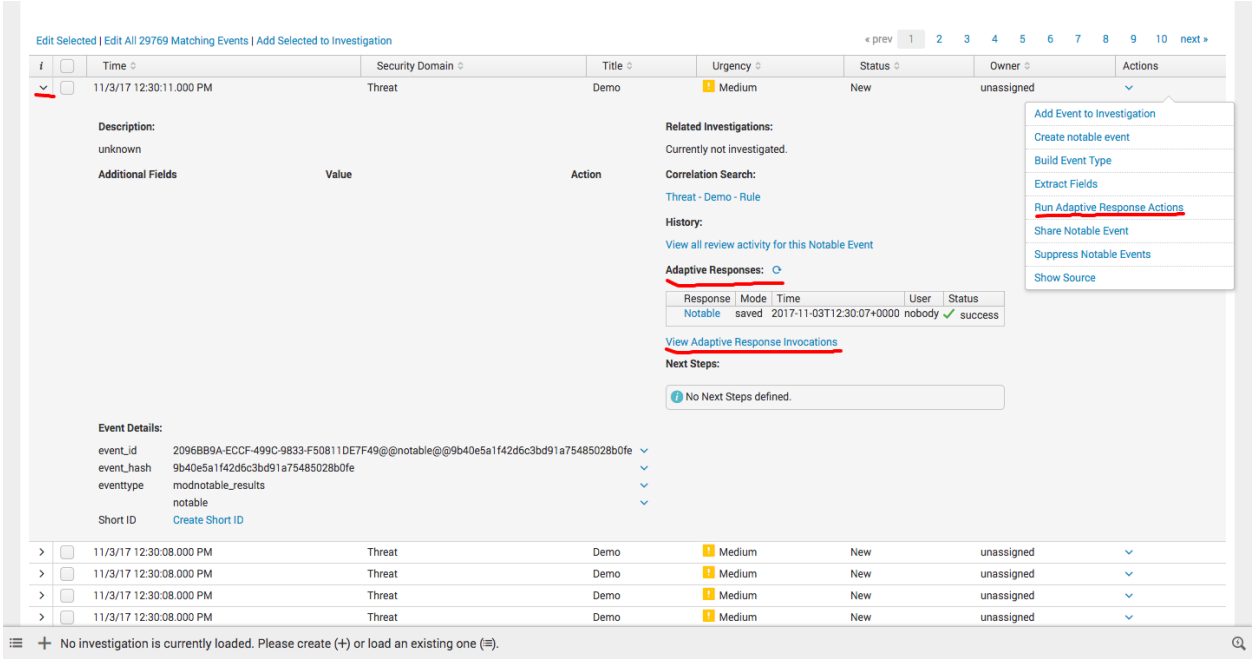
When using the Splunk Enterprise Security (ES) suite, the Illumio Splunk TA can be installed on a single ES Search Head (SH), or on both an ES SH and an associated ES Search Head Cluster (SHC). This allows the Adaptive Response to be invoked from any installed TA location. The Illumio data is stored on the indexers only, and not on the search head nodes, so the data is not duplicated. If the TA is installed only on a single ES SH, the data is normalized for the associated SHC.

The Incident Review dashboard:

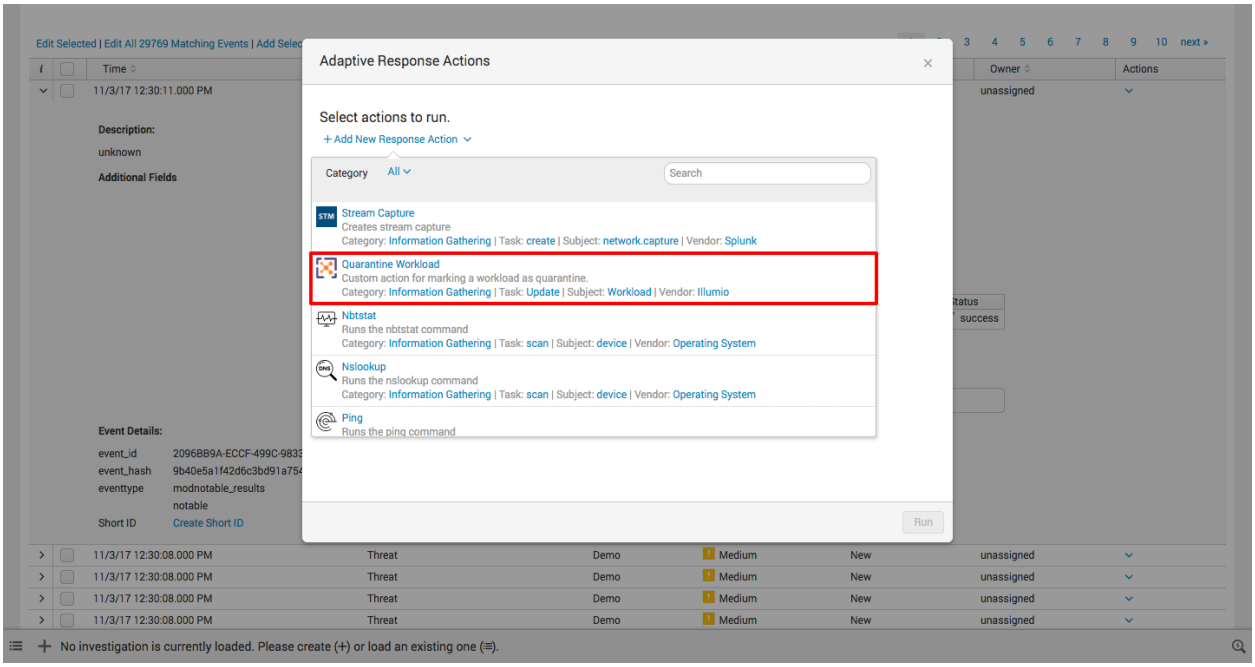


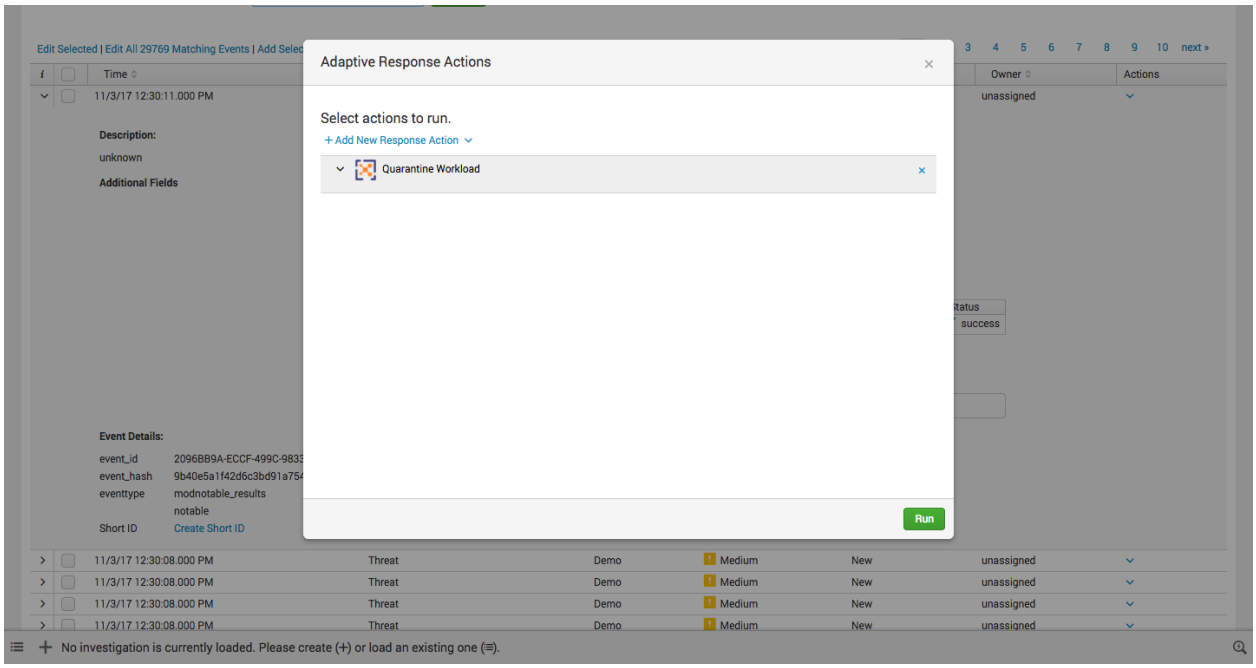
Splunk, as a part of the Adaptive Response Framework, has enhanced this Incident Review dashboard in the Enterprise Security Suite app, which provides the option to take actions on these notable events.

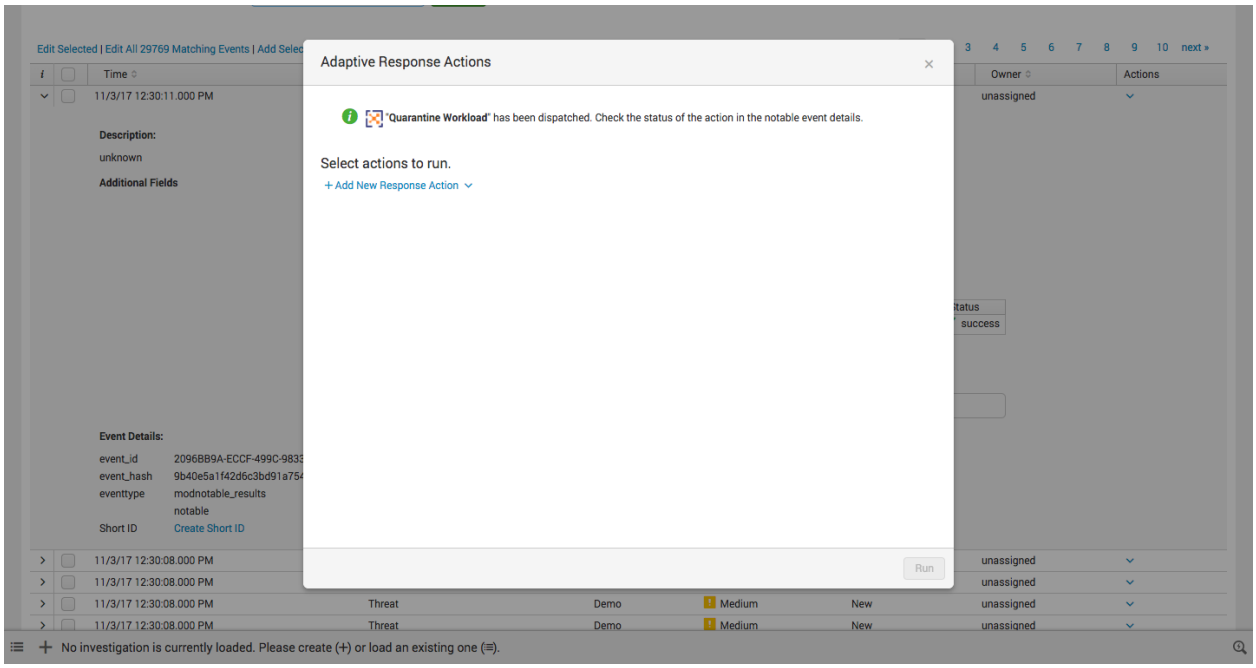
To view the notable event details, expand the left arrow for that notable event.To execute alert actions manually for each of the notable events, click **Run Adaptive Response Actions** for the notable event and select the specific Alert Action.



When you click Run Adaptive Response Actions for a notable event, a menu appears that lists all of the standard and custom actions. This list is created by reading the alert_actions.conf files of all the installed apps on the Splunk instance. Users can select multiple actions on this popup menu and run them for that notable event.







When these actions are run, each selected corresponding action is invoked from alert_actions.conf.

Quarantine Workload from Illumio Splunk App

If you have both the “admin” role and “Illumio_quarantine_workload” role, you can quarantine Workloads from the Illumio Splunk App by clicking the Quarantine button, which appears on the following dashboards:

- Port Scan (on Security Operations dashboard)
- Firewall Tampering (on Security Operations dashboard)

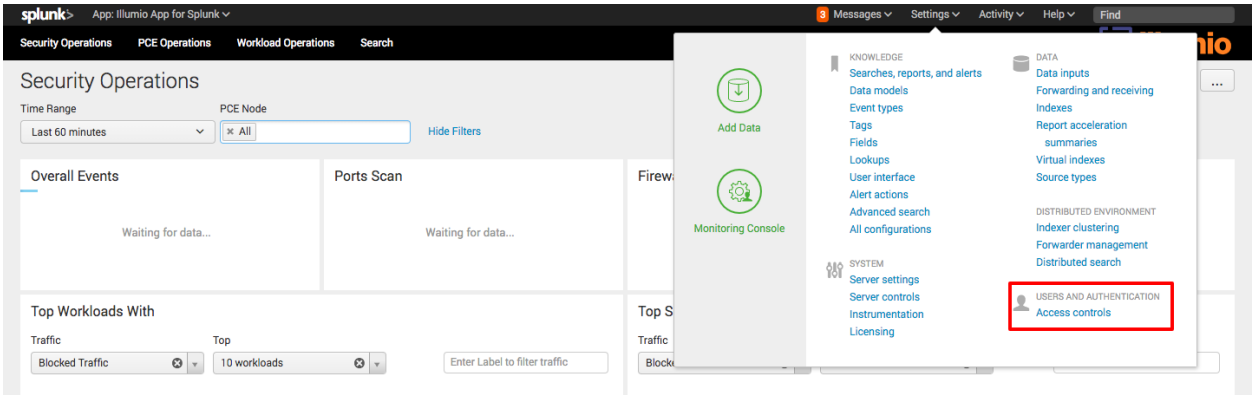
If the Quarantine button is greyed out, then you do not have adequate permissions to quarantine workloads. See “Access to Quarantine Workload Action.”

Access to Quarantine Workload Action

By default, users do not have access to the Quarantine Workload action either in the Splunk App or in Adaptive Response Action.

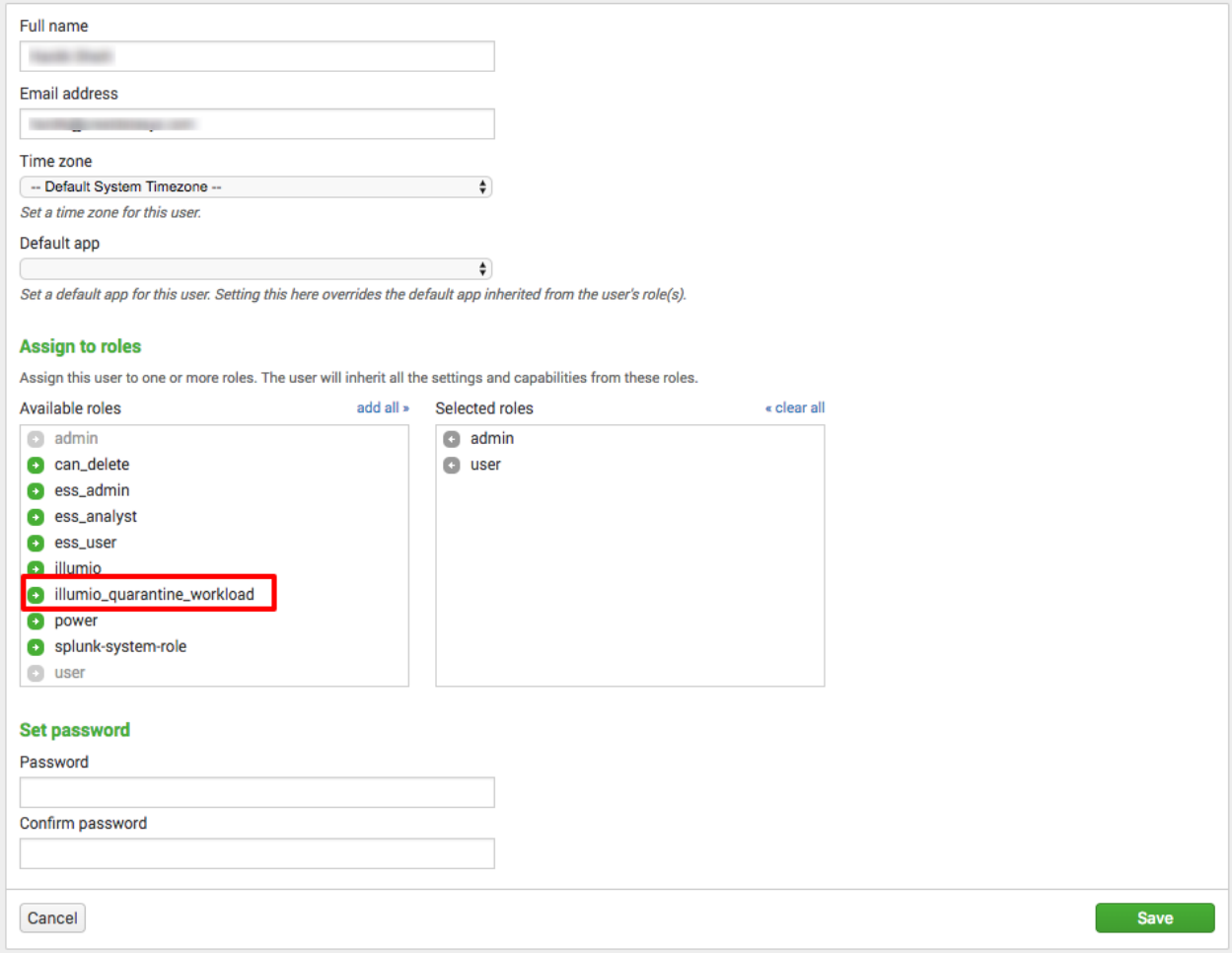
To enable a Splunk user to take quarantine actions on Workloads, grant the user the “Illumio_quarantine_workload” role and the “admin” role. Only local users can be granted this role. SAML users cannot, as their roles are controlled by an external system.

1. Click **Settings** > **Access Control**.



2. Click **Users**.

3. Click the username to which the role needs to be granted.
4. In the Role section of the edit screen, grant the required roles.



5. Click **Save**.

Example Splunk Queries

This section provides sample queries to help you get started writing your own Splunk queries using Illumio data.

Workload report

This is a fairly complicated query, but it can be used to generate a workload report showing the labels associated with each workload. The query results can be exported as CSV for reporting purposes.

```
`illumio_get_index` sourcetype="illumio:pce:metadata"
(illumio_type="illumio:pce:workload") | search "agent.href"="*" fqdn="*" |
rex field=href "orgs\/\d+\/workloads\/(?<workload_uuid>\S+)" | fields
labels{}.href uuid hostname os_id public_ip agent.config.mode
agent.config.log_traffic agent.status.status workload_uuid | mvexpand
labels{}.href | rename labels{}.href as href | lookup
illumio_workload_mapping_lookup href workload_uuid OUTPUTNEW type label |
eval {type}_label=label | stats values(*) as * by workload_uuid | table
hostname, public_ip, os_id, agent.config.mode, agent.config.log_traffic,
agent.status.status, role_label, app_label, env_label, loc_label
```

Top events

```
`illumio_get_index` sourcetype="illumio:pce" | top event_type
```

Top outgoing connections

```
sourcetype="illumio:pce:collector" |  search dir=O | top dst_ip
```

Top incoming connections

```
sourcetype="illumio:pce:collector" |  search dir=I | top src_ip
```

Most active machines

```
sourcetype="illumio:pce:collector" |   search dir=I | top dst_ip
```

Top source ports

```
sourcetype="illumio:pce:collector" |   top dest_port
```

Top machines making connections to machines with a given label

This example query returns the top machines making connections to machines with the Production label:

```
sourcetype="illumio:pce:collector" dest_env_label="Production" | top src_ip
Available label search keys:
dest_role_role, dest_app_label, dest_env_label, dest_loc_label
src_role_label, src_app_label, src_env_label, src_loc_label
```

Top machines with connections in a given network

This example query returns the top machines with connections in 10.0.0.0/8:

```
sourcetype="illumio:pce:collector" | search dst_ip=10.0.0.0/8 | top dst_ip
```

Geolocate destination IPs (plot on a map)

```
sourcetype="illumio:pce:collector"  | search dst_ip!=10.0.0.0/8 | iplocation
dst_ip | geostats count latfield=lat longfield=lon
```

Troubleshooting

This section provides tips to diagnose and fix common issues.

Data collection not working

After installing the application, all dashboards should start populating data. If you don't see data in the dashboards, use the following steps for troubleshooting:

- If you specified a non-default index in the Data Input, confirm that you have modified the macro `illumio_get_index` with indexes selected while creating Data Input (Modular input) and that you have modified the Advanced search for either the default index or your custom index. See "Index, Source, and Source Types".
- Run the following query to verify that data is being indexed into Splunk:

```
search `illumio_get_index` | stats count by sourcetype
```

- Verify that SPLUNK_HOME is pointing to the correct Splunk directory.
- Look for errors in the file ta-illumio.log. This file is in the $SPLUNK_HOME/var/log/TA-Illumio/ folder.
- Check to see whether the selected time range covers the time when the traffic flow summaries were generated.
- If a data model acceleration is disabled, graphs will not display. Enable data model acceleration. See "Data Model and Data Model Acceleration" earlier in this document.

Can't use same port in new Data Input (Modular Input)

Symptom: After deleting an existing configured data input (modular input), can't create a new modular input on the same port.

Cause: The port number is still in the Data Input TCP ports list.

Fix: Remove the port from the Data Input "TCP" ports list before you try to use the same port again. This enables you to re-use the port which was configured in the previous data input (modular input).

Data not available immediately after configuring data input (modular inputs)

Symptom: Upon successful creation of data inputs (modular input), 5 minutes elapse before data starts indexing.

Cause: 5 minutes is the default time interval configured.

Fix: No action is required. This is expected behavior.

Authentication failure on Data Input (Modular Input) page

Fix:

- Check the network connectivity in between applications to ensure that there are no connectivity issues.
- Ensure that the API Key and API Secret stored in the setup page are in sync with the API key generated by the Illumio PCE. As required by App certification, these secrets are stored in a secure key store. If the data input (modular input) is modified, they will need to be entered again, as they cannot be read back from the secure key store.
- If the Illumio Application is deployed on a non-trusted CA or using a self-signed certificate, the certificate directory path has to be provided. The certificate also needs the correct certificate validation trust chain.

Quarantine button is grayed out or does not work as expected

Cause: To use the Quarantine button, the Splunk user needs to have both the 'admin' role and the 'illumio_quarantine_workload' role. If the button is green but does not work as expected, it is likely because of a missing 'admin' role. To investigate the cause, check the file ta-illumio.log for error messages.

Fix: To grant the required roles, use the steps in "Access to Quarantine Workload Action."

Invalid Certificate File error on Data Input (Modular input) page

Cause: The PCE may present an SSL certificate issued by different authorities such as a primary CA, a secondary CA, Local CA authority or even a self-signed certificate. For correct SSL operation, the Splunk server must be able to fully trust the PCE's certificate and verify the certificate's trust chain.

Fix: When a local CA Authority issued SSL certificate or a self-signed SSL certificate is used with the PCE, the CA Certificate bundle needs to be uploaded onto the Splunk Server and the full path to the directory containing the certificate should be provided in the data input.

If using a local CA Authority or a certificate issued by a secondary CA, the Splunk server CA trust chain must be updated to verify the certificate presented by the PCE.

For example, on Linux, use the update-ca-trust tool. Copy the certificate chain to /etc/pki/ca-trust/source/anchors/ and then run the following commands:

```
update-ca-trust force-enable
update-ca-trust extract
update-ca-trust check
```

See Splunk documentation for further information.

PCE labels are not updated in Security Operations dashboard

Symptom: If there are new labels, or workloads are added to the PCE, the new labels and workloads will not be visible right away.

Cause: The default interval to sync workloads and labels from the PCE is set to a minimum of 60 minutes. This period is configurable through the data input. The newly added labels or workloads on the PCE should be available in the Splunk App after an interval of 60 minutes.

Fix: To force a resync of labels to the PCE, you can disable and enable the TA. This forces the TA to make API calls to the PCE. This operation should be used with caution, due to the additional API calls to the PCE.

Security Operations shows “Search is waiting for input”

Symptom: When upgrading an older version of the app, the Security Operations panels do not display graphs. Instead, they display "Search is waiting for input ...".

Cause: Old dashboard files stored locally on the Splunk server.

Fix:

1. Delete the folder $SPLUNK_HOME/etc/apps/IllumioAppforSplunk/local.
2. Restart Splunk.

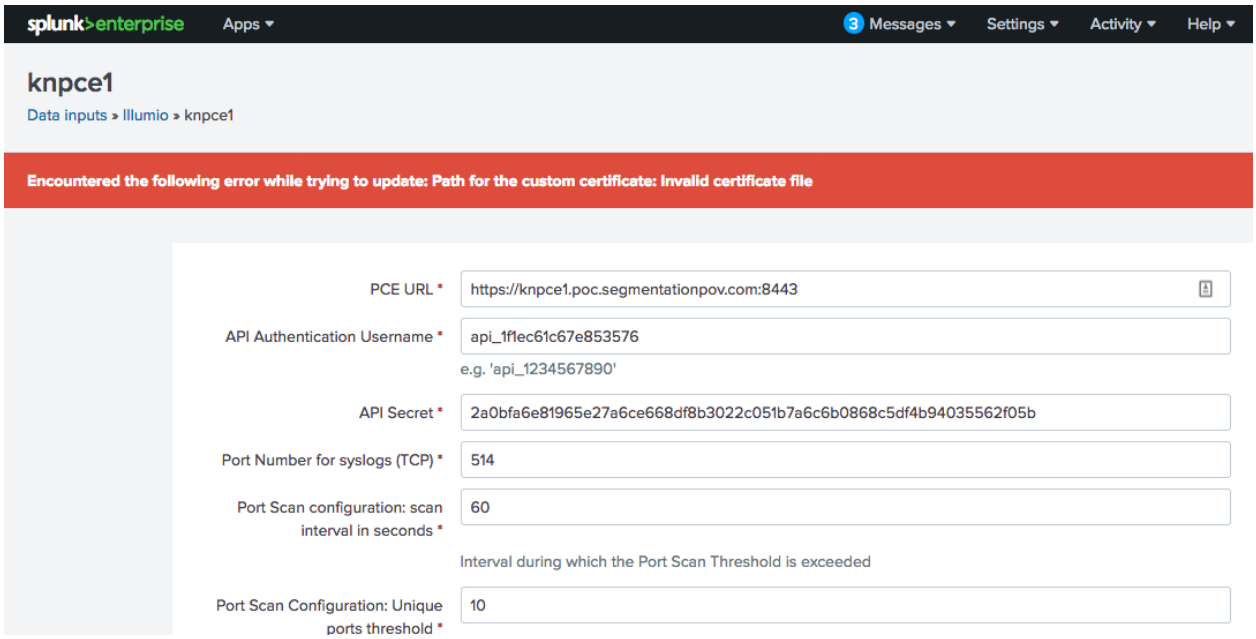
Path for the custom certificate: invalid certificate file

Symptom: An error is generated in the Policy Compute Engine (PCE) `ta-illumio.log` file when attempting to add Illumio Data Inputs. Saving any information for the Data Inputs is not allowed.

```
Error from file /opt/splunk/var/log/TA-Illumio/ta-illumio.log :

2018-10-24 16:33:48,844 - Illumio_MODINPUT - ERROR - Path for the
custom certificate: Invalid certificate file
```

A Splunk error, due to PCE certificate trust, is also displayed:



Cause: This error is an indication that a PCE certificate was not trusted, even though the certificate has already been added the local system certificate store.

Fix: Adding Illumio Data Inputs allows the Illumio App for Splunk to connect to a configured PCE to extract data for PCE health and workloads information. When the Illumio App for Splunk attempts a connection to the PCE, it can fail due to a certificate trust even when a local browser trusted the PCE certificate, since it was already added to the local system certificate store. Splunk uses a Python library that is local to the Splunk application; therefore, it carries its own local certificate authority file it trusts.

There are two ways to add a secure trust to the PCE:

- Add both intermediate and root certificate authority to the local Python cacert.pem file:
    - In Windows: C:\Program Files\Splunk\Python-2.7\Lib\site-packages\requests\cacert.pem
    - In Linux: /opt/splunk/lib/python2.7/site-packages/requests/cacert.pem

    OR,

- Create a certificate file that includes the PCE server certificate, intermediate certificate, and root CA certificate in that order, then place the file in the Splunk home directory. The certificate should be in PEM format. Added the certificate path to the Illumio Data Inputs. Use the following steps:

1. Use a text editor to cut and paste the certificate chain, and avoid extraneous characters. The Splunk home directory is as follows:
   - Windows Splunk home directory: `C:\Program Files\Splunk\`
   - Linux Splunk home directory: `/opt/splunk/`
2. Export the certificates using any browser, then cut and paste them together. The following is an example of what should be in a certificate file:

```
-----BEGIN CERTIFICATE-----

< Sever Certificate base64 encoded >

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

< Intermediate Certificate base64 encoded >

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

< Root CA Certificate base64 encoded >

-----END CERTIFICATE-----
```

3. Set the path in the Illumio Data Inputs under 'Settings > Data Inputs > Illumio > (select input) > checkbox "more settings" > Custom (self-signed) certificate path > (path of certificate)'.

Data Collection: Enabled

☑ More settings

Interval: 3600

Period between making API calls

Host: ILLUMIO-0S0BM9S

Set the host with this value.

Index: default

Set the destination index for this source.

Custom (self-signed) certificate path: c:\Program Files\Splunk\certificate.pem

Path for the custom certificate

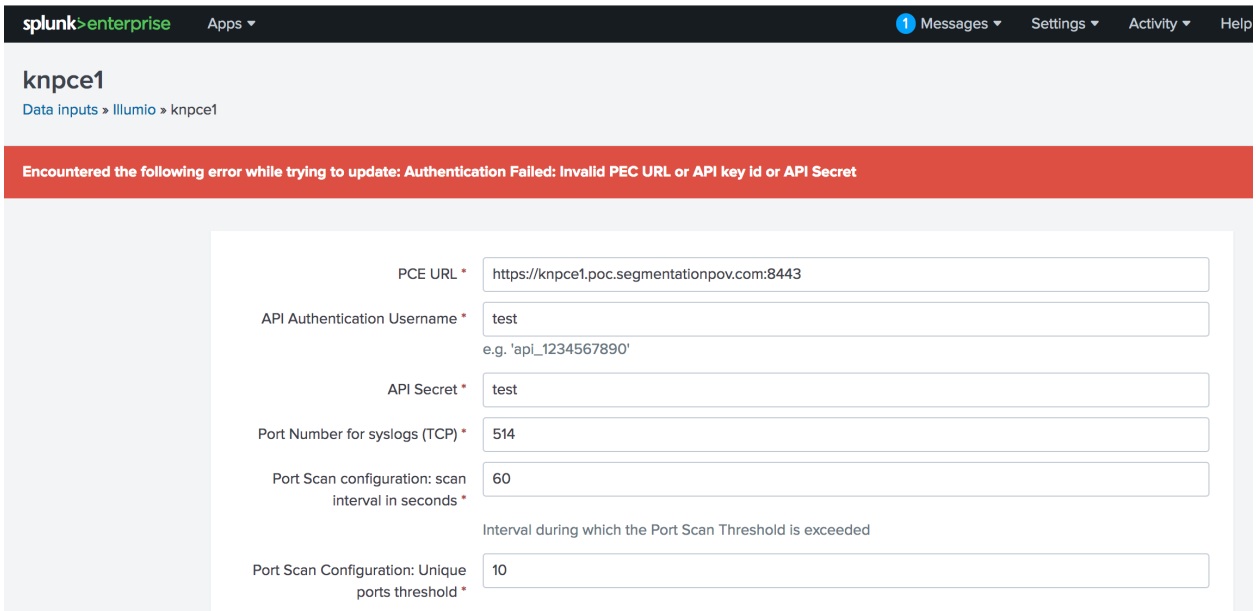
Allowed port scanner IP addresses:

Comma Separated list of hosts, which will be ignored in Port scans

Cancel | Save

Authentication Failed: Invalid PCE URL or API key id or API Secret

Symptom: When applying data inputs in Splunk for the Illumio App for Splunk, you receive the following error from the Splunk UI: “Authentication Failed: Invalid PEC URL or API key id or API Secret.”



The error also appears in the file /opt/splunk/var/log/TA-Illumio/ta-illumio.log.

Cause: This error is caused by an authentication issue to the Policy Compute Engine (PCE). When this occurs, data inputs will not be saved until a valid API response is received from the PCE with the correct API Authentication username and API secret.

Fix: To validate an authentication failure, look at the PCE core node haproxy logs, which will show a 401 auth failure HTTP response (highlighted in yellow in the example below):

```
Mar 11 11:20:36 level=info host=core0.domain.com
program=illumio_pce/agent[12311]:

sec=328436.974 sev=INFO  pid=12389 tid=35453020 rid=92e0c733-
b06f-4619-9624-7e1dbf515eb6 XStarted

GET /api/v1/product_version/ 10.6.7.40

Mar 11 11:20:37 level=warning host=core0.domain.com
program=illumio_pce/agent[12311]:

sec=328437.741 sev=WARN  pid=12389 tid=35453020 rid=92e0c733-
b06f-4619-9624-7e1dbf515eb6

{"category":"auditable","event_type":"authn_failure","severity":
"warning","timestamp":"2019-03-11T18:20:36+00:00",

"href":"/orgs/0/audit_log_events/4e28d281-7cf9-4046-97f1-
fb78060c3b4c","created_by":{"system":{}},

"data":{"uri_path":"/api/v1/product_version/","username":"api_1f
1ec61c67e853576","src_ip":"10.6.7.40"}}

Mar 11 11:20:37 level=info host=core0.domain.com
program=illumio_pce/agent[12311]:  sec=328437.745

sev=INFO  pid=12389 tid=35453020 rid=92e0c733-b06f-4619-9624-
7e1dbf515eb6 XCompleted 401

GET /api/v1/product_version/ 10.6.7.40 0.099828328

Mar 11 11:20:37 level=info host=core0.domain.com
program=haproxy[2624]:  10.6.7.40:56152

[11/Mar/2019:11:20:36.969] https~ agent/agent0 3/0/0/103/106 401
304 - - ---- 1/1/0/1/0 0/0

{|keep-alive} "GET /api/v1//product_version/ HTTP/1.1"
```

To see whether the API username/secret is correct, use the cURL command below and validate it with the logs from PCE core nodes:

```
Copy and paste the curl command below with the correct API
username/secret:



- - - Begin copy (change api username/secret) - - -

curl \

-u \

api_1f1ec61c67e853576:2a0bfa6e81965e27a6ce668df8b3022c051b7a6c6b
0868c5df4b94035562f05b \

-H Content-Type:application/json \

-X GET \

'https://pcecore0.domain.com:8443/api/v1//product_version/' \

| python -mjson.tool

- - - End copy - - -




Successful curl request logs from PCE core nodes with 200 http
response code:



Mar 11 11:45:44 level=info host=core0.domain.com
program=illumio_pce/agent[23340]:  sec=329944.610 sev=INFO

pid=23408 tid=24064620 rid=063accb6-7036-46f0-96a1-8726f14436ea
XStarted GET /api/v1/product_version/ 10.6.7.40

Mar 11 11:45:44 level=info host=core0.domain.com
program=illumio_pce/agent[23340]:  sec=329944.734 sev=INFO

pid=23408 tid=24064620 rid=063accb6-7036-46f0-96a1-8726f14436ea
XCompleted 200 GET /api/v1/product_version/ 10.6.7.40
0.124496975

Mar 11 11:45:44 level=info host=core0.domain.com
program=haproxy[2624]:  10.6.7.40:56446
[11/Mar/2019:11:45:43.966]

https~ agent/agent0 643/0/0/126/769 200 442 - - ---- 2/2/0/1/0
0/0 {115|keep-alive} "GET /api/v1//product_version/ HTTP/1.1"
```

On the Splunk server, a successful request will allow the data inputs to be saved without any errors in the PCE web console or the `/opt/splunk/var/log/TA-Illumio/ta-illumio.log` file. Tail the `ta-illumio.log` when configuring the data inputs to see the latest logs. Enabling and disabling the data inputs will trigger the request to the PCE, which is a good way to test it.

The data input information should be saved in the location below without the API username/password:

```
/opt/splunk/etc/apps/IllumioAppforSplunk/local/inputs.conf


[illumio://knpce1]

api_key_id =

api_secret =

cnt_port_scan = 10

enable_data_collection = Enabled

interval = 3600

pce_url = https://pce.domain.com:8443

port_number = 514

self_signed_cert_path = /opt/splunk/custom_certificate.cer

time_interval_port = 60

disabled = 0
```

Sankey diagram is not displayed in Traffic Explorer dashboard

- You need to install the Sankey Diagram App in order to visualize the diagram in the “Communications Map between Labeled Workloads” panel.

Label filters (i.e.App, Env and Loc) are not populated

- Try to run the "Illumio_Workload_Mapping" saved search via expanding time range.
- Make sure that interval configuration for input is less than 24 hours.

Known Limitations

- In case of multiple input configuration, port scan will be done based on the last configured input's port scanner threshold value for all the inputs.
- In Splunk version 7.1, real-time search options will not be disabled, because of a known Splunk issue. Reference: [SPL-76798] https://docs.splunk.com/Documentation/Splunk/7.1.0/ReleaseNotes/KnownIssues
- Due to certification requirements, the TA only supports TCP for syslog.
- Due to certification requirements, data model acceleration is disabled by default. Without data model acceleration, some visualizations will not work. You can enable data model acceleration, if needed, using the steps in "Data Model and Data Model Acceleration."
- Editing data input (modular input) while it is disabled can lead to exposing the Key_ID and the Secret of the user.

Compatibility Matrix

PCE Versions	Splunk Version	Illumio App for Splunk Version	Illumio TA Version
17.1, 17.2, 17.3, 18.1	6, 7	1.x	1.1.3
18.2.0*, 18.2.x, 18.3, 19.1, 19.3	7	2.x	2.2.1, 2.3.0
18.2.0*, 18.2.x, 18.3, 19.1, 19.3	7, 8**	3.x	3.x

PCE Versions	Splunk Version	Illumio App for Splunk Version	Illumio TA Version
18.2.0*, 18.2.x, 18.3, 19.1, 19.3, 20.1, 21.2.x	7.3, 8.0, 8.1, 8.2	3.2	3.2

* Special configuration is needed with version 18.2.0. Contact Illumio Support.

** The Illumio App for Splunk 3.x is compatible with Python 2 and Python 3. Python 3 is available starting in Splunk 8.0.