Illumio Application for QRadar 1.4.0

Integration Guide

The Illumio Application for QRadar integrates with the Illumio Policy Compute Engine (PCE) to provide security insights into your Illumio-secured data center.

Table of Contents

What's New in the Illumio App for QRadar

Learn how to install, configure, and troubleshoot the Illumio App for QRadar.

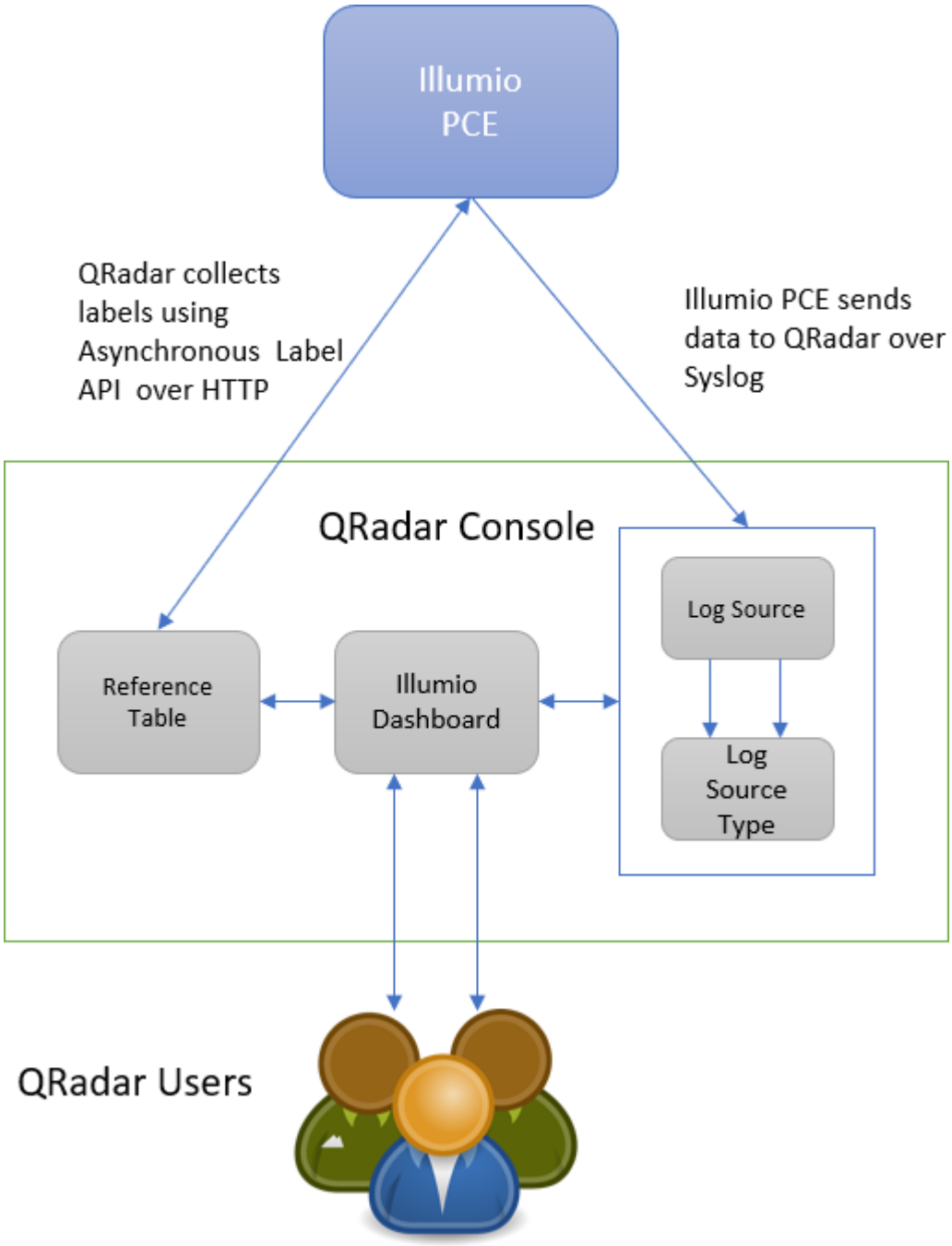
Version	Release Date	Release Notes
1.4.0	September 19, 2024	• Added support for PCE versions 21.5, 22.2, 22.5, 23.2, 23.5, and SaaS • Bug fixes and improvements
1.3.0	March 22, 2022	• Migrated application from QRadar v1 to v2 and python2 to python3 • Added support for PCE versions 21.2.0 and 21.2.1 • Added feature to download Investigations details as a .csv file • Added drilldown from the single value panels in the Security Operations Dashboard • Bug fixes

Deployment Architecture

IBM QRadar Security Information and Event Management (SIEM) is a network security management platform that provides situational awareness and compliance support. It collects, processes, aggregates, and stores network data in real-time. IBM Security QRadar SIEM has an architecture that provides real-time visibility into your IT infrastructure that you can use for threat detection and prioritization.

The Illumio Application for QRadar integrates with the Illumio Policy Compute Engine (PCE) to provide security insights into your Illumio-secured data center.

This diagram shows the data collection topology from Illumio PCE to QRadar.



The Illumio Application for QRadar provides two dashboards which are integrated into the QRadar user interface.

- With east-west traffic visibility on the Security Operations dashboard, you can see potential attacks and identify compromised workloads.
- The PCE Operations dashboard allows you to monitor the health of all deployed and managed PCEs.

The Illumio App for QRadar is supported with these PCE versions:

- 21.2.0, 21.2.1
- 21.5, 22.2, 22.5, 23.2, 23.5, and SaaS

Application Functionality

This section provides information about data collection, logs, and visualizations in the Illumio Application for QRadar.

Data Collection

The application has two sources for receiving data:

- API
- Syslog Port

From the API, the application fetches labels and stores them in a reference table. The data is used to populate the label filters on the dashboards. The application uses Asynchronous Label REST API calls to get data from the Illumio PCE server. These REST API calls are made from Python scripts in the application, which are run on a schedule you can define.

QRadar parses the data it receives from the application using a suitable log source. The log source is made up of two components:

- APIs
- Protocols

APIs in the Log Source

These APIs are used to fetch label data:

- Asynchronous Labels API: `https://<PCE_URL_DOMAIN>/api/v2/orgs/<ORG_ID>/labels`. It fetches labels from each PCE that is configured and enabled at that instance.

- Labels Location API: `https://<PCE_URL_DOMAIN>/api/v2/orgs/<ORG_ID>/jobs/<LOCATION>`

> **NOTE**
> PCE API version 2 is used to implement the Asynchronous Labels API.

This is an example response from the Asynchronous Labels API. It returns two role labels, "Web" and "Database":

```
[{
"href": "/orgs/1/labels/1", "key":
```

```
"role",

"value": "Web",

"created_at": "2017-04-12T22:02:02.953Z",
"updated_at": "2017-04-12T22:02:02.953Z",

"created_by": {

"href":
"/users/0"

},

"updated_by": {

"href":
"/users/0"

}

}, {

"href": "/orgs/1/labels/2", "key":
"role",

"value": "Database",

"created_at": "2017-04-12T22:02:02.960Z",
"updated_at": "2017-04-12T22:02:02.960Z",

"created_by": {

"href":
"/users/0"

},

"updated_by":{
```


After the application gets the lists of labels using the Asynchronous Labels API, it saves the response in QRadar's Reference table in the following format:


```
{
"https://<hostname>:8443/orgs/1/labels/1": {
"updated_by": "{u'href': u'/users/0'}",
"created_at": "1502975663000",

"updated_at": "1502975663000",
"created_by": "{u'href': u'/users/0'}", "href":
"/orgs/1/labels/1",

"value": "Web",

"key":
```

```
"role"

},

"https://<hostname>:8443/orgs/1/labels/2": {
"updated_by": "{u'href': u'/users/0'}",
"created_at": "1502975663000",

"updated_at": "1502975663000",
"created_by": "{u'href': u'/users/0'}", "href":
"/orgs/1/labels/2",
```

The primary key is `https://<hostname>:8443/orgs/1/labels/1`, which is the combination of the PCE link (hostname and port) and the href of the particular label. This primary key provides a unique identifier in the "labels" reference table for each PCE configured.

The `created_at` and `updated_at` timestamps are stored in epoch format, as QRadar requires.

Protocol in Log Source

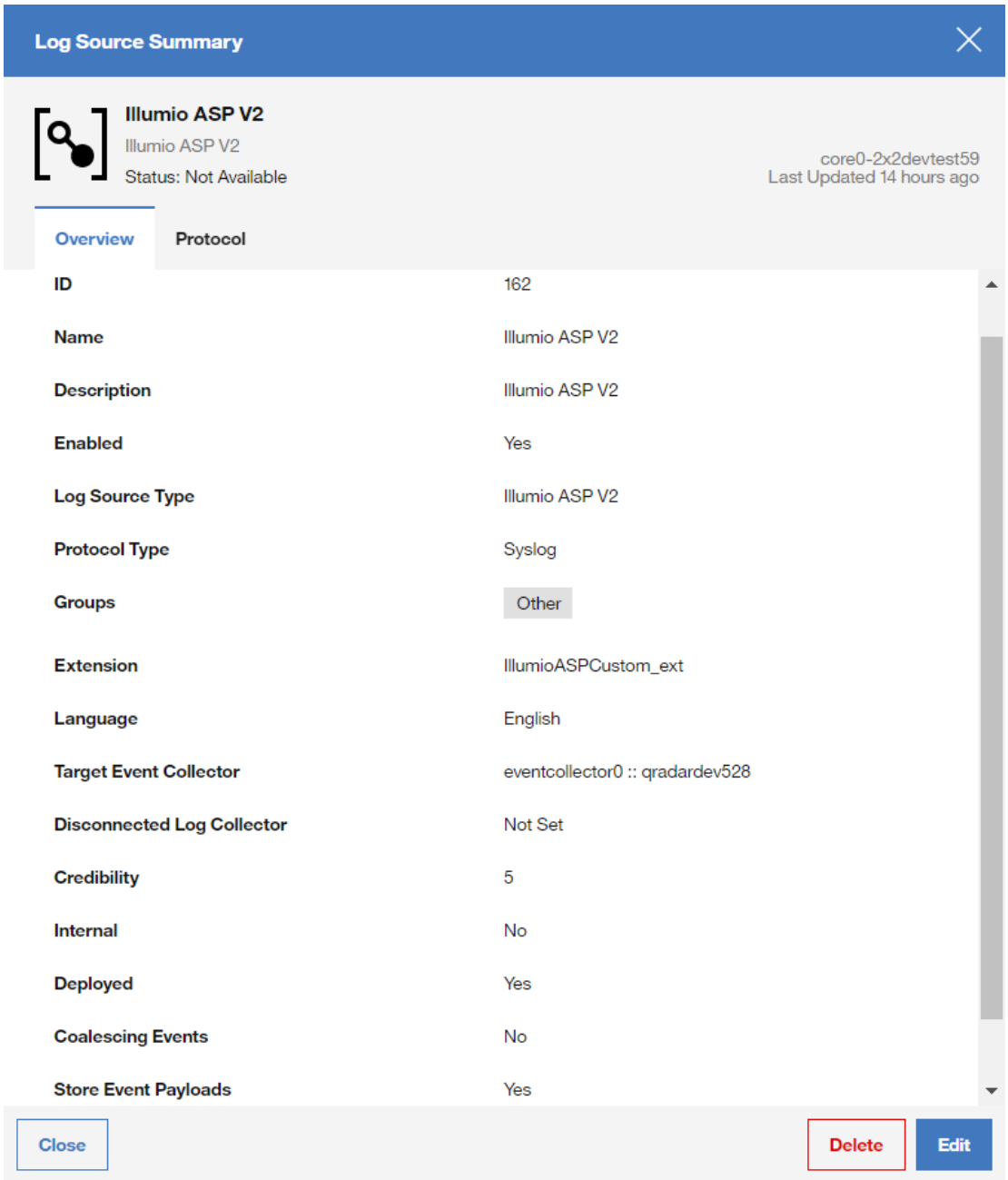
The protocol defines how data is communicated to QRadar. Data is forwarded to the Syslog port of QRadar from the PCE.

Log Sources

A log source named “Illumio ASP V2” is created automatically when the application is installed. All events that are sent from the application to QRadar include the log source as a prefix (such as `Illumio ASP V2: core0-2x2devtest59`).

You can create multiple log sources with different names if you want to create more descriptive identifiers, such as to convey more information about the usage of the event. You need to create a separate log source to collect data from each PCE.

This image shows the Illumio ASP V2 log source included in the app.



Log Source Types

Using log source types helps to define how data is parsed. You can attach Log Source Extension and Custom Event Properties to a log source to extend its capabilities. The log source type Illumio ASP V2 categorizes two types of events: Traffic Summary and Auditable Events.

Log Source Type	Event Data Type
Illumio ASP V2	Traffic Summary and Auditable Events (JSON + LEEF)

You can link the Illumio ASP V2 log source type to different log sources, as described in Add the PCE as a Log Source in QRadar [42].

Custom Property Extraction

The app performs extractions on the Audit Events and Traffic Summary Events received from Syslog on the QRadar instance. The app has a single Log Source Type that performs both JSON and LEEF extractions.

The following table lists the extractions (both JSON and LEEF) performed by the app:

Custom Property Name	Custom Property Expressions	Enabled
Action Api Endpoint	"?action"?[:=]\{.*?"api_endpoint":"?(.*?)"?[,}]	FALSE
Action Api Method	"?action"?[:=]\{.*?"api_method":"?(.*?)"?[,}]	FALSE
Action Errors	"action":.*?"errors":"?\[(.*?)\]"?	FALSE
Action HTTP Status Code	"?action"?[:=]\{.*?"http_status_code":"?(.*?)"?[,}]	FALSE
Action UUID	"?action"?[:=]\{.*?"uuid":"?(.*?)"?[,}]	FALSE
Agent Hostname	"?agent"?[:=]\{.*?"hostname":"?(.*?)"?[,}]	FALSE
Agent Href	"?agent"?[:=]\{.*?"href":"?(.*?)"?[,}]	FALSE
Created By Agent Href	"?created_by"?[:=]\{.*?"agent":\{.*?"href":"?(.*?)"?[,}]	FALSE
Created By User Href	"?created_by"?[:=]\{.*?"user":\{.*?"href":"?(.*?)"?[,}]	FALSE
Created By User Username	"?created_by"?[:=]\{.*?"user":\{.*?"username":"?(.*?)"?[,}]	FALSE
Destination Hostname	(\"dst_hostname\":\s*\"|dstHostname=)(.*?)(\"|\s)	TRUE
Destination Href	(\"dst_href\":\s*\"|dstHref=)(.*?)(\"|\s)	FALSE
Destination IPV4 or IPV6	dst=([\S]+?)((\s))	TRUE
Destination IPV4 or IPV6	"dst_ip":\"(.*?)\"	TRUE
Destination Labels App	(dstLabels=|\"dst_labels\":)\{[^\}]*?\"app\":\"(.*?)\"	TRUE
Destination Labels Environment	(dstLabels=|\"dst_labels\":)\{[^\}]*?\"env\":\"(.*?)\"	TRUE
Destination Labels Location	(dstLabels=|\"dst_labels\":)\{[^\}]*?\"loc\":\"(.*?)\"	TRUE
Destination Labels Role	(dstLabels=|\"dst_labels\":)\{[^\}]*?\"role\":\"(.*?)\"	TRUE
Direction	(\"dir\":\s*\"|dir=)(.*?)(\"|\s)	TRUE
Event Href	event_href=([^\s\t]+)	TRUE
Event Href Data	"?eventHref"?[=:]"?([^\s\t,}"]+)"?	FALSE
Event Severity	sev=(.*?)\s+	TRUE
Event Severity	"?severity"?[=:]"?([^\s\t,}"]+)"?	TRUE

Custom Property Name	Custom Property Expressions	Enabled
Hostname	(\s)(\S+?)(\s)illumio_pce	TRUE
Href	"?href"?[=:]"?([^\s\t,}"]+)"?	TRUE
Interval Sec	(intervalSec|"interval_sec"?)\s*[:=]?\s*(\d+(\.\d+)?)	FALSE
Notifications	"?notifications"?[:=]\[(.*)\]	FALSE
Outcome	outcome=([^\s\t]+)	FALSE
PCE FQDN	pce_fqdn=([^\s\t]+)	FALSE
PCE FQDN	"pce_fqdn":"?(.*?)"?[,}]	FALSE
Request Id	requestId=([^\s\t]+)	FALSE
Sec	sec=([^\s\t]+)	FALSE
Source Hostname	(\"src_hostname\":\s*\"|srcHostname=)(.*?)(\"|\s)	TRUE
Source Href	\"src_href\":\s*\"|srcHref=)(.*?)(\"|\s)	FALSE
Source IPV4 or IPV6	"src_ip":\"(.*?)\"	TRUE
Source IPV4 or IPV6	"data":.*"src_ip":\"(.*?)\"	TRUE
Source IPV4 or IPV6	src=([\S]+?)((\s))	TRUE
Source Labels App	(srcLabels=|\"src_labels\":)\{[^\}]*?\"app\":\"(.*?)\"	TRUE
Source Labels Environment	(srcLabels=|\"src_labels\":)\{[^\}]*?\"env\":\"(.*?)\"	TRUE
Source Labels Location	(srcLabels=|\"src_labels\":)\{[^\}]*?\"loc\":\"(.*?)\"	TRUE
Source Labels Role	(srcLabels=|\"src_labels\":)\{[^\}]*?\"role\":\"(.*?)\"	TRUE
Status	"?status"?[=:]"?([^\s\t,}"]+)"?	TRUE
Total Bytes In	"?tbi"?[:=]"?(.*?)"?[,}]	FALSE
Total Bytes Out	"?tbo"?[:=]"?(.*?)"?[,}]	FALSE
Traffic Count	count=([\S]+?)((\s))	TRUE
Traffic Count	"count":(\d+)	TRUE
URL	url=([^\s\t]+)	FALSE
Version	"?version"?[=:]"?([^\s\t,}"]+)"?	TRUE

Event Mappings

An event mapping is an association between an event ID and category combination and a QID record (referred to as an event categorization). Event ID and category values are extrac-

ted by DSMs from events and are then used to look up the mapped event categorization, or QID.

This table shows the high-level and low-level categories that are associated with each event.

Event Name	High-Level Category	Low-Level Category
Access restriction created	Audit	Create Activity Attempted
Access restriction deleted	Audit	Delete Activity Attempted
Access restriction updated	Audit	Update Activity Attempted
Agent clone activated	Audit	General Audit Event
Agent cloned detected	Audit	General Audit Event
Agent cloned detected	Audit	General Audit Event
Agent compatibility check report updated	Audit	General Audit Event
Agent compatibility report updated	Audit	Update Activity Succeeded
Agent disconnected	Audit	General Audit Event
Agent existing IP tables uploaded	Audit	General Audit Event
Agent fetched policy	System	Host-Policy Created
Agent firewall tampered	Suspicious Activity	Content Modified By Firewall
Agent interactive users updated	Audit	Update Activity Succeeded
Agent interfaces updated	Audit	General Audit Event
Agent machine identifiers updated	Audit	General Audit Event
Agent missed heartbeats	Audit	General Audit Event
Agent paired	Audit	General Audit Event
Agent properties updated	Audit	General Audit Event
Agent refreshed token	Audit	General Audit Event

Event Name	High-Level Category	Low-Level Category
Agent reported a service not running	Audit	General Audit Event
Agent request upgraded	Audit	General Audit Event
Agent service report updated	Audit	General Audit Event
Agent support report request created	Audit	General Audit Event
Agent support report request deleted	Audit	General Audit Event
Agent support report request updated	Audit	General Audit Event
Agent support report uploaded	Audit	General Audit Event
Agent suspended	Audit	General Audit Event
Agent unpaired	Audit	General Audit Event
Agent unsuspended	Audit	General Audit Event
Agent updated existing containers	Audit	Update Activity Succeeded
Agent updated existing iptables href	Audit	General Audit Event
Agent uploaded dev-alert logs	Audit	General Audit Event
Agent uploaded ops-alert logs	Audit	General Audit Event
Agents marked offline	Audit	General Audit Event
Agents unpaired	Audit	General Audit Event
API key created	Audit	General Audit Event
API key deleted	Audit	General Audit Event
API key updated	Audit	General Audit Event
API request authentication failed	Access	Unauthorized Access Attempt
API request authorization failed	Access	Unauthorized Access Attempt
API request failed due to internal server error	Audit	General Audit Event

Event Name	High-Level Category	Low-Level Category
API request failed due to unavailable service	Audit	General Audit Event
API request failed due to unknown server error	Audit	General Audit Event
Auth token returned for user authentication on PCE	Authentication	User Login Attempt
Authentication settings updated	Audit	General Audit Event
Blocked traffic event deleted	Audit	General Audit Event
Clear VEN authentication recovery condition	System	Daemon
Cleared a condition from a list of NetworkEnforcementNodes	Audit	Delete Activity Attempted
Computed policy for unmanaged workloads	System	Daemon
Condition cleared from a list of VENs	Audit	Delete Activity Attempted
Container cluster created	Audit	Create Activity Succeeded
Container cluster deleted	Audit	Delete Activity Succeeded
Container cluster label mappings updated all at once	Audit	Update Activity Attempted
Container cluster services provisioned	System	Daemon
Container cluster services updated from Kubelink	Audit	Create Activity Succeeded
Container cluster updated	Audit	Update Activity Succeeded
Container workload profile created	Audit	Create Activity Succeeded
Container workload profile deleted	Audit	Delete Activity Succeeded
Container workload profile updated	Audit	Update Activity Succeeded

Event Name	High-Level Category	Low-Level Category
Container workload updated	Audit	General Audit Event
Corporate ips setting updated	Audit	Update Activity Attempted
Creation of support report requested	Audit	General Audit Event
DB temp table cleanup completed	Audit	General Audit Event
DB temp table cleanup started	Audit	General Audit Event
Default VEN software version set	Audit	Update Activity Attempted
Deleted old cached perspectives	System	Daemon
Domain created	Audit	General Audit Event
Domain deleted	Audit	General Audit Event
Domain updated	Audit	General Audit Event
Enforcement boundary deleted	Audit	Delete Activity Succeeded
Enforcement boundary updated	Audit	Update Activity Succeeded
Enforcement instruction applied to a network device	Audit	General Audit Event
Enforcement instructions applied to multiple network devices	Audit	General Audit Event
Event pruning completed	Audit	General Audit Event
Event settings updated	Audit	Update Activity Succeeded
Event settings updated	Audit	Update Activity Succeeded
Existing or new unmanaged workload assigned to a network device	Audit	General Audit Event
Explorer settings updated	Audit	Update Activity Attempted
First user created	Audit	General Audit Event

Event Name	High-Level Category	Low-Level Category
Flow Allowed	Flow	Misc flow
Flow Blocked	Flow	Misc flow
Flow Potentially Blocked	Flow	Misc flow
Flow Unknown	Flow	Misc flow
Generate a new cert for signing SAML AuthN requests	Audit	Create Activity Attempted
Generate maintenance token for any agent	Audit	Update Activity Attempted
Global policy settings updated	Audit	General Audit Event
Group created	Authentication	Group Added
Group updated	Authentication	Group Removed
Ignored interfaces list updated	Audit	General Audit Event
Interservice call to log-in service to create LDAP config	Audit	Create Activity Succeeded
Interservice call to log-in service to delete LDAP config	Audit	Delete Activity Succeeded
Interservice call to log-in service to update LDAP config	Audit	Update Activity Succeeded
Interservice call to login service to veri-fy connection to the LDAP server	Audit	Configure Activity Succeeded
IP list created	Audit	General Audit Event
IP list deleted	Audit	General Audit Event
IP list updated	Audit	General Audit Event
IP lists deleted	Audit	Delete Activity Succeeded
IP tables rules created	Audit	General Audit Event
IP tables rules deleted	Audit	General Audit Event
IP tables rules updated	Audit	General Audit Event
Job deleted	Audit	Delete Activity Attempted

Event Name	High-Level Category	Low-Level Category
Label created	Audit	General Audit Event
Label deleted	Audit	General Audit Event
Label dimension created	Audit	Create Activity Attempted
Label dimension deleted	Audit	Delete Activity Attempted
Label dimension updated	Audit	Update Activity Attempted
Label group created	Audit	General Audit Event
Label group deleted	Audit	General Audit Event
Label group updated	Audit	General Audit Event
Label updated	Audit	General Audit Event
Labels deleted	Audit	Delete Activity Succeeded
LDAP configuration created	Audit	Create Activity Succeeded
LDAP configuration deleted	Audit	Delete Activity Succeeded
LDAP configuration updated	Audit	Update Activity Succeeded
LDAP server connection verified	Audit	Configure Activity Succeeded
License deleted	Audit	General Audit Event
License updated	Audit	General Audit Event
Local user password changed	Authentication	Password Change Succeeded
Local user profile created	Audit	General Audit Event
Local user profile deleted	Audit	General Audit Event
Local user reinvited	Audit	General Audit Event
Login Proxy Authentication settings updated	Authentication	Policy Change
Login Proxy Password policy updated	Authentication	Policy Change

Event Name	High-Level Category	Low-Level Category
Login Proxy RADIUS config shared secret verified	System	Successful Configuration Modification
Login Proxy RADIUS configuration deleted	Authentication	Policy Change
Login Proxy RADIUS configuration updated	Authentication	Policy Change
Login Proxy RADIUS configurations created	Audit	General Audit Event
Login Proxy SAML configuration updated	Authentication	Policy Change
Login Proxy User accepted invitation	System	Successful Configuration Modification
Login Proxy User invited	System	Successful Configuration Modification
Login Proxy User reset password	System	Successful Configuration Modification
Login Proxy User updated	System	Successful Configuration Modification
Login resource created	Audit	General Audit Event
Login resource deleted	Audit	General Audit Event
Login resource updated	Audit	General Audit Event
Login user authenticated	Authentication	General Authentication Successful
Login user password changed	Authentication	General Authentication Successful
Lost agent found	Audit	General Audit Event
Lost agent updated	Audit	General Audit Event
Network deleted	Application	Network Management
Network device created	Audit	General Audit Event
Network device deleted	Audit	General Audit Event
Network device updated	Audit	General Audit Event
Network endpoint created	Audit	General Audit Event

Event Name	High-Level Category	Low-Level Category
Network endpoint deleted	Audit	General Audit Event
Network endpoint updated	Audit	General Audit Event
Network enforcement node acknowledgment of policy	Audit	General Audit Event
Network enforcement node activated	Audit	General Audit Event
Network enforcement node deactivated	Audit	General Audit Event
Network enforcement node policy requested	Audit	General Audit Event
Network enforcement node reports when switches are not reachable	Audit	General Audit Event
Network function controller created	Audit	General Audit Event
Network function controller deleted	Application	Network Management
Network function controller policy status	Audit	General Audit Event
Network function controller policy status update	Audit	General Audit Event
Network function controller SLB state updated	Audit	General Audit Event
Network function controller virtual servers discovered	Audit	General Audit Event
Network updated	Application	Network Management
Networks created	Application	Network Management
Org created from JWT	Audit	General Audit Event
Organization created	Audit	Create Activity Succeeded
Organization information updated	Audit	General Audit Event
Organization setting updated	Audit	General Audit Event
Pairing profile created	Audit	General Audit Event

Event Name	High-Level Category	Low-Level Category
Pairing profile delete all pairing keys	Audit	Delete Activity Succeeded
Pairing profile deleted	Audit	General Audit Event
Pairing profile pairing key created	Audit	Create Activity Succeeded
Pairing profile pairing key generated	Audit	General Audit Event
Pairing profile pairing key generated	Audit	General Audit Event
Pairing profile updated	Audit	General Audit Event
Pairing profile updated	Audit	General Audit Event
Pairing profiles deleted	Audit	Delete Activity Succeeded
Pairing profiles deleted	Audit	Delete Activity Succeeded
Password policy created	Audit	General Audit Event
Password policy deleted	Audit	General Audit Event
Password policy updated	Audit	General Audit Event
PCE Application started	Audit	General Audit Event
PCE Application stopped	Audit	General Audit Event
PCE cluster created	Audit	General Audit Event
PCE cluster deleted	Audit	General Audit Event
PCE cluster updated	Audit	General Audit Event
PCE network interfaces reverted	Audit	General Audit Event
PCE software deleted	Audit	Delete Activity Succeeded
PCE support bundle request deleted	Audit	Delete Activity Attempted
PCE support bundle request generated	Audit	Create Activity Attempted
PCE syslog configuration update	Audit	Update Activity Succeeded

Event Name	High-Level Category	Low-Level Category
PCE system email tested	Audit	General Audit Event
PCE system network interfaces restarted	Audit	Update Activity Succeeded
PCE system restarted	Audit	General Audit Event
PCE system shutdown	Audit	General Audit Event
PCE system software upgraded	Audit	Update Activity Succeeded
PCE system software verified	Audit	General Audit Event
PCE system SSL/TLS certificates discarded	Audit	Update Activity Succeeded
PCE system SSL/TLS certificates uploaded	Audit	Update Activity Succeeded
PCE system web console password updated	Audit	Update Activity Succeeded
PCE system web email configuration updated	Audit	Update Activity Succeeded
Pending security policy deleted	Audit	Delete Activity Succeeded
RADIUS auth challenge issued	Audit	General Audit Event
RADIUS config shared secret verified	Audit	General Audit Event
RADIUS configuration deleted	Audit	General Audit Event
RADIUS configuration updated	Audit	General Audit Event
RADIUS configurations created	Audit	General Audit Event
Ran expired service account deletion task	System	Daemon
Ran service account expiry sweep task	System	Daemon
Ran SetServer sync task	System	Daemon
Ran task to check for offline endpoints	System	Daemon

Event Name	High-Level Category	Low-Level Category
Ran vacuum task for deactivated and deleted workloads	System	Daemon
RBAC Auth Security Principal created	Audit	General Audit Event
RBAC auth security principal deleted	Audit	General Audit Event
RBAC auth security principal updated	Audit	General Audit Event
RBAC permission created	Audit	General Audit Event
RBAC permission deleted	Audit	General Audit Event
RBAC permission updated	Audit	General Audit Event
RBAC security principal bulk deleted	Audit	General Audit Event
RBAC security principal bulk updated	Audit	General Audit Event
RBAC security principal created	Audit	General Audit Event
RBAC security principals bulk created	Audit	Create Activity Succeeded
Remote Syslog destination not reachable	Audit	Monitor Activity Failed
Remote Syslog destination reachable	Audit	Monitor Activity Succeeded
Rule set create	Audit	General Audit Event
Rule set deleted	Audit	General Audit Event
Rule set projected vulnerability exposure score updated	Audit	General Audit Event
Rule set updated	Audit	General Audit Event
Rule sets deleted	Audit	Delete Activity Succeeded
Rules for organization recalculated	Audit	General Audit Event
Running container updated	Audit	General Audit Event

Event Name	High-Level Category	Low-Level Category
SAML assertion consumer services updated	Audit	General Audit Event
SAML configuration created	Audit	General Audit Event
SAML configuration deleted	Audit	General Audit Event
SAML configuration updated	Audit	General Audit Event
SAML Service Provider created	Audit	General Audit Event
SAML Service Provider deleted	Audit	General Audit Event
SAML Service Provider updated	Audit	General Audit Event
Secure connect gateway deleted	Audit	General Audit Event
Secure connect gateway updated	Audit	General Audit Event
SecureConnect gateway created	Audit	General Audit Event
Security policies deleted	System	Host-Policy Deleted
Security policy created	Authentication	Policy Added
Security policy restored	Audit	General Audit Event
Security policy rules created	Audit	General Audit Event
Security policy rules deleted	Audit	General Audit Event
Security policy rules updated	Audit	General Audit Event
Server load balancer created	Audit	General Audit Event
Server load balancer deleted	Audit	General Audit Event
Server load balancer updated	Audit	General Audit Event
Service account created	Authentication	Computer Account Added

Event Name	High-Level Category	Low-Level Category
Service account deleted	Authentication	Computer Account Removed
Service account updated	Authentication	Computer Account Changed
Service binding created	Audit	General Audit Event
Service binding deleted	Audit	General Audit Event
Service bindings created	Audit	General Audit Event
Service bindings deleted	Audit	Delete Activity Succeeded
Service created	System	Service Started
Service deleted	System	Service Stopped
Service updated	Audit	Update Activity Succeeded
Services deleted	Audit	General Audit Event
SSL/TLS certificates applied	Audit	General Audit Event
Stale zone subnets removed	System	Daemon
Success or Failure to apply policy on VEN	Audit	Update Activity Attempted
Support report uploaded	Audit	General Audit Event
Syslog destination created	Audit	General Audit Event
Syslog destination deleted	Audit	General Audit Event
Syslog destination updated	Audit	General Audit Event
Syslog remote destination created	Audit	Create Activity Succeeded
Syslog remote destination deleted	Audit	Delete Activity Succeeded
Syslog remote destination updated	Audit	Update Activity Succeeded
System administrator deleted	Audit	General Audit Event

Event Name	High-Level Category	Low-Level Category
System administrators created	Audit	General Audit Event
TLS channel established	Audit	General Audit Event
TLS channel terminated	Audit	General Audit Event
Traffic collector setting created	Audit	Create Activity Succeeded
Traffic collector setting deleted	Audit	Delete Activity Succeeded
Traffic collector setting updated	Audit	Update Activity Succeeded
Trusted proxy IPs created or updated	Audit	Update Activity Attempted
Updated the target PCE of the network enforcement node	Audit	Update Activity Attempted
Upgrade started	Audit	General Audit Event
User authenticated	Authentication	General Authentication Successful
User created	Audit	General Audit Even
User deleted	Audit	General Audit Event
User entered expired password	Audit	General Audit Event
User failed authentication	Authentication	General Authentication Failed
User failed authorization	Access	Misc Authorization
User information updated	Audit	General Audit Event
User invitation accepted	Audit	General Audit Event
User invited	Access	Access Permitted
User local password updated	Audit	Update Activity Succeeded
User local profile created	Audit	Create Activity Succeeded
User local profile deleted	Audit	Delete Activity Succeeded

Event Name	High-Level Category	Low-Level Category
User local profile reinvited	Audit	General Audit Event
User logged in	Authentication	User Login Success
User logged out	Authentication	Misc Logout
User login session terminated	Access	Session Terminated
User logout from JWT	Audit	General Audit Event
User password reset	Authentication	Password Change Succeeded
User password updated	Audit	General Audit Event
User session created	Authentication	User Login Success
User session terminated	Audit	General Audit Event
User Sign in	Authentication	User Login Success
User Sign out	Authentication	General Authentication Successful
User verified MFA	Authentication	User Login Success
VEN missing heartbeat after upgrade	System	Daemon
VEN release created	Audit	General Audit Event
VEN release deleted	Audit	General Audit Event
VEN release deployed	Audit	General Audit Event
VEN release updated	Audit	General Audit Event
VEN self signed certificate housekeeping check	System	Daemon
VEN settings invalidation error state check	System	Daemon
VEN settings updated	Audit	Update Activity Attempted
VEN software release created	Audit	Create Activity Succeeded
VEN software release deleted	Audit	Delete Activity Succeeded
VEN software release deployed	Audit	Deploy Activity Succeeded

Event Name	High-Level Category	Low-Level Category
VEN software release updated	Audit	Update Activity Succeeded
VEN software release upgraded	Audit	Update Activity Succeeded
VEN uninstall timeout	System	Daemon
Virtual server created	Audit	General Audit Event
Virtual server deleted	Audit	General Audit Event
Virtual server updated	Audit	General Audit Event
Virtual service bulk created	Audit	General Audit Event
Virtual service bulk updated	Audit	General Audit Event
Virtual Service created	Audit	General Audit Event
Virtual Service Deleted	Audit	General Audit Event
Virtual Service Updated	Audit	General Audit Event
Virtual services created in bulk	Audit	Create Activity Succeeded
Virtual services updated in bulk	Audit	Update Activity Succeeded
Vulnerability record created	Audit	Create Activity Succeeded
Vulnerability record deleted	Audit	General Audit Event
Vulnerability record updated	Audit	General Audit Event
Vulnerability report deleted	Audit	General Audit Event
Vulnerability report updated	Audit	General Audit Event
Workload added to network endpoint	Audit	General Audit Event
Workload apply pending policy	Audit	General Audit Event
Workload bulk deleted	Audit	General Audit Event
Workload bulk updated	Audit	General Audit Event

Event Name	High-Level Category	Low-Level Category
Workload created	Audit	General Audit Event
Workload deleted	Audit	General Audit Event
Workload flow reporting frequency changed	Audit	General Audit Event
Workload interface created	Audit	General Audit Event
Workload interface deleted	Audit	General Audit Event
Workload interface network created	Audit	General Audit Event
Workload interface updated	Audit	General Audit Event
Workload interfaces created	Audit	General Audit Event
Workload interfaces updated	Audit	General Audit Event
Workload labels applied	Audit	General Audit Event
Workload network redetected	Audit	General Audit Event
Workload policy recalculated	Audit	General Audit Event
Workload queried	Audit	General Audit Event
Workload service report updated	Audit	General Audit Event
Workload service reports updated	Audit	General Audit Event
Workload settings updated	Audit	Update Activity Succeeded
Workload soft deleted	Audit	General Audit Event
Workload undeleted	Audit	General Audit Event
Workload upgraded	Audit	General Audit Event
Workload was powered on or rejoined network	Audit	General Audit Event
Workloads bulk created	Audit	General Audit Event

Event Name	High-Level Category	Low-Level Category
Workloads created in bulk	Audit	Create Activity Succeeded
Workloads deleted in bulk	Audit	Delete Activity Succeeded
Workloads labels removed	Audit	Delete Activity Succeeded
Workloads policies applied	Audit	General Audit Event
Workloads unpaired	Audit	General Audit Event
Workloads updated	Audit	Update Activity Succeeded
Workloads updated in bulk	Audit	Update Activity Succeeded

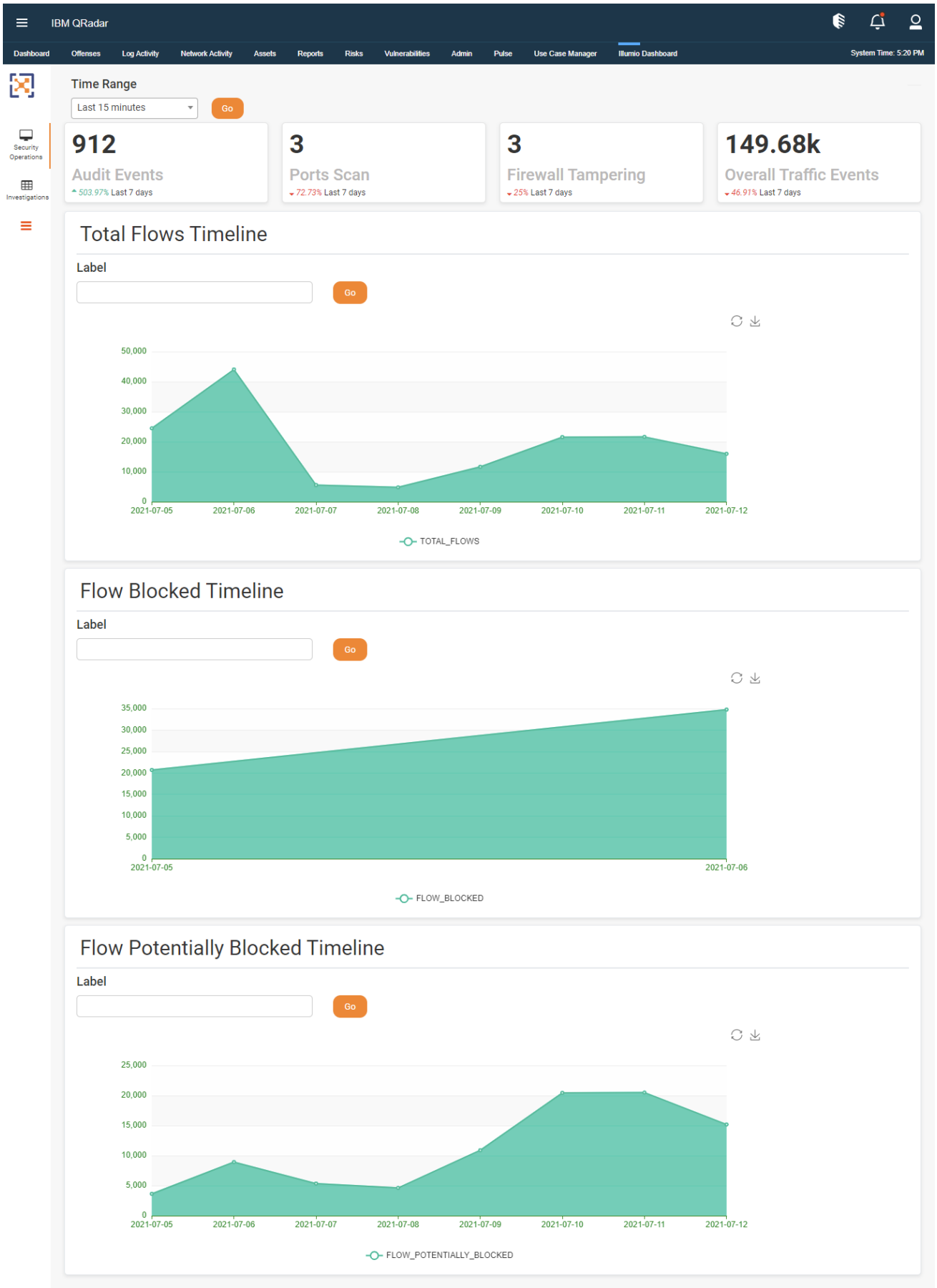
Visualizations

The Illumio App for QRadar provides two dashboards that are integrated into the QRadar UI. The dashboards consist of panels that plot specific metrics related to the events from the Illumio PCE. The data in all dashboards is populated from the Illumio ASP V2 log source type.

Security Operations Dashboard

The **Security Operations Dashboard** provides overall visibility into the Illumio App deployment. It gives a count of overall traffic events including **Audit Events**, **Port Scan**, and **Firewall Tampering**. You can filter the data for the entire dashboard by time range.

In each panel, you can also filter the data by label. The labels are grouped by type (app, env, role, or loc). If all the labels selected have the same type, the `OR` operator is applied. If the labels are of different types, the **AND** operator is applied. You can also use the **Direction** field to specify whether the labels are incoming or outgoing. If the value of the **Direction** field is I (Incoming), Destination labels are used in the filter. If the value of the **Direction** field is O (Outgoing), Source labels are used.


IBM QRadar
Dashboard
Offenses
Log Activity
Network Activity
Assets
Reports
Risks
Vulnerabilities
Admin
Pulse
Use Case Manager
Illumio Dashboard
System Time: 5:20 PM
Security Operations
Investigations
Time Range
Last 15 minutes
Go
912
Audit Events
503.97% Last 7 days
3
Ports Scan
72.73% Last 7 days
3
Firewall Tampering
25% Last 7 days
149.68k
Overall Traffic Events
46.91% Last 7 days
Total Flows Timeline
Label
Go
50,000
40,000
30,000
20,000
10,000
0
2021-07-05
2021-07-06
2021-07-07
2021-07-08
2021-07-09
2021-07-10
2021-07-11
2021-07-12
TOTAL_FLOWS
Flow Blocked Timeline
Label
Go
35,000
30,000
25,000
20,000
15,000
10,000
5,000
0
2021-07-05
2021-07-06
FLOW_BLOCKED
Flow Potentially Blocked Timeline
Label
Go
25,000
20,000
15,000
10,000
5,000
0
2021-07-05
2021-07-06
2021-07-07
2021-07-08
2021-07-09
2021-07-10
2021-07-11
2021-07-12
FLOW_POTENTIALLY_BLOCKED

Investigation Dashboard

This dashboard provides a list of the top 1000 Investigations sorted on the basis of time.

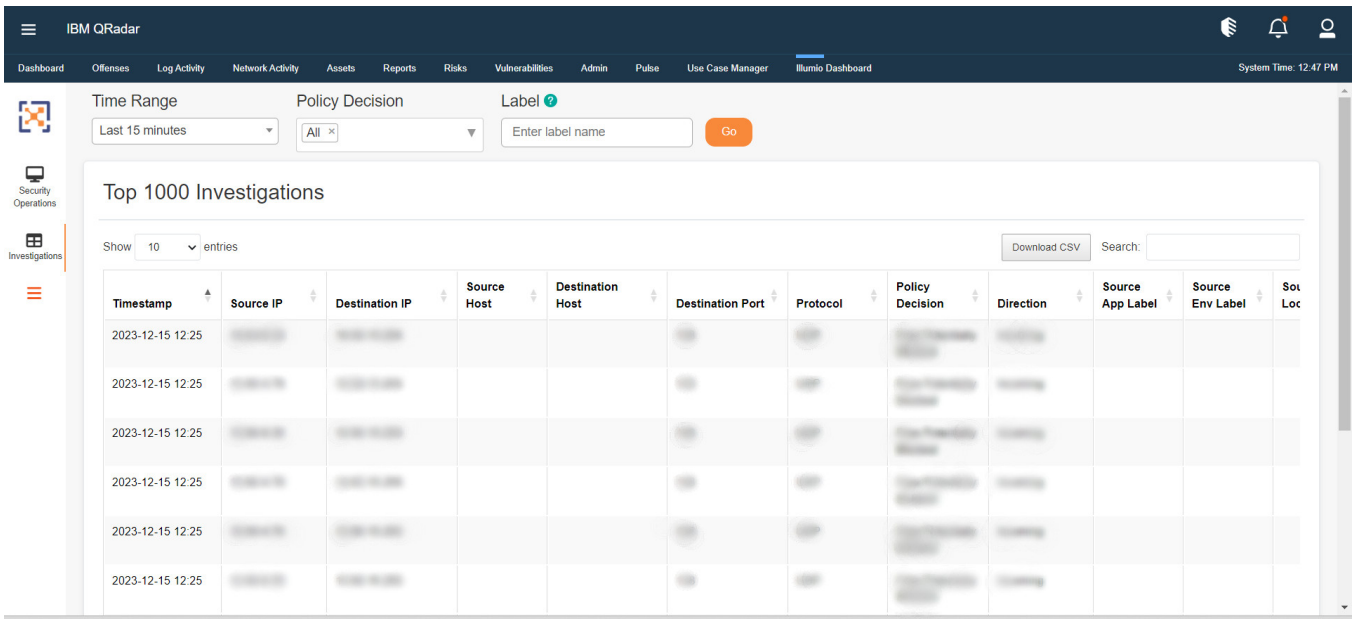
- The filters used for this dashboard are **Time Range**, **Policy**, and **Label**.
- For the **Label** filter, select from a drop-down or type the label value.
  If you type the label value, you must use this format for the label value: LabelCategory:LabelValue, such as app:abc.
- Label Categories can be “app”, ”role”, ”env”, or ”loc”.

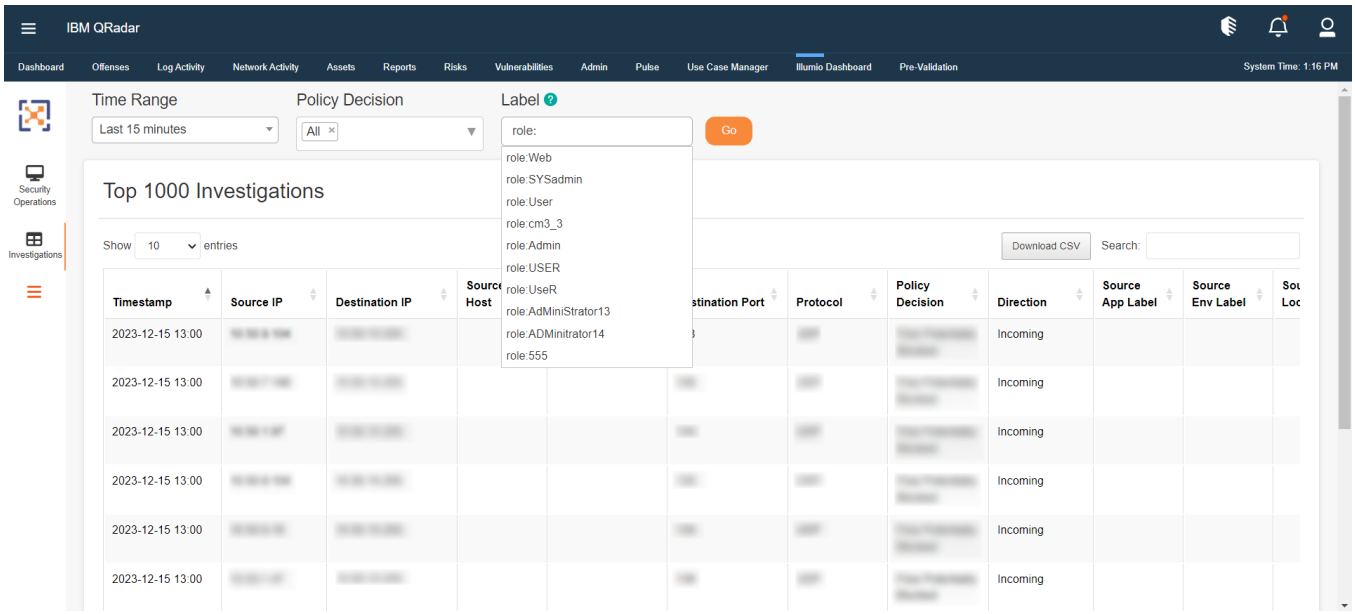
Label Value	Expected Result
app:	Top 1000 results in which Source Label Application or Destination Application label is not null.
app:Abc	Top 1000 results in which Source Label Application or Destination Application label is “Abc”

NOTE

You must configure the account in the configuration page to see the labels in the label filter in the dashboard. Do not use special characters when you are searching with labels because the result may be inaccurate.

The labels in this dashboard are from the `src_labels` and `dst_labels` fields in JSON (`srcLabels` and `dstLabels` in LEEF).



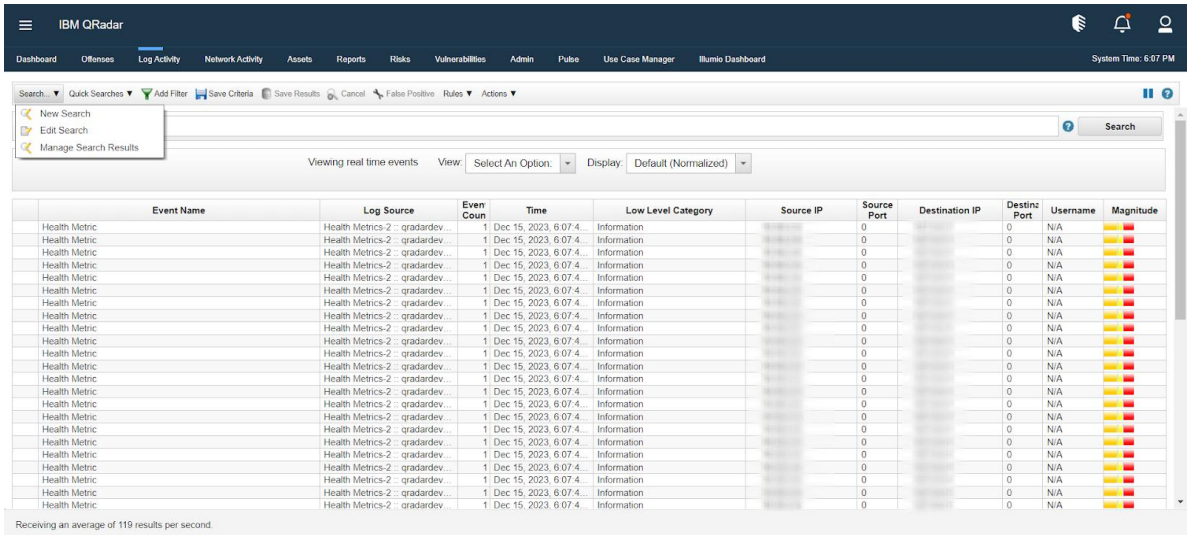


Saved Search

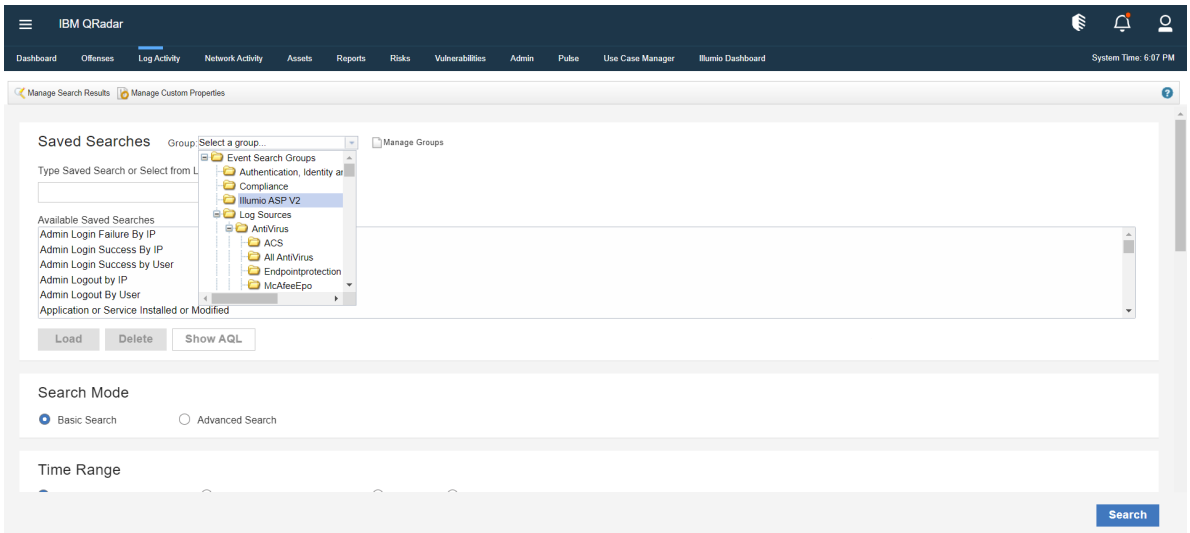
You can view the data in the **Log Activity** tab to see the ingested PCE events in QRadar. To change the time range in the saved search, change 7 days to the appropriate value. For example, to search for the last 2 days, change 7 days ago to 2 days ago.

Use the following procedure to run a saved search in QRadar:

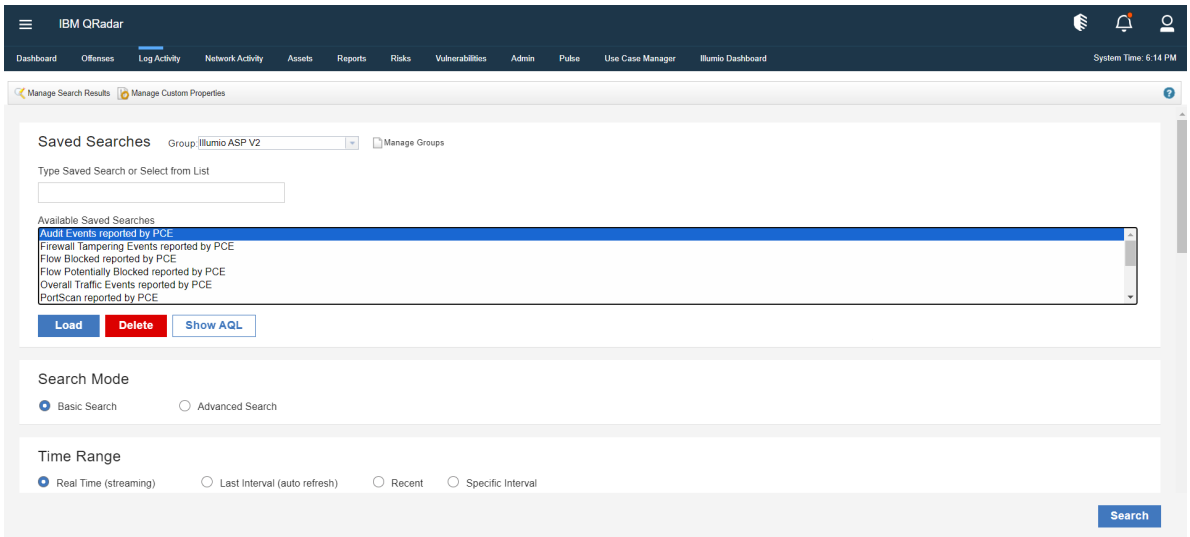
1. Go to the **Log Activity** tab in QRadar.
2. Click the **Search** drop-down and select **New Search**.



3. Click the **Group** drop-down and select Illumio ASP V2.



4. Select a search from the list of **Available Saved Searches** and click **Load**. To run the search in the **Log Activity** tab, click the **Search** button located in the bottom-right corner.



Name	Saved Search
Audit Events reported by PCE	select COUNT(*) AS 'COUNT' from events where LOGSOURCETYPENAME(devicetype) = 'Illumio ASP V2' AND ("Event Href" MATCHES '.*/orgs/[0-9]*/events.*' OR "Href" MATCHES '.*/orgs/[0-9]*/events.*') AND "version"=2 AND QIDNAME(qid) not in ('Unknown', 'IllumioASPCustom Message') AND devicetime BETWEEN PARSEDATETIME('7 days ago') AND PARSEDATETIME(NOW()) START PARSEDATETIME('7 days ago')
Firewall Tampering Events reported by PCE	select COUNT(*) AS 'COUNT' from events where QIDNAME(qid) in ('Agent firewall tampered') AND LOGSOURCETYPENAME(devicetype) = 'Illumio ASP V2' AND devicetime BETWEEN PARSEDATETIME('7 days ago') AND PARSEDATETIME(NOW()) START PARSEDATETIME('7 days ago')
Flow Blocked reported by PCE	SELECT DATEFORMAT(devicetime,'yyyy-MM-dd') AS 'LOGDATE', sum("Traffic Count") as 'COUNT', QIDNAME(qid) as 'Event Name' from events where QIDNAME(qid) in ('Flow Blocked') AND LOGSOURCETYPENAME(devicetype) = 'Illumio ASP V2' AND devicetime BETWEEN PARSEDATETIME('7 days ago') AND PARSEDATETIME(NOW()) GROUP BY DATEFORMAT(devicetime,'yyyy-MM-dd') START PARSEDATETIME('7 days ago')

Name	Saved Search
Flow Potentially Blocked reported by PCE	SELECT DATEFORMAT(devicetime,'yyyy-MM-dd') AS 'LOGDATE', sum("Traffic Count") as 'COUNT', QIDNAME(qid) as 'Event Name' from events where QIDNAME(qid) in ('Flow Potentially Blocked') AND LOGSOURCETYPENAME(devicetype) = 'Illumio ASP V2' AND devicetime BETWEEN PARSEDATETIME('7 days ago') AND PARSEDATETIME(NOW()) GROUP BY DATEFORMAT(devicetime,'yyyy-MM-dd') START PARSEDATETIME('7 days ago')
Overall Traffic Events reported by PCE	select sum("Traffic Count") AS 'COUNT' from events where QIDNAME(qid) in ('Flow Allowed', 'Flow Potentially Blocked', 'Flow Blocked') AND LOGSOURCETYPENAME(devicetype) = 'Illumio ASP V2' AND devicetime BETWEEN PARSEDATETIME('7 days ago') AND PARSEDATETIME(NOW()) START PARSEDATETIME('7 days ago')
PortScan reported by PCE	SELECT "Source IPV4 or IPV6", "Destination IPV4 or IPV6",LONG(UNIQUECOUNT(destinationport)) AS 'PORTCOUNT', LONG(starttime/600000) AS LOGDATE from events where QIDNAME(qid) in ('Flow Allowed','Flow Potentially Blocked','Flow Blocked') AND LOGSOURCETYPENAME(devicetype) = 'Illumio ASP V2' AND "direction" = 'I' AND devicetime BETWEEN PARSEDATETIME('7 days ago') AND PARSEDATETIME(NOW()) GROUP BY "Source IPV4 or IPV6","Destination IPV4 or IPV6",LOGDATE HAVING PORTCOUNT>1 ORDER BY LOGDATE START PARSEDATETIME('7 days ago')
Top 10 Blocked Hosts reported by PCE	SELECT sum("Traffic Count") as "Count","Source IPV4 or IPV6" as "Source IP", "Destination IPV4 or IPV6" as "Destination IP", DATEFORMAT(starttime,'yyyy-MM-dd') AS "Timestamp", destinationport as "Destination Port",IF "direction"='O' THEN 'Outgoing' ELSE 'Incoming' AS 'direction","Source Labels App" AS 'Source Labels App', "Source Labels Environment" AS 'Source Labels Environment' ,"Source Labels Location" AS 'Source Labels Location","Source Labels Role" AS 'Source Labels Role","Destination Labels App" AS 'Destination Labels App","Destination Labels Environment" AS 'Destination Labels Environment","Destination Labels Location" AS 'Destination Labels Location","Destination Labels Role" AS 'Destination Labels Role',IF "direction"='I' THEN "Destination Hostname" ELSE "Source Hostname" AS "Hostname" from events where QIDNAME(qid) in ('Flow Blocked') AND LOGSOURCETYPENAME(devicetype) = 'Illumio ASP V2' AND devicetime BETWEEN PARSEDATETIME('7 days ago') AND PARSEDATETIME(NOW()) GROUP BY Hostname ORDER BY "Count" DESC LIMIT 10 START PARSEDATETIME('7 days ago')
Top 10 Blocked Services reported by PCE	SELECT sum("Traffic Count") as "Count","Source IPV4 or IPV6" as "Source IP", "Destination IPV4 or IPV6" as "Destination IP", DATEFORMAT(starttime,'yyyy-MM-dd') AS "Timestamp", destinationport as "Destination Port",IF "direction"='O' THEN 'Outgoing' ELSE 'Incoming' AS 'direction","Source Labels App" AS 'Source Labels App', "Source Labels Environment" AS 'Source Labels Environment' ,"Source Labels Location" AS 'Source Labels Location","Source Labels Role" AS 'Source Labels Role","Destination Labels App" AS 'Destination Labels App","Destination Labels Environment" AS 'Destination Labels Environment","Destination Labels Location" AS 'Destination Labels Location","Destination Labels Role" AS 'Destination Labels Role","Destination Hostname" AS 'Destination Host Name","Source Hostname" AS 'Source Host Name' from events where QIDNAME(qid) in ('Flow Blocked') AND LOGSOURCETYPENAME(devicetype) = 'Illumio ASP V2' AND devicetime BETWEEN PARSEDATETIME('7 days ago') AND PARSEDATETIME(NOW()) GROUP BY destinationport,protocolid ORDER BY "Count" DESC LIMIT 10 START PARSEDATETIME('7 days ago')

Name	Saved Search
Top 10 Potentially Blocked Hosts reported by PCE	SELECT sum("Traffic Count") as "Count","Source IPV4 or IPV6" as "Source IP", "Destination IPV4 or IPV6" as "Destination IP", DATEFORMAT(starttime,'yyyy-MM-dd') AS "Timestamp", destinationport as "Destination Port",IF "direction"='O' THEN 'Outgoing' ELSE 'Incoming' AS 'direction','Source Labels App" AS 'Source Labels App', "Source Labels Environment" AS 'Source Labels Environment' ,"Source Labels Location" AS 'Source Labels Location','Source Labels Role" AS 'Source Labels Role','Destination Labels App" AS 'Destination Labels App','Destination Labels Environment" AS 'Destination Labels Environment','Destination Labels Location" AS 'Destination Labels Location','Destination Labels Role" AS 'Destination Labels Role',IF "direction"='I' THEN "Destination Hostname" ELSE "Source Hostname" AS "Hostname" from events where QIDNAME(qid) in ('Flow Potentially Blocked') AND LOGSOURCETYPENAME(devicetype) = 'Illumio ASP V2' AND devicetime BETWEEN PARSEDATETIME('7 days ago') AND PARSEDATETIME(NOW()) GROUP BY Hostname ORDER BY "Count" DESC LIMIT 10 START PARSEDATETIME('7 days ago')
Top 10 Potentially Blocked Services reported by PCE	SELECT sum("Traffic Count") as "Count","Source IPV4 or IPV6" as "Source IP", "Destination IPV4 or IPV6" as "Destination IP", DATEFORMAT(starttime,'yyyy-MM-dd') AS "Timestamp", destinationport as "Destination Port",IF "direction"='O' THEN 'Outgoing' ELSE 'Incoming' AS 'direction','Source Labels App" AS 'Source Labels App', "Source Labels Environment" AS 'Source Labels Environment' ,"Source Labels Location" AS 'Source Labels Location','Source Labels Role" AS 'Source Labels Role','Destination Labels App" AS 'Destination Labels App','Destination Labels Environment" AS 'Destination Labels Environment','Destination Labels Location" AS 'Destination Labels Location','Destination Labels Role" AS 'Destination Labels Role','Destination Hostname" AS 'Destination Host Name','Source Hostname" AS 'Source Host Name' from events where QIDNAME(qid) in ('Flow Potentially Blocked') AND LOGSOURCETYPENAME(devicetype) = 'Illumio ASP V2' AND devicetime BETWEEN PARSEDATETIME('7 days ago') AND PARSEDATETIME(NOW()) GROUP BY destinationport,protocolid ORDER BY "Count" DESC LIMIT 10 START PARSEDATETIME('7 days ago')
Top 1000 Investigations reported by PCE	SELECT "Source IPV4 or IPV6", "Destination IPV4 or IPV6", DATEFORMAT(devicetime,'yyyy-MM-dd H:mm') AS 'Timestamp', destinationport, PROTOCOLNAME(protocolid) as 'Protocol', QIDNAME(qid) as 'Policy Decision', IF "direction"='O' THEN 'Outgoing' ELSE 'Incoming' AS 'Direction', "Source Labels App", "Source Labels Environment","Source Labels Location","Source Labels Role","Destination Labels App","Destination Labels Environment","Destination Labels Location", "Destination Labels Role", "Destination Hostname", "Source Hostname" from events where QIDNAME(qid) in ('Flow Allowed','Flow Potentially Blocked','Flow Blocked') AND LOGSOURCETYPENAME(devicetype) = 'Illumio ASP V2' AND devicetime BETWEEN PARSEDATETIME('7 days ago') AND PARSEDATETIME(NOW()) ORDER BY 'Timestamp' DESC LIMIT 1000 START PARSEDATETIME('7 days ago')
Total Flows reported by PCE	SELECT DATEFORMAT(devicetime,'yyyy-MM-dd') AS 'LOGDATE', sum("Traffic Count") as 'COUNT', QIDNAME(qid) as 'Event Name' from events where QIDNAME(qid) in ('Flow Allowed','Flow Potentially Blocked','Flow Blocked') AND LOGSOURCETYPENAME(devicetype) = 'Illumio ASP V2' AND devicetime BETWEEN PARSEDATETIME('7 days ago') AND PARSEDATETIME(NOW()) GROUP BY DATEFORMAT(devicetime,'yyyy-MM-dd') START PARSEDATETIME('7 days ago')

Install and Configure the Illumio App for QRadar

The following topics describe how to install and configure the Illumio App for QRadar.

Before You Begin

Install this software before you can run the Illumio 1.4.0 app on QRadar:

- Illumio App Bundle (v1.4.0)
- QRadar version 7.4.3 GA or later
- Access to the Illumio PCE
- Illumio credentials to access labels from PCEs

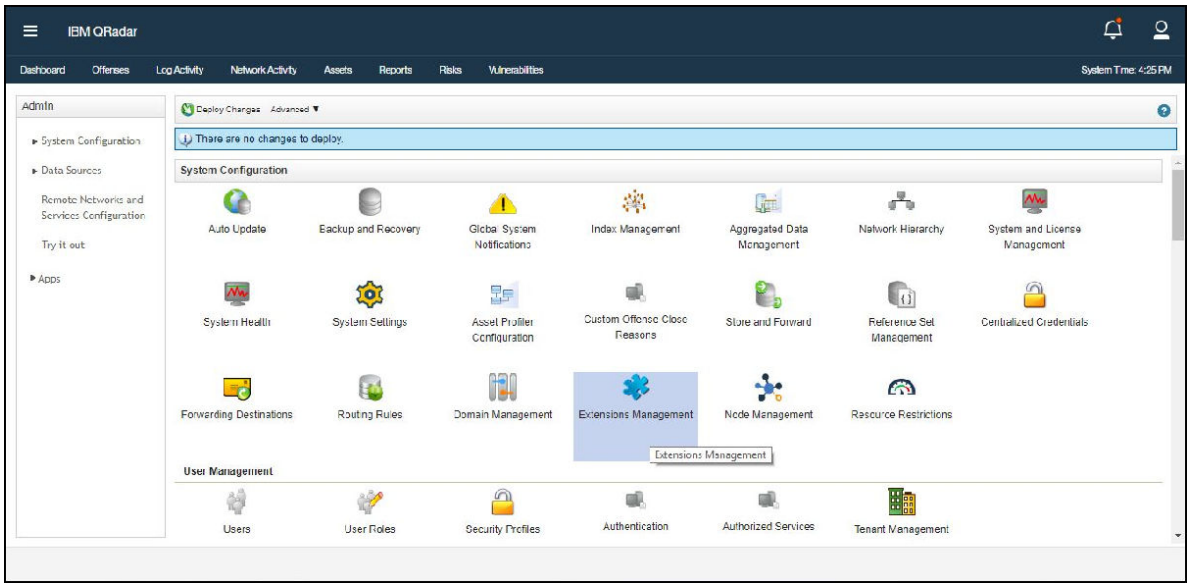
Install QRadar

The application installation requires access to the QRadar console through a web interface at https://<<QRadarconsoleIP>>/.

For details about logging into QRadar, see the IBM QRadar documentation.

1. Log into the QRadar console.

2. Go to **Admin** > **Extension Management**.



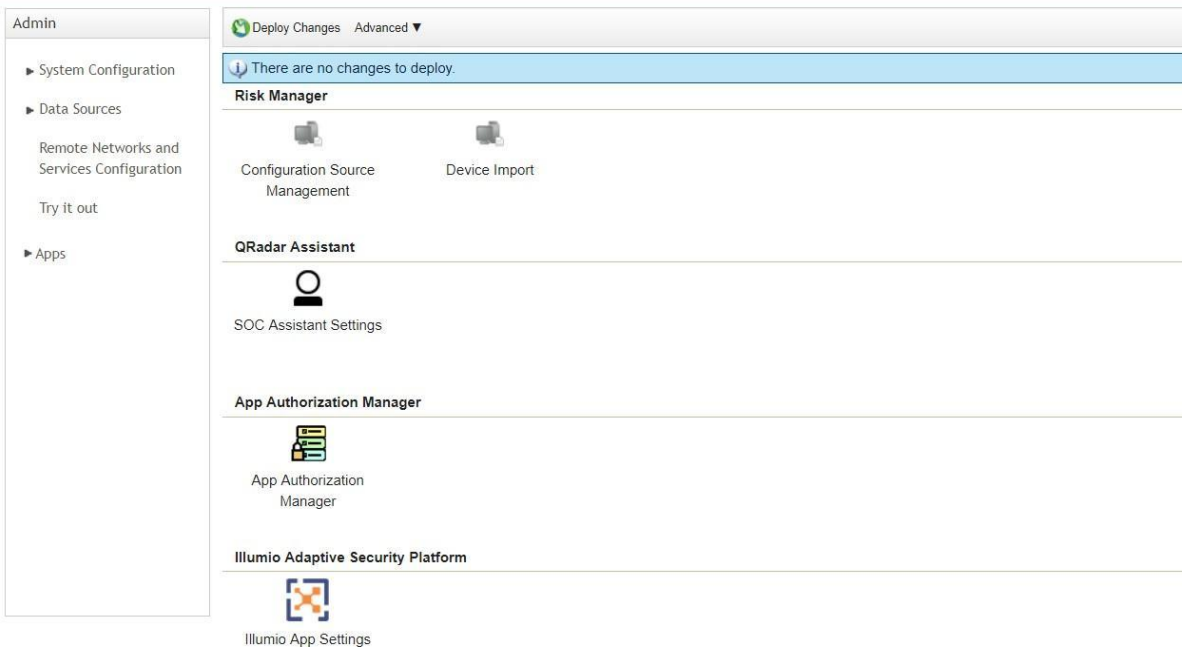
3. Click **Add** and select the downloaded Illumio App zip file.
   QRadar displays a list of changes that the app is making.
4. Click **Install**.
   After the application is installed, it will create a Docker container in the backend.
5. Deploy the changes on the **Admin** panel.
6. Refresh the browser to display the configuration page.

Configure the Application

After you complete the installation, you must configure the application to start data collection.

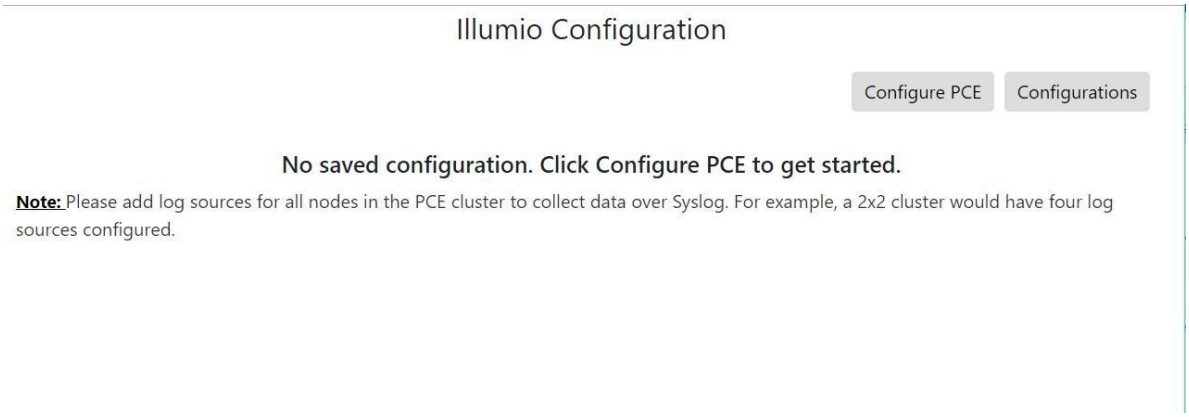
If you finished installing the app, you are already on the **Configuration** page. Skip to the second step.

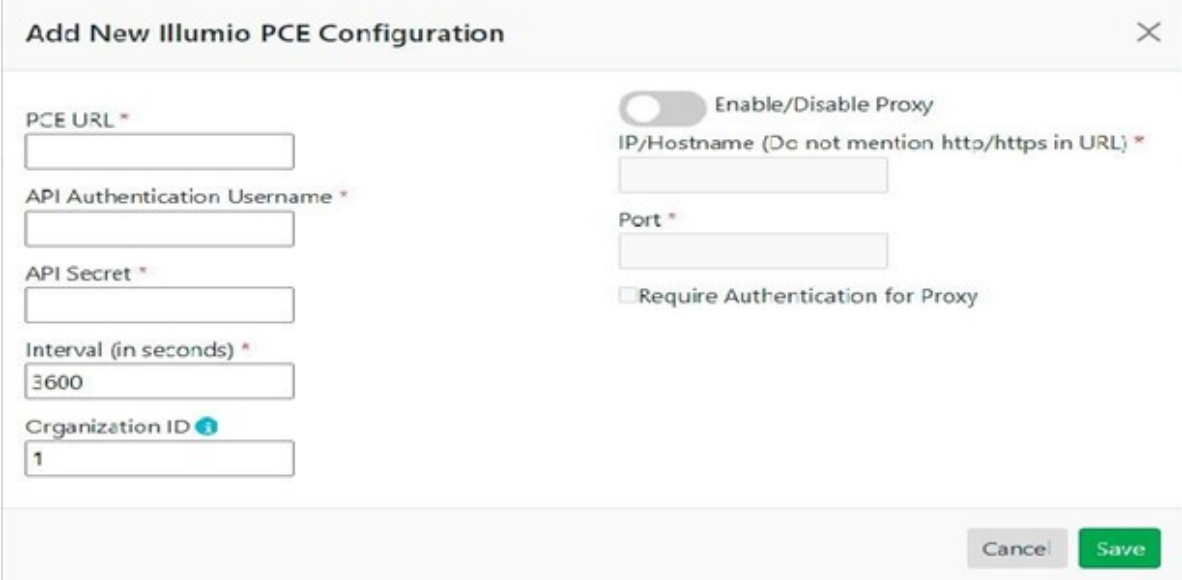
1. To get to the **Configuration** page, find the installed app on the QRadar Admin Panel under **Apps**.



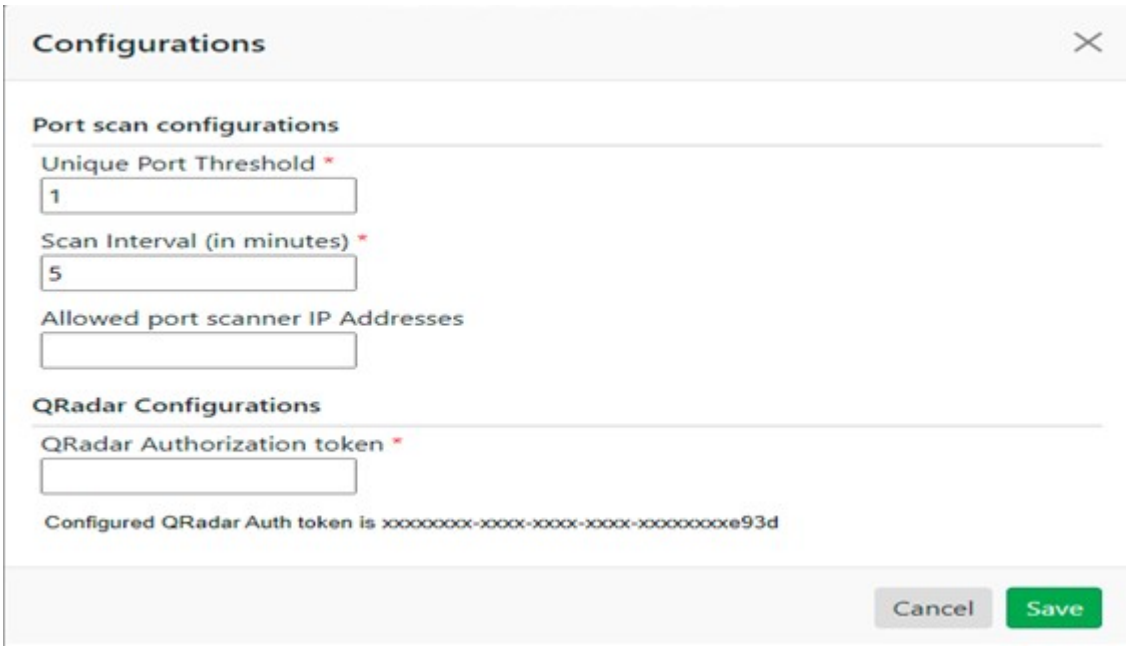
2. Open the Illumio App Configuration page, and click **Configure PCE**.

> **NOTE**
> The app supports multiple accounts for PCE configurations.





3. In the following screen, the **Authorized Service Token** is a value obtained from the QRadar App Authorization Manager.



4. Configure the PCE URL and your Illumio credentials, and your data collection will start. If Illumio PCE contains self-signed or internal CA certificates, make sure that the certificates are present in QRadar. If they are not, see Add Illumio PCE SSL Certificates in QRadar [47].

NOTE
Saved credentials are listed and you can set a proxy to fetch data from Illumio PCE configurations.

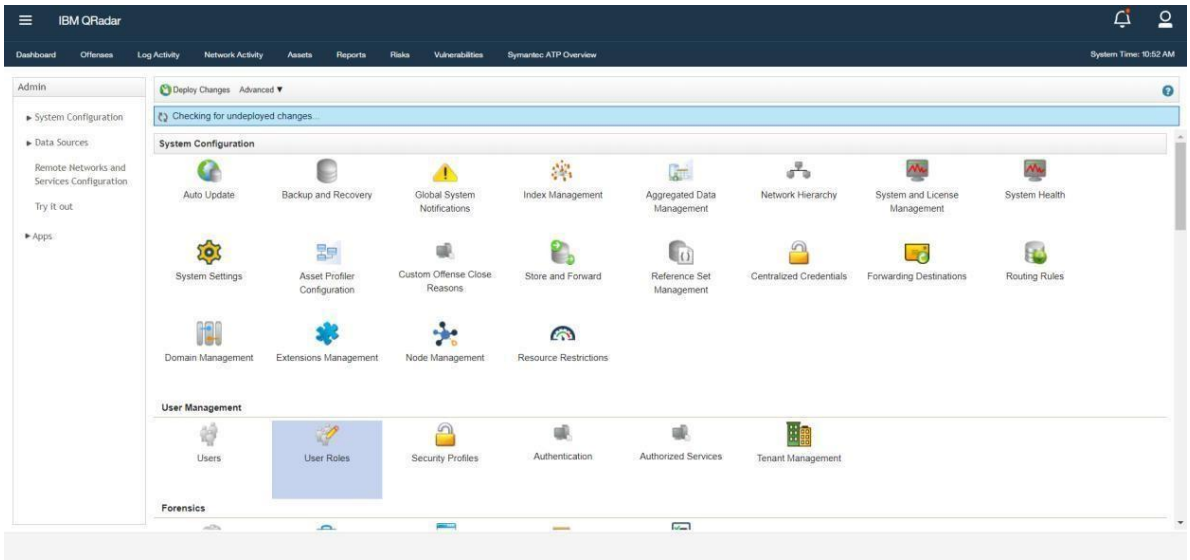
Assign User Roles and Capabilities

QRadar supports access-control lists (ACL) configurations for restricting access to different actions and dashboards. The Illumio App for QRadar adds a new capability that controls

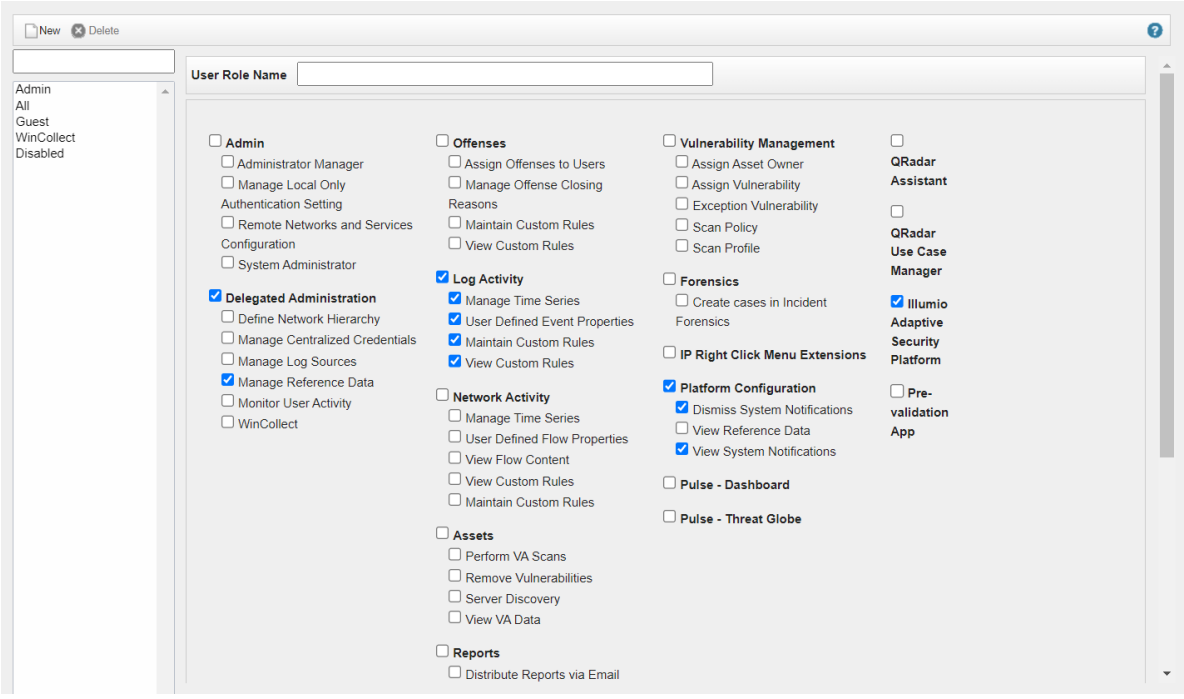
access to the Illumio dashboards. To access the Illumio dashboards, a user must be assigned a role that has this capability. By default, admin users have access to all the capabilities.

Use the following steps to add a new QRadar role with the Illumio dashboard capability:

1. Log into the QRadar console.
2. Go to **Admin** > **User Roles**.



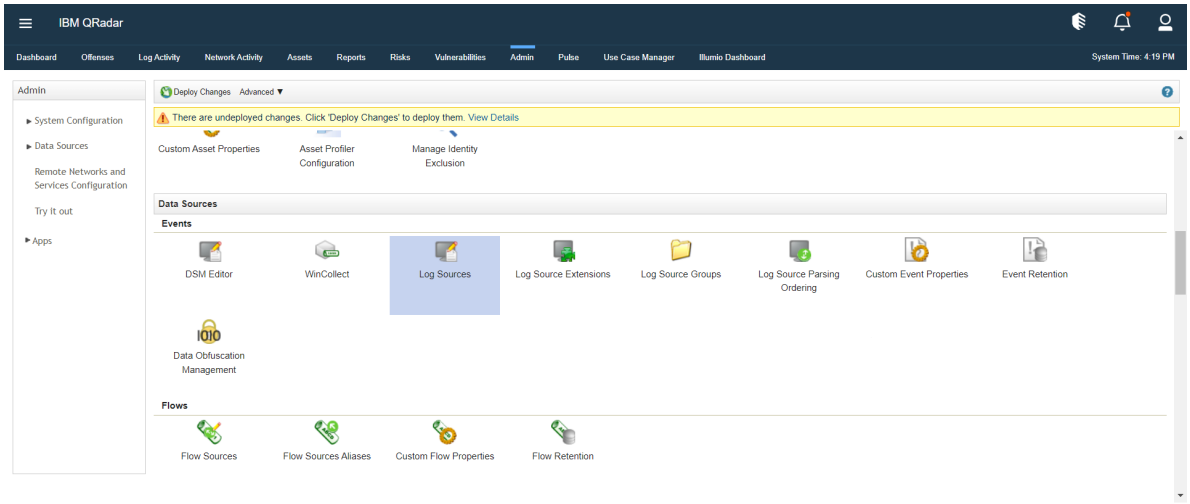
3. Click **New** and enter the name of the role.
4. Assign the **Illumio Adaptive Security Platform** capability, as shown in the following figure. This role is for users who should be allowed to view Illumio dashboards.



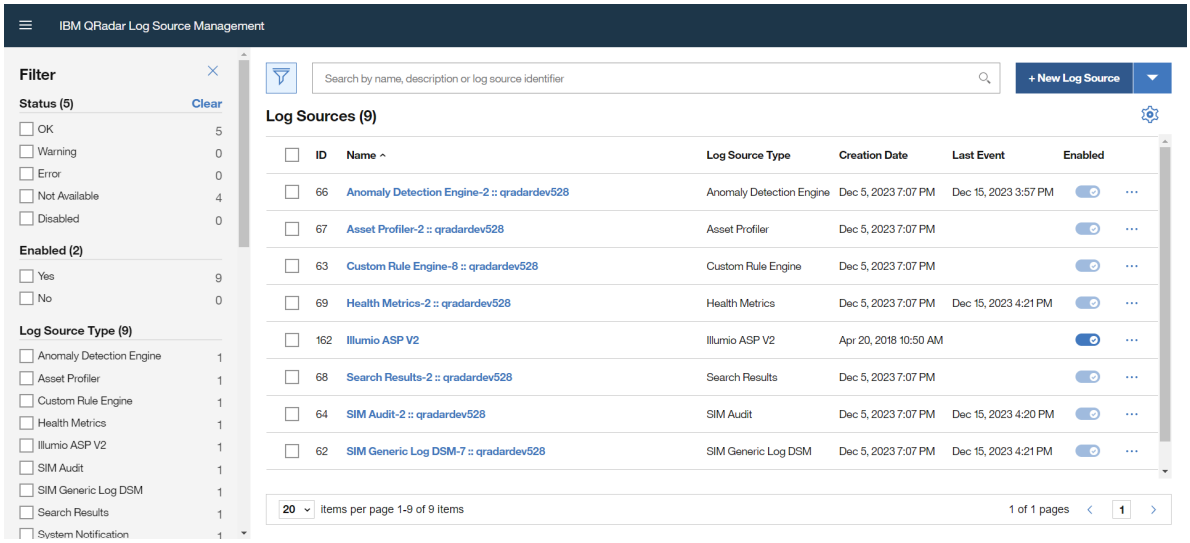
Add the PCE as a Log Source in QRadar

To enable QRadar to receive events from the Illumio App, you must add the Illumio PCE to QRadar as a log source. You need to add a separate log source to collect data from each PCE.

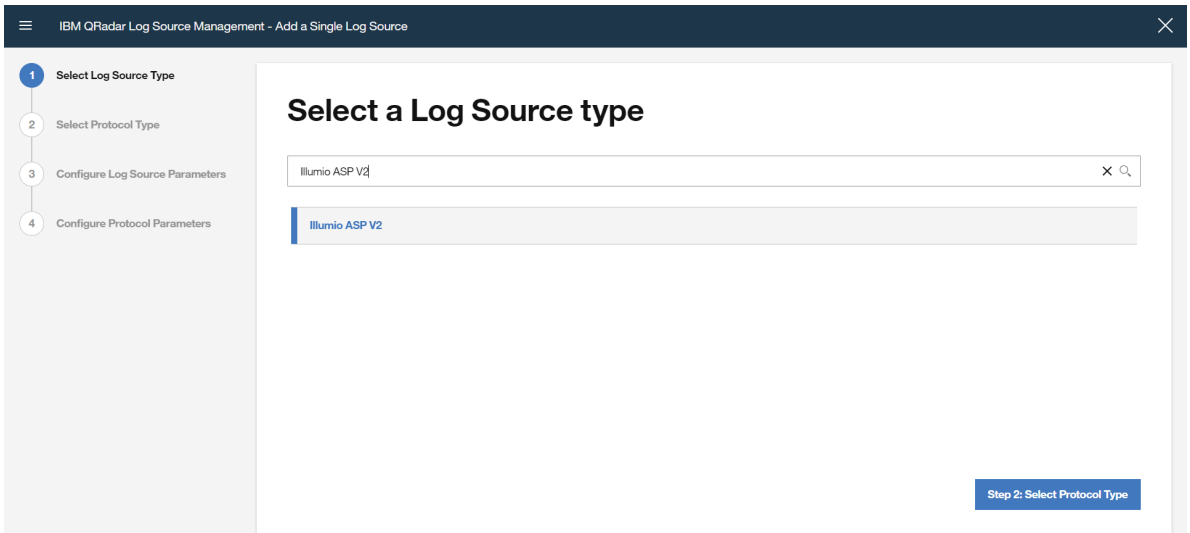
1. On the **Admin** tab in QRadar, select **Log Sources**, and click **Launch**.



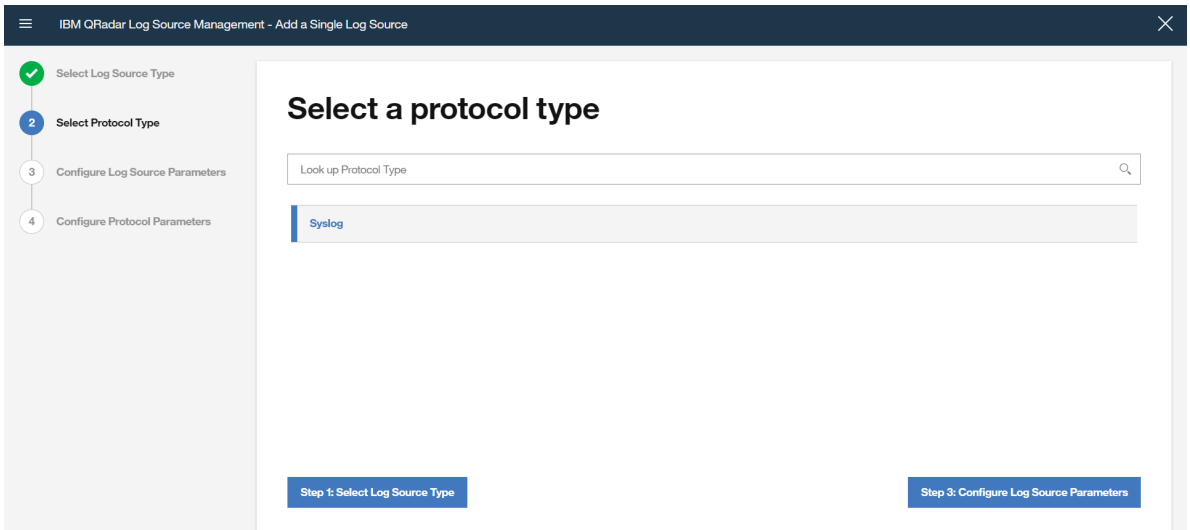
2. Select the **Log Sources** option, click **New Log Source** in the top-right corner, and select the Single Log source option.



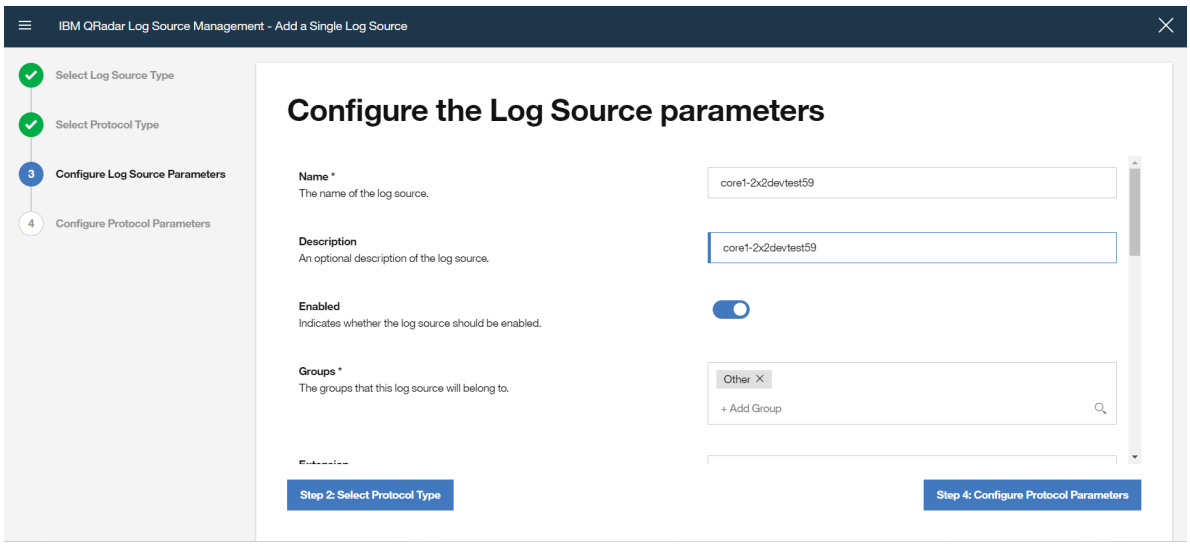
3. Select the Illumio ASP v2 option and click Step 2: Select Protocol Type in the left pane.



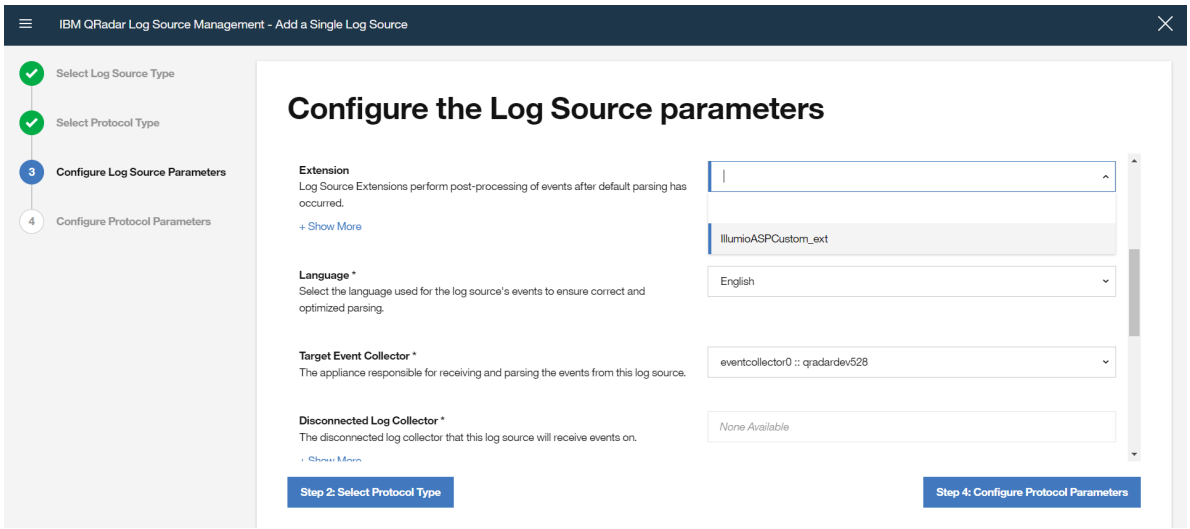
4. Select the Syslog option and click Step 3: Configure Log Source Parameters in the left pane.



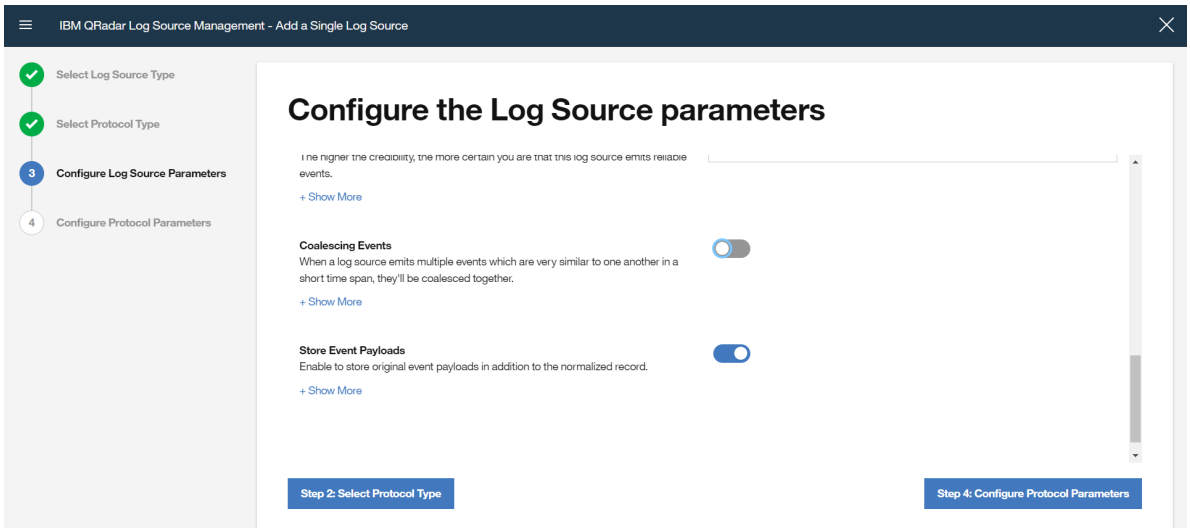
5. Give the log source a suitable name for the PCE node, add a description if you want, and make sure to select **Enabled**.



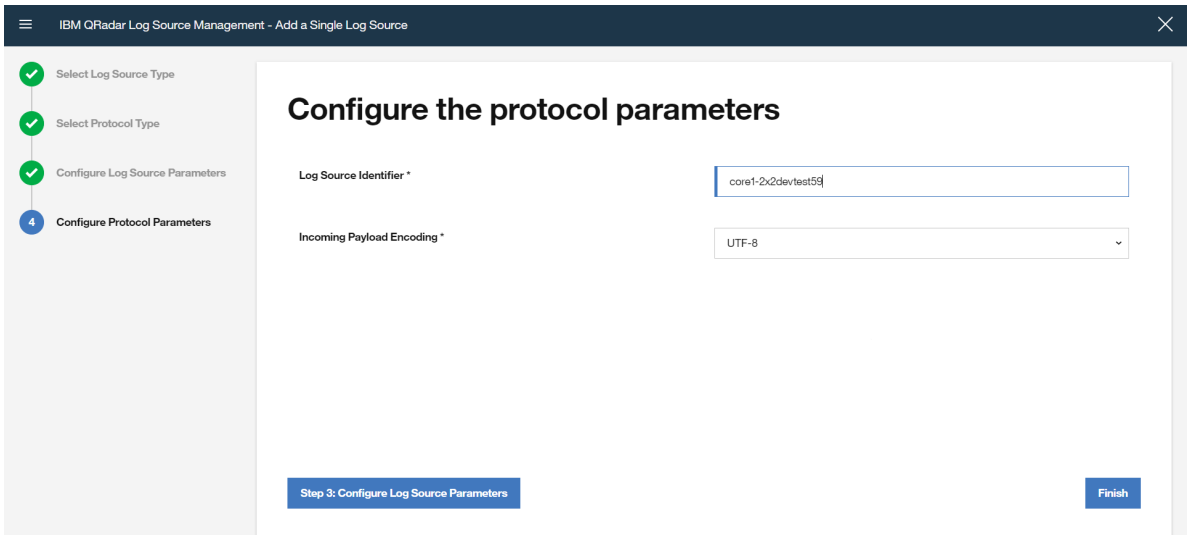
6. For the **Extension** field, choose IllumioASPCustom_ext.



7. Turn off the **Coalescing Events** configuration and then click Step 4: Configure Protocol Parameters in the left pane.



8. In **Log Source Identifier**, enter the log source identifier as set in the syslog header on the host. This is typically the hostname (such as core1-2x2devtest59).
9. Keep the **Incoming Payload Encoding** field as the default value (UTF-8).



10 Click **Finish**.

.

11. Go back to the QRadar console, and in the Admin tab, click **Deploy Changes**.
12. Repeat these steps for all other core and database nodes in the cluster (such as core1, db1, db0).

Collect Data from the Amazon S3 Bucket

A log source with the "Illumio ASP V2" log source type is required to collect data from the Amazon S3 bucket.

If a log source with "Illumio ASP V2" is not available, create it by following the steps listed in Add the PCE as a Log Source in QRadar [42].

You can provide any valid log source identifier for the "Illumio ASP V2" log source type if you are using it only to collect data from the Amazon S3 bucket.

You can use the following ways to enable QRadar to receive events from the Amazon S3 buckets:

- With an SQS queue
- With a directory prefix

Collect Data from the Amazon S3 Bucket with an SQS Queue

Use the following steps to create a log source for collecting Illumio events from Amazon S3.

1. On the **Admin** tab in QRadar, select **Log Sources** > **Add**, and enter the following values:
   a. For Log Source type, select Amazon AWS CloudTrail.
   b. For Protocol type, select Amazon AWS S3 REST API.
   c. Add a name.
   d. Add a description.
   e. Set Enabled to True.
   f. Set Coalescing Events to False.
   g. Set Store Event Payloads to True.
   h. For Log Source Identifier, enter the same value as you did for the name, to avoid confusion.
2. Continue adding the following values:
   a. For Authentication Method, select Access Key ID/Secret Key.
   b. For Access Key ID, select AWS S3 bucket access key ID.
   c. For Secret Key, select AWS S3 bucket Secret Key.
   d. For S3 Collection Method, select SQS Event Notifications.
   e. For SQS Queue URL, enter the URL of the created SQS Queue.
   f. For Region Name, enter the AWS Region of the SQS Queue resource.
   g. For Bucket Name, enter the S3 bucket name.
   h. For Event Format, select LINEBYLINE.
   i. For User as a Gateway Log Source, select True.

3. For Log Source Identifier Pattern, enter (=.*) after the Illumio log source identifier, such as {ILLUMIO_LOG_SOURCE_IDENTIFIER}=.* You can find the log source identifier value from the “Illumio ASP v2” log source. For example, if Illumio’s log source identifier is `core0-2x2devtest59`, then enter `core0-2x2devtest59=. *` in this field.

> **NOTE**
> The Gateway log source collects events from the Amazon S3 bucket and those events can be parsed as "Illumio ASP V2" log source type events because the Illumio ASP V2 log source type's identifier is used while configuring Gateway Log Source.

4. Set **Show Advanced Options** to True.
   a. File Pattern: .*\.gz (To consume only .gz files from the S3 bucket)
   b. File Pattern: .* (To consume all files from the S3 bucket)
5. Set **Automatically Acquire Server Certificate(s)** to Yes.
6. Set a value for Recurrence. This designates how often the Amazon AWS S3 REST API Protocol connects to the Amazon cloud API, checks for new files, and if they exist, retrieves them. Every access to an AWS S3 bucket incurs a cost to the account that owns the bucket. The time interval can include values in hours (H), minutes (M), or days (D). For example: 2H = 2 hours, 15M = 15 minutes, 30 = 30 seconds.
7. Set the value for EPS Throttle. This is the maximum number of events per second (EPS) that this log source should not exceed. (The default value is 5000.)
8. In the Admin tab, click **Deploy Changes**.

Collect Data from the Amazon S3 Bucket with a Directory Prefix

Use the following steps to create a log source for collecting Illumio events from Amazon S3.

1. On the **Admin** tab in QRadar, select **Log Sources** > **Add** and enter the following:
   a. For Log Source type, select Amazon AWS CloudTrail.
   b. For Protocol type, select Amazon AWS S3 REST API.
   c. Add a name.
   d. Add a description.
   e. Set Enabled to True.
   f. Set Coalescing Events to False.
   g. Set Store Event Payloads to True.
2. Continue entering values:
   a. For Log Source Identifier, enter the same value as you did for the name, to avoid confusion.
   b. For Authentication Method, select Access Key ID/Secret Key.
   c. For Access Key ID, select AWS S3 bucket access key ID.
   d. For Secret Key, select AWS S3 bucket Secret Key.
   e. For S3 Collection Method, use a specific prefix - Single Account/Region Only.
   f. For Bucket Name, enter the S3 bucket name.
   g. For Directory Prefix, enter the root directory location on the AWS S3 bucket from which the files are retrieved. (Directories are separated by '/'.)
   h. For Signature Version, select AWS Signature V2.
   i. For Event Format, select LINEBYLINE.
   j. For User as a Gateway Log Source, select True.
3. For Log Source Identifier Pattern, enter (=.*) after Illumio log source identifier, such as {ILLUMIO_LOG_SOURCE_IDENTIFIER}=.* You can find the log source identifier value

from the “Illumio ASP v2” log source. For example, if Illumio’s log source identifier is core0-2x2devtest59, then enter core0-2x2devtest59=. * in this field.

> **NOTE**
> The Gateway log source collects events from the Amazon S3 bucket and those events can be parsed as "Illumio ASP V2" log source type events because the Illumio ASP V2 log source type's identifier is used while configuring Gateway Log Source.

4. Set **Show Advanced Options** to **True**.
   a. File Pattern: .*\.gz (To consume only .gz files from the S3 bucket)
   b. File Pattern: .* (To consume all files from the S3 bucket)
5. Set Automatically Acquire Server Certificate(s) to Yes.
6. Set the value for Recurrence. This designates how often the Amazon AWS S3 REST API Protocol connects to the Amazon cloud API, checks for new files, and if they exist, retrieves them. Every access to an AWS S3 bucket incurs a cost to the account that owns the bucket. The time interval can include values in hours (H), minutes (M), or days (D). For example: 2H = 2 hours, 15M = 15 minutes, 30 = 30 seconds.
7. Set a the value for EPS Throttle. This designates the maximum number of events per second (EPS) that this log source should not exceed. (The default value is 5000.)
8. In the **Admin** tab, click **Deploy Changes**.

Add S3 Bucket Certificates

After you create a log source, make sure that the SSL certificates of the S3 buckets are present in QRadar. If the certificates are not present, the data from the S3 bucket will not be collected.

Use the following procedure to add certificates to the S3 bucket:

1. Log into QRadar using a secure connection.
2. Run the following command:

```
/opt/qradar/bin/getcert.sh <bucket name>.s3.amazonaws.com
```

Add Illumio PCE SSL Certificates in QRadar

The Illumio app collects labels with SSL verification. If PCE contains self-signed or internal CA certificates, then you need to perform the following steps to add certificates in QRadar.

1. Log into your QRadar console.
2. Go to the Admin panel and open the **Configuration** page.
3. From the configuration window of the Illumio app, copy the app id from the URL. The app id is the number after /console/plugins/. For example, if the URL is `https://1.1.1.1/console/plugins/1062/app_proxy/index`, you would copy **1062**.
4. Perform the `docker ps` command on your QRadar instance using SSH.
5. Find the Container id of the Illumio App. (The container id for the Illumio app is an image column containing a previously copied number, such as ...qapp-1062...)

6. Perform the `docker exec -it <container-id> /bin/bash` command (to go inside Docker).
7. Perform the following steps inside the Docker container of the Illumio v1.4.0 app:
   a. Copy or move the certificate file of the Illumio app from `root` to `/etc/pki/ca-trust/source/anchors`.
   b. Run the commands listed in Using certificates that are signed by an internal certificate authority.

      ```
      /opt/qradar/support/all_servers.sh -p /etc/pki/ca-trust/source/anchors/<root_certificate> -r /etc/pki/ca-trust-source/anchors
      /opt/qradar/support/all_servers.sh -C update-ca-trust
      ```
   c. Restart the Docker container of the app.

NOTE

When you reinstall the app or the Docker container of the Illumio App gets restarted, these changes may be reverted. If that occurs, you need to perform these steps again.

Upgrade the Application to v1.4.0

Perform the following steps to upgrade the application:

1. Remove all saved searches and custom properties associated with the “Illumio ASP V2” log source type.
2. Go to **Admin** > **Extension Management** and click **Add** to select the downloaded zip file.
3. Within the QRadar prompt, click **Install**. After the application is installed, it will create a Docker container in the backend.
4. Within the Admin Panel, select **Deploy Full Configuration**.
5. Clear the browser cache and refresh the page.

NOTE

The PCE filter functionality on the dashboard has been removed in Illumio App for QRadar v1.2.0. You need to manually delete the “pce_nodes” reference table or it will remain in QRadar after the app is upgraded.

QRadar Cloud Support

Illumio App for QRadar 1.4.0 supports all functionalities on the QRadar cloud.

If the PCE is installed on a port other than 443, contact IBM to open that port.

Check the Application Logs

View the application logs by accessing the application from QRadar using a remote connection.

1. Log into QRadar using a remote connection.
2. List all installed applications and their App-ID values using this command: `/opt/qradar/support/recon ps`.
3. If no issues are detected, the recon command output might look like this example:

```
App-ID  Name                                Managed Host ID Workload ID                          Service Name          Container Name        Port
                                            0               Failed to decode workloads      -
2701    IBM QRadar Pre-Validation App Service 53            apps                                 qapp-2701       -                             0
2702    IBM QRadar Pre-Validation App UI    53              apps                                 qapp-2702       -                             0
1051    QRadar Log Source Management        53              apps                                 qapp-1051       -                             0
4352    Illumio Adaptive Security Platform  53              apps                                 qapp-4352       -                             0
1055    QRadar Use Case Manager             53              apps                                 qapp-1055       -                             0
```

4. Connect to the app container using the following command: `/opt/qradar/support/recon connect APP-ID`.

> **NOTE**
> For the preceding image, the Illumio App-ID is 4352.

5. Use the following command to go to the log directory: `cd /opt/app-root/store/log`.
6. In the log directory, use the *'ls'* command to list all files and the *'cat'* command to print log file content:

```
ls
cat app.log
```

The app.log file contains all of the logs related to the configuration page and dashboard and the label_data_collect.log file contains logs related to label collection from the Illumio PCE.

Uninstall the App

To uninstall the application:

1. In QRadar, go to the **Admin** page and open **Extension Management**.
2. Select Illumio App for QRadar, and click **Uninstall**.

Troubleshooting QRadar

This section describes common issues that might occur when you are deploying or running the app and steps to resolve these issues. If the issue that you encounter is not described here, see General Troubleshooting [58] for instructions about how to collect information about your issue and provide supporting documentation to Illumio Support.

Events Displayed As Custom Message

Problem: Illumio events are named IllumioASPCustom Message rather than being identified with the correct QRadar category. This is seen in the Log Activity tab in QRadar when you are searching for events related to created log sources.

	Event Name	Log Source
	IllumioASPCustom Message	db1-2x2devtest59
	IllumioASPCustom Message	db1-2x2devtest59
	IllumioASPCustom Message	db1-2x2devtest59
	IllumioASPCustom Message	db1-2x2devtest59
	IllumioASPCustom Message	db1-2x2devtest59
	IllumioASPCustom Message	db1-2x2devtest59

Cause: This issue can be caused by improper Event ID and Event Category extractions. If any new type of event appears in the Log Source and its Event ID or Event Category extractions are not written, the value of that property will be empty.

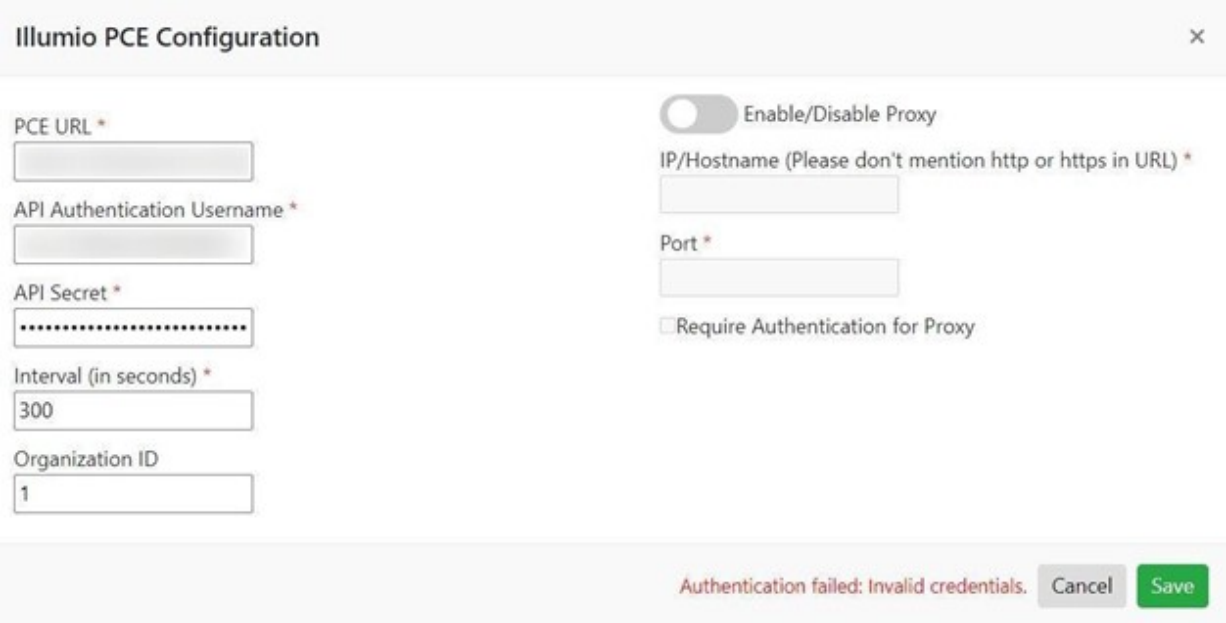
1. Go to **Log Activity**.
2. In **Filter Log Source Type**, choose Illumio ASP V2.
3. In the View filter, select **Last 7 Days**.
4. Right-click on the event that has the IllumioASPCustom Message and select **View** in DSM Editor.
5. Check the value of Event ID and Event Category under **Log Activity Preview**.
6. If Event ID and Event Category are unknown, create a support ticket with Illumio Support.

Troubleshooting Configuration Failure Errors

The following topics describe configuration errors and workarounds (if applicable).

Authentication

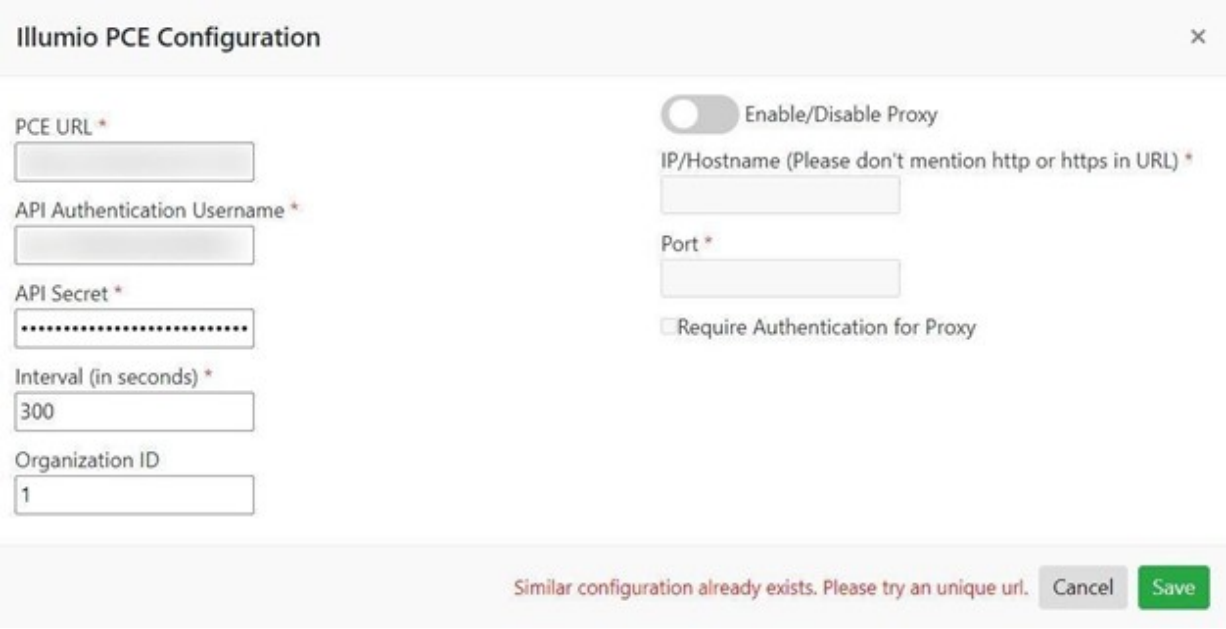
A new configuration fails with the "Authentication failed. Invalid credentials." error message.



You have entered incorrect credentials, so authentication failed while saving the new configuration. Check the credentials and try again.

Configuration Exists

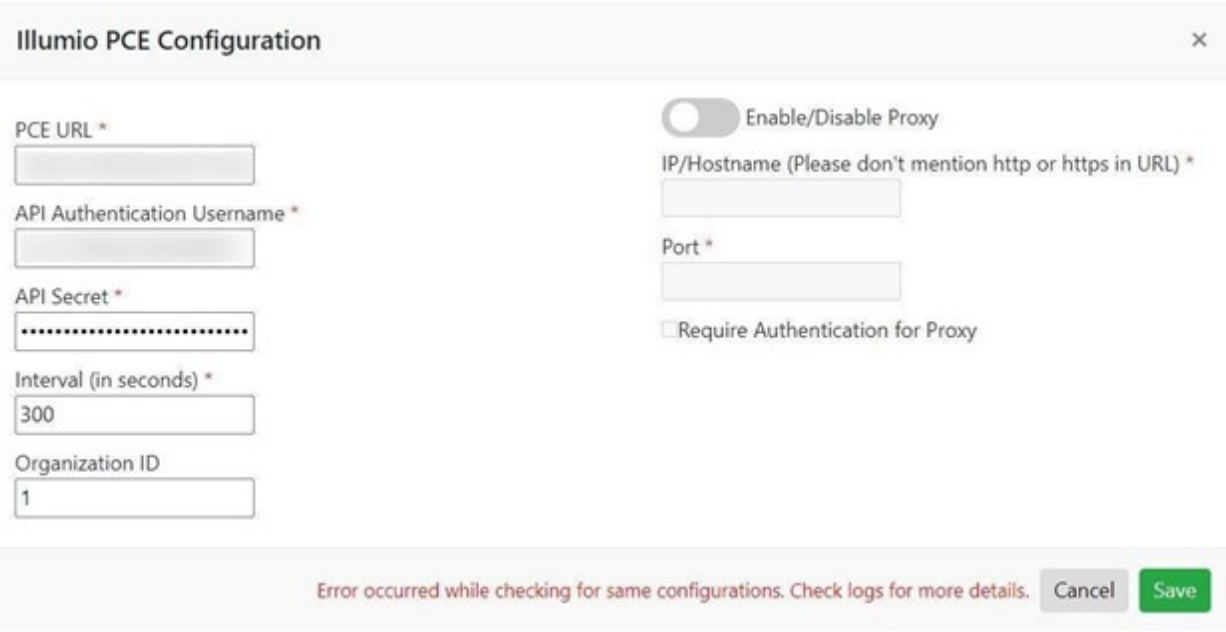
A new configuration fails with the "Same configuration already exists. Please try a unique url" error message.



You might have entered an account that is already configured. Enter new credentials that have not already been provided.

Error Checking Configurations

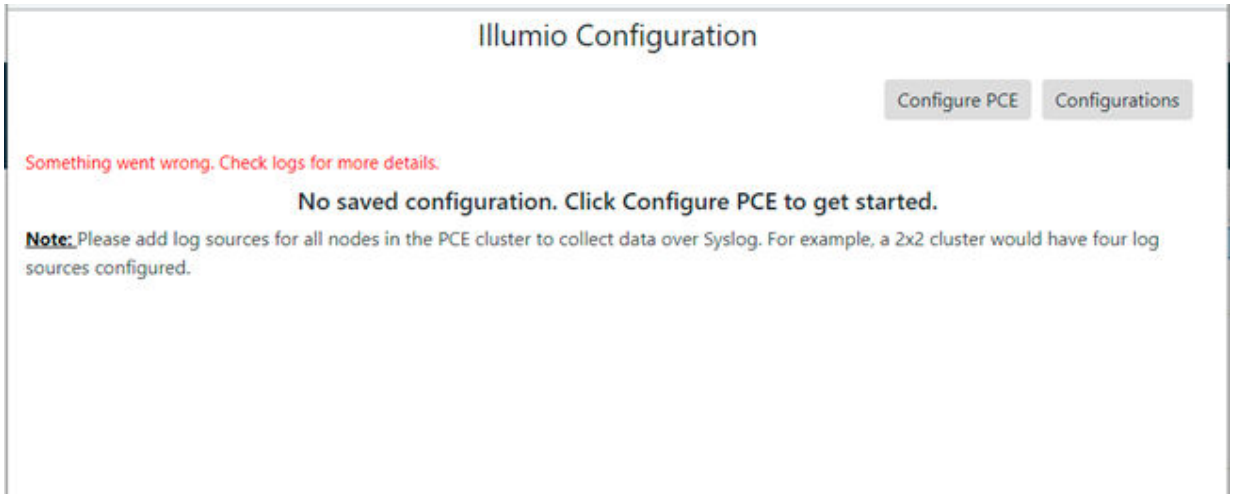
Configuring Illumio fails with the "Error occurred while checking for same configurations. Check logs for more details." error message.



This happens while the app is checking for similar configurations. Try the configuration again and check the app.log file for more information. See Check the Application Logs [49].

Error Message on Illumio Configuration Page

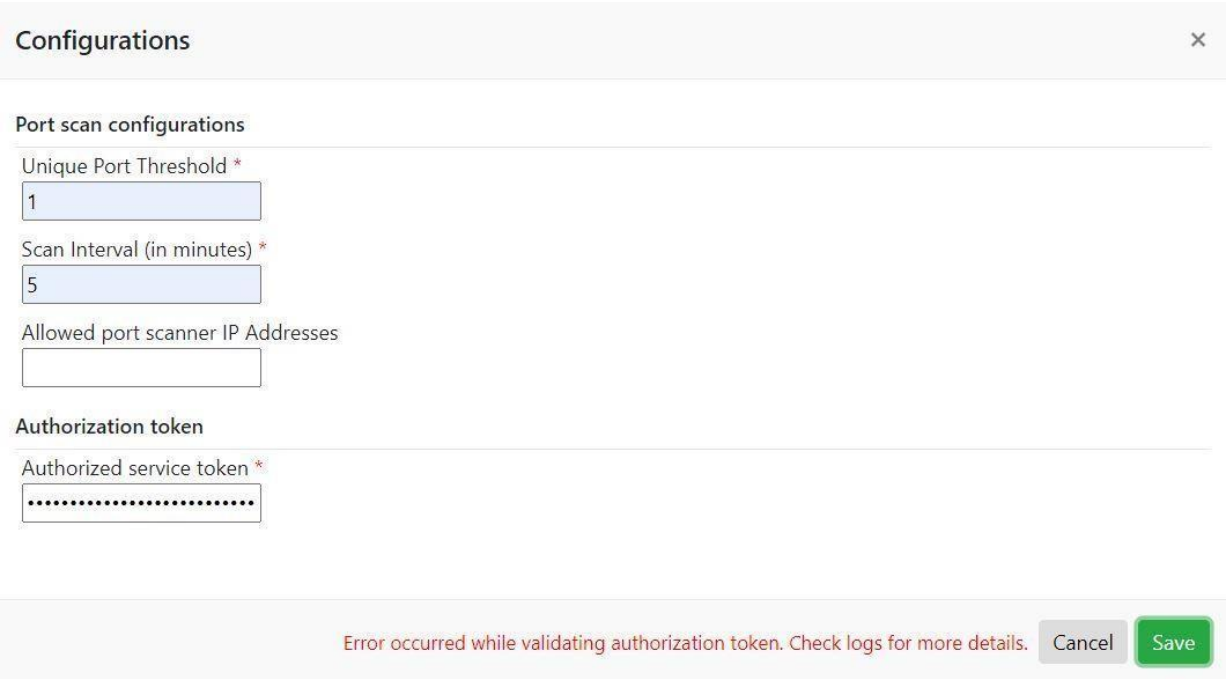
The "Something went wrong. Check logs for more details." error message displays on the configuration page.



The app is not able to reach the PCE using the credentials stored in files. There can be multiple reasons for this issue. One possible cause is that the secret data files have been tampered with. Check the `app.log` file for more details. See Check the Application Logs [49].

Error Validating Authorization Token

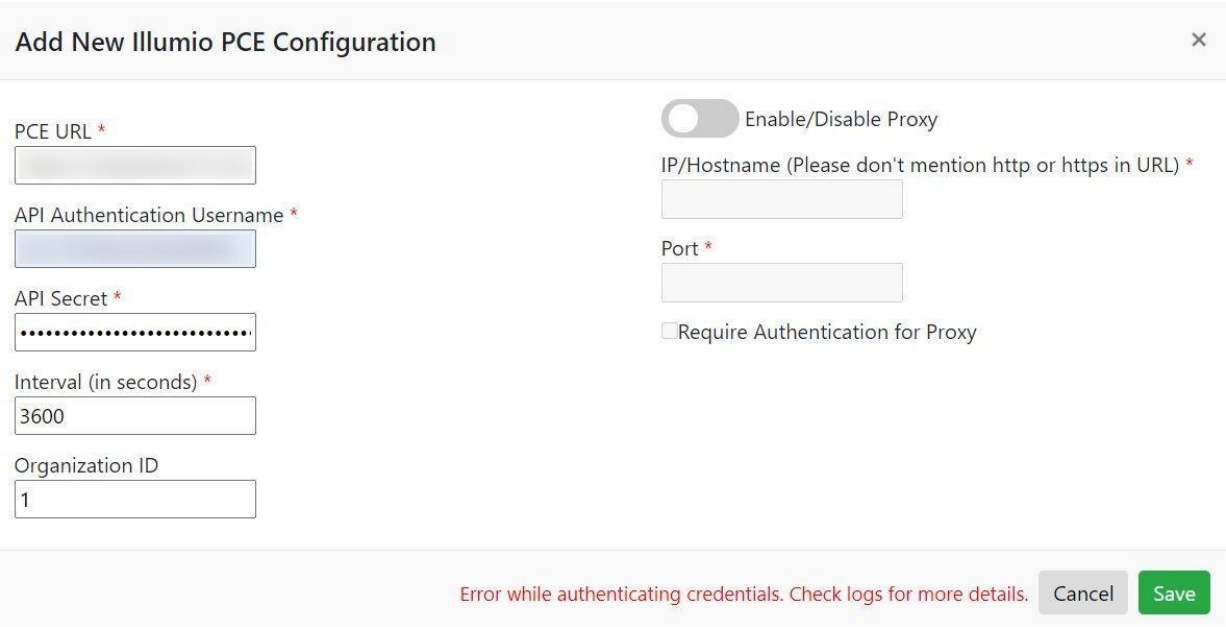
Configuring the Illumio apps fails with the "Error occurred while validating authorization token." error message.



This happens while the app is checking the Authorized Service Token. Try again, and check the `app.log` file for more information. To check logs, see Check the Application Logs [49].

Error While Authenticating Credentials

The new Illumio App configuration fails with the "Error while authenticating credentials. Check logs for more details." error message.



The app is not able to reach the PCE using the provided PCE URL or proxy credentials. There can be multiple reasons for this issue. Check the `app.log` file for more information. To check logs, see Check the Application Logs [49].

Error While Initiating Socket Connection with QRadar

The "Error while initiating socket connection with IBM QRadar. Error = [Errno 111] Connection refused" log message appears in the log files.

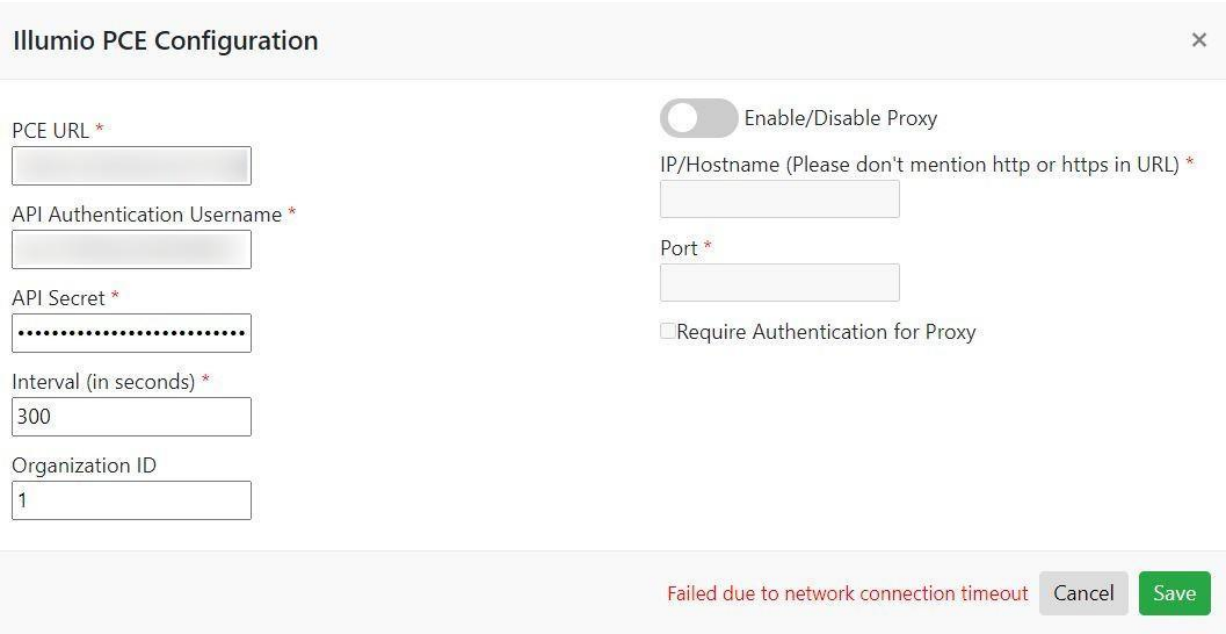
While using QRadar v7.5.0 UP4 with an encrypted app host, events are not forwarded to QRadar through the TCP socket channel.

Use the following steps to disable the app host encrypted connection:

1. Click **System and License Management** in the Admin Panel.
2. Select the host on which the Illumio App for QRadar v7.4.3 GA+ is installed.
3. Click **Deployment Actions** in the top panel and select the **Edit Host** option.
4. In the **Edit Managed Host** window, make sure that the **Encrypt Host Connections** field is not checked.
5. In the **Admin** tab, click **Deploy Changes**.

Network Connection Timeout

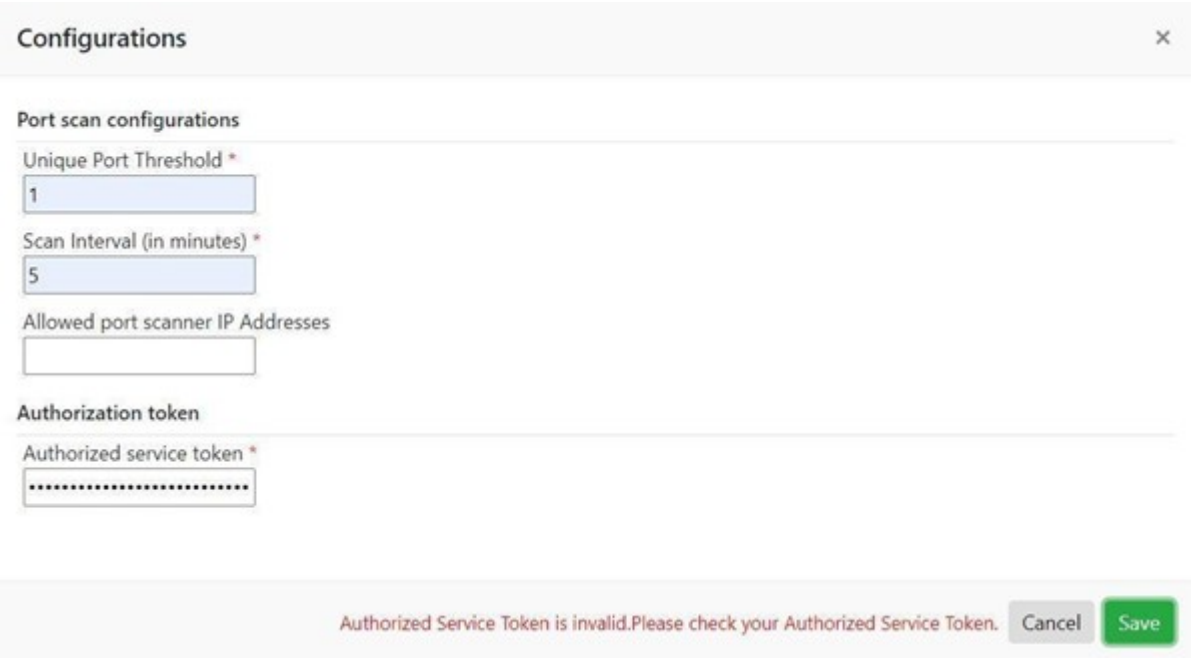
Configuring the Illumio App fails with the "Failed due to network connection timeout." error message.



The app is not able to connect to the server. There may be network issues. If you have a proxy in your network, try to save the credentials with the proxy. For more information about the error, check the `app.log` file. See Check the Application Logs [49].

Service Token Invalid

The new Illumio App configuration fails with the "Authorized Service Token is invalid. Please check your Authorized Service Token." error message.



You have entered an incorrect Authorized Service Token. Check the token and try again.

Events Unknown

Problem: Illumio App events are shown as unknown in QRadar.

Use the following steps to troubleshoot:

1. Go to **Log Activity** and set Filter Log Source Type to Illumio ASP V2.
2. In **Views**, select Last 7 Days.
3. If any events show as unknown, do the following:
   a. Right-click on the event and select **View** in DSM Editor.
   b. Under **Log Activity Preview**, check the value of **Event ID** and **Event Category**.
   c. If **Event ID** and **Event Category** are unknown, create a support ticket with Illumio.
   d. If the **Event ID** and **Event Category** values are not unknown but **Event Name** is unknown, then add a new event mapping using the following steps:
      i. Navigate to the **Event Mapping** tab and click **Add**.
      ii. Click **Choose QID**.
      iii. Click **Create New QID Record** and enter an appropriate name in the **Name** field.
      iv. Select relevant values for the **High Level Category** and **Low Level Category** fields.
      v. Click **Save** and then click OK.
      vi. Click **Create**.

Data Not Added to Reference Table

Problem: Data is not being added into the reference table even though the PCE and port connections were saved successfully.

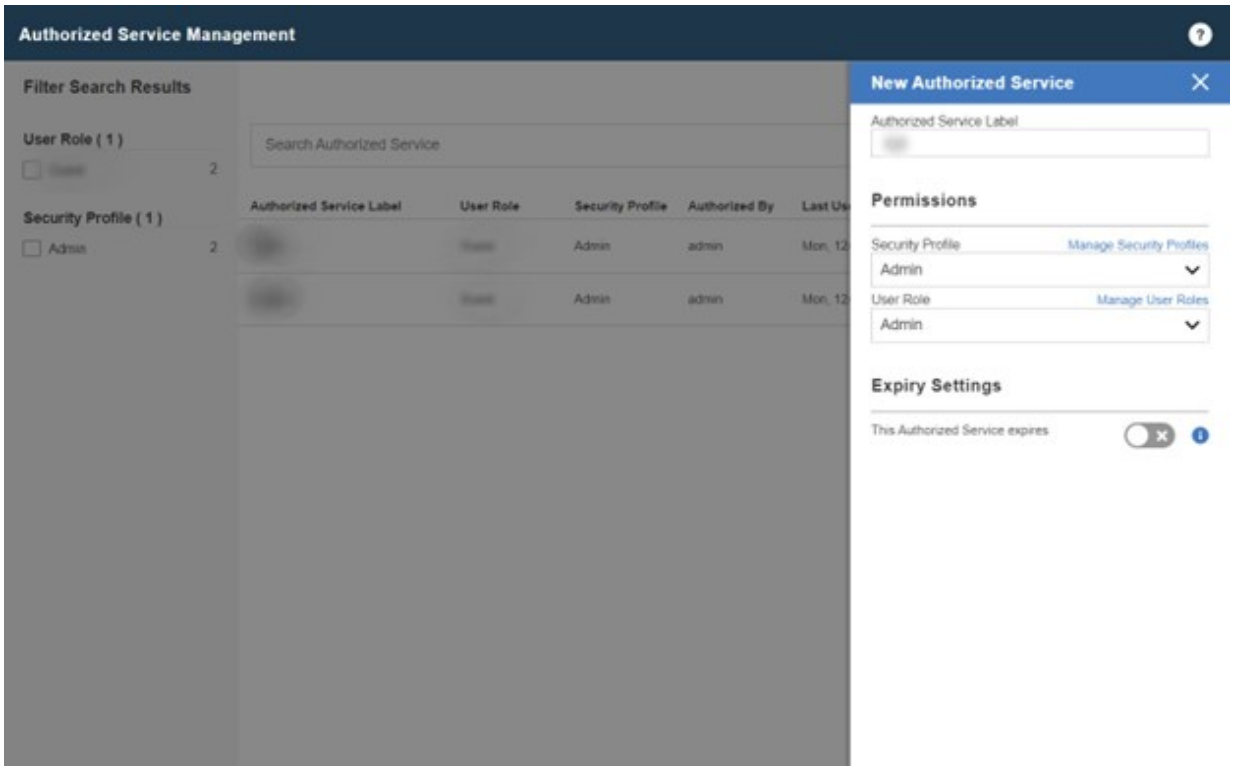
The problem may be that the configured QRadar Authorization Token has read-only access.

1. Perform the `docker ps` command on your QRadar instance using SSH.
2. Find the Container ID of of the Illumio App. The Container ID for the Illumio App will be an image column that contains a previously copied number, such as qapp-1062.
3. Perform the `docker exec -it <container-id> /bin/bash` command to go inside the Docker container.
4. Inside the Docker container of the Illumio App v1.4.0, do the following:
   a. Change the working directory: `cd/opt/app-root/store/log`.
   b. View data collection logs: `tail -f label_data_collect.log`.
   c. Verify log messages with the following screenshot.

```
2023-12-18 12:07:08,016 - [LABELDATACOLLECTION] - INFO - b'Starting label data collection.'
2023-12-18 12:07:08,017 - [LABELDATACOLLECTION] - INFO - b'Port Scan config file and PCE config file found. Starting data collection.'
2023-12-18 12:07:08,195 - [LABELDATACOLLECTION] - INFO - b'[check_reference_table] Checking Reference Table.....'
2023-12-18 12:07:08,315 - [LABELDATACOLLECTION] - ERROR - b'[check_reference_table] Response received with status code: 404 Response: {"http_respo
nse":{"code":404,"message":"We could not find the resource you requested."},"code":1002,"description":"The reference table does not exist","detail
s":{},"message":"labels does not exist"}'
2023-12-18 12:07:08,316 - [LABELDATACOLLECTION] - ERROR - b'[check_reference_table] Reference table does not exist.'
2023-12-18 12:07:08,316 - [LABELDATACOLLECTION] - INFO - b'[create_reference_table] Creating Reference Table.....'
2023-12-18 12:07:08,350 - [LABELDATACOLLECTION] - ERROR - b'[create_reference_table] Error while creating reference table. Response: {"http_respon
se":{"code":403,"message":"Your account is not authorized to access the requested resource"},"code":26,"description":"","details":{},"message":"Us
er has insufficient capabilities to access this endpoint resource"} Status code: 403'
2023-12-18 12:07:08,351 - [LABELDATACOLLECTION] - ERROR - b'[create_reference_table] API call failed. HTTP error. Error = 403 Client Error: 403 fo
r url: https://qradar210.cdsys.local//api/reference_data/tables?element_type=ALN&name=labels&outer_key_label=href&key_name_types=%5B%7B%27element_
type%27%3A%27ALN%27%2C+%27key_name%27%3A%27href%27%7D%2C%7B%27element_type%27%3A%27ALN%27%2C%27key_name%27%3A%27key%27%7D%2C%7B%27element_type%27%
3A%27ALN%27%2C%27key_name%27%3A%27value%27%7D%2C%7B%27element_type%27%3A%27DATE%27%2C%27key_name%27%3A%27created_at%27%7D%2C%7B%27element_type%27%
3A%27DATE%27%2C%27key_name%27%3A%27updated_at%27%7D%2C%7B%27element_type%27%3A%27ALN%27%2C%27key_name%27%3A%27updated_by%27%7D%2C%7B%27element_typ
e%27%3A%27ALN%27%2C%27key_name%27%3A%27created_by%27%7D%5D'
2023-12-18 12:07:08,351 - [LABELDATACOLLECTION] - ERROR - b'[create_reference_table] Create Reference table API for labels failed.'
2023-12-18 12:07:08,351 - [LABELDATACOLLECTION] - ERROR - b'Reference table labels is not present. Retry after 60 seconds'
```

This happens when the configured QRadar Authorization Token doesn't have create/edit access to the Reference Table.

Make sure that the created QRadar authorization token has sufficient access. See Assign User Roles and Capabilities [40].



Data Not Collected

Problem: Data is not being collected by the app.

Follow the steps in General Troubleshooting [58].

UI Issues

A dashboard panel, configuration page, or chart shows errors or displays unintended behavior.

1. Clear the browser and reload the page.
2. Try reducing the time range of the filter and retry. QRadar queries can expire if too much data is matched in the query.

Reinstall the Application

If you encounter any errors, reinstall the application.

1. Remove all saved searches and custom properties associated with the Illumio ASP V2 log source type.
2. Navigate to **Admin Panel** > **Log Sources** and delete the log source associated with the Illumio ASP V2 log source type.
3. Uninstall the app.
   See Uninstall the App [49].

4. Refresh the page and make sure that you cannot see the **Illumio Overview Dashboard** tab after you have uninstalled the app.
5. Reinstall the app from Extension Management.
   See Install QRadar [37].

General Troubleshooting

If you encounter a problem that is not described in this document, follow these steps to troubleshoot your issue.

1. Click **System and License Management** in the Admin Panel.
2. Select the host on which the Illumio application is installed.
3. On the top panel, click **Actions**, and select **Collect Log Files**.
4. On the **Log File Collection** window, click **Advanced Options** and check the following check boxes:
   - Include Debug Logs
   - Application Extension Logs
   - Setup Logs (Current Version)
5. For data input, select 2 Days.
6. Click **Collect Log Files**.
7. Click the **Click here to download files** link.
   This downloads all the logs in a single zip file on your local machine.
8. Create a support case with Illumio Support and attach the zipped log files.