



Illumio App for QRadar

App Specification Guide

 2, Garden View Corporate House, Opp. Bodakdev Auda Garden, Bodakdev, Ahmedabad 38005

 +91 (79) 4004-4200  www.crestdatasys.com

Table of Contents

INTRODUCTION	3
DEPLOYMENT ARCHITECTURE.....	3
APP ARCHITECTURE.....	4
DATA COLLECTION	4
LOG SOURCES	5
<i>Add PCE as a Log Source.....</i>	<i>5</i>
LOG SOURCE TYPES	8
<i>Custom Property Extraction</i>	<i>8</i>
<i>Event Mappings.....</i>	<i>10</i>
VISUALIZATIONS	17
<i>Security Operations Dashboard.....</i>	<i>17</i>
<i>Investigation Dashboard.....</i>	<i>18</i>
APP INSTALLATION & CONFIGURATION.....	19
PREREQUISITES	19
INSTALLATION.....	19
APP CONFIGURATION	20
UNINSTALLING THE APPLICATION.....	25
QRADAR CLOUD SUPPORT	25
TROUBLESHOOTING.....	25
CASE #1 – EVENTS ARE SHOWN UP AS “CUSTOM MESSAGE”	25
CASE #2 – APP CONFIGURATION FAILS WITH VARIOUS ERROR MESSAGES	26
CASE #3 – EVENTS ARE COMING AS UNKNOWN.....	29
CASE #4 – DATA IS NOT GETTING COLLECTED IN THE APP	29
CASE #5 – UI RELATED ISSUES IN THE APP.....	30
CASE #6 – RE INSTALLATION OF APP	30
CASE #7 – LABELS FILTER SHOWING DUPLICATE VALUES.....	30
CASE #7 – ALL OTHER ISSUES WHICH ARE NOT PART OF THE DOCUMENT	31

Introduction

This document is intended to provide overall App Specification for the Illumio App built for QRadar. It contains details of overall App specification and uses cases which will be executed as part of this integration.

Deployment Architecture

IBM QRadar 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 (Security Information and Event Management) is a modular **architecture** that provides real-time visibility of your IT infrastructure, which you can use for threat detection and prioritization.

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

Below is the topology of data collection from Illumio PCE to QRadar.

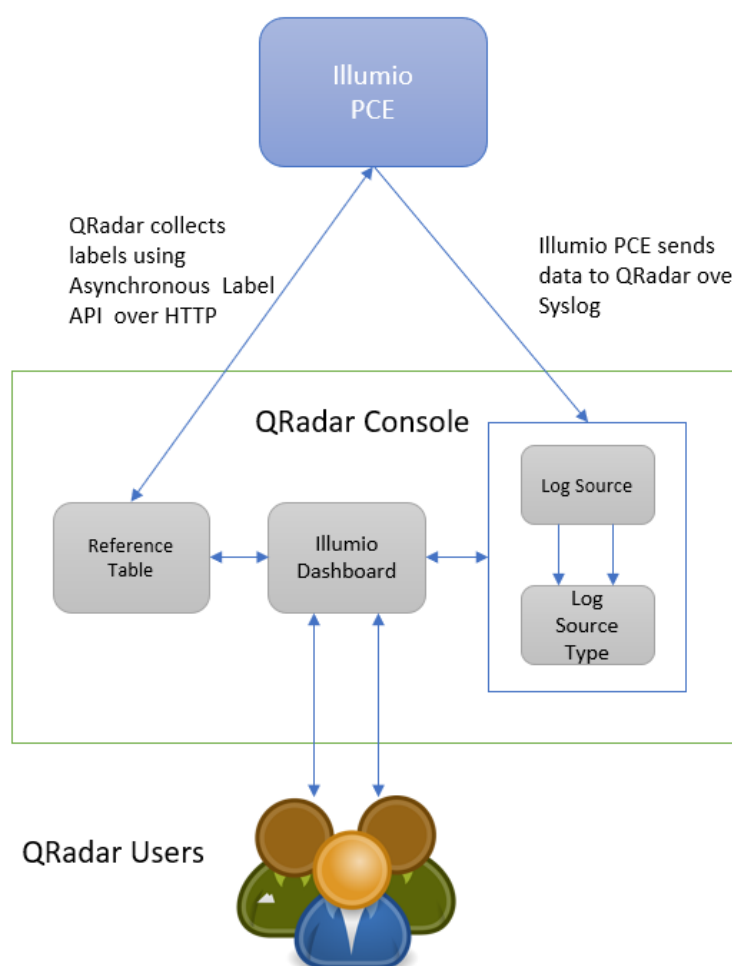


Figure 1: Illumio integration with IBM QRadar

The Illumio App for QRadar provides couple of visibility dashboards. With east-west traffic visibility, staff can pinpoint potential attacks and identify compromised workloads with Security Operations dashboard. Using the PCE Operations dashboard, admins get a single-pane-of-glass to monitor the health of all deployed and managed PCEs.

The Illumio App for QRadar is supported with PCE version 18.2.

App Architecture

Data Collection

The app has 2 sources of receiving data: API and Syslog Port. From API, we fetch labels and store that data in reference table. Then that data is used to populate labels in autocomplete labels filter on Security Operations dashboard. The app uses Asynchronous Label REST API calls to onboard data from Illumio PCE server. The application contains python scripts, which makes REST calls to mentioned APIs. These scripts are run on user-defined schedule.

QRadar parses received data using suitable Log source. The log source is made up of two components:

- **APIs**

APIs used for fetching label data are:

1. Asynchronous Labels API:
https://<<PCE_URL_DOMAIN>>/api/v1/orgs/<<ORG_ID>>/labels
2. Labels location API:
https://<<PCE_URL_DOMAIN>>/api/v1/orgs/<<ORG_ID>>/jobs/<<LOCATION>>

Asynchronous Label API is implemented which will fetch labels from each PCE configured and enabled at that instance. **API_VERSION** as: **'api/v1'** is used for the implementation. The fetched response is:

```
[{
  "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": {
    "href": "/users/0"
  }
}]
```

]

Once the app fetches lists of labels from that label API, it saves the fetched response into QRadar's Reference table in below format:

```
{
  "https://2x2devtest79.ilabs.io: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://2x2devtest79.ilabs.io: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",
    "value": "Database",
    "key": "role"
  }
}
```

Where `https://2x2devtest79.ilabs.io:8443/orgs/1/labels/1` is the primary key which is the combination of PCE link and href of the particular label. This primary key will provide the uniqueness in the reference table named “labels” for each PCE configured.

`created_at` and `updated_at` timestamps are stored in epoch format as per required by QRadar.

- **Protocol**
It defines how data gets into QRadar. Data is forwarded to Syslog port of QRadar from PCE

Log Sources

“Illumio ASP V2” is created automatically when the app is installed. This log source will identify all events that are coming to QRadar because all events have log source identifier as follows:

1. Illumio ASP V2: core0-2x2devtest59

User can create multiple log sources having different log source identifier as per their usage.

Add PCE as a Log Source

1. On the Admin tab, select Log Sources -> Add.

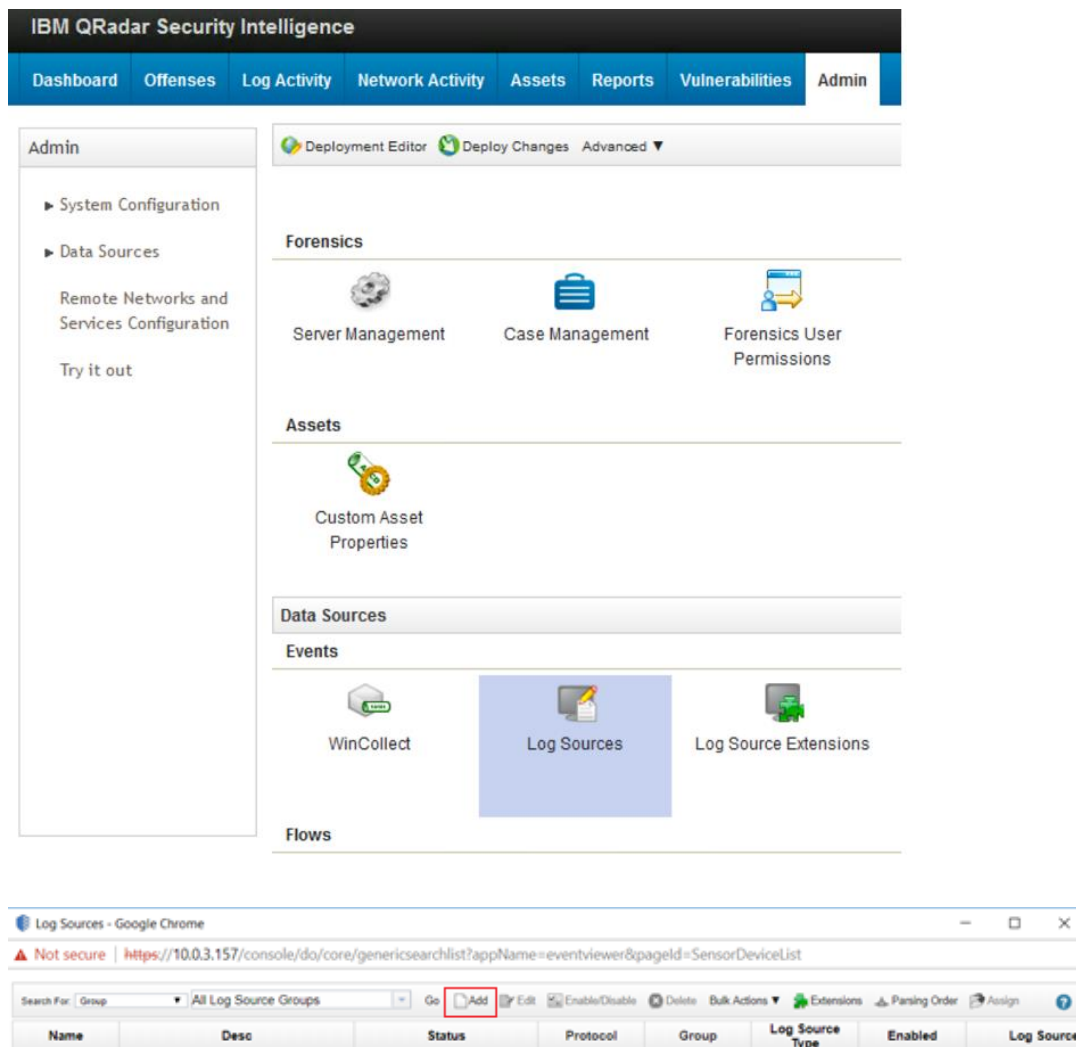
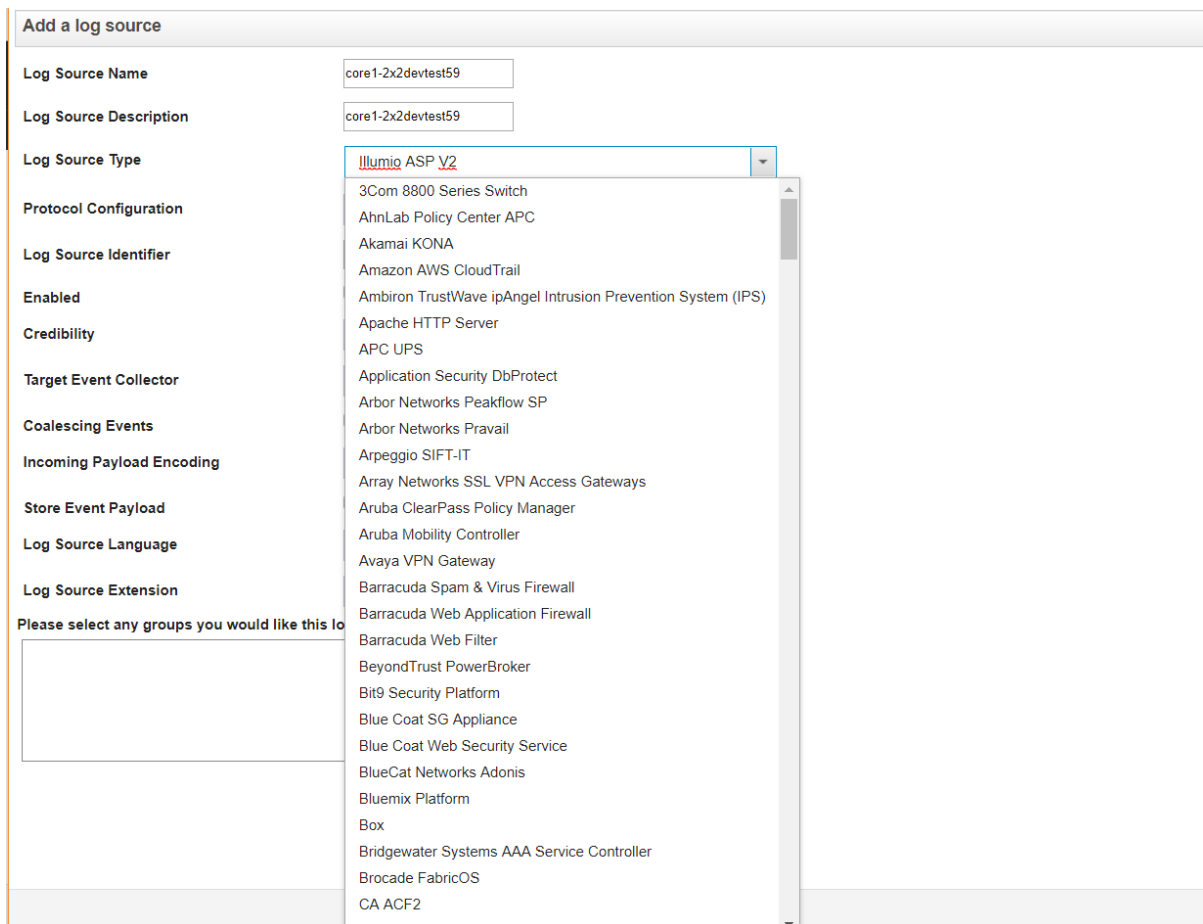


Figure 2 and 3 Adding a Log Source

2. Give the log source a suitable name for the PCE node. Add a description if desired. Repeat the same process for the other nodes in the 2x2 cluster.

3. Select log source type of 'Illumio ASP V2'.



Add a log source

Log Source Name: core1-2x2devtest59

Log Source Description: core1-2x2devtest59

Log Source Type: **Illumio ASP V2**

Protocol Configuration: 3Com 8800 Series Switch

Log Source Identifier: AhnLab Policy Center APC

Enabled: Akamai KONA

Credibility: Amazon AWS CloudTrail

Target Event Collector: Ambion TrustWave ipAngel Intrusion Prevention System (IPS)

Coalescing Events: Apache HTTP Server

Incoming Payload Encoding: APC UPS

Store Event Payload: Application Security DbProtect

Log Source Language: Arbor Networks Peakflow SP

Log Source Extension: Arbor Networks Pravail

Please select any groups you would like this log source to be associated with: Arpeggio SIFT-IT

Figure 4 Selecting a Log Source Type as Illumio ASP V2

4. Select Protocol configuration as 'Syslog'.
5. Enter the log source identifier as set in the syslog header on the host, typically the hostname. For example: 'core1-2x2devtest59'.
6. Ensure 'Enabled' is selected, then deselect the collector that receives the events as 'Coalescing Events'.
7. Select UTF-8 as the Payload encoding.
8. Select the Log Source Extension as 'IllumioASPCustom_ext'.
9. Click **Save**.
10. Click on **Deploy Changes** on Admin Tab.
11. Repeat for the other core node (e.g., db0, db1 or core0).

Sample Log Source included in the app is:

Edit a log source

Note that the connection information for this log source is shared amongst one or more other log sources.

Log Source Name

Illumio ASP V2

Log Source Description

Illumio ASP V2

Log Source Type

Illumio ASP V2

Protocol Configuration

Syslog

Log Source Identifier

core0-2x2devtest59

Enabled

☒

Credibility

5

Target Event Collector

eventcollector0 :: qradar230

Coalescing Events

☐

Incoming Payload Encoding

UTF-8

Store Event Payload

☒

Log Source Language

Log Source Extension

IllumioASPCustom_ext

Please select any groups you would like this log source to be a member of:

Save

Cancel

Figure 5 Selecting a Log Source Type as Illumio ASP

Log Source Types

It helps in defining how data is parsed. Log Source Extension and Custom Event Properties can be attached to a Log Source to extend its capability. There is 1 log source type that categorizes both type of events: Traffic Summary and Audit Events. Following is the name of the log source type associated with events:

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

The above Log source type can be linked to different log sources as specified in **Add Log Source** section as explained above.

Custom Property Extraction

The app performs extractions on the events received from Syslog on the QRadar instance i.e. Audit Events and Traffic Summary Events. For that the app has single Log Source Type which will perform both JSON and LEEF extractions.

List of extractions (both JSON and LEEF) performed are:

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 Host Name	(\"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	"?severity"?[:]=]"?([^\s\t,}]+)"?	FALSE
Hostname	(\s)(\[S+?)(\[s])illumio_pce	TRUE
Href	"?href"?[:]=]"?([^\s\t,}]+)"?	TRUE
Interval Sec	"?interval_sec"?[:]=]"?(.*)"?[,}]	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
Severity	sev=([^\s\t]+)	FALSE
Source Host Name	(\"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
State	\"?state\"?[=:]\"?([^\s\t,}]+)\"?	FALSE
Status	\"?status\"?[=:]\"?([^\s\t,}]+)\"?	FALSE
Total Bytes In	\"?tbi\"?[=:]\"?(.*?)\"?[,,]	FALSE
Total Bytes Out	\"?tbo\"?[=:]\"?(.*?)\"?[,,]	FALSE
Traffic Count	count=([\\S]+?)(\\s))	TRUE
Traffic Count	\"count\"\\:([d+])	TRUE
URL	/\"test\"	TRUE
URL	url=([^\s\t]+)	FALSE
Version	\"?version\"?[=:]\"?([^\s\t,}]+)\"?	TRUE

Event Mappings

An event mapping represents an association between an event ID and category combination and a QID record (referred to as event categorization). Event ID and category values are extracted by DSMs from events and are then used to look up the mapped event categorization or QID. These events are mapped to specific High level and low-level category.

Event Name	High Level Category	Low Level Category
Admin forced recalculation of policy	Audit	General Audit Event
Agent compatibility check report updated	Audit	General Audit Event
Agent interfaces updated	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 paired	Audit	General Audit Event
Agent clone activated	Audit	General Audit Event
Agent unpaired	Audit	General Audit Event
Agent fetched policy	System	Host-Policy Created
Workload shutdown	Audit	General Audit Event
Agent interactive users updated	Audit	General Audit Event
Agent machine identifiers updated	Audit	General Audit Event
Success or Failure to apply policy on VEN	System	Successful Host-Policy Modification
Agent refreshed token	Audit	General Audit Event
Agent reported a service not running	Audit	General Audit Event
Agent suspended	Audit	General Audit Event
Agent firewall tampered	Suspicious Activity	Content Modified By Firewall
Agent unsuspended	Audit	General Audit Event
Agent properties updated	Audit	General Audit Event
Agent updated existing iptables href	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
RBAC auth security principal deleted	Audit	General Audit Event
RBAC auth security principal updated	Audit	General Audit Event
Authentication settings updated	Audit	General Audit Event
Blocked traffic event deleted	Audit	General Audit Event
Cluster created	Audit	General Audit Event
Cluster deleted	Audit	General Audit Event
Cluster updated	Audit	General Audit Event
Container workload updated	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
Domain created	Audit	General Audit Event
Domain deleted	Audit	General Audit Event
Domain updated	Audit	General Audit Event
Global policy settings updated	System	Successful Host-Policy Modification
Ignored interfaces list updated	Audit	General Audit Event
IP list created	Audit	General Audit Event
IP list deleted	Audit	General Audit Event
IP list updated	Audit	General Audit Event
IP tables rules created	Audit	General Audit Event
IP tables rule delete	Audit	General Audit Event

IP tables rule updated	Audit	General Audit Event
Label group created	Audit	General Audit Event
Label group deleted	Audit	General Audit Event
Label group updated	Audit	General Audit Event
Label created	Audit	General Audit Event
Label deleted	Audit	General Audit Event
Label updated	Audit	General Audit Event
License deleted	Audit	General Audit Event
License updated	Audit	General Audit Event
Local user profile created	Audit	General Audit Event
Local user profile deleted	Audit	General Audit Event
Local user password changed	Authentication	Password Change Succeeded
Local user reinvited	Audit	General Audit Event
Authentication settings updated	Authentication	Policy Change
Password policy updated	Authentication	Policy Change
RADIUS configurations created	Authentication	Policy Added
RADIUS configuration deleted	Authentication	Policy Change
RADIUS configuration updated	Authentication	Policy Change
RADIUS config shared secret verified	System	Successful Configuration Modification
SAML configuration updated	Authentication	Policy Change
User accepted invitation	System	Successful Configuration Modification
User invited	System	Successful Configuration Modification
User reset password	System	Successful Configuration Modification
User updated	System	Successful Configuration Modification
Login user authenticated	Authentication	General Authentication Successful
Login user password changed	Authentication	General Authentication Successful
Lost agent updated	Audit	General Audit Event
Networks created	Application	Network Management
Network deleted	Application	Network Management
Network updated	Application	Network Management
Network function controller created	Application	Network Management
Network function controller deleted	Application	Network Management
Network function controller list of discovered virtual servers updated	Audit	General Audit Event
Network function controller policy status update	Audit	General Audit Event

Network function controller SLB state updated	Audit	General Audit Event
Organization setting updated	Audit	General Audit Event
Organization information updated	Audit	General Audit Event
Pairing profile created	Audit	General Audit Event
Pairing profile deleted	Audit	General Audit Event
Pairing profiles deleted	Audit	General Audit Event
Pairing profile pairing key generated	Audit	General Audit Event
Pairing profile updated	Audit	General Audit Event
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
RBAC permission created	Audit	General Audit Event
RBAC permission deleted	Audit	General Audit Event
RBAC permission updated	Audit	General Audit Event
RADIUS configurations created	Audit	General Audit Event
RADIUS configuration deleted	Audit	General Audit Event
RADIUS configuration updated	Audit	General Audit Event
RADIUS config shared secret verified	Audit	General Audit Event
RADIUS auth challenge issued	Audit	General Audit Event
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
API request failed due to internal server error	Audit	General Audit Event
API request failed due to unavailable service	Audit	General Audit Event
API request failed due to unknown server error	Audit	General Audit Event
Login resource created	Audit	General Audit Event
Login resource deleted	Audit	General Audit Event
Login resource updated	Audit	General Audit Event
Rule set created	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
Workload running containers updated	Audit	General Audit Event
Running container updated	Audit	General Audit Event

SAML assertion consumer services updated	Audit	General Audit Event
SAML assertion consumer service 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
Security policies created	Authentication	Policy Added
Security policies deleted	System	Host-Policy Deleted
Security policy restored	Audit	General Audit Event
Security policy rules created	Audit	General Audit Event
Security policy rule deleted	Audit	General Audit Event
Security policy rule updated	Audit	General Audit Event
Secure connect gateway deleted	Audit	General Audit Event
Secure connect gateway updated	Audit	General Audit Event
Secure connect gateways created	Audit	General Audit Event
RBAC security principals bulk created	Audit	General Audit Event
RBAC security principals created	Audit	General Audit Event
RBAC security principal deleted	Audit	General Audit Event
RBAC security principal updated	Audit	General Audit Event
Service binding created	Audit	General Audit Event
Service binding deleted	Audit	General Audit Event
Service created	System	Service Started
Service deleted	System	Service Stopped
Service updated	System	Successful Service Modification
Server load balancers created	Audit	General Audit Event
Server load balancer deleted	Audit	General Audit Event
Server load balancer updated	Audit	General Audit Event
System administrator deleted	Audit	General Audit Event
System administrators created	Audit	General Audit Event
Agent missed a few heartbeats	Audit	General Audit Event
Agents marked offline	Audit	General Audit Event
Event pruning completed	Audit	General Audit Event
TLS channel established	Audit	General Audit Event
TLS channel terminated	Audit	General Audit Event
Upgrade started	Audit	General Audit Event
User accepted invitation	Audit	General Audit Event
User failed authentication	Authentication	General Authentication Failed

User failed authorization	Access	Misc Authorization
User created	Audit	General Audit Event
First user created	Audit	General Audit Event
User deleted	Audit	General Audit Event
User login	Authentication	User Login Success
User logout	Authentication	Misc Logout
User logout from JWT	Audit	General Audit Event
User session created	Authentication	User Login Success
User session terminated	Authentication	General Authentication Successful
User updated	Audit	General Audit Event
User password updated	Audit	General Audit Event
User expired password used	Audit	General Audit Event
Virtual servers 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
Vulnerability report deleted	Audit	General Audit Event
Vulnerability report updated	Audit	General Audit Event
Vulnerability deleted	Audit	General Audit Event
Vulnerability updated	Audit	General Audit Event
Workload interfaces created	Audit	General Audit Event
Workload interface deleted	Audit	General Audit Event
Workload interface network created	Audit	General Audit Event
Workload settings updated	Audit	General Audit Event
Workload apply pending policy	Audit	General Audit Event
Workloads bulk created	Audit	General Audit Event
Workload bulk deleted	Audit	General Audit Event
Workload bulk updated	Audit	General Audit Event
Workload created	Audit	General Audit Event
Workload deleted	Audit	General Audit Event
Workload policy recalculated	Audit	General Audit Event
Workload network redetected	Audit	General Audit Event
Workloads labels removed	Audit	General Audit Event
Workload service reports updated	Audit	General Audit Event
Workload flow reporting frequency changed	Audit	General Audit Event

Workload labels applied	Audit	General Audit Event
Workload soft deleted	Audit	General Audit Event
Workload undeleted	Audit	General Audit Event
Workloads unpaired	Audit	General Audit Event
Workload updated	Audit	General Audit Event
Workloads updated	Audit	General Audit Event
Workload upgraded	Audit	General Audit Event
Flow Allowed	Flow	Misc flow
Flow Blocked	Flow	Misc flow
Flow Potentially Blocked	Flow	Misc flow
Agent cloned detected	Audit	General Audit Event
RBAC Auth Security Principal created	Audit	General Audit Event
Agent compatibility check report updated	Audit	General Audit Event
Org created from JWT	Audit	General Audit Event
User session terminated	Audit	General Audit Event
Workload came online	Audit	General Audit Event
Workload queried	Audit	General Audit Event

Visualizations

All the dashboards consist of individual panels which plot specific metric related to the events from Illumio PCE server. The data in all dashboards is populated from 1 log source type: Illumio ASP V2. All the dashboards allow the user to filter events by time.

Security Operations Dashboard

This dashboard is built to provide overall visibility into Illumio App deployment. It gives a count of Overall Audit Events, Ports Scan, Firewall Tampering etc. Filters used for this dashboard are Time Range and PCE filter (configured from Illumio Configuration page). For Label filter if the label selected have the same type which can be any of (app, env, role, loc) then the OR operator is applied for these labels else the AND operator is applied for the selected labels. Also, the consideration of source labels or destination labels is made based on the value for the Direction field. So, if the value of the Direction field is I which signifies Incoming then the Destination Labels are considered and if the value of the Direction field is O which signifies Outgoing then the Source Labels are considered

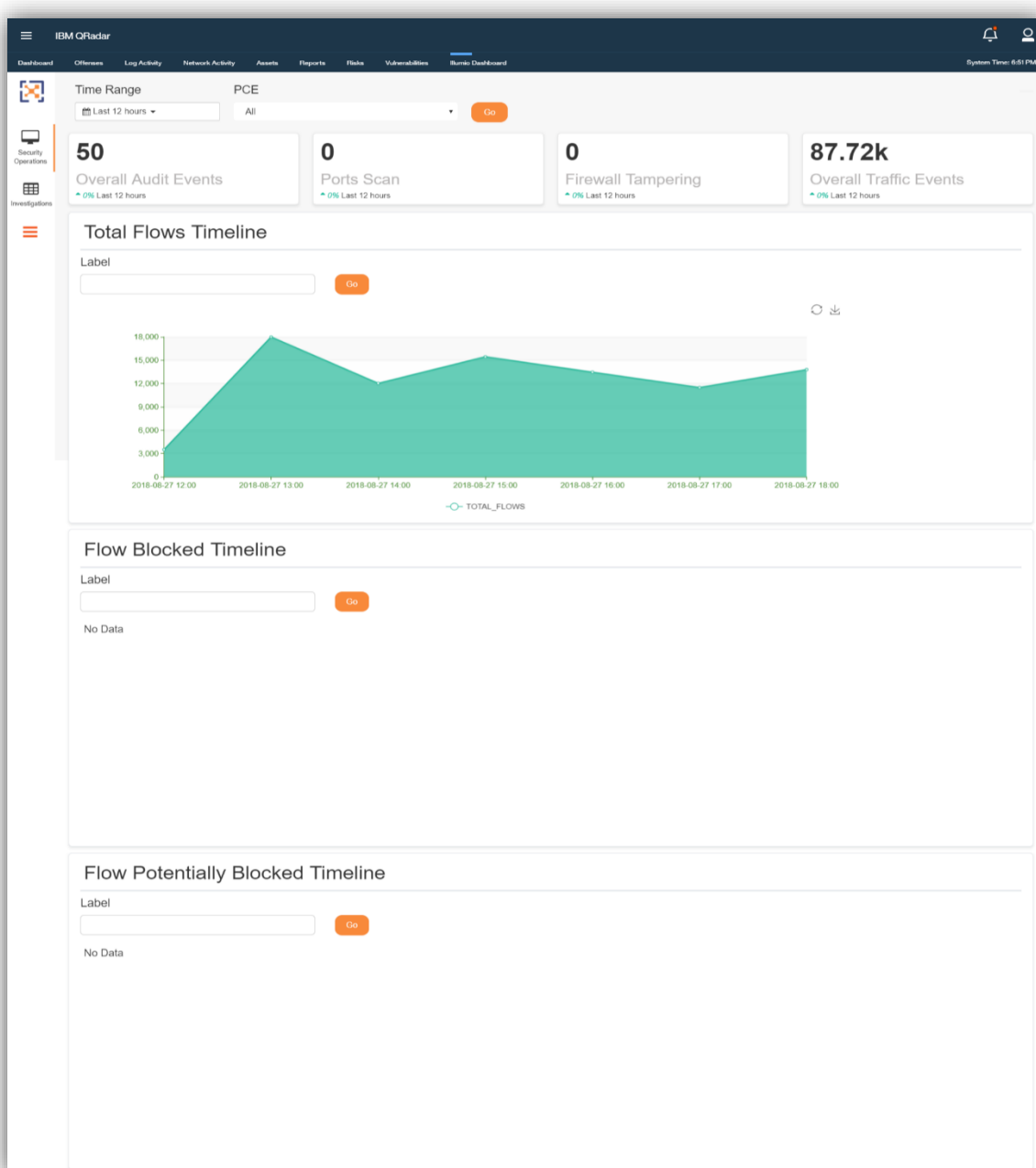


Figure 6: Security Operations Dashboard

Investigation Dashboard

This dashboard is built to provide a list of Top 1000 Investigations sorted on the basis of Time. Filters used for this dashboard are Time Range, PCE and Label Name. The Labels represented are taking into consideration the Direction so if the value of Direction is I which signifies Incoming then the Destination Labels are taken into consideration and the value of Hostname column is set as Destination Host Name and if the value of Direction field is O which signifies Outgoing then the Source Labels are considered and the value of Hostname column is set as Source Host Name

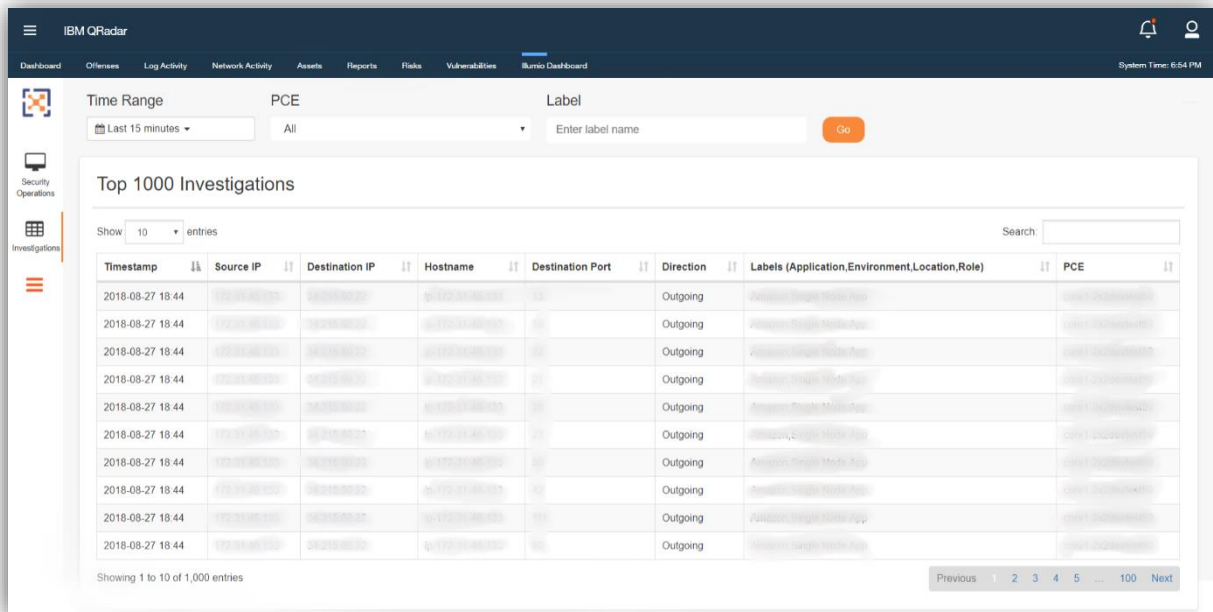


Figure 7: Investigation Dashboard

App Installation & Configuration

Prerequisites

Below is a list of requirements needed to run Illumio app v1.0.0 on QRadar

- Illumio App Bundle (v1.0.0)
- QRadar version: 7.3.1 onwards
- Access to Illumio Endpoint.
- Illumio Credentials to access labels from PCEs.

Installation

The application installation requires access to QRadar console machine via a web interface. The web interface can be accessed via <https://<<QRadarconsoleIP>>/>. The installation process is as follows:

- a. Login to QRadar console



Figure 8: IBM QRadar 7.3.1 login screen

- b. Go to Admin → Extension Management

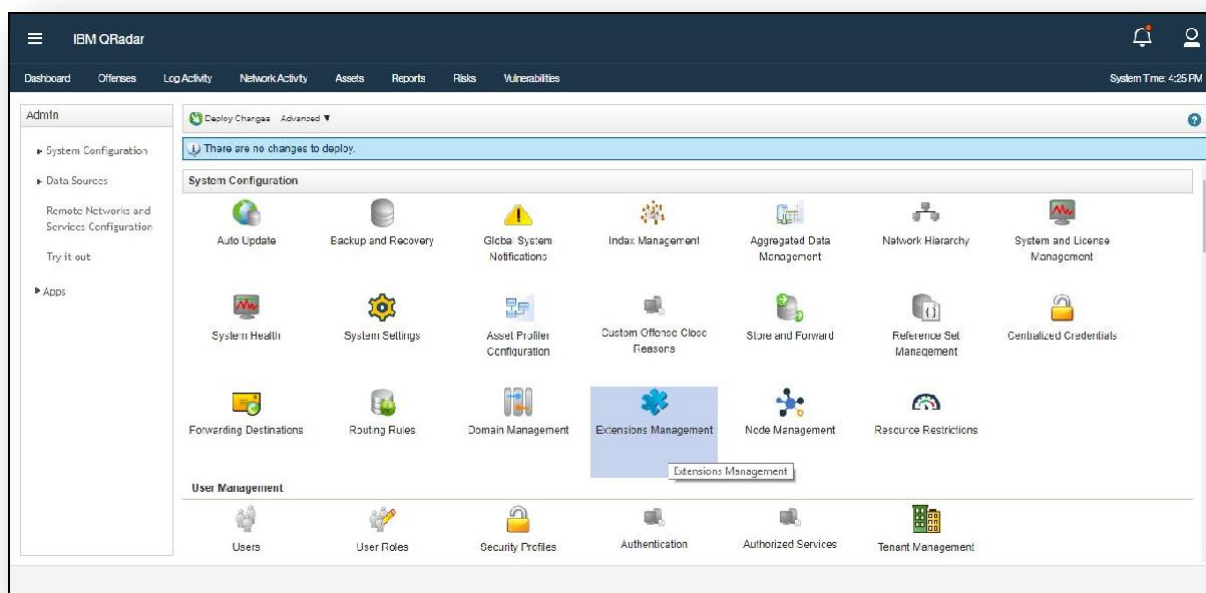


Figure 9: IBM QRadar Admin Panel

- c. Choose the downloaded zip file by clicking on **Add**.
- d. The QRadar will prompt list of changes being made by the app. Click on install button. After the Application is installed it will create a Docker container in the backend.
- e. Deploy changes on Admin Panel and refresh the browser window for configuration page to show up on the Admin Panel.

App Configuration

After completing the installation, you must complete the configuration to start the data collection.

The setup process for configuring is as follows:

- Find the installed app on Admin Panel under Apps as shown in fig.

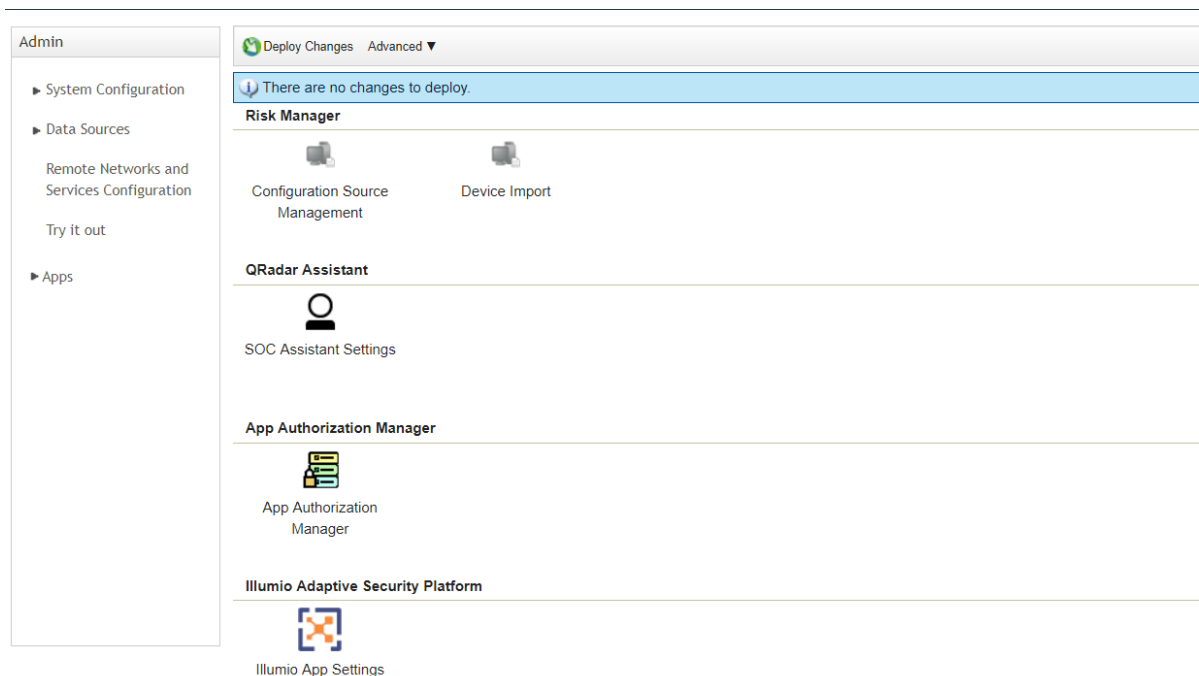


Figure 10: Installed apps configuration page

- Open configuration page and it shows setup page as follows:

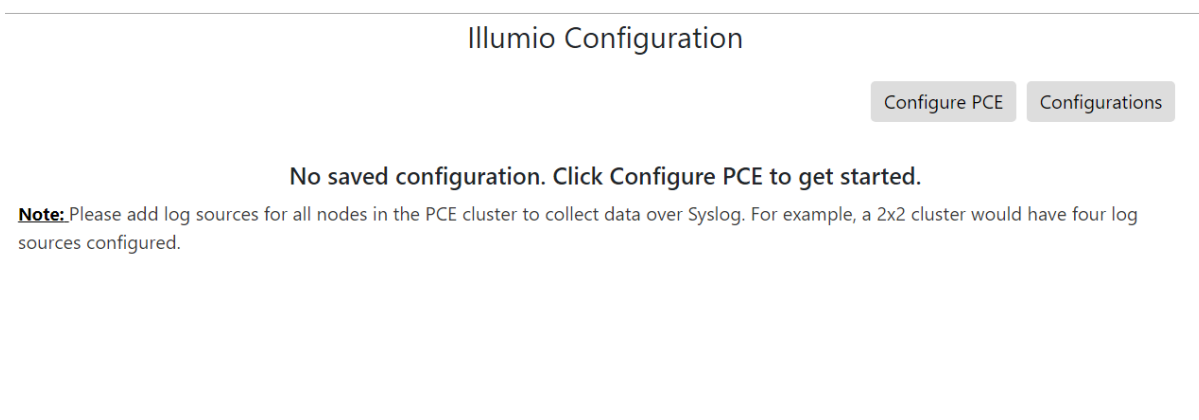


Figure 11: Illumio App configuration page

Note: The app supports multiple accounts for PCE configurations

Add New Illumio PCE Configuration

PCE URL *

API Authentication Username *

API Secret *

Interval (in seconds) *

3600

Organization ID

1

Enable/Disable Proxy

IP/Hostname (Please don't mention http or https in URL) *

Port *

☐ Require Authentication for Proxy

Cancel

Save

Configurations

Port scan configurations

Unique Port Threshold *

1

Scan Interval (in minutes) *

5

Allowed port scanner IP Addresses

Authorization token

Authorized service token *

Configured Auth token is xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx6ab8

Cancel

Save

Figure 12 and 13: New PCE Configurations and General Configurations form

- Configure your Illumio credentials and your data collection will start.
- Save credentials can be found in the table below where you can edit/delete the same.
- You can set proxy to fetch data from Illumio PCE configurations.

User Roles / Capabilities

The QRadar supports ACL configurations for restricting access to different actions/dashboards. This app adds a new capability, which controls access to Illumio dashboard. For accessing Illumio dashboard, the user should be assigned a role that has this capability. By default, admin users have access to all the capabilities. To configure Role in QRadar, use following steps.

Login to QRadar console, go to Admin User Roles.

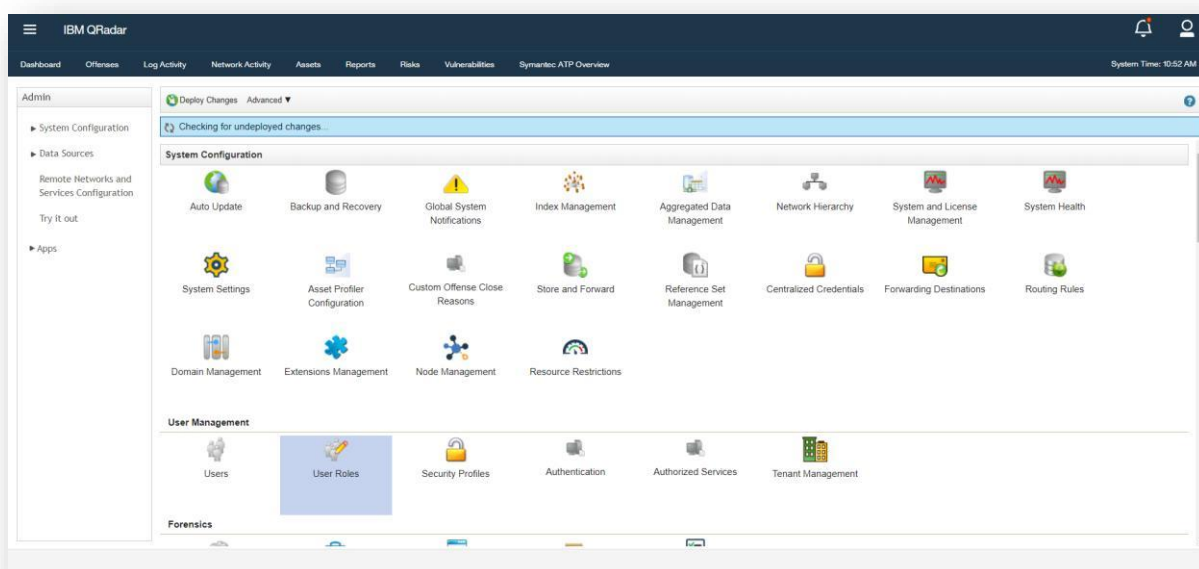


Figure 14: User Role

1. Click on New button.
2. Enter the name of the role. Assign the required capabilities as shown in the screenshot. Assign these roles to Users who should be able to view Illumio Dashboard.

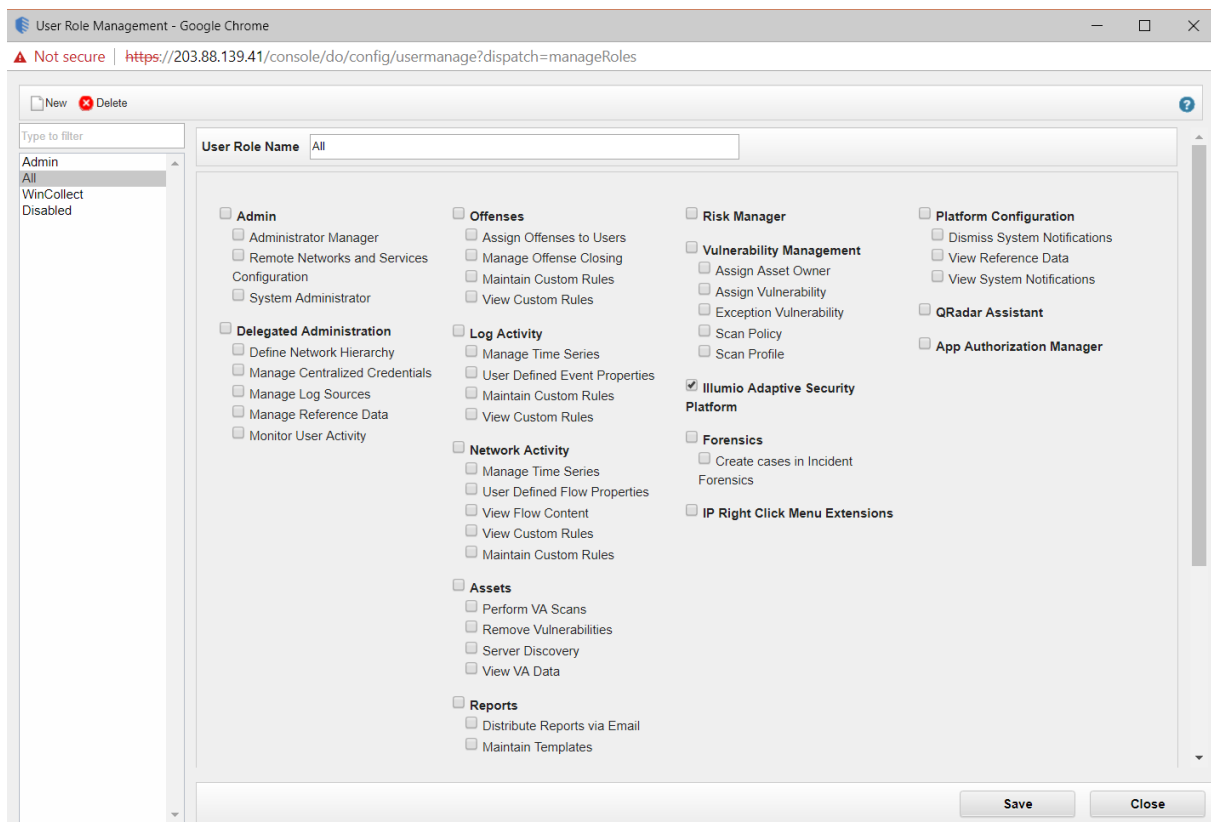


Figure 15: Assign App Permissions

Uninstalling the Application

To uninstall the application, the user needs to perform the following steps.

1. Go to Admin Page
2. Open Extension Management
3. Select Illumio App for QRadar application
4. Click on Uninstall

QRadar Cloud Support

Illumio QRadar v1.0.0 supports all its functionalities on QRadar cloud. If the PCE is installed on the port other than **443**, then they need to contact to IBM to open that port.

Troubleshooting

This section describes the common issues that might happen during the deployment or the running of the app and the steps to resolve the issues.

Case #1 – Events are shown up as “Custom Message”

Problem: Illumio events will show up as **IllumioASPCustom Message** rather than getting identified as the right QRadar category. This will be seen in “Log Activity” tab in QRadar when the user might be searching for event pertaining to created log sources

Below is a screenshot how it will look

	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

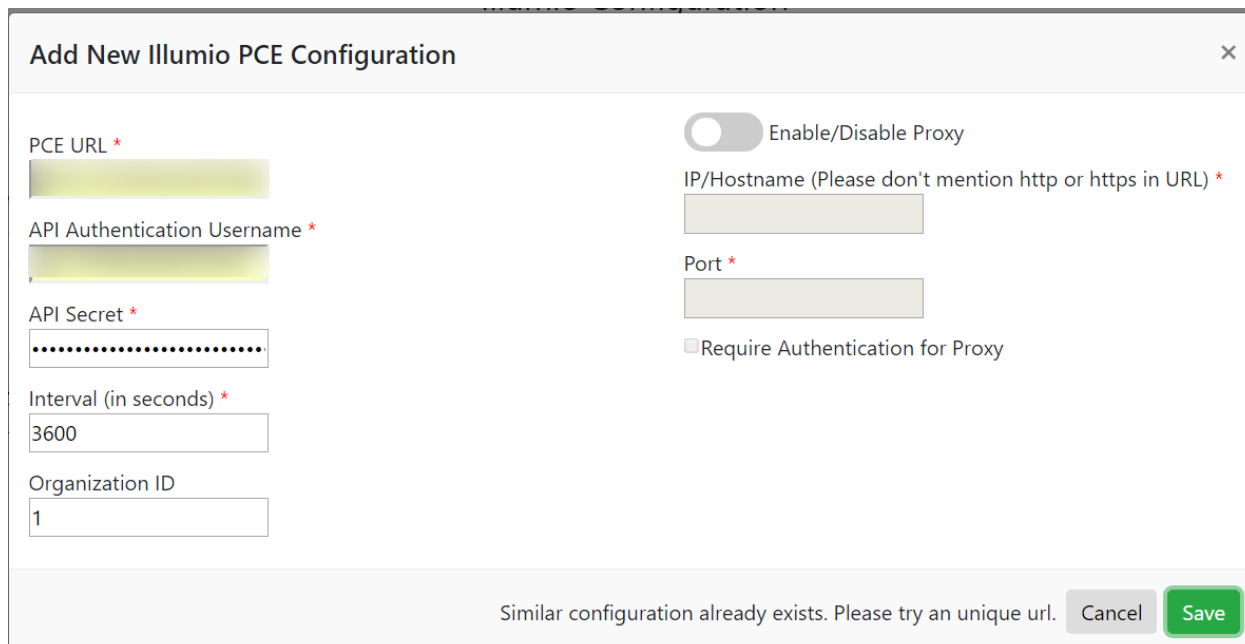
Figure 16: Custom Message Issue

Troubleshooting steps: This issue can be caused due to 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, then the value of that property will be empty.

1. Go to Log Activity.
2. Add Filter Log Source Type Equals Illumio ASP V2
3. Select Last 7 Days in Views filter.
4. Right click on that particular event.
5. View in DSM editor.
6. Check the value of Event ID and Event Category under Log activity Preview
7. If Event ID and Event Category is coming unknown, create a support ticket with Illumio Support.

Case #2 – App configuration fails with various error messages

Problem: New configuration fails with error message “Same configuration already exists. Please try an unique url”. Below is a screenshot for quick reference.



The screenshot shows a dialog box titled "Add New Illumio PCE Configuration" with a close button (X) in the top right corner. The form contains the following fields and controls:

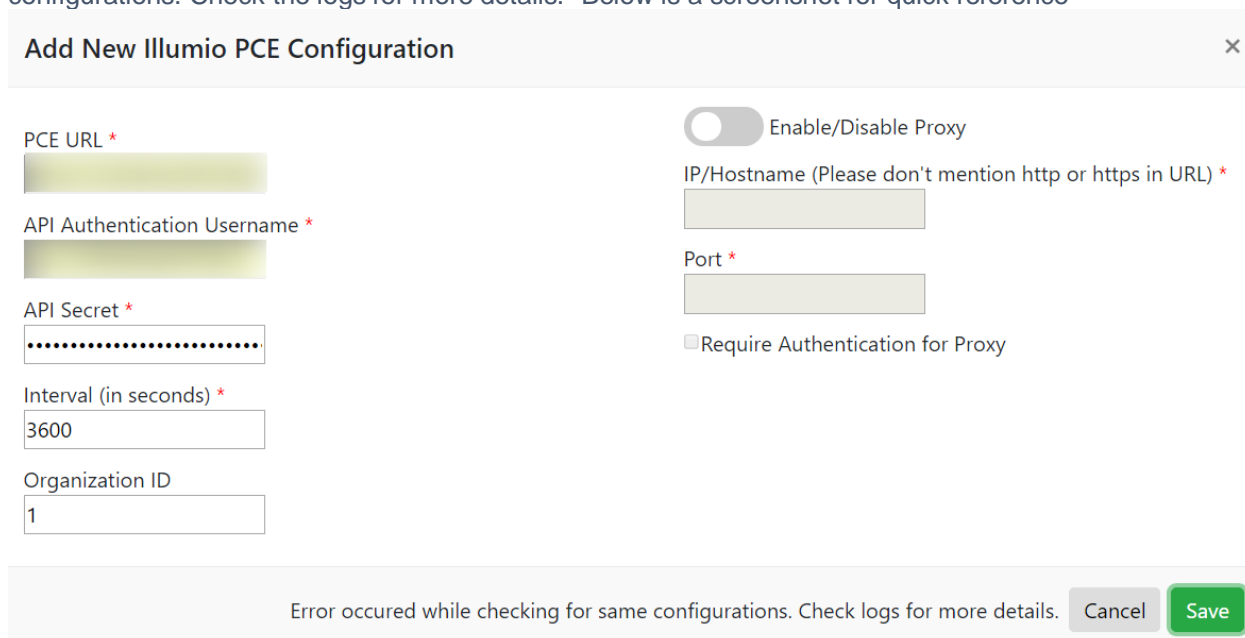
- PCE URL ***: A text input field with a yellow highlight.
- API Authentication Username ***: A text input field with a yellow highlight.
- API Secret ***: A password input field with a yellow highlight and a masked view icon.
- Interval (in seconds) ***: A text input field containing the value "3600".
- Organization ID**: A text input field containing the value "1".
- Enable/Disable Proxy**: A toggle switch that is currently turned off.
- IP/Hostname (Please don't mention http or https in URL) ***: A text input field.
- Port ***: A text input field.
- Require Authentication for Proxy**: A checkbox that is currently unchecked.

At the bottom of the dialog, there is an error message: "Similar configuration already exists. Please try an unique url." To the right of the message are two buttons: "Cancel" and "Save".

Figure 17: Duplicate credentials error

Troubleshooting Steps: User might have entered account which is already configured. The user is recommended to enter new credentials which are not already provided.

Problem: Configuration of Illumio fails with error message “Error occurred while checking for same configurations. Check the logs for more details.” Below is a screenshot for quick reference



The screenshot shows a dialog box titled "Add New Illumio PCE Configuration" with a close button (X) in the top right corner. The form contains the following fields and controls:

- PCE URL ***: A text input field with a yellow highlight.
- API Authentication Username ***: A text input field with a yellow highlight.
- API Secret ***: A password input field with a yellow highlight and a masked view icon.
- Interval (in seconds) ***: A text input field containing the value "3600".
- Organization ID**: A text input field containing the value "1".
- Enable/Disable Proxy**: A toggle switch that is currently turned off.
- IP/Hostname (Please don't mention http or https in URL) ***: A text input field.
- Port ***: A text input field.
- Require Authentication for Proxy**: A checkbox that is currently unchecked.

At the bottom of the dialog, there is an error message: "Error occurred while checking for same configurations. Check logs for more details." To the right of the message are two buttons: "Cancel" and "Save".

Figure 18: Similar Configuration Check error

Troubleshooting Steps: This happens while the app is checking for similar configurations. The user is recommended to try it once again or else follow steps as mentioned in case #6

Problem: New configuration fails with error message “Authentication failed. Invalid credentials”. Below is a screenshot for quick reference.

Add New Illumio PCE Configuration

PCE URL *

API Authentication Username *

API Secret *

Interval (in seconds) *

Organization ID

☐ Enable/Disable Proxy

IP/Hostname (Please don't mention http or https in URL) *

Port *

☐ Require Authentication for Proxy

Authentication failed: Invalid credentials.
Cancel
Save

Figure 19: Incorrect Credentials error

Troubleshooting Steps: This happens when the user has entered wrong credentials so authentication failed while saving the new configuration. The user is recommended to check the credentials and try again

Problem: New configuration of Illumio App fails with error message “Authorized Service Token is invalid. Please check your Authorized Service Token”. Below is a screenshot for quick reference

Configurations

Port scan configurations

Unique Port Threshold *

Scan Interval (in minutes) *

Allowed port scanner IP Addresses

Authorization token

Authorized service token *

Authorized Service Token is invalid. Please check your Authorized Service Token.
Cancel
Save

Figure 20: Incorrect Authorized Service error

Troubleshooting Steps: This happens when the user has entered wrong authorized service token. The user is recommended to check the authorized service token and try again.

Problem: Configuration of Illumio App fails with error message “Error occurred while validating authorization token”. Below is a screenshot for quick reference

Configurations

Port scan configurations

Unique Port Threshold *

1

Scan Interval (in minutes) *

5

Allowed port scanner IP Addresses

Authorization token

Authorized service token *

.....

Error occurred while validating authorization token. Check logs for more details.

CancelSave

Figure 21: Authorized Service Token Check error

Troubleshooting Steps: This happens while the app is checking for authorized service token. The user is recommended to try it once again or else follow steps as mentioned in case #6

Problem: Configuration of Illumio App with the error message “Failed due to network connection timeout”. Below is a screenshot for quick reference

Illumio PCE Configuration

PCE URL *

API Authentication Username *

API Secret *

.....

Interval (in seconds) *

3600

Organization ID

1

☐ Enable/Disable Proxy

IP/Hostname (Please don't mention http or https in URL) *

Port *

☐ Require Authentication for Proxy

Failed due to network connection timeout

CancelSave

Figure 22: Network connection timeout error

Troubleshooting Steps: This happens when the app is not able to connect to the server. The user is recommended to check whether the port is open or not or else follow steps as mentioned in case #6

Problem: New configuration fails with error message “Connection failed to be established”. Below is a screenshot for quick reference.

Add New Illumio PCE Configuration

PCE URL *

API Authentication Username *

API Secret *

.....

Interval (in seconds) *

3600

Organization ID

1

Enable/Disable Proxy

IP/Hostname (Please don't mention http or https in URL) *

Port *

☐

Require Authentication for Proxy

Connection failed to be established.

Cancel

Save

Figure 23: Connection error

Troubleshooting Steps: This issue can happen when the app is not able to reach entered PCE URL or entered proxy credentials. The user is recommended to follow the troubleshooting steps as mentioned in Case #6.

Case #3 – Events are coming as Unknown

Problem: Illumio App events come as Unknown

Troubleshooting steps:

1. Go to Log Activity.
2. Add Filter Log Source Type Equals to Illumio ASP V2
3. Select Last 7 Days in Views filter.
4. If any events come as **Unknown**,
 - a. Right click on that particular event.
 - b. View in DSM editor.
 - c. Check the value of Event ID and Event Category under Log activity Preview
 - d. If Event ID and Event Category value come as unknown, create a support ticket with Illumio.

Case #4 – Data is not getting collected in the app

Problem: Data is not getting collected by the app

Troubleshooting steps:

1. Click on System and License Management in Admin Panel
2. Select the host on which Illumio App is installed
3. Click on Actions in the top panel and select the option Collect Log Files
4. A pop-up named Log File Collection will open
5. Click on Advance Options
6. Select the checkbox to Include Debug Logs, Application Extension Logs, Setup Logs (Current Version)
7. Click on Collect Log Files Button after selecting 2 days as data input.

8. Click on "Click here to download files"
9. This will download all the log files in a single zip on your local machine
10. Create support case with Illumio and attach this log file

Case #5 – UI related issues in the app

Problem: Any dashboard panel, configuration pages, charts shows errors or unintended behavior.

Troubleshooting Steps:

1. Clear the browser cache and reload the webpage
2. Try reducing the time range of the filter and retry. It has been seen that QRadar queries expire if too much data is being matched in the query.

Case #6 – Re installation of App

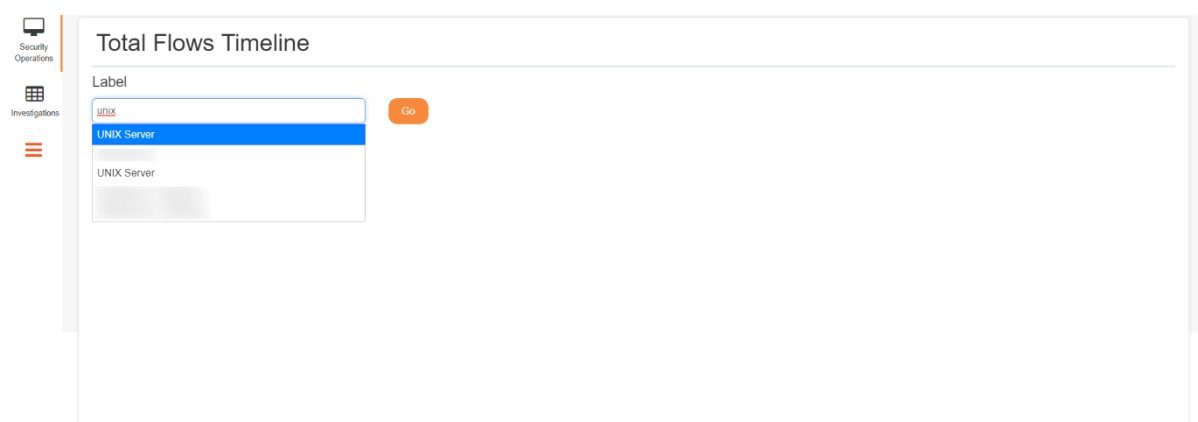
Problem: The application is exhibiting aberrant behavior and user wishes to perform clean installation again.

Troubleshooting Steps: To perform a reinstallation of the app please perform the following steps:

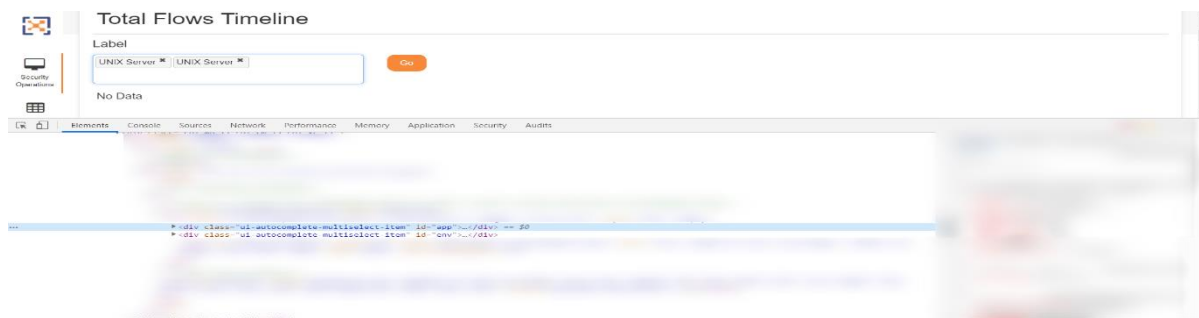
1. Remove all saved searches and custom properties associated with the log source type Illumio ASP V2
2. Delete the log source associated with log source type Illumio ASP V2 by navigating to Log Sources via Admin panel
3. Uninstall the app
4. Refresh the page and check the Dashboard tab of Illumio Overview is not seen after uninstallation
5. Now install the app from Extension Management

Case #7 – Labels Filter showing duplicate values

Problem: The auto populate filter for Labels shows same value more than once in the options to select

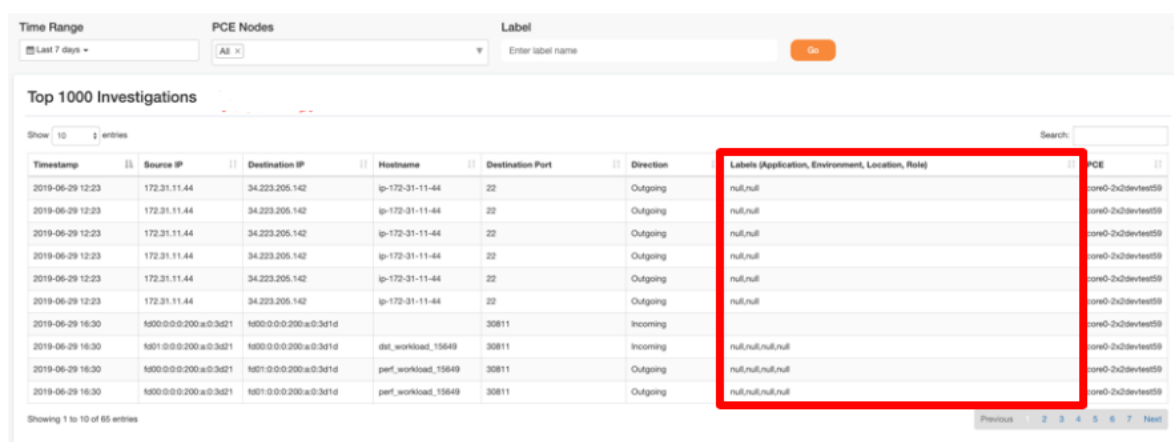


Troubleshooting Steps: This behavior is expected as the two labels shown have different value for the type of label. To differentiate between the labels inspect the label filter text box via browser dev tools and click on the selected label, the value of the type is seen in the id tag of the html. Please refer to the below screenshot



Case #6 – Top 1000 Investigations Table shows null value

Problem: Null values are seen in Top 1000 Investigations Table. Below is the screenshot for your reference:



Timestamp	Source IP	Destination IP	Hostname	Destination Port	Direction	Labels (Application, Environment, Location, Role)	PCE
2019-06-29 12:23	172.31.11.44	34.223.205.142	ip-172-31-11-44	22	Outgoing	null	core0-2x2devtest59
2019-06-29 12:23	172.31.11.44	34.223.205.142	ip-172-31-11-44	22	Outgoing	null	core0-2x2devtest59
2019-06-29 12:23	172.31.11.44	34.223.205.142	ip-172-31-11-44	22	Outgoing	null	core0-2x2devtest59
2019-06-29 12:23	172.31.11.44	34.223.205.142	ip-172-31-11-44	22	Outgoing	null	core0-2x2devtest59
2019-06-29 12:23	172.31.11.44	34.223.205.142	ip-172-31-11-44	22	Outgoing	null	core0-2x2devtest59
2019-06-29 12:23	172.31.11.44	34.223.205.142	ip-172-31-11-44	22	Outgoing	null	core0-2x2devtest59
2019-06-29 16:30	1600:0:0:200:a0:3a1d	1600:0:0:200:a0:3a1d		30811	Incoming	null	core0-2x2devtest59
2019-06-29 16:30	1601:0:0:200:a0:3a1d	1600:0:0:200:a0:3a1d	dat_workload_15649	30811	Incoming	null,null,null	core0-2x2devtest59
2019-06-29 16:30	1600:0:0:200:a0:3a1d	1601:0:0:200:a0:3a1d	perf_workload_15649	30811	Outgoing	null,null,null	core0-2x2devtest59
2019-06-29 16:30	1600:0:0:200:a0:3a1d	1601:0:0:200:a0:3a1d	perf_workload_15649	30811	Outgoing	null,null,null	core0-2x2devtest59

Troubleshooting Steps: This is a known issue where the IS NOT keyword for AQL query does not work properly. To resolve this upgrade Qradar instance to 7.3.2. patch 2 as the issue is resolved from this version. Link to Qradar APAR: <https://www-01.ibm.com/support/docview.wss?uid=swg1IJ15591>

Case #7 – All other issues which are not part of the document

Problem: If the problem is not listed in the document, please follow the below steps.

Troubleshooting Steps: Please follow the below steps:

1. Click on System and License Management in Admin Panel
2. Select the host on which Illumio App is installed
3. Click on Actions in the top panel and select the option Collect Log Files
4. A pop-up named Log File Collection will open
5. Click on Advance Options
6. Select the checkbox to Include Debug Logs, Application Extension Logs, Setup Logs (Current Version)
7. Click on Collect Log Files Button after selecting 2 days as data input.
8. Click on "Click here to download files"
9. This will download all the log files in a single zip on your local machine
10. Create support case with Illumio and attach these log file

----- End of Document -----