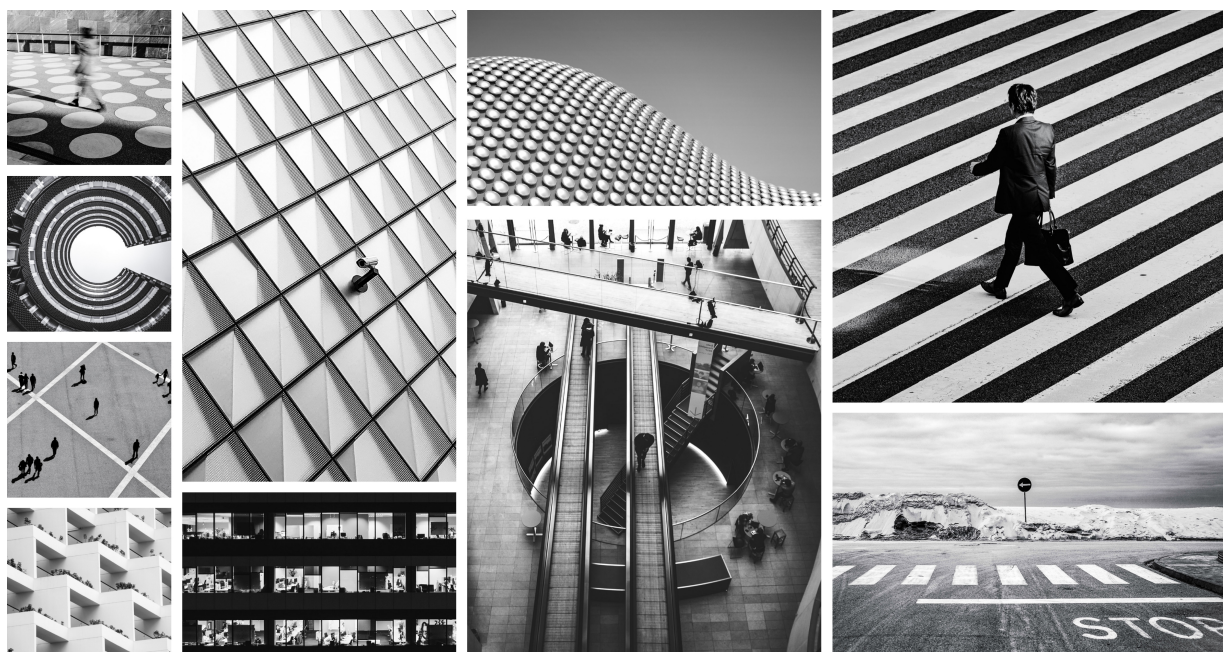




Illumio App for Splunk Version 4.0.x

Integration Guide



The Illumio App for Splunk integrates with the Illumio Policy Compute Engine (PCE) to provide security and operational insights into your Illumio-secured data center with seven visibility dashboards.

The Illumio Technology Add-On for Splunk enriches Illumio Policy Compute Engine (PCE) data with Common Information Model (CIM) field names, event types, and tags. This TA enables Illumio data to be easily used with Splunk Enterprise Security, Splunk App for PCI Compliance, etc.

Table of Contents

What's in This Guide	5
What's New in This Guide	6
Illumio Technology Add-On for Splunk 4.0.3	7
What's New in Version 4.0.3	7
Illumio Technology Add-On for Splunk 4.0.2	8
What's New in Version 4.0.2	8
Configure the Search Head for Splunk Enterprise	8
Illumio Technology Add-On for Splunk 4.0.1	10
What's New in Version 4.0.1	10
Related Links	10
Introducing the Illumio Technology Add-On for Splunk	10
Related Links	11
Workload Quarantine Action	11
Run the Action Manually	11
Illumio App for Splunk 4.0	13
What's New in This Guide	13
About the Illumio Splunk Integration	13
Supported Splunk Versions	14
About Illumio Event Data Collection	14
About the Illumio Technology Add-On for Splunk	15
Sourcetypes	16
Distributed Splunk Architecture	16
Field Extractions	17
Workload Quarantine Action	19
About the Illumio App for Splunk	19
Distributed Splunk Architecture	19
Dashboards	20
Data Model	25
Install the Illumio Splunk Apps	27
Install the Illumio Splunk Apps in a Distributed Environment	27
Install the Illumio Technology Add-On for Splunk in a Standalone Environ- ment	28
Configure the Illumio Technology Add-On for Splunk	28
Working with Alert Actions and Quarantines	29
Configure the Illumio Modular Input	29
Configure TCP SSL	32
Configure Syslog Forwarding for On-Prem PCEs	33
Configure Syslog Forwarding for Cloud PCEs	33
Install the Illumio App for Splunk	34
Configure the Illumio App for Splunk	34
Upgrade the Illumio App for Splunk	35
About Alerting Actions and the Adaptive Response Framework	36
Provide Access to the Quarantine Workload Action	36
Quarantine Workloads Using Splunk Core Alert Actions	38
Quarantine Workload Using Enterprise Security Suite	38
Quarantine Workloads from the Illumio Splunk App	41
Uninstall the Splunk Integration Apps	42
Troubleshooting Splunk Integration Apps	42
Illumio Technology Add-On for Splunk	42
Event Forwarding (On-Premises PCE)	43
Forwarded Events Do Not Show Up In Splunk	43
Data Not in kvstore	43
Test the PCE Connection	44

Troubleshooting the Illumio App for Splunk	44
Troubleshooting Illumio Technology Add-On for Splunk Version 4.0.2	45
Known Issues and Limitations	46
Service Account API Keys	46
Illumio Supercluster	46
Known Issue on TA-Illumio 4.0.2 and Above	47

What's in This Guide

This guide documents how to install, configure, and troubleshoot the Illumio App for Splunk and the Illumio Technology Add-On for Splunk for version 4.0 through version 4.0.3.

For information about how to install and configure the Illumio App for Splunk and the Illumio Technology Add-On for Splunk, see [Install the Illumio Splunk Apps \[27\]](#).

What's New in This Guide

This guide documents how to install, configure, and troubleshoot the Illumio App for Splunk and the Illumio Technology Add-On for Splunk for version 4.0 through version 4.0.3.

Version	Release Date	Release Notes
4.0.3	December 11, 2024	<ul style="list-style-type: none">• Updates the Splunk SDK to 2.1.0.• Updates the datatypes in collections.conf to use only string, number, bool, and time for Splunk Cloud vetting standards.
4.0.2	August 14, 2024	<ul style="list-style-type: none">• Addresses limitations in kvstore files in a Splunk Enterprise distributed deployment.
4.0.1	November 30, 2023	<ul style="list-style-type: none">• Enriches Illumio Policy Compute Engine (PCE) with Common Information Model (CIM) field names, event types, and logs.
4.0.0	November 17, 2023	<ul style="list-style-type: none">• Initial release of version 4.0.0.

Illumio Technology Add-On for Splunk 4.0.3

What's New in Version 4.0.3

Illumio Technology Add-On for Splunk version 4.0.3 updates the Splunk SDK to 2.1.0 and updates the datatypes in collections.conf to use only string, number, bool, and time in accordance with Splunk Cloud vetting standards.

Illumio Technology Add-On for Splunk 4.0.2

What's New in Version 4.0.2

Illumio Technology Add-On for Splunk version 4.0.2 has been developed to address limitations of kvstore files in a Splunk Enterprise distributed deployment. These updates are specific to the Illumio Technology Add-On (TA) for Splunk.

Configure the Search Head for Splunk Enterprise



IMPORTANT

This procedure is applicable to Illumio Technology Add-On for Splunk version 4.0.2.

While you configure modular input on Splunk Enterprise, ensure that the following section is configured according to your environment.

Search head configuration

Enter fqdn and username in the format username@fqdn and password of splunk search head instance. This setting is only applicable to Splunk Enterprise deployment.

Search Head Credentials

Delete

Add Search Head credentials

After you enter the data, save it. The search head credentials are saved in the storage/passwords endpoint.

To ensure that the credentials have been saved, invoke the following URL:

```
https://<splunk_url>:8089/servicesNS/nobody/TA-Illumio/storage/passwords?output_mode=json&search=kvstore://
```

Note that the username and password are saved with 'kvstore//' as the prefix.

Ensure that the search head credentials are configured as follows:

1. Configure the username as `username@fqdn_search_head`. An example would be `splunk@splunkindsearch.ilabs.io`, where `splunk` is the username to log into `splunkindsearch.ilabs.io`.
2. Enter the password, and click Add search credentials to add more search head entries. This ensures that kvstore files are copied over to all search heads that you configured previously after the modular input runs.

Whenever the modular input runs, an API call is made to the PCE, responses are stored in kvstores, and data is copied over to search head nodes as configured in the modular input.

Illumio Technology Add-On for Splunk 4.0.1

What's New in Version 4.0.1

The Illumio Technology Add-On (TA) for Splunk enriches Illumio Policy Compute Engine (PCE) with Common Information Model (CIM) field names, event types, and logs.

The TA enables Illumio data to be used with Splunk Enterprise Security, Splunk App for PCI Compliance, and more.



IMPORTANT

In version 4.0.0, Syslog prefixes are stripped at index-time for JSON-formatted events. Because of this change, the search-time extractions and transforms for version 4.0.0 are incompatible with data indexed by previous versions of the TA. See the Upgrade section in the README (or the Installation Instructions pane) for instructions about how to convert data and custom searches from previous versions of the TA.

Related Links

For dashboards with Illumio data, install the [Illumio App for Splunk](#).

Introducing the Illumio Technology Add-On for Splunk

The Illumio Technology Add-On (TA) for Splunk enriches Illumio Policy Compute Engine (PCE) data with Common Information Model (CIM) field names, event types, and tags.

The TA enables Illumio data to be used with Splunk Enterprise Security, Splunk App for PCI Compliance, and more.



IMPORTANT

In version 4.0.0 and later, Syslog prefixes are stripped at index-time for JSON-formatted events. Due to this change, the search-time extractions and transforms for version 4.0.0 are incompatible with data indexed by previous versions of the TA. See the Upgrade section in the README (or the Installation Instructions pane) for instructions on how to convert data and custom searches from previous versions of the TA.

Related Links

For dashboards with Illumio data, install the [Illumio App for Splunk](#).

Workload Quarantine Action



NOTE

This information in this topic applies to Illumio Technology Add-On for Splunk version 4.0.1.

Illumio Technology Add-On for Splunk version 4.0.1 provides a scripted alert action to move a workload into a configured quarantine zone.



IMPORTANT

You must first define the policy and labels for this quarantine zone on the PCE.

The action takes the following parameters:

- `workload_href`: This is the PCE workload HREF of the workload to move into quarantine.
- `pce_fqdn`: The PCE fully-qualified domain name.
- `org_id`: This is the PCE organization ID. The value defaults to 1.

When triggered, the alert action script looks up the modular input matching the given `pce_fqdn` and `org_id` and uses the configured PCE connection details while updating the specified workload.



IMPORTANT

For the action to run successfully, you must configure the API key for the input to have write permissions for workloads.

Run the Action Manually

Run this search query from the Splunk UI to quarantine the workload with the specified HREF:

```
| makeresults 1 | sendalert illumio_quarantine param.workload_href="/orgs/1/workloads/
```

```
00f13a7b-0386-4943-a96c-cfd71d4096dd" param.pce_fqdn="my.pce.com"  
param.org_id=1
```


Illumio App for Splunk 4.0

What's New in This Guide

Ver-sion	Release Date	Release Notes
4.0.0	November 17, 2023	<ul style="list-style-type: none"> Initial release of version 4.0.0.
4.0.1	November 30, 2023	<ul style="list-style-type: none"> Enriches Illumio Policy Compute Engine (PCE) with Common Information Model (CIM) field names, event types, and logs. See What's New in Version 4.0.1 [10].
4.0.2	August 14, 2024	<ul style="list-style-type: none"> Addresses limitations in kvstore files in a Splunk Enterprise distributed deployment. See What's New in Version 4.0.2 [8].
4.0.3	December 11, 2024	<ul style="list-style-type: none"> Updates the Splunk SDK to 2.1.0 Updates the datatypes in collections.conf to use only string, number, bool, and time for Splunk Cloud vetting standards. See What's New in Version 4.0.3 [7].

About the Illumio Splunk Integration

The Illumio Splunk integration contains two parts:

- The Illumio Technology Add-On, or TA, which performs metadata collection and event parsing.
- The Illumio App for Splunk, which provides dashboards and reports to display important data from the Illumio PCE.

Install the TA to each tier of a distributed Splunk deployment, but install the app only on the search head or search head cluster:

Component	Forwarder	Indexer	Search Head
Illumio Technology Add-On for Splunk	Yes (Heavy Forwarder only) - data collection and modular input	Yes - index-time filtering and transforms	Yes - search-time field extractions and transforms
Illumio App for Splunk	No	No	Yes

Specific recommendations for the configuration and topology of a distributed Splunk environment are outside the scope of this document. See the documentation on [Splunk Validated Architectures](#) for suggestions on topology for distributed deployments.

Supported Splunk Versions

- v4.0.2: Splunk 9.3, 9.2, 9.1, 9.0, 8.1 + PCE 21.5, 22.2, 22.5, 23.2, 23.5, and SaaS
- v4.0.1: Splunk 9.1, 9.0, 8.2, 8.1 + PCE 21.5, 22.2, 22.5, 23.2, and SaaS



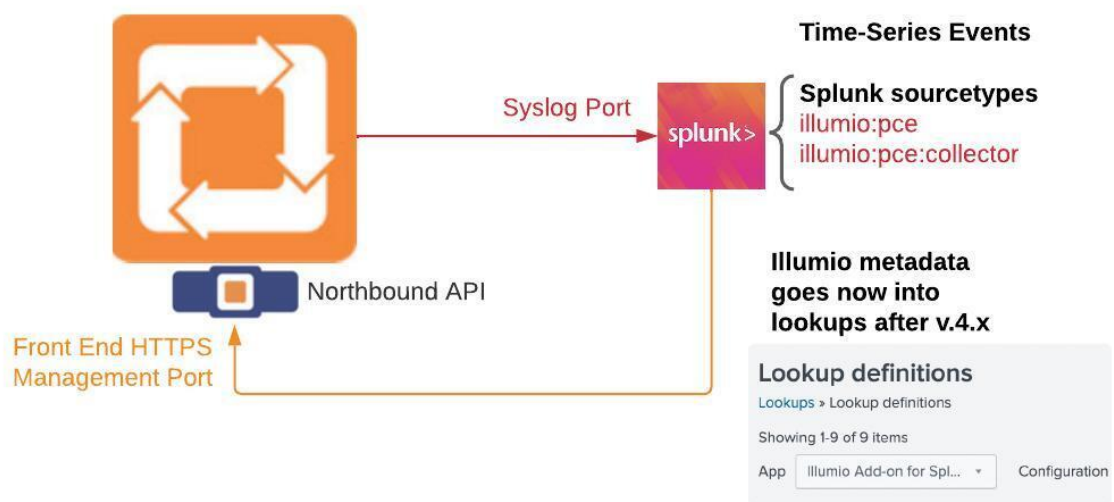
IMPORTANT

Version 4.0.2 consists of TA-Illumio version 4.0.2 and Illumio App for Splunk version 4.0.1.

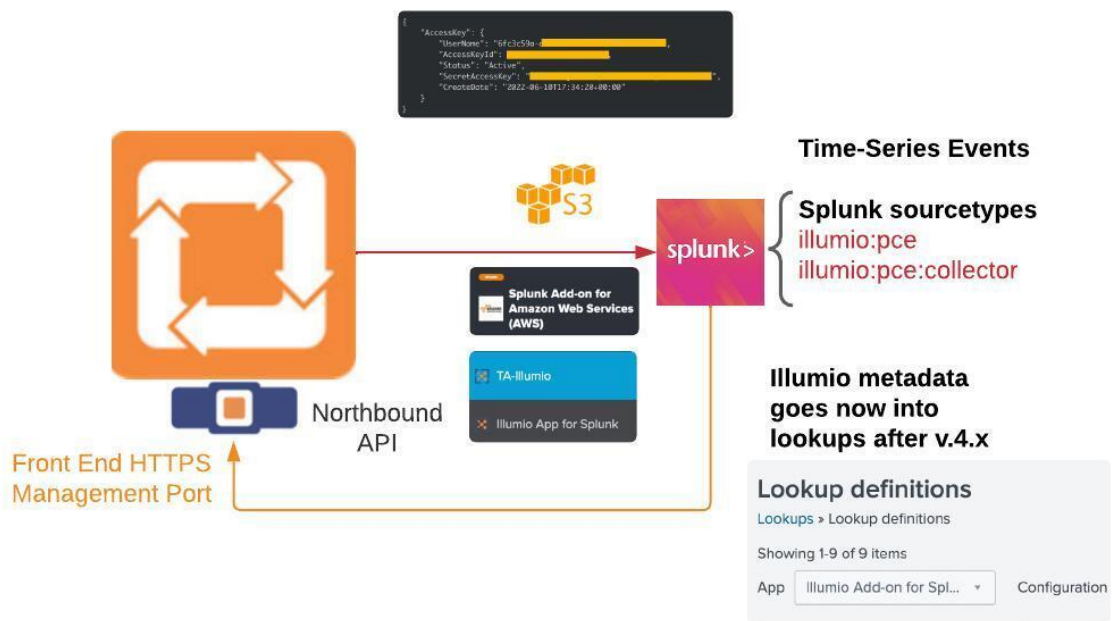
Splunk Common Information Model (CIM) versions 4.x and 5.x are supported.

About Illumio Event Data Collection

The following diagram describes how Illumio event data is collected for On-Premises deployments:



The following diagram describes how Illumio event data is collected for Cloud deployments:



The following diagram describes how often Illumio event data is collected and is then available for search:

How often is Illumio event data collected ?

Type of PCE Solution	Sourcetype	Data Input Mechanism	Frequency (Data availability)
OnPrem	illumio:pce	Syslog	Real-Time. Not configurable Illumio Audit Events are sent to the Syslog Server as soon as they happen.
	illumio:pce:collector		Every 10 minutes. Not configurable. VEN collects Traffic flow logs for 10 minutes and then sends them to the PCE.
	illumio:pce:metadata	API	60 minutes (Default) Configurable
SaaS	illumio:pce	Amazon S3 Bucket	Every 15 minutes. Illumio Audit Events are instantly sent to the S3 bucket but availability of data will depend on polling interval configuration on Data Input
	illumio:pce:collector		Every 15 minutes. Illumio Traffic Flow logs are sent approximately every 10 minutes from PCE to the S3 bucket but availability of data will depend on polling interval configuration on Data Input
	illumio:pce:metadata	API	60 minutes (Default) Configurable

Data is available

About the Illumio Technology Add-On for Splunk

The Illumio Technology Add-On for Splunk (TA) pulls data into Splunk and performs data normalization and enrichment. Illumio event fields are aliased and transformed to be compatible with the Common Information Model (CIM) and used with other Splunk products and add-ons.

The Illumio TA defines a custom Illumio modular input that can be configured on a stand-alone Splunk instance or Heavy Forwarder to retrieve data from the PCE. See [Configure the Illumio Technology Add-On for Splunk \[28\]](#).

The TA receives data from the Illumio Policy Compute Engine (PCE) in two forms:

- Metadata pulled by the Illumio modular input from the PCE REST APIs
The Illumio modular input pulls Illumio object metadata and status information from the PCE over HTTPS. The input calls the following endpoints:
 - **/api/v2/health**
 - **/api/v2/orgs/<org_id>/workload_settings** (used to verify the org ID when validating the PCE connection configuration)
 - **/api/v2/orgs/<org_id>/labels**
 - **/api/v2/orgs/<org_id>/workloads**
 - **/api/v2/orgs/<org_id>/sec_policy/active/ip_lists**
 - **/api/v2/orgs/<org_id>/sec_policy/active/services**
 - **/api/v2/orgs/<org_id>/sec_policy/active/rule_sets**
- Syslog events forwarded directly from the PCE (on-prem) or pulled using a third-party add-on as described in the document (SaaS)

Sourcetypes

The Illumio modular input writes to a user-configured Splunk index and predefined source-types:

Sourcetype	Description
illumio:pce	Contains PCE auditable events written to Syslog.
illumio:pce:health	Contains PCE system health events.
illumio:pce:collector	Contains PCE network traffic flow events.

Distributed Splunk Architecture

Install the Illumio Technology Add-On for Splunk on each tier of a distributed Splunk installation. For more information, see the [Splunk documentation on where to install add-ons](#).

Heavy Forwarder: Configure Illumio modular input instances and TCP receivers to retrieve PCE data and forward it to the indexer/indexer cluster.

Indexer: Install on the indexer/indexer cluster to perform index-time filtering and transformations, including stripping the Syslog prefix for JSON-formatted events.

Search head: Install on the search head/search head cluster to perform search-time transformations such as lookups, field extractions, and field aliasing.

Field Extractions

The custom Illumio sourcetypes define field extractions to enhance event data at search time. Extractions and aliases modify field names and values for CIM compatibility as shown in the following table.

Table 1. CIM Mapping

Sourcetype	CIM Data Model	Tags	CIM Field	Illumio Field
illumio:pce	Authentication	authentication	action	"success" or "failure"
			app	"illumio_pce"
			src	action.src_ip
			user	resource.user.user-name OR notifications.info.*user.username
			src_user	created_by.user.user-name
	All Change	change	change_type	same as object_category
			dest	pce_fqdn
			dest_host	pce_fqdn
			object	object name or value
			object_category	object type (such as workload or rule_set)
			object_id	object HREF
			src	action.src_ip
			status	status
			user	created_by.user.user-name
			user_name	alias for user
			vendor_product	"illumio:pce"
			src_user	created_by.user.user-name
	Network Changes	change network	action	"modified"

Sourcetype	CIM Data Model	Tags	CIM Field	Illumio Field
	Auditing Changes	change audit	action	"created", "updated", or "deleted"
	Account Management	change account	action	"created", "updated", "deleted", or "modified"
			user	resource.user.username OR notifications.info.*user.username
illumio:pce:collector	Network Traffic	network communicate	action	"allowed", "potentially-blocked", "blocked", or "unknown"
			app	"illumio_pce"
			bytes	tbi + tbo
			bytes_in	tbi
			bytes_out	tbo
			dest	dst_ip
			dest_ip	dst_ip
			dest_host	dst_hostname
			dest_port	dst_port
			direction	"inbound", "outbound", or "unknown"
			dvc	pce_fqdn
			protocol_version	version
			src	src_ip
			src_ip	src_ip
			src_host	src_hostname
			transport	proto
			user	un
			vendor_product	"illumio:pce"

Workload Quarantine Action

The Illumio Technology Add-On for Splunk provides a scripted alert action to move a workload into a configured quarantine zone. You must first define the policy and labels for this quarantine zone on the PCE.

The action takes the following parameters:

- **workload_href** - PCE workload HREF of the workload to move into quarantine.
- **pce_fqdn** - PCE fully qualified domain name.
- **org_id** - PCE organization ID. Defaults to 1.

When triggered, the alert action script looks up the modular input matching the given **pce_fqdn** and **org_id** and uses the configured PCE connection details when updating the specified workload.



NOTE

For the action to run successfully, the API key configured for the input *must* have write permission for workloads.

Manually Trigger Quarantine

The following search can be run from the Splunk UI to quarantine the workload with the specified HREF:

```
| makeresults 1 | sendalert illumio_quarantine param.workload_href="/orgs/1/workloads/00f13a7b-0386-4943-a96c-cfd71d4096dd" param.pce_fqdn="my.pce.com" param.org_id=1
```

About the Illumio App for Splunk

The Illumio App for Splunk integrates with the Illumio Policy Compute Engine (PCE) to provide security and operational insights into your Illumio secured data center. A dashboard view displays an overview of the security posture of the data center.

With improved visibility of east-west traffic, Security Operations Center (SOC) staff can detect unauthorized activity and potential attacks from traffic blocked by Illumio segmentation policy on workloads in "Enforcement" mode. Additionally, the Illumio App for Splunk provides visibility into potentially blocked traffic for workloads in "Test" mode. SOC staff can quickly pinpoint potential attacks and identify workloads with a significant number of blocked flows.

Distributed Splunk Architecture

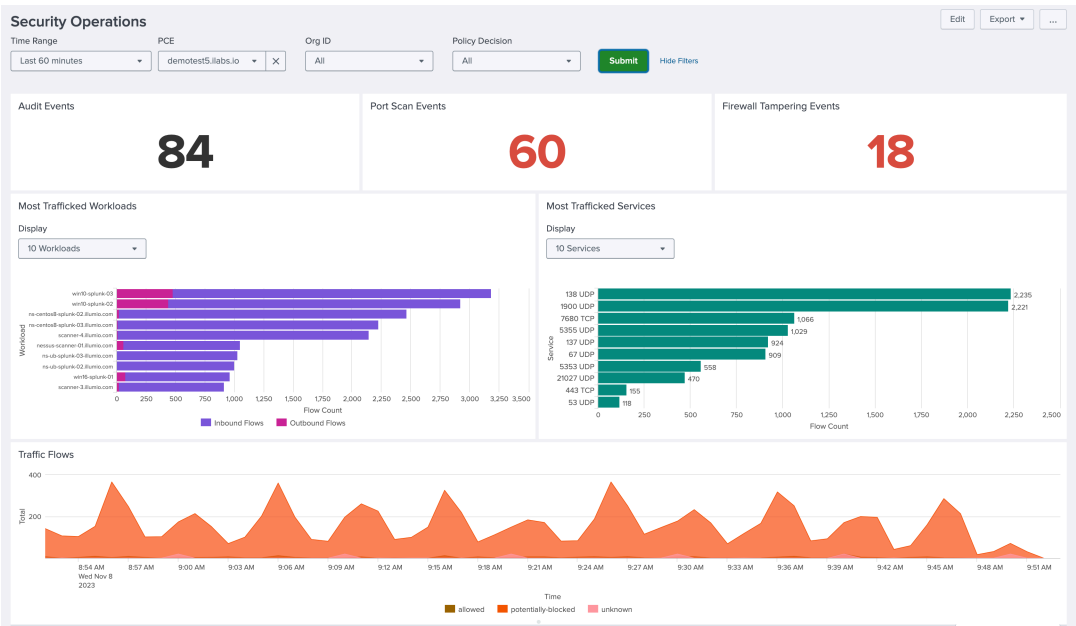
The app only needs to be installed on the search tier of a distributed Splunk installation.

Dashboards

The Illumio app provides multiple dashboards to visualize important data from the Illumio PCE.

Security Operations Dashboard

The **Security Operations** dashboard provides an overview of the PCE security posture, allowing Splunk admins to monitor the state of the network at a glance.



The **Port Scan Events** and **Firewall Tampering Events** panels provide drill-down into detailed views of potentially compromised workloads. From these views, the triggering events can be investigated, and the devices can be quarantined using the Illumio Quarantine alert action.



NOTE

Only users with the *illumio_quarantine_workload* role can trigger the quarantine action. Also, note that when the Illumio Quarantine action is performed, the workload will lose all labels and the action will apply the labels that were originally configured on the Illumio Data Input. The past labels are overwritten to avoid triggering policy rules and to maintain the Quarantine action.

Firewall Tampering Host

Hostname lookup may result in multiple records. Please select the hostname to investigate or quarantine.

Timestamp	PCE	Org ID	Labels	Hostname	Quarantine
2023-11-08 09:03:00 PST	demotest5.ilabs.io	1	Physical:Physical role:scanner app:Network Scanner loc:Dallas env:Production	scanner-2.illumio.com	Quarantine Workload
2023-11-08 09:05:00 PST	demotest5.ilabs.io	1	Physical:Physical role:scanner app:Network Scanner loc:Dallas env:Development	scanner-1.illumio.com	Quarantine Workload
2023-11-08 09:10:00 PST	demotest5.ilabs.io	1	Physical:Physical role:scanner app:Network Scanner loc:Dallas env:Production	scanner-3.illumio.com	Quarantine Workload

PCE Operations Dashboard

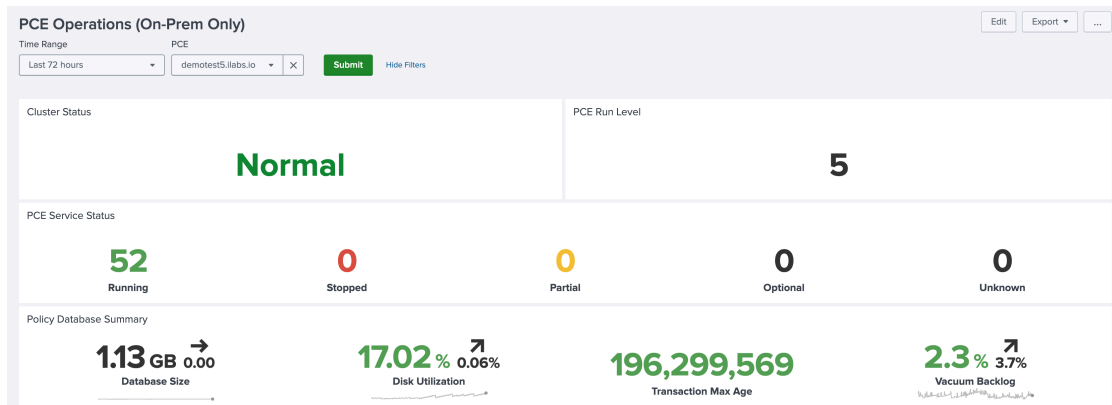


NOTE

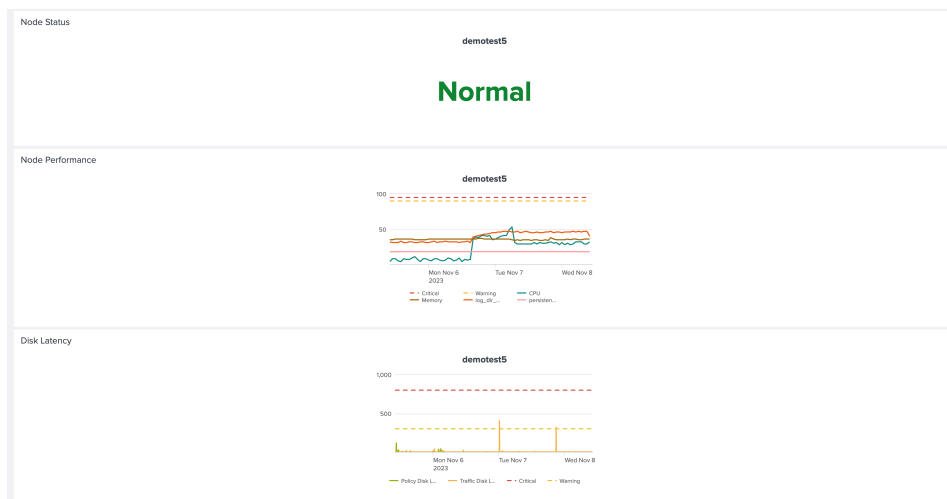
The **PCE Operations** dashboard is only available for On-Premises deployments.

The **PCE Operations** dashboard shows the status of the PCE cluster. The top panels provide an overview of the whole cluster state, including the Unix run level, service statuses, and policy database metrics.

Refer to the *PCE Administration Guide* for your version of the Illumio PCE for detailed explanations of these metrics.



The **Node Status**, **Node Performance**, and **Disk Latency** panels show trellis charts for each host in the PCE cluster. The dashed yellow and red lines indicate warning and critical thresholds for the tracked metrics respectively.



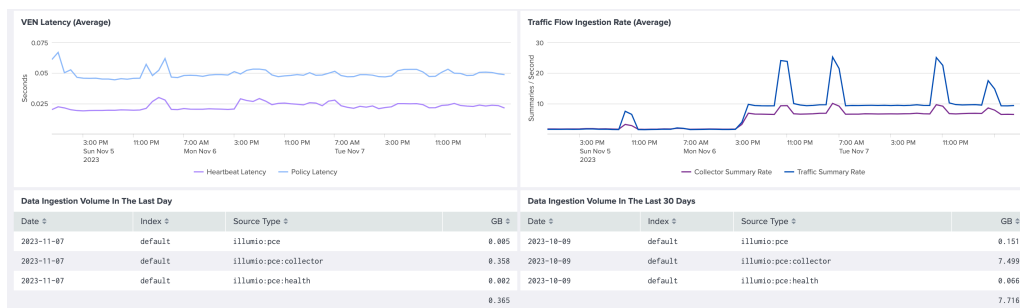
The **VEN Latency** panel provides an aggregate view of heartbeat and policy latency times for all VENs. The **Traffic Flow Ingestion Rate** panel shows average traffic flow collection rates to the PCE.

Finally, the **Data Ingestion** panels at the bottom of the dashboard show the index volume, in gigabytes, broken down by sourcetype.



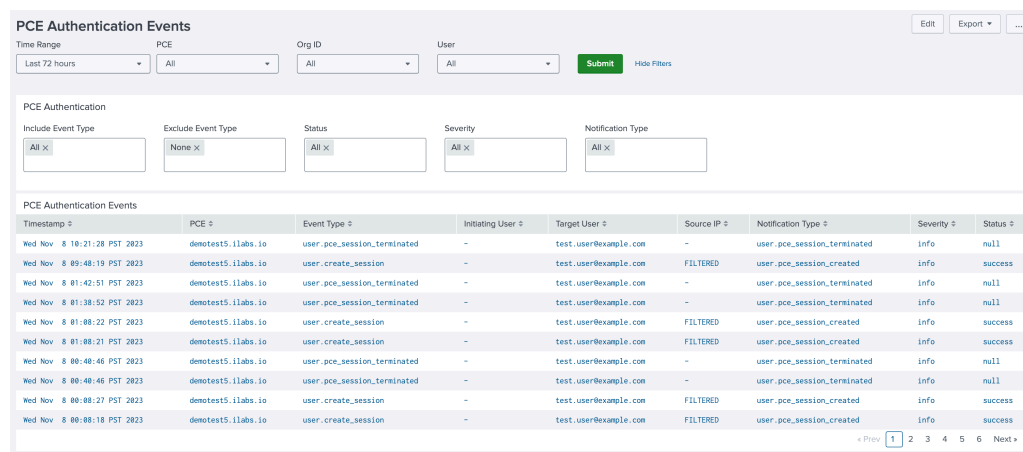
NOTE

Only users with the *admin* or *sc_admin* roles can view the data ingestion panels.



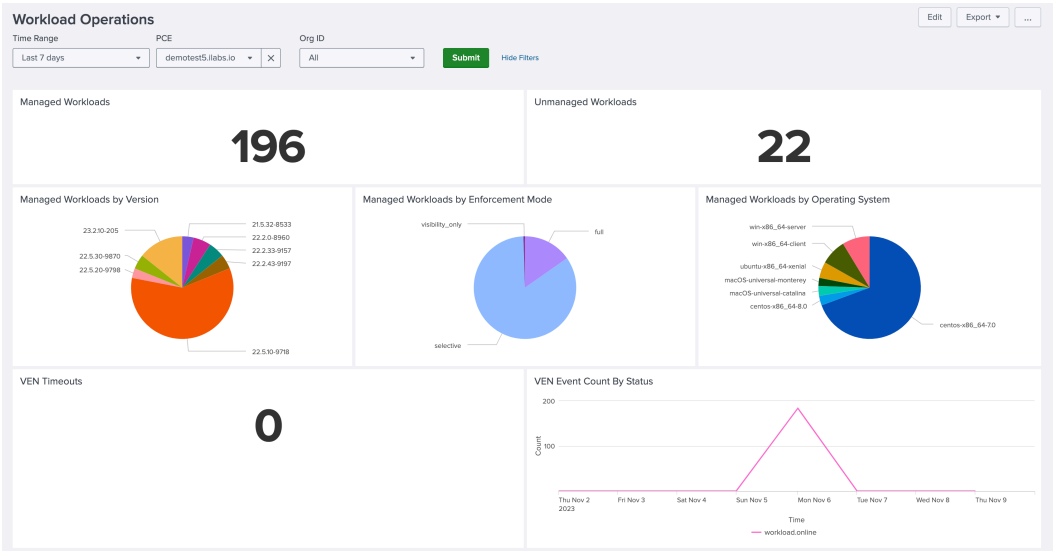
PCE Authentication Events Dashboard

The **PCE Authentication Events** dashboard shows all authentication and authentication-related events that were made to the PCE. Events can be filtered by user, type, and severity.



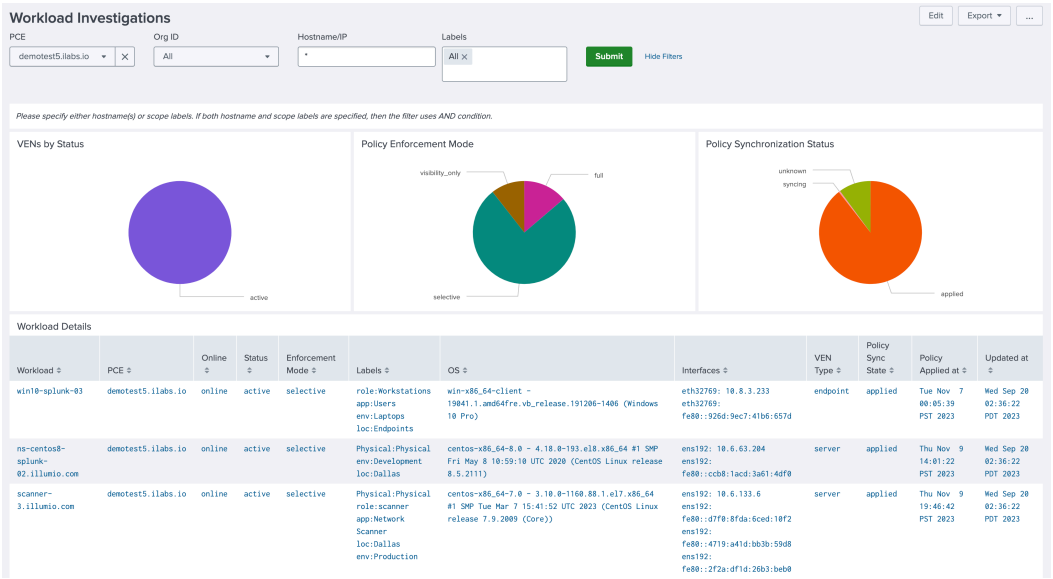
Workload Operations Dashboard

The **Workload Operations** dashboard shows breakdowns of managed and unmanaged workloads by VEN version, enforcement mode, and operating system. It also shows VEN timeouts and VEN/workload events over time.



Workload Investigations Dashboard

The **Workload Investigations** dashboard shows a more detailed breakdown of workload metadata and events, as well as VEN status and policy synchronization status.



The **Audit Events** table at the bottom of the dashboard highlights the most recent VEN and workload events on the PCE.

Audit Events

Time Range: Last 60 minutes | Event Type: All | Severity: All | Status: All

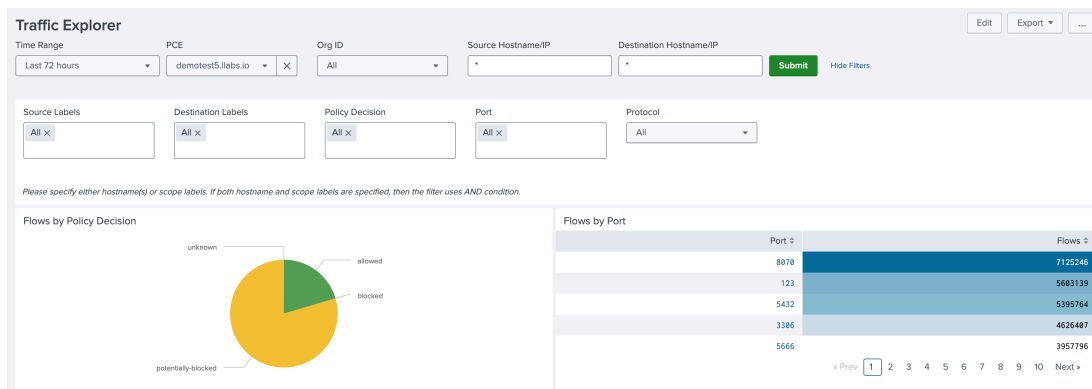
Timestamp	PCE	Workload	Labels	Event Type	Notification Type	Severity	Status
Thu Nov 9 11:53:39 PST 2023	demotest5.ilabs.io	scanner-1.illumio.com	Physical:Physical role:scanner app:Network Scanner loc:Dallas env:Development	agent.tampering	workload.oob_policy_changes	err	success
Thu Nov 9 11:51:55 PST 2023	demotest5.ilabs.io	scanner-2.illumio.com	Physical:Physical role:scanner app:Network Scanner loc:Dallas env:Production	agent.tampering	workload.oob_policy_changes	err	success
Thu Nov 9 11:46:00 PST 2023	demotest5.ilabs.io	scanner-3.illumio.com	Physical:Physical role:scanner app:Network Scanner loc:Dallas env:Production	agent.tampering	workload.oob_policy_changes	err	success
Thu Nov 9 11:42:00 PST 2023	demotest5.ilabs.io	scanner-1.illumio.com	Physical:Physical role:scanner app:Network Scanner loc:Dallas env:Development	agent.tampering	workload.oob_policy_changes	err	success
Thu Nov 9 11:42:00 PST 2023	demotest5.ilabs.io	scanner-2.illumio.com	Physical:Physical role:scanner app:Network Scanner loc:Dallas env:Production	agent.tampering	workload.oob_policy_changes	err	success

« Prev 1 2 3 4 Next »

Traffic Explorer Dashboard

The **Traffic Explorer** dashboard visualizes traffic flows reported from managed workloads or otherwise uploaded to the PCE. The visualizations show traffic grouped by policy decision, port, and source/destination.

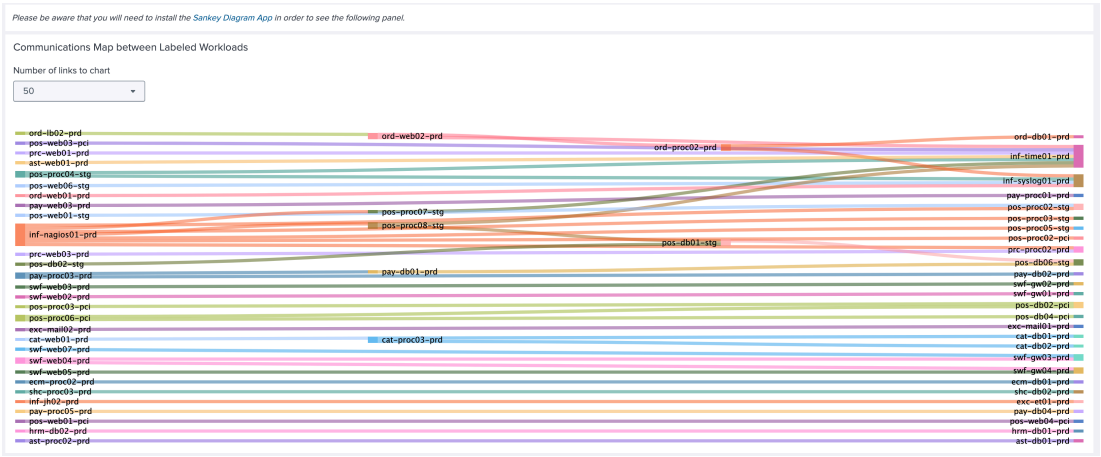
Traffic can be filtered by source/destination hostname or IP address, assigned labels, policy decision, port, and transport protocol.



NOTE

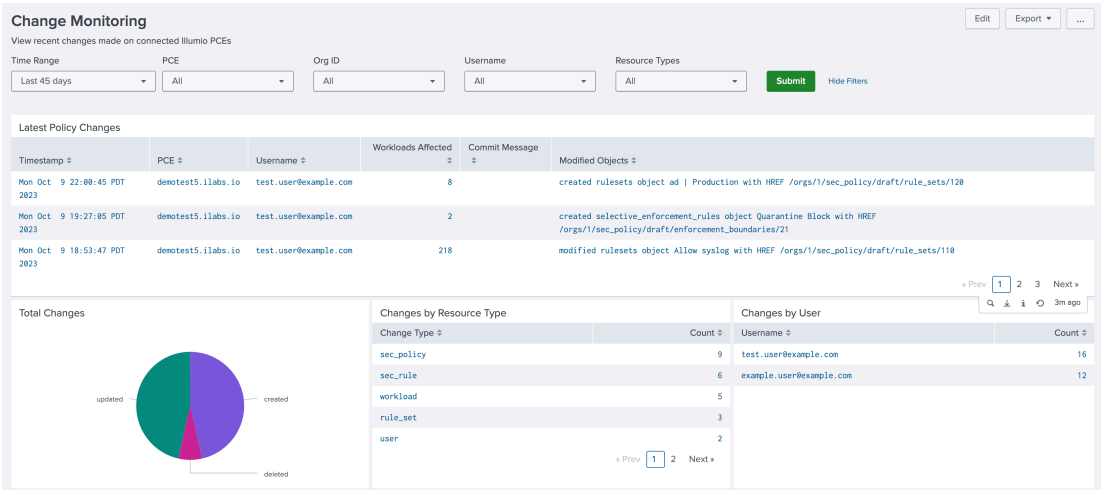
The Communications Map between Labeled Workloads chart shown below uses the [Splunk Sankey Diagram Custom Visualization](#) app. You must install the app to render the chart.

Each link in the chart is grouped by source, destination, and destination port. The thickness of the link represents relative flow count.




Change Monitoring Dashboard

The **Change Monitoring** dashboard shows recent security policy changes, and groups auditable change events (creates, updates, and deletes) by count, resource type, and initiating user.



Data Model

The Illumio App for Splunk provides an Illumio data model that can help to improve search performance at the cost of disk space by building a limited index of PCE syslog event fields.

 **NOTE**

According to Splunk app guidelines, model acceleration is disabled by default.

The model provides the following objects:

Name	Type	Parent	Base Search	Description
Audit	Root event node	-	illumio_get_index sourcetype="illumio:pce"	Auditable syslog events
Traffic	Root event node	-	illumio_get_index sourcetype="illumio:pce:collector"	Traffic flow events
Status	Root event node	-	illumio_get_index sourcetype="illumio:pce:health"	PCE system health and status events
Status.Policy	Child event node	Status	event_source="policy"	Policy service events
Status.Collector	Child event node	Status	event_source="collector"	Collector service events
Status.FlowAnalytics	Child event node	Status	event_source="flow_analytics"	Flow analytics service events

Illumio data model nodes can be referenced using the [tstats command](#). For example, the following search uses the **Traffic** node to sum flow counts from a given PCE over time by source/destination IP:

```
| tstats sum(Traffic.count) AS flows FROM datamodel=Illumio.Traffic WHERE Traffic.pce_fqdn="my.pce.com" BY Traffic.timestamp, Traffic.src_ip, Traffic.dest_ip
```

Data Model Acceleration



NOTE

Enabling or disabling acceleration for the Illumio data model requires the `accelerate_datamodel` capability. The `admin` or `sc_admin` roles have this capability by default.

To enable acceleration for the Illumio data model:

1. Navigate to **Settings > Data models**.
2. Select **Illumio App for Splunk** from the App dropdown menu.
3. Click the **Edit** dropdown under Actions for the **Illumio** data model.
4. Click **Edit Acceleration**.
5. Check the **Acceleration** toggle in the dialog and adjust the Summary Range and advanced settings as needed. See the Splunk documentation on [data model acceleration](#) for a more detailed explanation of the individual parameters for configuring acceleration.
6. Click **Save**. It may take a while to build the summary for the accelerated model.
Click the arrow to the left of the model name to view the progress in the **ACCELERATION** section.

**NOTE**

If you are using a distributed search head cluster, see [Sharing data model acceleration summaries among search heads](#) to avoid rebuilding the summary on each search head in the cluster.

To rebuild the Illumio data model summary:

1. Navigate to **Settings > Data models**.
2. Select **Illumio App for Splunk** from the **App** dropdown menu.
3. Click the arrow to the left of the Illumio data model name.
4. Click **Rebuild** under the **ACCELERATION** section.

Install the Illumio Splunk Apps

You can install the Illumio Splunk integration apps in either a distributed or a standalone Splunk environment.

**NOTE**

Recommendations for the configuration and topology of a distributed Splunk environment are outside of the scope of this document. See [About Splunk Validated Architectures](#) for suggestions on topology for distributed deployments.

Install the Illumio Splunk Apps in a Distributed Environment

For a distributed environment, install the TA to a Splunk Heavy Forwarder, as well as the indexer/indexer cluster and search head/search head cluster. Configure the Illumio modular input to run on the Heavy Forwarder. You need to install on the search head tiers if you want to use index-time and search-time transforms in the app.

**NOTE**

You only need to install the Illumio App for Splunk on the search tier.

**NOTE**

You cannot install the Illumio Technology Add-On for Splunk on a Universal Forwarder.

Install the Illumio Technology Add-On for Splunk in a Standalone Environment

The following procedures describe how to install the TA through the Splunk UI and manually.

Use the following procedure to install the TA through the Splunk UI.

1. In the Splunk UI, navigate to the **Manage Apps** page using the **Apps** drop-down in the top-left corner or by clicking the gear icon next to Apps on the Splunk homepage.
2. Click **Browse More Apps**, and search for TA-Illumio.
3. Click **Install**.
4. Enter your Splunk login credentials when prompted, and then click **Agree and Install**.
5. When prompted, restart Splunk.

Use the following procedure to install Illumio TA manually.

1. Navigate to the **Illumio-TA** app in Splunkbase.
2. Log in using your Splunk credentials.
3. Click **Download**.
4. Read through and accept the EULA and Terms and Conditions, and then click **Agree to Download**.
5. Transfer the downloaded .tgz or .spl file to the Splunk server.
6. Install the app manually:
Using the Splunk binary:

```
$SPLUNK_HOME/bin/splunk install app /path/to/TA-Illumio.spl
```


Or by extracting directly under /apps:

```
tar zxf /path/to/TA-Illumio.spl -C $SPLUNK_HOME/etc/apps/
```
7. Restart Splunk.

Configure the Illumio Technology Add-On for Splunk

After installing the Illumio TA, you will need to configure the Illumio modular input and a TCP receiver for Syslog events from the PCE.

Start by creating a PCE API key to use when setting up the input.

Create a User-Scoped API Key

1. In the PCE, open the user menu drop-down in the top-right corner of the page, and select **My API keys**.
2. Click **Add**, note the **Org ID** shown in the dialog, and enter a display name for the key.
3. Click **Create**, and then copy or download the API key credentials and store them somewhere secure.

Create a Service Account API Key

The Org ID value is not shown when you create a Service Account key. It is displayed when you create a User API key, as described in [Create a User-Scoped API Key \[28\]](#).

**NOTE**

The Org ID value is not shown when you create a Service Account key. It is displayed when you create a User API key, as described in the preceding procedure.

1. In the PCE, open the **Access** submenu on the left side of the screen and select **Service Accounts**.
2. Click **Add**, and enter a display name and one or more Roles to assign to the key. The TA-Illumio Add-On requires only read-only access to policy object endpoints, so the **Global Viewer** role should be sufficient.

**NOTE**

To use the workload quarantine action, the API key that is used for the input must have write permissions for workloads.

3. Click **Save**, and then copy or download the API key credentials and store them somewhere secure.

**WARNING**

Service Account API keys have a default lifetime of 90 days. Take note of the expiration data for your key and replace it before it expires.

Working with Alert Actions and Quarantines

Configure the Illumio Modular Input

UDP Listen on a UDP port for incoming data, e.g. syslog.	0	+ Add new
Scripts Run custom scripts to collect or generate more data.	5	+ Add new
Input Go to the add-on's configuration UI and configure modular inputs under the Inputs menu.	0	+ Add new
Illumio Enable data inputs for splunk add-on for Illumio	0	+ Add new

1. Navigate to **Settings > Data inputs** and find the **Illumio** input type.
2. Click the **+ Add New** action to create a new input.
3. Enter a display name for the input and the connection details for your PCE. Enter the Organization ID and API key username and secret values copied from the steps above.
4. (On-prem only) To receive syslog events forwarded from an on-prem PCE, a TCP input must be configured in Splunk. Setting the **Syslog Port (TCP)** value will automatically cre-

ate one when the input runs if it does not already exist. The **Enable TCP-SSL** option determines whether a `[tcp-ssl]` or `[tcp]` stanza will be created (See [Configure TCP SSL \[32\]](#) for more information.)

5. Adjust any of the remaining parameters as needed. Make sure that the index is set correctly. (Check the **More settings** checkbox to display additional settings.) To enable automated quarantine using the `illumio_quarantine` action, specify one or more labels that make up a quarantine policy scope in the PCE in the **Quarantine Labels** field.
6. Click **Next**. If an error dialog appears, double-check the field values and refer to the [Troubleshooting \[42\]](#) section.

Name *	<input type="text"/>
PCE URL *	<input type="text"/> Full URL of the PCE to connect to, including port. Example value: <code>https://my.pce.com:8443</code>
Organization ID *	<input type="text" value="1"/> PCE Organization ID
API Key Username *	<input type="text"/> Illumio API key username. Example value: <code>'api_145a5c788e63c30a3'</code>
API Key Secret *	<input type="password"/>
Confirm API secret *	<input type="password"/>

TCP Syslog Settings

Settings for receiving TCP syslogs from on-prem PCE installations. If a TCP input with the configured port does not exist, one will be created. If the input already exists, this setting will have no effect

Syslog Port (TCP)	<input type="text"/> Port for Splunk to receive syslogs from the PCE. Not required syslogs are pulled from S3. Example value: 514
Enable TCP-SSL	<input checked="" type="checkbox"/> Receive encrypted syslog events from the PCE. Requires [SSL] stanza to be configured in inputs.conf

Port Scan Settings

Per-PCE configuration settings for detecting port scan events on paired workloads

Interval *	<input type="text" value="60"/> A port scan alert will be triggered if the scan threshold count is met during this interval (in seconds)
------------	--

Parameter	Description	Required	Default Value	Example Value
Name	Modular input display name. Must be unique.	Y	-	<i>mypce_input</i>
PCE URL	The full URL of the Illumio PCE to connect to. If a scheme is not provided, <i>https://</i> is used by default. If a port is not provided, it is assumed to be the default for the given scheme (80 for HTTP, 443 for HTTPS).	Y	-	<i>https://my.pce.com:8443</i>
Organization ID	The ID number of the PCE organization to connect to.	Y	1	-
API Key Username	The API key ID to use when connecting to the PCE.	Y	-	<i>api_145a5c788e63c30a3</i>
API Key Secret	The API key secret to use when connecting to the PCE.	Y	-	-
Syslog Port (TCP)	Designates a port on the Splunk server to receive syslog events from the Illumio PCE. There must not be an existing TCP input for the given port. Only used for direct forwarding from the PCE. Syslog events pulled from Amazon S3 must be configured separately using the AWS S3 TA.	N	-	<i>514</i>
Enable TCP SSL	Toggles SSL for the created TCP syslog input. The <i>[SSL]</i> stanza must be configured separately.	N	True	-
Port Scan Interval	The interval, in seconds, within which Port Scan Threshold scanned ports will trigger an alert.	Y	60	-
Port Scan Threshold	Defines a threshold that will trigger an alert when more than the configured number of ports are scanned within Port Scan Interval seconds.	Y	10	-
Port Scan Allowed IPs	Comma-separated list of source IP addresses to exempt from port scan alerts.	N	-	<i>10.0.0.1,10.0.0.2</i>

Parameter	Description	Required	Default Value	Example Value
Quarantine Labels	Optional comma-separated list of label key:value pairs that represent a quarantine zone scope in the PCE. Configured labels are applied to selected workloads when the <i>illumio_quarantine</i> action is run. The labels must exist in the PCE and any policy that restricts access to the quarantine zone must be defined separately. It must be of the form key1:value1,...,keyN:valueN Keys and values are case-sensitive.	N	-	<i>app:A-Quarantine,env:EQuarantine, loc:L-Quarantine</i>
CA Certificate Path	Optional path to a custom CA certificate bundle	N	-	<i>\$SPLUNK_HOME/etc/apps/TA-Illumio/certs/ca.pem</i>
HTTP Proxy Address	HTTP proxy address.	N	-	<i>http://my.proxy-server.com:8080</i>
HTTPS Proxy Address	HTTPS proxy address.	N	-	<i>https://my.proxy-server.com:8443</i>
HTTP Retry Count	Number of times to retry the connection to the PCE.	N	5	-
HTTP Retry Interval	The total HTTP request timeout for the PCE in seconds.	N	30	-
Interval	Input run schedule in seconds or as a cron expression.	Y	1800	<i>*/30 * * * *</i>
Index	Splunk index for the input to write events to.	Y	default (main)	-

Configure TCP SSL

To configure syslog forwarding encrypted with TLS, both a *[tcp-ssl]* stanza and an *[SSL]* stanza must be configured in `$SPLUNK_HOME/etc/apps/TA-Illumio/local/inputs.conf`.

The TCP-SSL stanza will be created automatically as described above, but the `'[SSL]'` stanza must be created manually. This step only needs to be done once for any number of Illumio inputs.

When using an existing certificate authority, generate a server certificate for Splunk with the CN or SAN set to the Splunk instance hostname or IP address.

When using a self-signed certificate, refer to the [Splunk documentation](#) on generating and configuring self-signed TLS certificates. Make sure that the root CA certificate is created with extensions and the `ca` flag is set to true (checked by syslog-ng validation).

1. Create the SSL stanza with the following fields:

```
[SSL]
serverCert = /path/to/my/splunk_server.crt
sslPassword = splunk_server_cert_pass
```

2. Restart Splunk.

**NOTE**

Do not use the Splunk default certificates when configuring SSL.

Configure Syslog Forwarding for On-Prem PCEs

1. In the PCE, open the **Settings** submenu on the left side of the screen and select **Event Settings**.
2. Click **Add** to create a new Event Forwarding rule.
3. Select the event types to forward to Splunk.
4. Click **Add Repository**.
5. Enter a description for the repository and the Splunk hostname/IP and the port value of the TCP stanza created for the **illumio** input. Leave the protocol value as **TCP**.
6. If TCP-SSL is configured in Splunk for the target port, set the TLS field to **Enabled** and upload a certificate bundle containing the root and any intermediate certificates in the chain for your CA.

**NOTE**

If you are enabling TLS, the address value must match the CN or SAN of the Splunk server certificate.

7. Select the **Verify TLS** option to ensure that your certificates and TLS configuration are valid.
8. Click **Add** and select the option for the created repository.
9. Click **Save**.
A test event will be sent to Splunk to verify the connection.
- 10 In Splunk, run the following search to make sure that the test event arrived:

```
index=illumio_index sourcetype="illumio:pce" "Testing syslog
connection from PCE"
```

Configure Syslog Forwarding for Cloud PCEs

1. Reach out to Illumio Customer Support to configure Syslog event forwarding to AWS S3. The target bucket can be internal or managed by Illumio.
2. After the bucket is configured, make sure the Syslog files are being sent.
3. Install the [AWS S3 TA](#) from Splunkbase.
4. Follow the configuration instructions for Generic S3 inputs in the [AWS S3 TA documentation](#).
5. Create two inputs, one for auditable events and one for collector (traffic flow) events.

6. In each input, specify a Log File/S3 Key Prefix with the path to either auditable or collector event logs within the S3 bucket.

Install the Illumio App for Splunk



NOTE

The Illumio Add-On is required for the Illumio App for Splunk to work.

Installing the Illumio App for Splunk Using the Splunk UI

1. In the Splunk UI, navigate to the **Manage Apps** page using the **Apps** drop-down in the top-left corner or by clicking the gear icon next to Apps on the Splunk homepage.
2. Click **Browse More Apps** and search for **IllumioAppforSplunk**.
3. Click **Install**.
4. Enter your Splunk login credentials when prompted, and then click **Agree and Install**.
5. If prompted, restart Splunk.

Installing the Illumio App for Splunk Manually

1. Navigate to the Illumio App for Splunk app in Splunkbase.
2. Log in using your Splunk credentials.
3. Click **Download**.
4. Read through and accept the EULA and Terms and Conditions, and then click **Agree to Download**.
5. Transfer the downloaded *.tgz* or *.spl* file to the Splunk server.
6. Install the app manually:
Using the Splunk binary:

```
$SPLUNK_HOME/bin/splunk install app /path/to/IllumioAppforSplunk.tgz
```


Or by extracting directly under */apps*:

```
tar zxf /path/to/IllumioAppforSplunk.tgz -C $SPLUNK_HOME/etc/apps/
```
7. Restart Splunk.

Configure the Illumio App for Splunk

Use the procedures in the following topics to configure the Illumio App for Splunk.

Create an Index for Illumio Events



NOTE

This is an optional step, but it is recommended. If you already created one or more indexes when you configured the Illumio Technology Add-On for Splunk, skip this step.

1. Navigate to **Settings > Indexes**.
2. Click **New Index** in the top-right corner.
3. Enter an index name and select **Illumio App for Splunk** from the **App** drop-down menu.
4. Set the other index parameters based on your expected event volume and retention policy.
5. Click **Save**.

**NOTE**

Make sure to configure the index based on your organization's compliance requirements and data retention policies. See [Managing Indexers and Clusters of Indexers](#).

Update the `illumio_get_index` Macro

1. Navigate to **Settings > Advanced Search > Search Macros**.
2. Select **Illumio App for Splunk** from the **App** drop-down menu.
3. Click the `illumio_get_index` macro name to open the edit form.
4. Update the definition to reference one or more indexes, such as `(index="illumio_pce1" OR index="illumio_pce2")`.
5. Click **Save**.

Accelerate the Illumio Data Model

This step is optional, but it is recommended. See [Data Model Acceleration \[26\]](#).

Install the Sankey Diagram App

The Traffic Explorer dashboard renders traffic flows using the [Sankey diagram custom visualization app](#). The app is required for displaying the panel but it is not required.

Upgrade the Illumio App for Splunk

Use the installation steps above to upgrade the app using the Splunk UI or manually by downloading the app bundle from Splunkbase. Refer to the app's Splunkbase documentation for detailed upgrade steps.

**NOTE**

The search-time extractions and transforms for version 4.0.0 are incompatible with data that was indexed by previous versions of the Illumio Technology Add-On for Splunk. When you are upgrading from an earlier version, see the version 4.0.0 upgrade steps in the Splunkbase documentation for detailed instructions.

About Alerting Actions and the Adaptive Response Framework

This section tells how Alerting Actions and the 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 [Create an adaptive response action](#) 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 a 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 the 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:

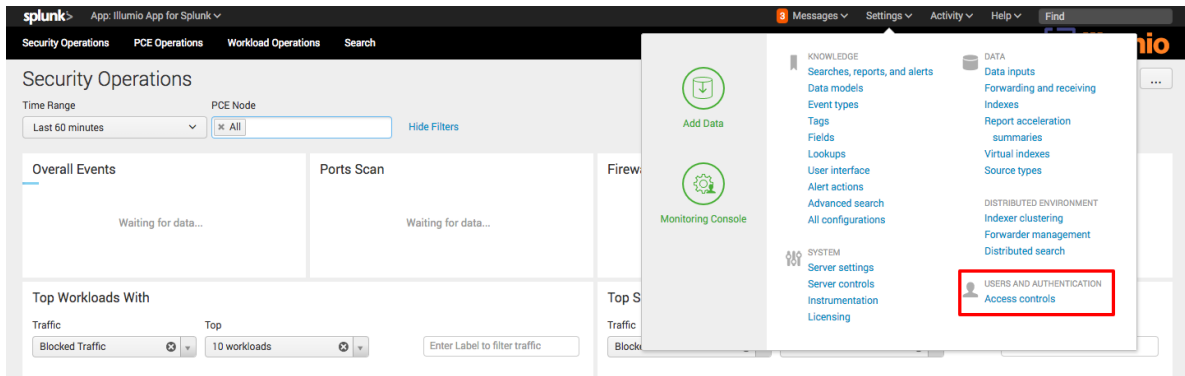
- Quarantine workloads using Splunk Core Alert Actions.
- Quarantine workloads using Splunk Enterprise Security Suite's Adaptive Response Framework.

Provide Access to the 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, because their roles are controlled by an external system.

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

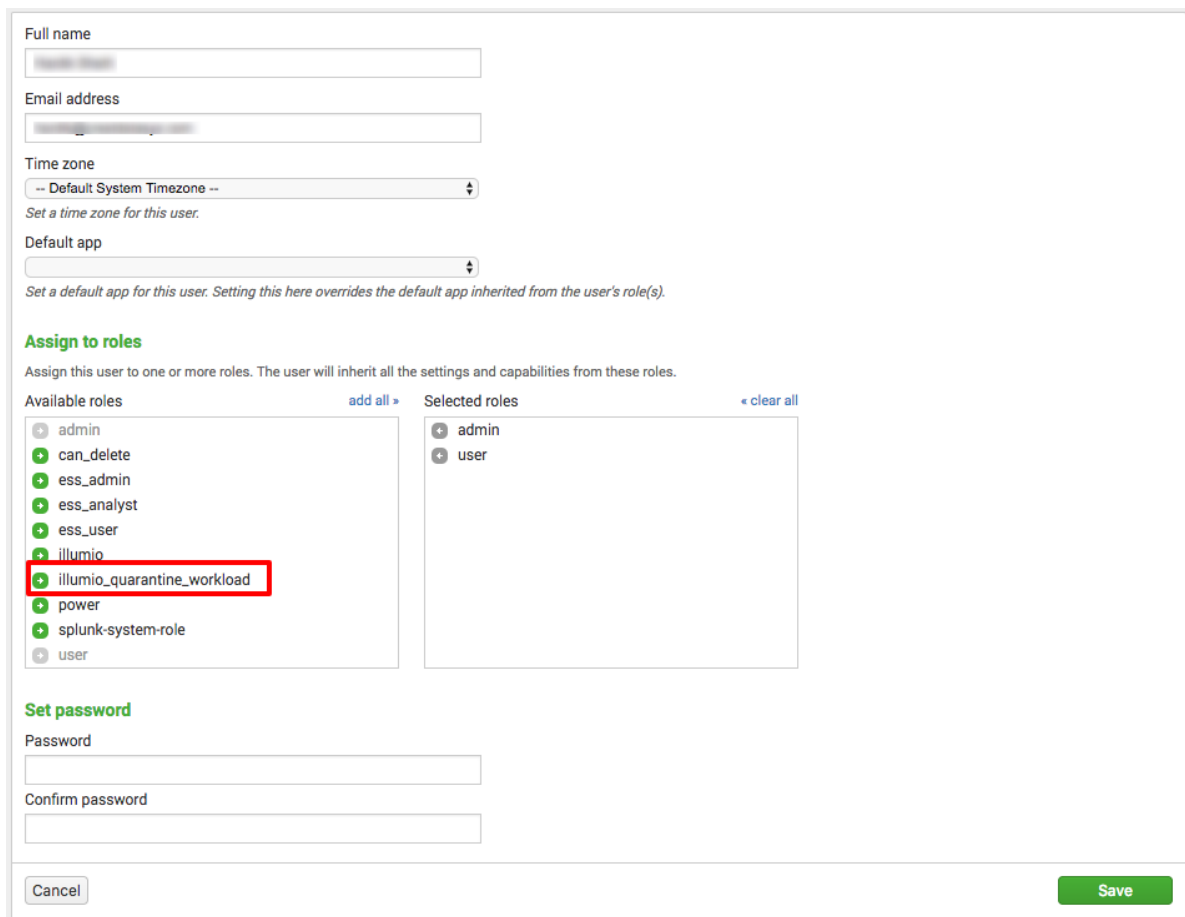


2. Click **Users**.



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**.

Quarantine Workloads 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 drilldowns 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 the 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:

Incident Review

Urgency: CRITICAL 0, HIGH 0, MEDIUM 49615, LOW 0, INFO 0

Status: [x All] Correlation Search Name: []

Owner: [x All] Search: []

Security Domain: [x All] Time | Associations: Last 24 hours

Tag: [] Submit

49,615 of 89,319 events matched

Format Timeline Zoom Out + Zoom to Selection x Deselect 1 hour per column

50,000 Nov 3, 2017 12:00 PM 50,000

30,000 12:00 PM 6:00 PM 12:00 AM 6:00 AM

Thu Nov 2 2017 Fri Nov 3

Edit Selected | Edit All 49615 Matching Events | Add Selected to Investigation

i	Time	Security Domain	Title	Urgency	Status	Owner	Actions
>	11/3/17 12:30:11.000 PM	Threat	Demo	Medium	New	unassigned	▼
>	11/3/17 12:30:08.000 PM	Threat	Demo	Medium	New	unassigned	▼
>	11/3/17 12:30:08.000 PM	Threat	Demo	Medium	New	unassigned	▼
>	11/3/17 12:30:08.000 PM	Threat	Demo	Medium	New	unassigned	▼
>	11/3/17 12:30:08.000 PM	Threat	Demo	Medium	New	unassigned	▼
>	11/3/17 12:30:08.000 PM	Threat	Demo	Medium	New	unassigned	▼
>	11/3/17 12:30:08.000 PM	Threat	Demo	Medium	New	unassigned	▼
>	11/3/17 12:30:08.000 PM	Threat	Demo	Medium	New	unassigned	▼
>	11/3/17 12:30:08.000 PM	Threat	Demo	Medium	New	unassigned	▼
>	11/3/17 12:30:08.000 PM	Threat	Demo	Medium	New	unassigned	▼
>	11/3/17 12:30:08.000 PM	Threat	Demo	Medium	New	unassigned	▼
>	11/3/17 12:30:08.000 PM	Threat	Demo	Medium	New	unassigned	▼
>	11/3/17 12:30:08.000 PM	Threat	Demo	Medium	New	unassigned	▼

+ No investigation is currently loaded. Please create (+) or load an existing one (=).

As a part of the Adaptive Response Framework, Splunk 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.

Edit Selected | Edit All 29769 Matching Events | Add Selected to Investigation

i	Time	Security Domain	Title	Urgency	Status	Owner	Actions
▼	11/3/17 12:30:11.000 PM	Threat	Demo	Medium	New	unassigned	▼

Description:
unknown

Additional Fields

Value

Action

Related Investigations:
Currently not investigated.

Correlation Search:
Threat - Demo - Rule

History:
View all review activity for this Notable Event

Adaptive Responses:

Response	Mode	Time	User	Status
Notable	saved	2017-11-03T12:30:07+0000	nobody	success

View Adaptive Response Invocations

Next Steps:
No Next Steps defined.

Event Details:
event_id: 2096BB9A-ECCF-499C-9833-F50811DE7F49@notable@9b40e5a1f42d6c3bd91a75485028b0fe
event_hash: 9b40e5a1f42d6c3bd91a75485028b0fe
eventtype: modnotable_results
notable
Short ID: Create Short ID

Add Event to Investigation

Create notable event

Build Event Type

Extract Fields

Run Adaptive Response Actions

Share Notable Event

Suppress Notable Events

Show Source

>	11/3/17 12:30:08.000 PM	Threat	Demo	Medium	New	unassigned	▼
>	11/3/17 12:30:08.000 PM	Threat	Demo	Medium	New	unassigned	▼
>	11/3/17 12:30:08.000 PM	Threat	Demo	Medium	New	unassigned	▼
>	11/3/17 12:30:08.000 PM	Threat	Demo	Medium	New	unassigned	▼

+ No investigation is currently loaded. Please create (+) or load an existing one (=).

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.

Adaptive Response Actions

Select actions to run.

+ Add New Response Action

Category: All

Search

- Stream Capture**
Creates stream capture
Category: Information Gathering | Task: create | Subject: network.capture | Vendor: Splunk
- Quarantine Workload**
Custom action for marking a workload as quarantine.
Category: Information Gathering | Task: Update | Subject: Workload | Vendor: Illumio
- Nbtstat**
Runs the nbtstat command
Category: Information Gathering | Task: scan | Subject: device | Vendor: Operating System
- Nslookup**
Runs the nslookup command
Category: Information Gathering | Task: scan | Subject: device | Vendor: Operating System
- Ping**
Runs the ping command

Run

Event Details:

event_id: 2096BB9A-ECCF-499C-9835
event_hash: 9b40e5a1f42d6c3bd91a754
eventtype: modnotable_results
notable
Short ID: Create Short ID

Time	Threat	Demo	Severity	Priority	Status	Owner	Actions
11/3/17 12:30:08.000 PM	Threat	Demo	Medium	New	unassigned		
11/3/17 12:30:08.000 PM	Threat	Demo	Medium	New	unassigned		
11/3/17 12:30:08.000 PM	Threat	Demo	Medium	New	unassigned		
11/3/17 12:30:08.000 PM	Threat	Demo	Medium	New	unassigned		

+ No investigation is currently loaded. Please create (+) or load an existing one (≡).

Adaptive Response Actions

Select actions to run.

+ Add New Response Action

- Quarantine Workload**

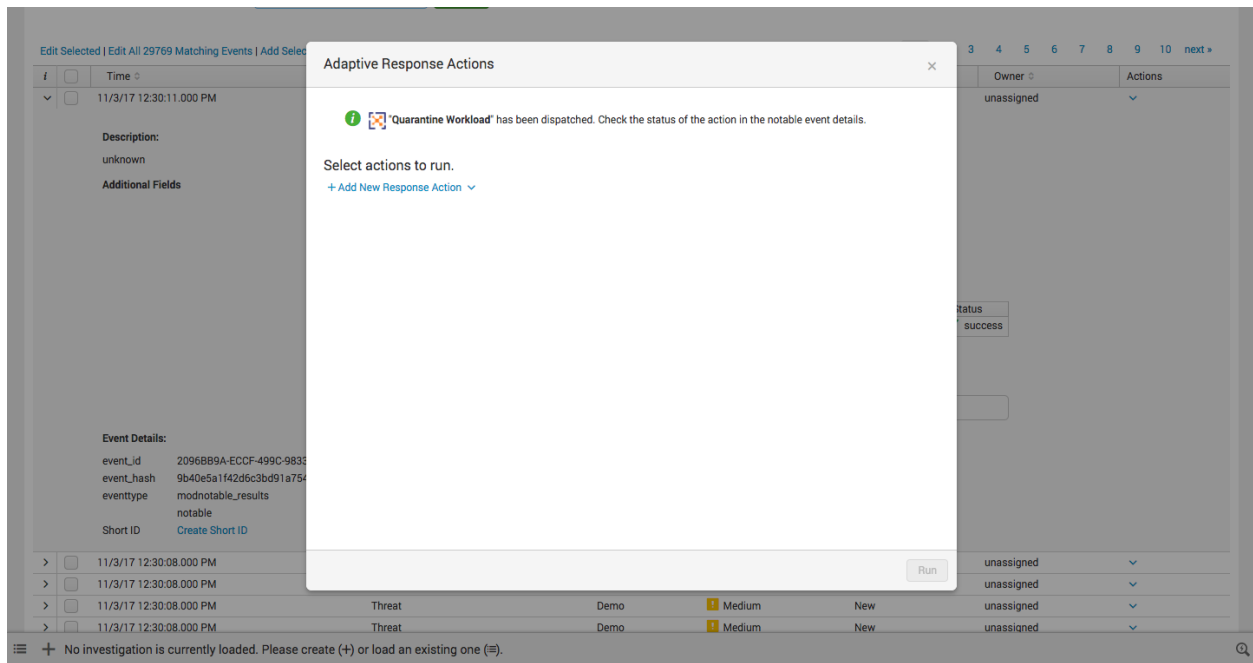
Run

Event Details:

event_id: 2096BB9A-ECCF-499C-9835
event_hash: 9b40e5a1f42d6c3bd91a754
eventtype: modnotable_results
notable
Short ID: Create Short ID

Time	Threat	Demo	Severity	Priority	Status	Owner	Actions
11/3/17 12:30:08.000 PM	Threat	Demo	Medium	New	unassigned		
11/3/17 12:30:08.000 PM	Threat	Demo	Medium	New	unassigned		
11/3/17 12:30:08.000 PM	Threat	Demo	Medium	New	unassigned		
11/3/17 12:30:08.000 PM	Threat	Demo	Medium	New	unassigned		

+ No investigation is currently loaded. Please create (+) or load an existing one (≡).



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

Quarantine Workloads from the Illumio Splunk App

If you have both the `admin` role and the `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 the **Security Operations** dashboard)
- **Firewall Tampering** (on the **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 \[36\]](#).

Port Scan								Edit	Export	...
Time	Source IP	Source	Destination IP	Destination	Source Label	Destination Label	Quarantine	Investigate		
2019-12-12 23:03:00 UTC	fd00:0000:0000:0000:0200:000a:0000:011b	-	fd00:0000:0000:0000:0200:000a:0000:015d	-	app:Point-of-Sale env:PCI loc:CA role:Database	app:HREnrollment env:Production loc:CA role:Processing	Quarantine	Investigate		
2019-12-12 23:03:00 UTC	fd00:0000:0000:0000:0200:000a:0000:011a	-	fd00:0000:0000:0000:0200:000a:0000:015d	-	app:Point-of-Sale env:PCI loc:CA role:Database	app:HREnrollment env:Production loc:CA role:Processing	Quarantine	Investigate		
2019-12-12 23:03:00 UTC	fd00:0000:0000:0000:0200:000a:0000:0116	-	fd00:0000:0000:0000:0200:000a:0000:015d	-	app:Point-of-Sale env:PCI loc:CA role:Web	app:HREnrollment env:Production loc:CA role:Processing	Quarantine	Investigate		
2019-12-12 23:03:00 UTC	fd00:0000:0000:0000:0200:000a:0000:0111	-	fd00:0000:0000:0000:0200:000a:0000:015d	-	app:HRM env:Staging loc:NY role:Database	app:HREnrollment env:Production loc:CA role:Processing	Quarantine	Investigate		
2019-12-12 23:03:00 UTC	fd00:0000:0000:0000:0200:000a:0000:0110	-	fd00:0000:0000:0000:0200:000a:0000:015d	-	app:HRM env:Staging loc:NY role:Database	app:HREnrollment env:Production loc:CA role:Processing	Quarantine	Investigate		
2019-12-12 23:03:00 UTC	fd00:0000:0000:0000:0200:000a:0000:015c	-	fd00:0000:0000:0000:0200:000a:0000:0155	-	app:ShoppingCart env:Production loc:AMS role:Database	app:Commerce env:Production loc:Azure role:Database	Quarantine	Investigate		
2019-12-12 23:03:00 UTC	fd00:0000:0000:0000:0200:000a:0000:0114	-	fd00:0000:0000:0000:0200:000a:0000:0155	-	app:HRM env:Staging loc:NY role:Web	app:Commerce env:Production loc:Azure role:Database	Quarantine	Investigate		
2019-12-12 23:03:00 UTC	fd00:0000:0000:0000:0200:000a:0000:0172	-	fd00:0000:0000:0000:0200:000a:0000:0152	-	app:Catalog env:Production loc:AMS role:Database	app:Commerce env:Production loc:Azure role:Web	Quarantine	Investigate		
2019-12-12 23:03:00 UTC	fd00:0000:0000:0000:0200:000a:0000:0147	-	fd00:0000:0000:0000:0200:000a:0000:0152	-	app:CoreServices env:Production loc:CA role:DomainController	app:Commerce env:Production loc:Azure role:Web	Quarantine	Investigate		
2019-12-12 23:03:00 UTC	fd00:0000:0000:0000:0200:000a:0000:0132	-	fd00:0000:0000:0000:0200:000a:0000:0152	-	app:Ordering env:Production loc:CA role:Load Balancer	app:Commerce env:Production loc:Azure role:Web	Quarantine	Investigate		

Uninstall the Splunk Integration Apps

To uninstall one of the Illumio Splunk integration apps:

1. Access the filesystem of the Splunk server where the app is installed.
2. Navigate to `$SPLUNK_HOME/etc/apps`.
3. Remove the app folder and its contents.
4. Restart Splunk.

Troubleshooting Splunk Integration Apps

Use the information in the following topics to troubleshoot your Splunk integration apps.

Illumio Technology Add-On for Splunk

If you encounter a problem with the TA, check the logs in `splunkd.log` by running the following search in the UI:

```
index=_internal sourcetype=splunkd TA-Illumio
```

Or by searching the log directly from the filesystem:

```
tail -c1000000 $SPLUNK_HOME/var/log/splunk/splunkd.log | grep -i TA-Illumio
```

If the Illumio input is not running:

- Make sure that the `python.version` value for the server and input are set to `python3`.
- Check that the input interval is not too high.
- Make sure that the input is enabled under **Settings > Data Inputs > Illumio**.
- Check the Splunk logs for any issues that could cause modular inputs to fail.
- Check that you aren't hitting your Splunk license limits.
- Restart Splunk to force the input to run.

Event Forwarding (On-Premises PCE)

If you see a validation error while configuring Event Forwarding using TLS:

- Make sure that the CA certificate being used contains the entire CA chain, including the root and any intermediate certificates.
- Check that the PCE can resolve the Splunk server using a tool like `nslookup` or `dig`.
- Make sure that the `[tcp-ssl]` stanza in Splunk is correct and the Splunk server is listening on the specified port. For example, to check that Splunk is listening on port 514:

```
sudo lsof -i -n -P | grep TCP | grep 514
```

- Verify that the hostname or IP address used for the connection is set as the CN or a SAN in the Splunk server certificate:

```
openssl x509 -text -noout -in $SPLUNK_HOME/etc/certs/splunk.pem
```

- Test the TLS connection from the PCE to Splunk:

```
openssl s_client -connect my.splunk.com:8443 -CApath /path/to/ca/certificates/
```

Forwarded Events Do Not Show Up In Splunk

- Make sure that the index value configured for the Illumio input is correct.
- Check that all desired event types are selected in the PCE's **Event Forwarding** settings.
- Check for errors in the `syslog-ng` logs in `/var/log/messages` on the PCE.
- If TLS is enabled for the connection, make sure that the `[tcp-ssl]` and `[SSL]` stanzas are configured correctly in `inputs.conf`.
- Make sure that the TCP input has `sourcetype = illumio:pce`.

Data Not in kvstore

If data is not showing up in the `illumio_*` metadata stores:

- If you are using a distributed Splunk environment, make sure to set `replicate = true` for all collections in `$SPLUNK_HOME/etc/apps/TA-Illumio/local/collections.conf` to enable replication across all indexes.
- Check `$SPLUNK_HOME/var/log/splunk/mongodb.log` for any start-up or runtime errors with MongoDB.
- Call the [Splunk API endpoint](#) for the collection to check if objects are being stored.
- Check that the `transforms.conf` stanza for the collection lookup is configured correctly.

Test the PCE Connection

When an Illumio modular input is created, the connection to the PCE is validated, and any connection issues will be presented to the user in the error dialog on the input configuration page. Check `splunkd.log` for additional error logs. If you can't determine the cause from the logs, try the following:

- Use a tool like `nslookup` or `dig` from the Splunk server to make sure that the PCE host is resolvable and that there is no issue with the DNS nameserver.
- Use **curl** or **wget** to establish an HTTP connection from the Splunk server to the PCE:
`curl -L -U "<api_key>:<api_secret>" "https://my.pce.com:8443/api/v2/health"`
- Make sure that the API key used for the connection is valid and has read access to policy objects.
- If you are using internal or self-signed certificates, make sure that Splunk is using the correct CA chain.

You can also use the `illumio_connection_test.py` script to validate the PCE connection from the command line:

```
> python $SPLUNK_HOME/etc/apps/TA-Illumio/bin/illumio_connection_test.py

Enter PCE hostname: my.pce.com

Enter PCE port: 8443

Enter PCE org ID: 1

Username or API key ID: api_...

Password or API key secret: ...
```

You can also set these values using the following environment variables:

```
export ILLUMIO_PCE_HOST=my.pce.com

export ILLUMIO_PCE_PORT=8443

export ILLUMIO_PCE_ORG_ID=1

export ILLUMIO_API_KEY_USERNAME=api_...

export ILLUMIO_API_KEY_SECRET=...
```

The script output should help to narrow down the cause of the connection failure.

Troubleshooting the Illumio App for Splunk

Make sure that **TA-Illumio** is installed and configured. Check that events and metadata are being received from the PCE.

If the app dashboards are not being populated:

- Check that the `illumio_get_index` macro has been set and make sure that it points to the correct index.
- Make sure that the configured index or indexes contain data within the given time range by running the following search:

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

The results should contain one or more sourcetypes with their respective event counts.

- Check if the search time range extends further back than the index retention policy.
- Check that you aren't hitting your Splunk license limits.

If the dashboards or visualizations appear to load incorrectly or behave in expected ways:

- Try to clear the static cache using your Splunk instance's `https://my.splunk.com/en-us/bump` endpoint.

If the dashboard visualizations are slow to load or searches are delayed:

- Try reducing the time range of the search.
- Enable acceleration for the Illumio data model (see [Data Model Acceleration \[26\]](#)).
- Check if searches are lagging or being delayed because of other jobs or processes running in the background.
- Check if the time range your search is being run in accesses cold buckets in your index. If your daily volume is high, you may need to increase the `maxWarmDBCount` in `indexes.conf` to delay the roll-over from warm to cold.
- Increase the compute resources allocated to your Splunk instance or cluster.

Troubleshooting Illumio Technology Add-On for Splunk Version 4.0.2

Check `splunkd.log` for the logs for kvstore operations.

```
08-09-2024 23:04:54.884 -0700 INFO ExecProcessor [10044 ExecProcessor] - message from "/opt/splunk/bin/python3.7 /opt/splunk/etc/apps/TA-Illumio/bin/illumio.py" Downloaded KV store collection successfully: TA-Illumio/illumio_rule_sets
08-09-2024 23:04:54.884 -0700 INFO ExecProcessor [10044 ExecProcessor] - message from "/opt/splunk/bin/python3.7 /opt/splunk/etc/apps/TA-Illumio/bin/illumio.py" result from downloading collection illumio_rule_sets, is success and source uri is https://127.0.0.1:8089
08-09-2024 23:04:54.897 -0700 INFO ExecProcessor [10044 ExecProcessor] - message from "/opt/splunk/bin/python3.7 /opt/splunk/etc/apps/TA-Illumio/bin/illumio.py" Response code from deleting collection illumio_rule_sets is 200
08-09-2024 23:04:54.908 -0700 INFO ExecProcessor [10044 ExecProcessor] - message from "/opt/splunk/bin/python3.7 /opt/splunk/etc/apps/TA-Illumio/bin/illumio.py" Stats for copy collection illumio_rule_sets is {'app': 'TA-Illumio', 'collection': 'illumio_rule_sets', 'result': 'success', 'download_time': '0:00:00.005949', 'delete_time': '0:00:00.024434', 'upload_time': '0:00:00.011182', 'download_count': 9, 'upload_count': 9}
08-09-2024 23:04:54.914 -0700 INFO ExecProcessor [10044 ExecProcessor] - message from "/opt/splunk/bin/python3.7 /opt/splunk/etc/apps/TA-Illumio/bin/illumio.py" Counted 16 total records and 16 in this loop.
08-09-2024 23:04:54.915 -0700 INFO ExecProcessor [10044 ExecProcessor] - message from "/opt/splunk/bin/python3.7 /opt/splunk/etc/apps/TA-Illumio/bin/illumio.py" Downloaded KV store collection successfully: TA-Illumio/illumio_rules
08-09-2024 23:04:54.915 -0700 INFO ExecProcessor [10044 ExecProcessor] - message from "/opt/splunk/bin/python3.7 /opt/splunk/etc/apps/TA-Illumio/bin/illumio.py" result from downloading collection illumio_rules, is success and source uri is https://127.0.0.1:8089
08-09-2024 23:04:54.927 -0700 INFO ExecProcessor [10044 ExecProcessor] - message from "/opt/splunk/bin/python3.7 /opt/splunk/etc/apps/TA-Illumio/bin/illumio.py" Response code from deleting collection illumio_rules is 200
08-09-2024 23:04:54.942 -0700 INFO ExecProcessor [10044 ExecProcessor] - message from "/opt/splunk/bin/python3.7 /opt/splunk/etc/apps/TA-Illumio/bin/illumio.py" Stats for copy collection illumio_rules is {'app': 'TA-Illumio', 'collection': 'illumio_rules', 'result': 'success', 'download_time': '0:00:00.006479', 'delete_time': '0:00:00.027326', 'upload_time': '0:00:00.015444', 'download_count': 16, 'upload_count': 16}
```

Do the following:

- Create a local copy of all collections defined in TA-Illumio.
- Delete the collections on remote nodes.
- Upload local files to the remote nodes.

If dashboards are not loading as expected and are empty, on the HF, verify that the lookups contain data using the following command:

```
| inputlookup illumio_labels_lookup
```

If the results are empty, then verify that the data inputs that were defined using modular input and verify that the HF is able to reach the search head using the credentials that you added in the modular input.

Also verify events coming into Splunk, because sometimes the HF forwards data to the search head but the search head fails to render any dashboards. The HF contains an option to keep a copy of the data that is being forwarded. Select the copy to verify that the data was input.

Refer to splunkd.log to see if uploading or copying kvstore files to the remote nodes is erroring out.

```
08-09-2024 23:04:54.942 -0700 INFO ExecProcessor [10044 ExecProcessor] - message from "/opt/splunk/bin/python3.7 /opt/splunk/etc/apps/TA-Illumio/bin/illumio.py" Stats for copy collection illumio_rules is {'app': 'TA-Illumio', 'collection': 'illumio_rules', 'result': 'success', 'download_time': '0:00:00.006479', 'delete_time': '0:00:00.027326', 'upload_time': '0:00:00.015444', 'download_count': 16, 'upload_count': 16}
The "result" variable denotes if the operation of copying collection to remote node was successful
```

Known Issues and Limitations

The following topics describe known issues for Splunk.

- The **PCE Operations** dashboard will not be populated for SaaS customers because PCE system health information is not available.
- Label Group objects are not currently imported by the Illumio TA.
- The Illumio TA only supports TCP for Syslog.

Service Account API Keys

- Service Account keys have a default expiration of 90 days. Make sure to rotate them before they expire.
- For some versions of the PCE (21.5), some API endpoints may return a 403 despite the Service Account key having the necessary permissions. When you see 403 errors in the TA logs, create a new key or use a User-scoped API key instead.

Illumio Supercluster

- The illumio_* metadata collections set the pce_fqdn field value to be the domain name of the PCE referenced in the input configuration. This could lead to these metadata objects having different pce_fqdn values from the syslog events pushed by individual supercluster members.

Known Issue on TA-Illumio 4.0.2 and Above

The following known issue applies to TA-Illumio 4.0.2 and above.

TA-Illumio 4.0.2 Does Not Pull Data from PCEs with Over 25,000 VEN

Splunk TA v4.0.2 and above does not support pulling metadata from PCEs with more than 25,000 VENs.

The following error occurred in splunkd.log when trying to ingest metadata from a PCE with around 27,000 VENs:

```
"StateStoreError: 'Batch save to KV store failed with code 400. Error details: Request exceeds API limits - see limits.conf for details. (Batch save size=53468786 too large)' "53 MB greater than the default (50 MB) on max_size_per_batch_save_mb
```

This occurs because of the default API limits on the Splunk side. See the following article: [limits.conf](#).

To set custom configurations, create a new file called limits.conf in the \$SPLUNK_HOME/etc/system/local directory. Then add the specific settings that you want to customize to the local configuration file.

Add the following setting to limits.conf:

```
[kvstore]
max_size_per_batch_save_mb = 100
```

The limits.conf file is located here: "\$SPLUNK_HOME/etc/system/local".

After you have added the setting, restart the Illumio Technology Add-On.