# Illumio App for QRadar 1.3.0

Illumio ASP 21.2.1
Last Revised: 2022-03-22

**Document History**

| Date | Changes |
|---|---|
| August 19, 2019 | Initial publication of this Guide. |
| September 10, 2019 | Support of App version 1.1.0 |
| June 16, 2020 | Support of App version 1.2.0 |
| March 22, 2022 | Support of App version 1.3.0 |

# Table of Contents

# 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.

The following diagram shows the topology of data collection from Illumio PCE to QRadar
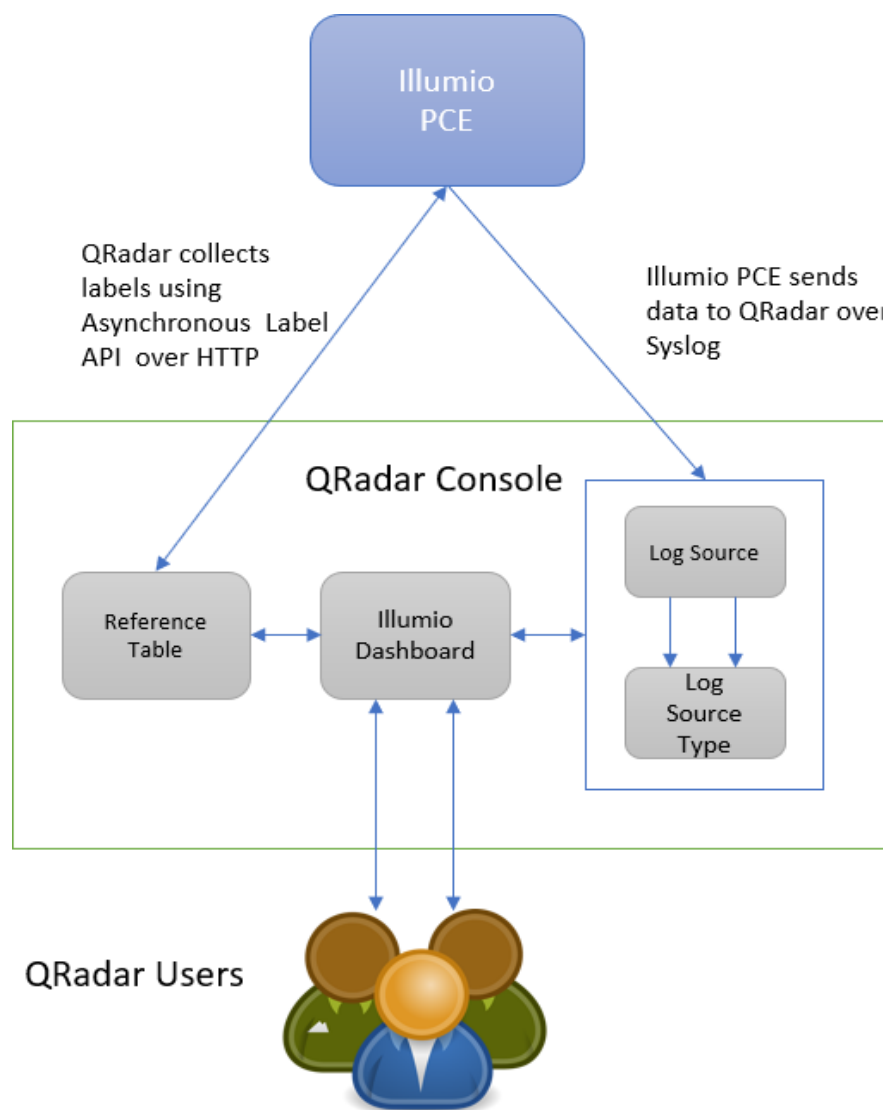
*Figure 1: Illumio integration with IBM QRadar*

The Illumio App for QRadar provides two dashboards which are integrated in the QRadar UI:

- With east-west traffic visibility on the Security Operations dashboard, you can pinpoint potential attacks and identify compromised workloads.
- The PCE Operations dashboard provides a comprehensive overview where you can monitor the health of all deployed and managed PCEs.

The Illumio App for QRadar is supported with PCE version 18.1.0, 18.2.0, 18.3.0, 19.1.0, 19.3.0,19.3.3, 20.1.0, 21.2.0, 21.2.1.

# App Architecture

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

## Data Collection

The app has two sources for receiving data:
- API
- Syslog Port

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

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

### APIs in Log Source

The following APIs are used to fetch label data.
- Asynchronous Labels API:

  ```
  https://<PCE_URL_DOMAIN>/api/v2/orgs/<ORG_ID>/labels
  ```

- Labels Location API:

  ```
  https://<PCE_URL_DOMAIN>/api/v2/orgs/<ORG_ID>/jobs/<LOCATION>
  ```

The Asynchronous Labels API fetches labels from each PCE that is configured and enabled at that instance.

**Note:** The PCE API v2 is used to implement the Asynchronous Labels API.

Following is an example response from the Asynchronous Labels API. This example 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": {
                "href": "/users/0"
        }
}
]
```

After the app gets 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",
            "value": "Database",
            "key": "role"
    }
}
```

The primary key is `https://<hostname>:8443/orgs/1/labels/1`, 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 required by QRadar.

### 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.
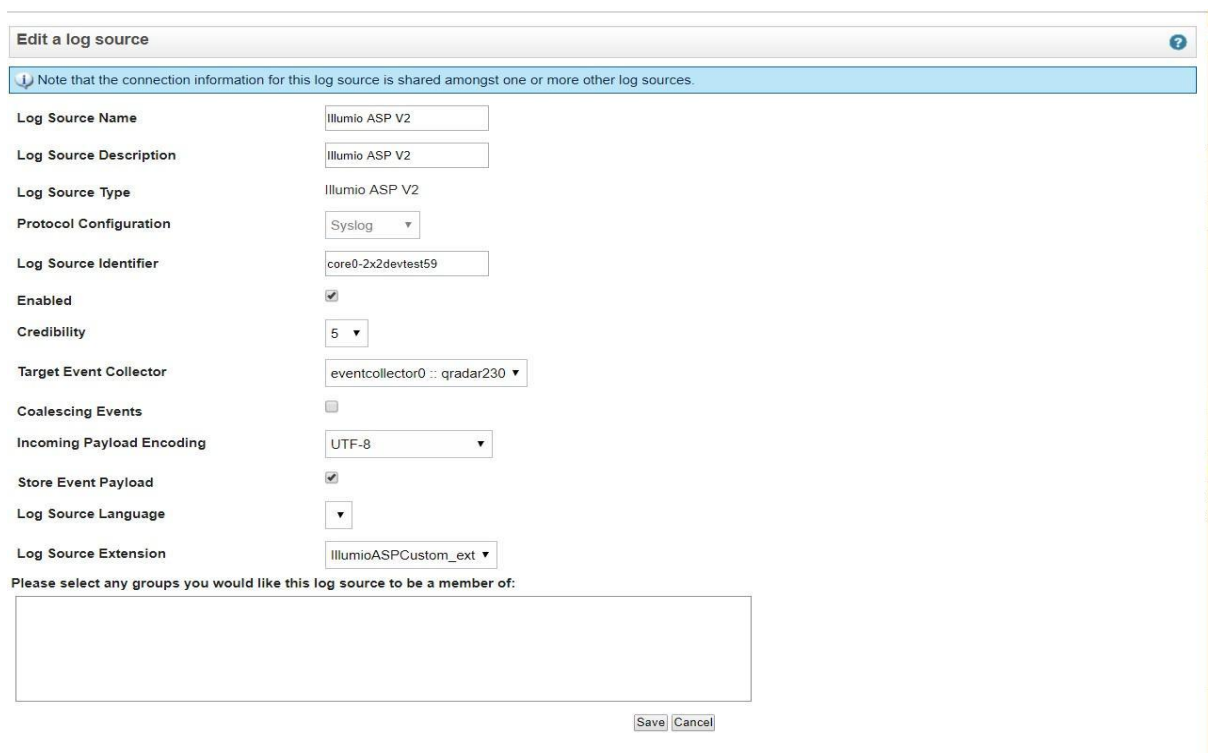
## Log Sources

A log source named "Illumio ASP V2" is created automatically when the app is installed. All events that are sent from the app to QRadar include the log source as a prefix. For example:

> 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. A separate log source needs to be created to collect data from each PCE.

The following illustration shows the Illumio ASP V2 log source that is included in the app.

*Figure 5 Log Source Type Illumio ASP V2*

# Log Source Types

The use of log source types helps in defining how data is parsed. Log Source Extension and Custom Event Properties can be attached 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) |

The log source type Illumio ASP V2 can be linked to different log sources, as described in Adding the PCE as a Log Source in QRadar.

## 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 which will perform 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 |

| Custom Property Name | Custom Property Expressions | Enabled |
|---|---|---|
| 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 |

| Custom Property Name | Custom Property Expressions | Enabled |
|---|---|---|
| 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 |
| 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 Host Name | `(\"src_hostname\":\s*\"|srcHostname=)(.*?)(\"|\s)` | TRUE |
|---|---|---|

| Custom Property Name | Custom Property Expressions | Enabled |
|---|---|---|
| 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,}"]+)"?` | 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 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.

The following table shows which high-level and low-level categories are associated with each event.

| Event Name | High Level Category | Low Level Category |
|------------|---------------------|--------------------|
| Admin forced recalculation of policy | Audit | General Audit Event |
| Agent clone activated | 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 |
| 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 |
| Agents 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 |
| 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 |
| API request failed due to unavailable service | Audit | General Audit Event |
| API request failed due to unknown server error | Audit | General Audit Event |
| Authentication settings updated | Audit | General Audit Event |
| Blocked traffic event deleted | Audit | General Audit Event |
| Container cluster created | Audit | Create Activity |

| | | Succeeded |
|---|---|---|
| Container cluster deleted | Audit | Delete Activity Succeeded |
| 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 |
| Container workload updated | Audit | General Audit Event |
| Creation of support report requested | Audit | General Audit Event |
| Domain created | Audit | General Audit Event |
| Domain deleted | Audit | General Audit Event |
| DB temp table cleanup completed | Audit | General Audit Event |
| DB temp table cleanup started | 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 |
| Existing or new unmanaged workload assigned to a network device | Audit | General Audit Event |
| First user created | Audit | General Audit Event |
| Flow Allowed | Flow | Misc flow |
| Flow Blocked | Flow | Misc flow |
| Flow Potentially Blocked | Flow | Misc flow |
| Flow Unknown | Flow | Misc flow |
| Event settings updated | Audit | Update Activity Succeeded |
| Global policy settings updated | Audit | General Audit Event |
| Ignored interfaces list updated | Audit | General Audit Event |
| Interservice call to login service to create LDAP config | Audit | Create Activity Succeeded |
| Interservice call to login service to delete LDAP config | Audit | Delete Activity Succeeded |

| | | |
|---|---|---|
| Interservice call to login service to update LDAP config | Audit | Update Activity Succeeded |
| Interservice call to login service to verify 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 |
| Label created | Audit | General Audit Event |
| Label deleted | 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 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 |

| 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 |
| 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 |
| 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 updated | Audit | General Audit Event |
| 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 syslog configuration update | Audit | Update Activity Succeeded |
| PCE system email tested | Audit | General Audit Event |

| | | |
|---|---|---|
| Pairing profile pairing key generated | Audit | General Audit Event |
| Pairing profile updated | Audit | General Audit Event |
| Pairing profiles deleted | Audit | Delete Activity Succeeded |
| 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 |
| 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 |
| 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 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 |

| | | |
|---|---|---|
| Success or Failure to apply policy on VEN | Audit | Update Activity Attempted |
| 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 |
| 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 |
| 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 |
| 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 terminated | Audit | General Audit Event |
| User Sign in | Authentication | User Login Success |
| User Sign out | Authentication | General Authentication Successful |
| 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 software release created | Audit | Create Activity Succeeded |
| VEN software release deleted | Audit | Delete Activity Succeeded |
| VEN software release deployed | Audit | Deploy Activity Succeeded |

| VEN software release updated | Audit | Update Activity Succeeded |
|---|---|---|
| VEN software release upgraded | Audit | Update Activity Succeeded |
| 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 |
| 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 |
| 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 which plot specific metrics related to the events from the Illumio PCE. The data in all dashboards is populated from the log source type Illumio ASP V2.

## 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, Ports 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.
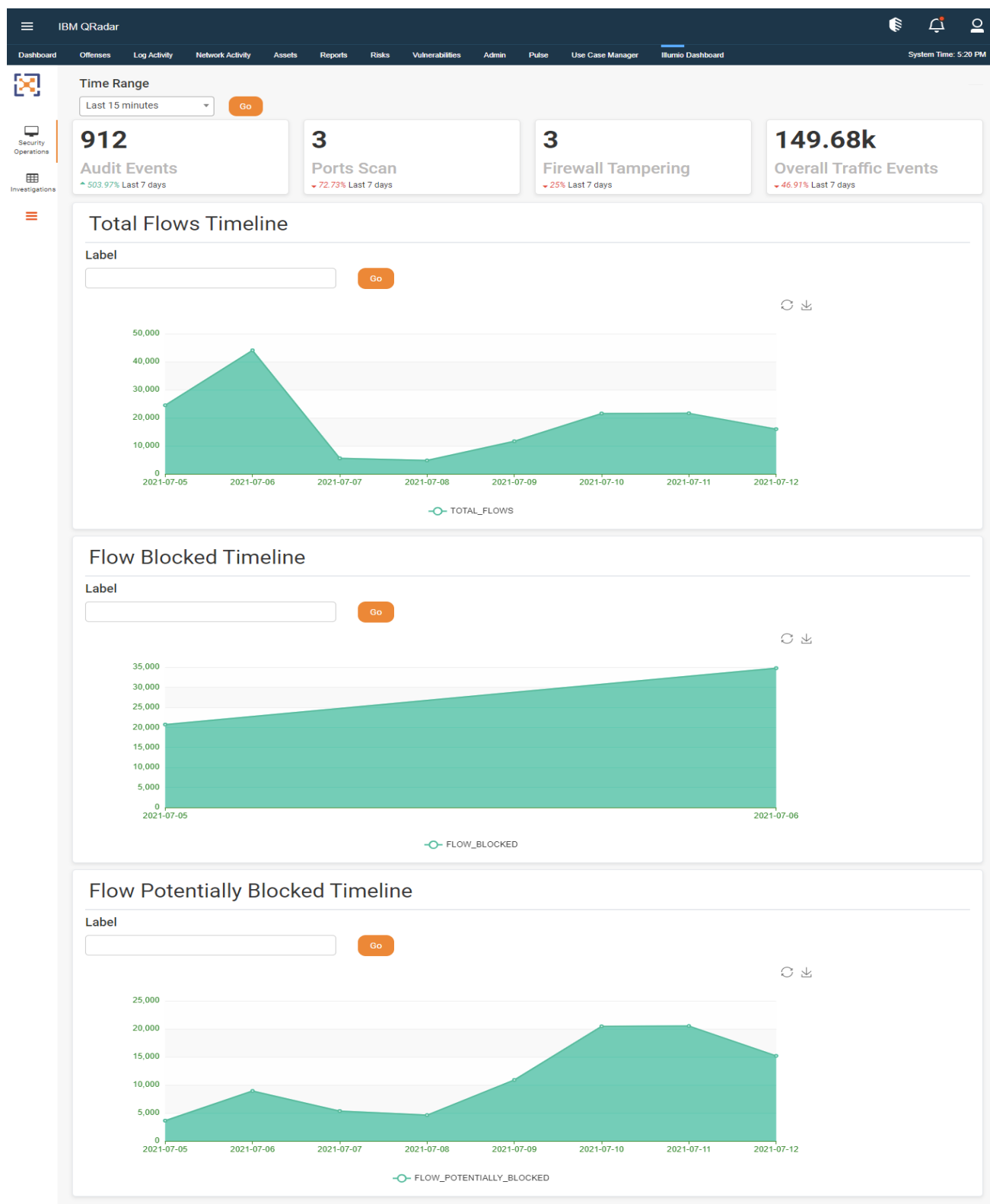
*Figure 6: Security Operations Dashboard*

## 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, Policy and Label. For Label filter, user can select from drop-down as well as type label value. If user types the label value then, label value must be in following format. LabelCategory:LabelValue. E.g. app:abc

Label Categories can be any of "app","role","env","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: User need to configure the account into configuration page in order to see the labels into label filter in dashboard. Do not use special characters while searching with label. Result may not be accurate.

The labels in this dashboard are from the fields `src_labels` and `dst_labels` in JSON (`srcLabels` and `dstLabels` in LEEF).
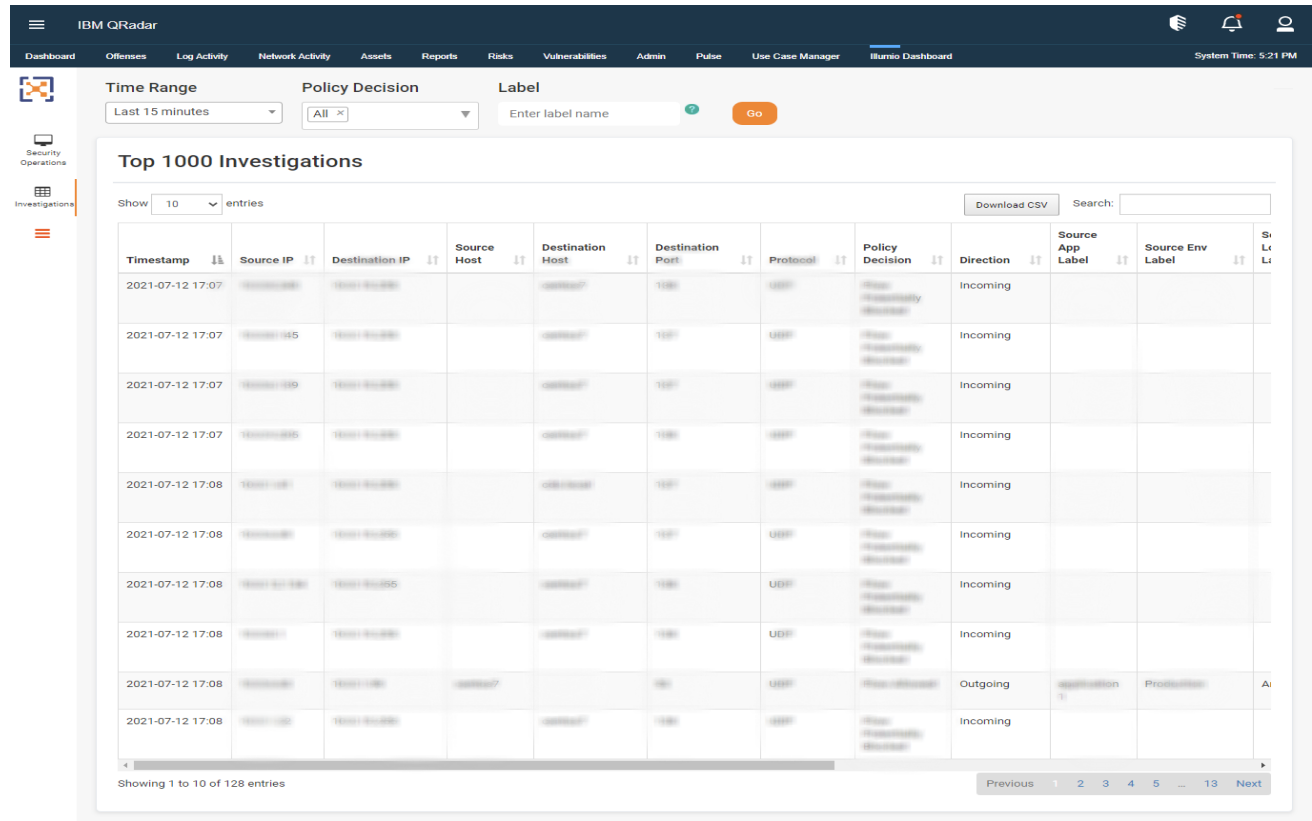
Figure 7: Investigation Dashboard
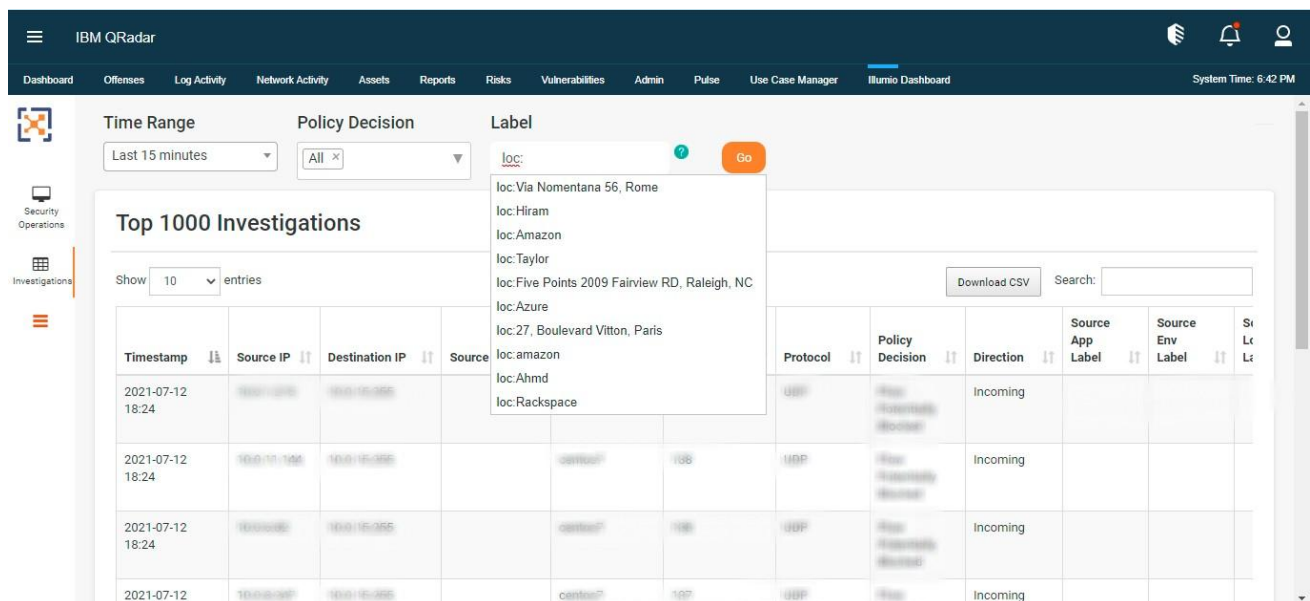


Figure 7.1: Investigation dashboard with labels suggestion in label filter

# Installation and Configuration

This section tells how to install the Illumio App for QRadar.

## Prerequisites

The following are required to run Illumio App v1.3.0 on QRadar:
- Illumio App Bundle (v1.3.0)
- QRadar version 7.4.1 or later
- Access to Illumio PCE
- Illumio credentials to access labels from PCEs

## Installation

The application installation requires access to the QRadar console through a web interface at https://<<QRadarconsoleIP>>/ For details about logging in to QRadar, see IBM QRadar documentation.*Figure 8: IBM QRadar 7.3.1 login screen*

1. Log in to the QRadar console.
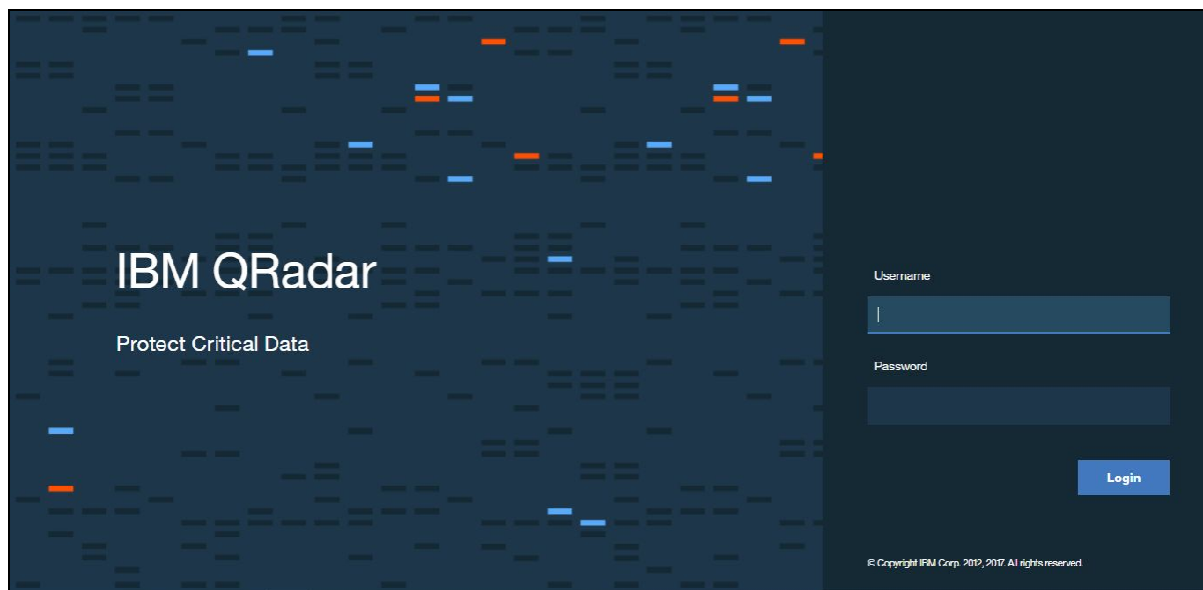


*Figure 8: IBM QRadar 7.3.1 login screen*

2. Go to Admin > Extension Management.
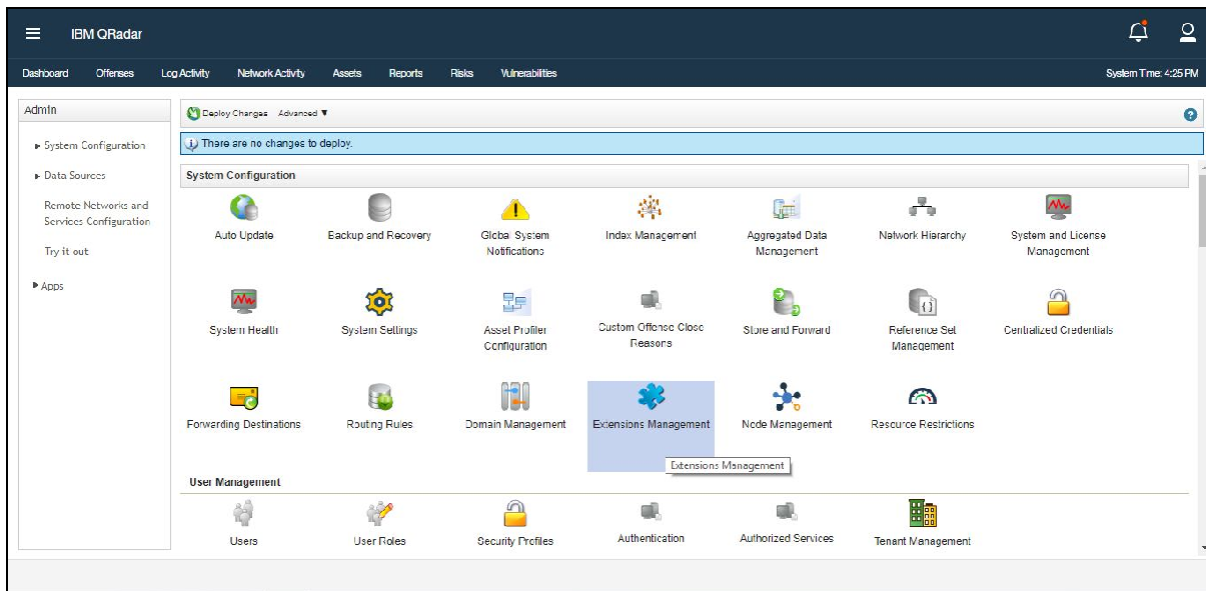


*Figure 9: IBM QRadar Admin Panel*

3. Click Add and choose the downloaded Illumio App zip file.
   QRadar prompts with a list of changes being made by the app.

4. Click Install.
   After the Application is installed, it will create a Docker container in the backend.

5. Deploy changes on the Admin Panel.

6. Refresh the browser window.
   The configuration page is displayed.

# App Configuration

After completing the installation, you must configure the app to start data collection.

1. If you just finished installing using the steps above, you are already in
   the Configuration page. Skip to step 2.

If you need to get to the Configuration page:

a)  Find the installed app on the QRadar Admin Panel under Apps.
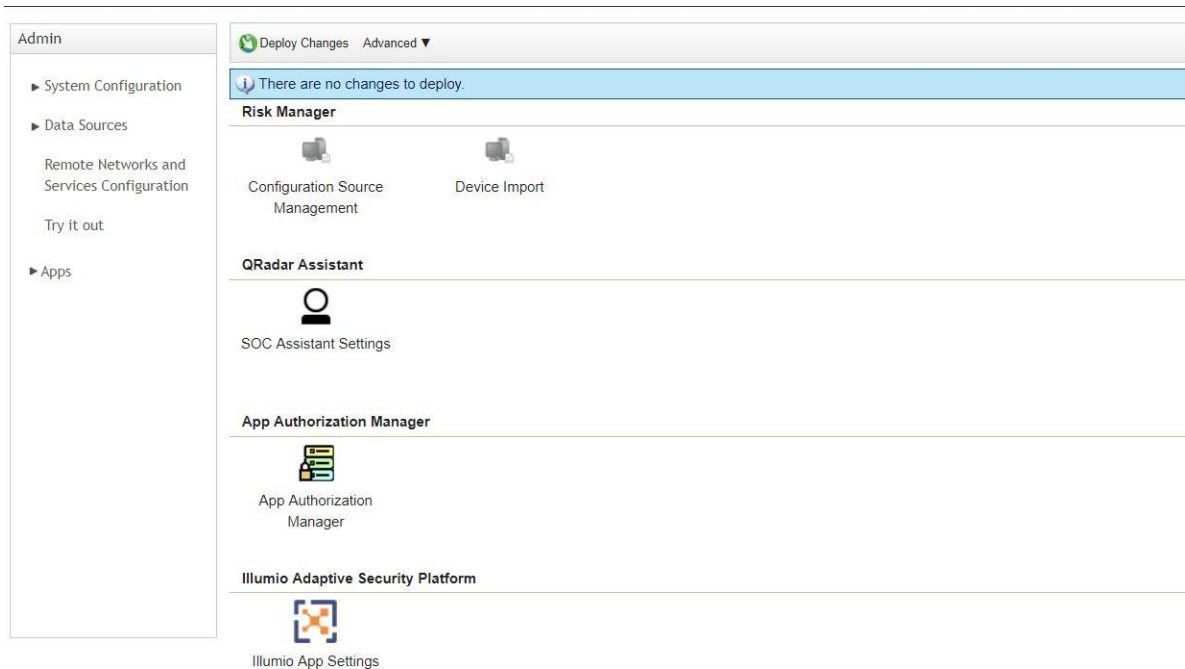


*Figure 10: Installed apps configuration page*

b)  Open the Illumio App configuration page.
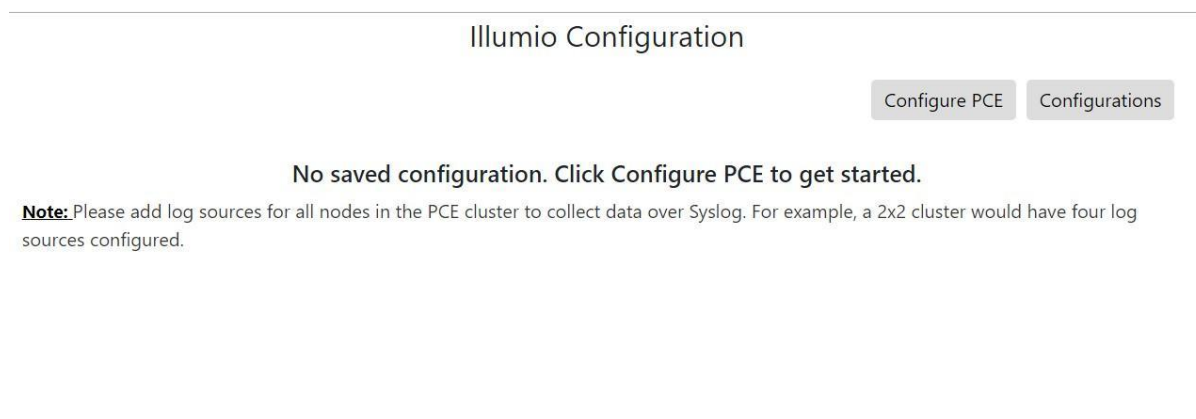


*Figure 11: Illumio App configuration page*

2. Click **Configure PCE**.

**Note:** The app supports multiple accounts for PCE configurations.



*Figure 12: New PCE Configurations form*

In the next screen, the Authorized Service Token is a value obtained from the QRadar App Authorization Manager.
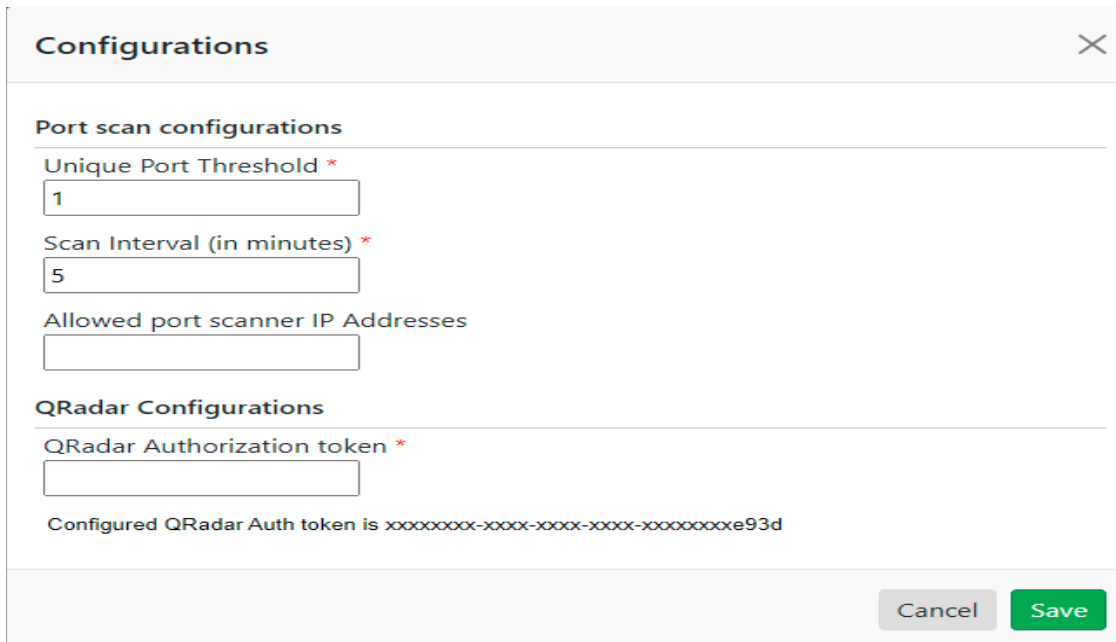
*Figure 13: General Configurations form*

3. Configure the PCE URL and your Illumio credentials, and your data collection will start, If Illumio PCE contains self-signed or internal ca certificate, make sure that certificates are present in QRadar. If not, perform these [steps to add certificate](#)
4. Saved credentials are listed, and you can edit or delete them.
5. You can set proxy to fetch data from Illumio PCE configurations.

## User Roles / Capabilities

QRadar supports ACL configurations for restricting access to different actions and dashboards. The Illumio App for QRadar adds a new capability, which 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.

To add a new QRadar role with Illumio dashboard capability, use the following steps.
**Note:** You can also add this capability to an existing role.

1. Log in to the QRadar console.
2. Go to Admin > User Roles.
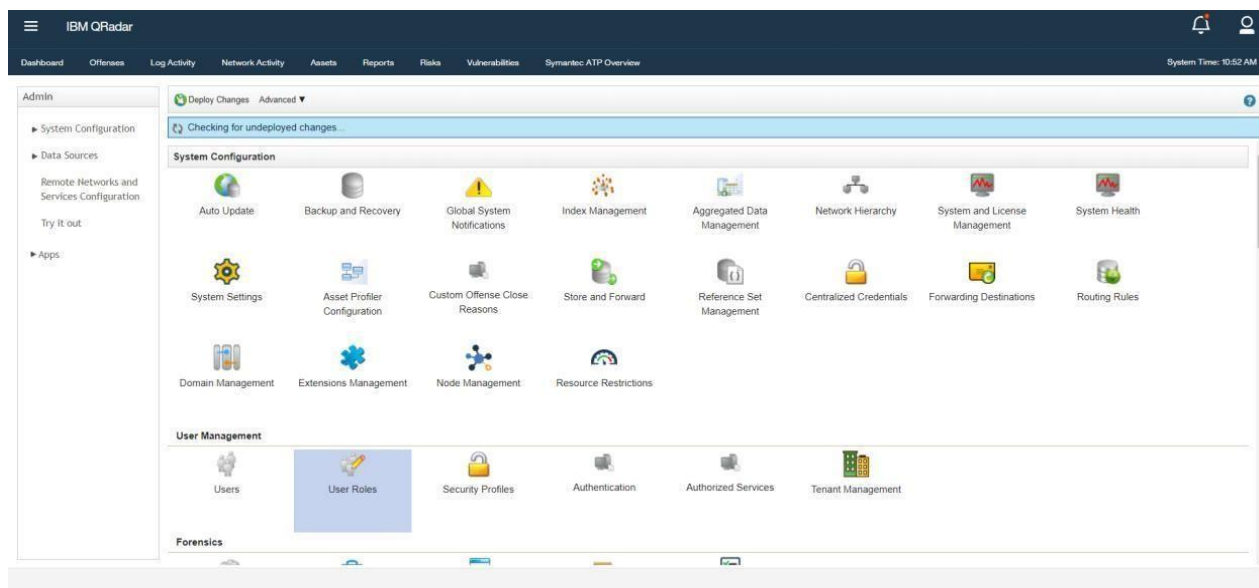
*Figure 14: User Role*

3. Click **New**.
4. Enter the name of the role.
5. Assign the Illumio Adaptive Security Platform capability, as shown in the screen shot.
6. Assign this role to Users who should be allowed to view Illumio dashboards.
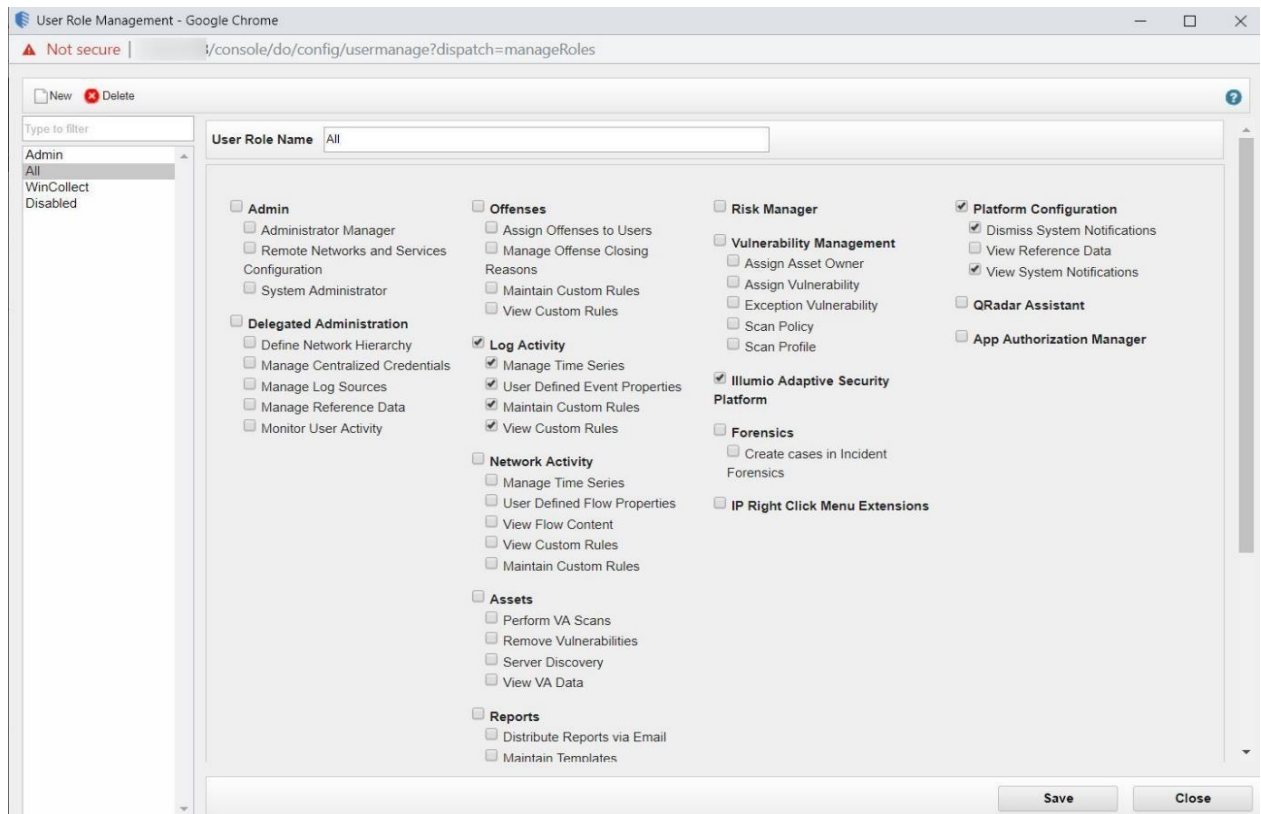
*Figure 15: Assign App Permissions*

## Adding 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. A separate log source needs to be created to collect data from each PCE.

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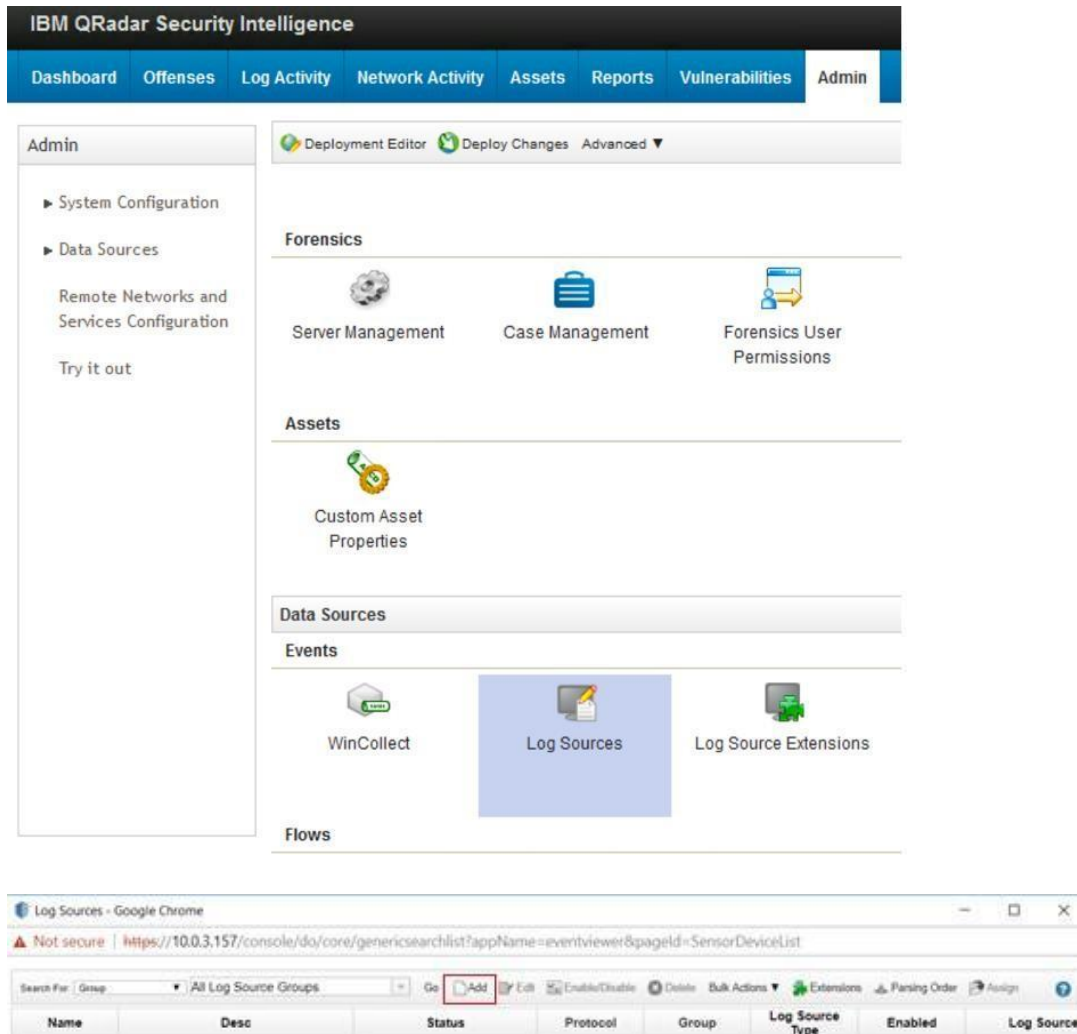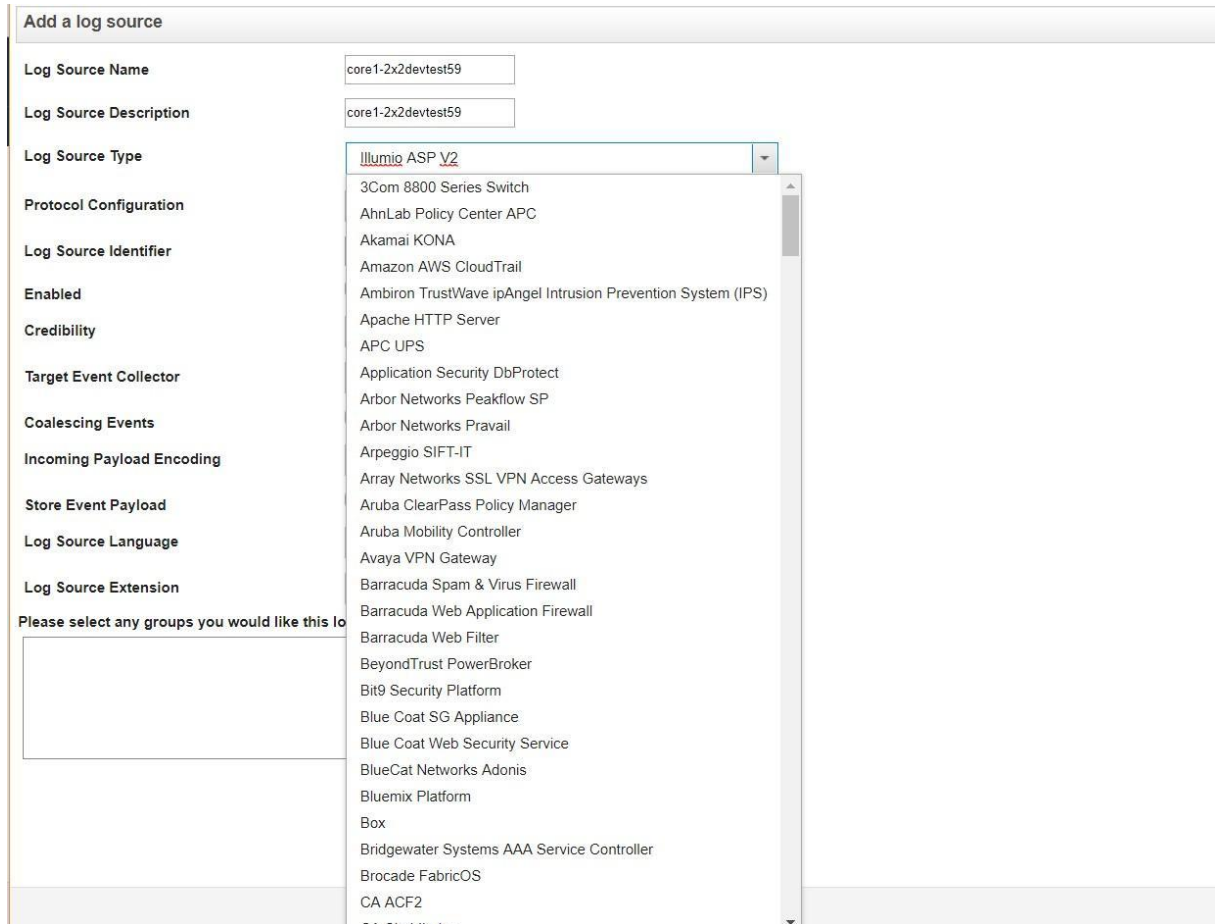


*Figure 2 and 3 Adding a Log Source*

2. Give the log source a suitable name for the PCE node. Add a description if desired.

3. In Log Source Type, select Illumio ASP V2.



*Figure 4 Selecting a Log Source Type as Illumio ASP V2*

4. In Protocol Configuration, choose Syslog.
5. In Log Source Identifier, enter the log source identifier as set in the syslog header on the host. This is typically the hostname. For example, core1-2x2devtest59.
6. Be sure Enabled is selected.
7. In Coalescing Events, deselect the collector that receives the events.
8. In Incoming Payload Encoding, choose UTF-8.
9. In Log Source Extension, choose IllumioASPCustom_ext.
10. Click **Save**.
11. In the Admin tab, click **Deploy Changes**.

12. Repeat these steps for all other core and database nodes in the cluster (for example, core1, db1, db0).

### Collecting Data from Amazon S3 bucket

#### Pre-requisite:

A log source with log source type "Illumio ASP V2" is required for collecting data from Amazon S3 bucket. If log source with "Illumio ASP V2" is not available then users can create it by following steps mention in Adding the PCE as a Log Source in QRadar section. Users can provide any valid log source identifier for log source type "Illumio ASP V2" if they are using it only for collecting data from Amazon S3 bucket.

To enable QRadar to receive events from the Amazon S3 buckets, Below two ways are possible:

- With an SQS queue
- With a directory prefix

#### With an SQS queue:

Users need to create a log source for collecting Illumio events from Amazon S3. Follow below steps :

1. On the Admin tab in QRadar, select Log Sources > Add.
2. Select a Log Source type: Amazon AWS CloudTrail
3. Select a protocol type: Amazon AWS S3 REST API
4. Name: Add a suitable name
5. Description: Add a suitable description
6. Enabled: True
7. Coalescing Events: False
8. Store Event Payloads: True
9. Log Source Identifier: Prefer to give same as Name to avoid confusion
10. Authentication Method: Access Key ID / Secret Key
11. Access Key ID: AWS S3 bucket access key ID
12. Secret Key: AWS S3 bucket Secret Key
13. S3 Collection Method: SQS Event Notifications
14. SQS Queue URL - URL of the created SQS Queue
15. Bucket Name: S3 bucket name
16. Event Format: LINEBYLINE
17. Use as A Gateway Log Source: True

a. Log Source Identifier Pattern: Please enter (=.*) after Illumio log source identifier i.e.{ILLUMIO_LOG_SOURCE_IDENTIFIER}=.*
   i. You can find log source identifier value from the "Illumio ASP v2" log source.
   ii. E.g.: If Illumio's log source identifier is **core0-2x2devtest59** than enter
   iii. **core0-2x2devtest59=. *** in this field.

**Note** - With the help of Gateway log source we can collect events from Amazon S3 bucket and parse those events as "Illumio ASP V2" log source type events as we are using "Illumio ASP V2" log souce type's identifier while configuring Gateway Log Source.

18. Show Advanced Options: True
    a. File Pattern: .*\.gz (To consume only .gz files from s3 bucket)
    b. File Pattern: .* (To consume all files from s3 bucket)
19. Automatically Acquire Server Certificate(s): Yes
20. Recurrence: How often the Amazon AWS S3 REST API Protocol connects to the Amazon cloud API, checks for new files, and if they exist, retrieve 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
21. EPS Throttle: Maximum number of events per second (EPS) that this log source should not exceed. (default:5000)
22. In the Admin tab, click **Deploy Changes.**


### With a directory prefix:

Users need to create a log source for collecting Illumio events from Amazon S3. Follow below steps:

1. On the Admin tab in QRadar, select Log Sources > Add.
2. Select a Log Source type: Amazon AWS CloudTrail
3. Select a protocol type: Amazon AWS S3 REST API
4. Name: Add a suitable name
5. Description: Add a suitable description
6. Enabled: True
7. Coalescing Events: False
8. Store Event Payloads: True
9. Log Source Identifier: Prefer to give same as Name to avoid confusion
10. Authentication Method: Access Key ID / Secret Key
11. Access Key ID: AWS S3 bucket access key ID
12. Secret Key: AWS S3 bucket Secret Key

13. S3 Collection Method: Use a Specific Prefix - Single Account/Region Only
14. Bucket Name: S3 bucket name
15. Directory Prefix: Root directory location on the AWS S3 bucket from which the files are retrieved. (directories are separated by '/')
16. Signature Version: AWS Signature V2
17. Event Format: LINEBYLINE
18. Use as A Gateway Log Source: True
    a. Log Source Identifier Pattern: Please enter (=.*) after Illumio log source identifier i.e.{ILLUMIO_LOG_SOURCE_IDENTIFIER}=.*
        i. You can find log source identifier value from the "Illumio ASP v2" log source.
        ii. E.g.: If Illumio's log source identifier is **core0-2x2devtest59** than enter
        iii. **core0-2x2devtest59=. *** in this field.

    **Note** - With the help of Gateway log source we can collect events from Amazon S3 bucket and parse those events as "Illumio ASP V2" log source type events as we are using "Illumio ASP V2" log souce type's identifier while configuring Gateway Log Source.

19. Show Advanced Options: True
    a. File Pattern: .*\.gz (To consume only .gz files from s3 bucket)
    b. File Pattern: .* (To consume all files from s3 bucket)
20. Automatically Acquire Server Certificate(s): Yes
21. Recurrence: How often the Amazon AWS S3 REST API Protocol connects to the Amazon cloud API, checks for new files, and if they exist, retrieve 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
22. EPS Throttle: Maximum number of events per second (EPS) that this log source should not exceed. (default:5000)
23. In the Admin tab, click **Deploy Changes.**

**Note:** After creating a log source make sure that SSL certificates of S3 buckets are present in the QRadar. If certificates are not present, then data from S3 bucket will not be collected.

Follow below steps to add certificates of S3 bucket.
1. Open QRadar via SSH
2. Run below command.
   /opt/qradar/bin/getcert.sh <bucket name>.s3.amazonaws.com

## Uninstalling the App

To uninstall the application:

1. In QRadar, go to the Admin page.
2. Open Extension Management.
3. Select Illumio App for QRadar.
4. Click **Uninstall**.

## Adding Illumio PCE SSL certificates in QRadar

In the Illumio app, we are collecting labels with SSL verification. If PCE contains self-signed or internal CA certificates, then user needs to perform below steps to add certificates in QRadar.

- Login into your QRadar console
- Go to admin panel
- Open configuration page of Illumio app.
- From configuration window of Illumio app, from above URL copy the app id, the number after /console/plugins/
  - E.g. suppose URL is:
    https://1.1.1.1/console/plugins/1062/app_proxy/index Copy "1062"

Perform below command on your QRadar instance via SSH.

- docker ps
- Find the Container id of Illumio App. (container id for Illumio app will be an image column containing a previous copied number. E.g. ...qapp-1062...)
- docker exec -it <container-id> /bin/bash (to go inside the docker)

Performed the following steps inside the docker container of the Illumio app v1.3.0:

- Copy/Move the certificate file of Illumio app from root to /etc/pki/ca-trust/source/anchors
- Run the commands given on page - https://www.ibm.com/docs/en/qsip/7.4?topic=sc-using-certificates-that-are-signed-by-internal-certificate-authority ,i.e.

      /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

- Restart the docker container of the app.

Note: When a user reinstall the app or docker container of Illumio App gets restarted, these changes might get reverted. In this case, user need to reperform these steps.

## Upgrade the Application to v1.3.0

To upgrade the application, the user needs to perform the following steps.
1. Remove all saved searches and custom properties associated with the log source type "Illumio ASP V2"
2. Go to Admin → Extension Management
3. Choose the downloaded zip file by clicking on **Add**.
4. The QRadar will prompt a list of changes being made by the app. Click on the install button. After the Application is installed it will create a Docker container in the backend.
5. "Deploy Full Configuration" in the Admin panel.
6. Clear cache of the browser and refresh and page.

**Note:** PCE filter functionality on dashboard is removed in Illumio App for QRadar v1.2.0. Users need to manually delete a reference table named "pce_nodes", else it will always remain there in QRadar after upgrading the app.

## QRadar Cloud Support

Illumio App for QRadar v1.3.0 supports all its functionalities on the QRadar cloud. If the PCE is installed on a port other than 443, contact IBM to open that port.

## Release Notes

v1.3.0
- 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 csv file.
- Added drilldown from the single value panels in Security Operations Dashboard.
- Bug fixes.

## Checking logs of the Application

Users can see the application logs by accessing the application from the QRadar via SSH.

1. Login into QRadar via SSH
2. lists all installed applications and their App-ID values using below command -

   `/opt/qradar/support/recon ps`

3. If no issues are detected, the recon command output might look like the following example:

   

4. Connect to the app container -

   `/opt/qradar/support/recon connect APP-ID`

   **Note** - For `the above image App-ID is 4352 for Illumio app.`

5. Go to log dir -

   `cd /opt/app-root/store/log`

6. Once inside the log directory, You can view them with a command like '*ls*' to list all files and *'cat'* to print log file content.

   `ls`

   `cat app.log`

app.log – Contains all the logs related to the configuration page and dashboard.

label_data_collect.log – Contains logs related to label collection from Illumio PCE.

# Troubleshooting

This section describes the common issues that might happen when deploying or running the app and the steps to resolve the issues.

## 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 might be searching for events pertaining 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 |

*Figure 16: Custom Message Issue*
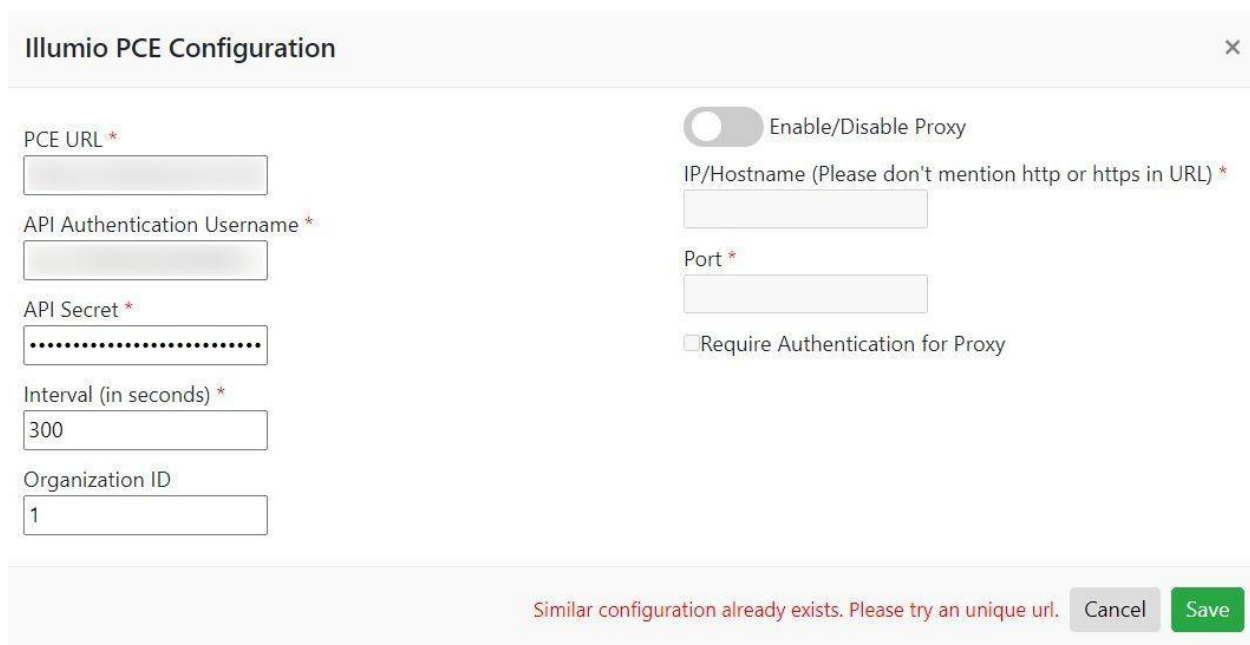
**Cause:** This issue can be caused by improper Event ID and Event Category extractions. If any new type of event appears in the Log Source and its Event ID or Event Category extractions are not written, then the value of that property will be empty.

**Troubleshooting Steps:**

1. Go to Log Activity.
2. In Filter Log Source Type, choose Illumio ASP V2.
3. In the Views filter, select Last 7 Days.
4. Right click on the event that has the IllumioASPCustom Message.
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 are unknown, create a support ticket with Illumio Support.

## Configuration Fails: Configuration Exists

**Problem:** New configuration fails with error message "Same configuration already exists. Please try a unique url".



*Figure 17: Duplicate credentials error*

**Troubleshooting Steps:** You might have entered an account which is already configured. Enter new credentials which have not already been provided.

## Configuration Fails: Error Checking Configurations

**Problem:** Configuration of Illumio fails with error message "Error occurred while checking for same configurations. Check logs for more details."
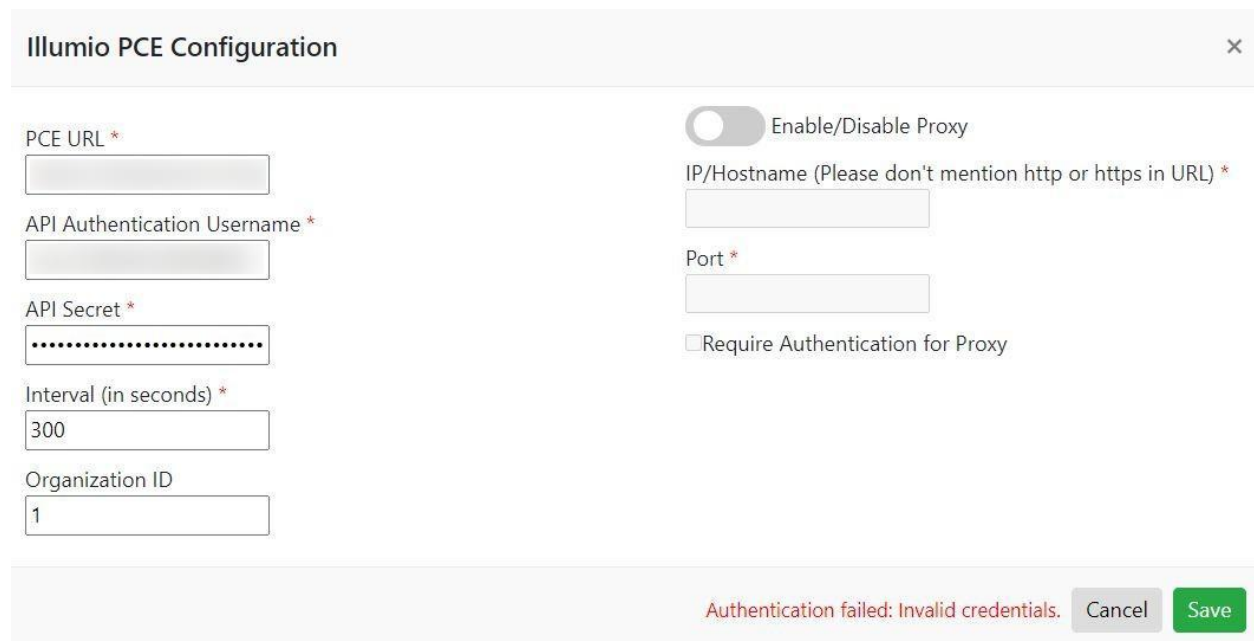
*Figure 18: Similar Configuration Check error*

**Troubleshooting Steps:** This happens while the app is checking for similar configurations. Try the configuration once again. Check app.log log file for more details. To check logs, follow the steps of Checking logs of the Application

## Configuration Fails: Authentication

**Problem:** New configuration fails with error message "Authentication failed. Invalid credentials".



*Figure 19: Incorrect Credentials error*

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

## Configuration Fails: Service Token Invalid

**Problem:** New configuration of Illumio App fails with error message "Authorized Service Token is invalid. Please check your Authorized Service Token".



*Figure 20: Incorrect Authorized Service error*

**Troubleshooting Steps:** You have entered an incorrect Authorized Service Token. Check the token and try again.

# Configuration Fails: Error Validating Authorization Token

**Problem:** Configuration of Illumio App fails with error message "Error occurred while validating authorization token".



*Figure 21: Authorized Service Token Check error*

**Troubleshooting Steps:** This happens while the app is checking the Authorized Service Token. Try once again. Check app.log log file for more details. To check logs, follow the steps of Checking logs of the Application

## Configuration Fails: Network Connection Timeout

**Problem:** Configuration of Illumio App fails with the error message "Failed due to network connection timeout".



*Figure 22: Network connection timeout error*

**Troubleshooting Steps:** The app is not able to connect to the server. There might be a network issues. If you have proxy in your network, try to save credentials with proxy. Check app.log log file for more details. To check logs, follow the steps of Checking logs of the Application

## Configuration Fails: Error while authenticating credentials

**Problem:** New configuration fails with error message "Error while authenticating credentials. Check logs for more details."



*Figure 23: Connection error*

**Troubleshooting Steps:** 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 app.log log file for more details. To check logs, follow the steps of [Checking logs of the Application](#)

## Error message on configuration page

**Problem:** On opening the configuration page it shows an error message "Something went wrong. Check logs for more details."
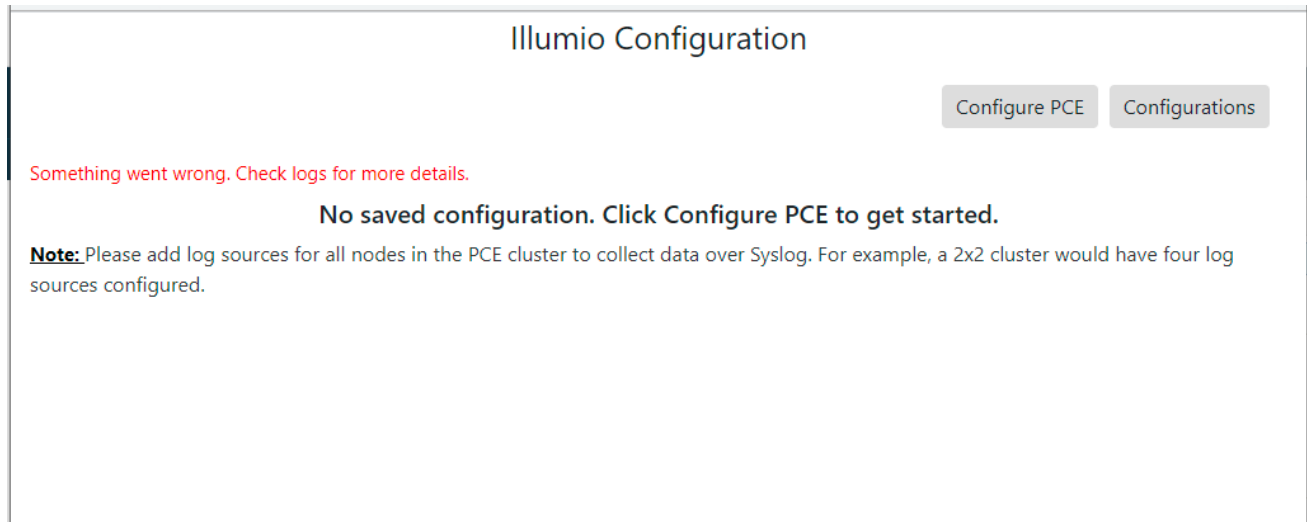
Illumio Configuration

Configure PCE    Configurations

Something went wrong. Check logs for more details.

No saved configuration. Click Configure PCE to get started.

**Note:** Please add log sources for all nodes in the PCE cluster to collect data over Syslog. For example, a 2x2 cluster would have four log sources configured.

*Figure 24:Secret Data Error*

**Troubleshooting Steps:** 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 issue is that files of secret data are tamere. Check app.log log file for more details. To check logs, follow the steps of [Checking logs of the](#) [Application](#)

## Events Unknown

**Problem:** Illumio App events are shown in QRadar as Unknown.

**Troubleshooting steps:**
1. Go to Log Activity.
2. Set Filter Log Source Type to Illumio ASP V2.
3. In Views, select Last 7 Days.
4. If any events are shown as Unknown**:**
    a. Right click on the 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 are unknown, create a support ticket with Illumio

## Data Not Collected

**Problem:** Data is not getting collected by the app.

**Troubleshooting steps:**
1. Follow the steps of General Troubleshooting

## UI Issues

**Problem:** Any dashboard panel, configuration page, or chart 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. QRadar queries might expire if too much data is being matched in the query.

## Reinstalling the App

**Problem:** The application is exhibiting undesired behavior and troubleshooting steps have failed to fix the issue.

**Troubleshooting Steps:** To reinstall the app:
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 the Admin panel > Log Sources.
3. Uninstall the app. See Uninstalling the App.
4. Refresh the page and check to be sure the Dashboard tab of Illumio Overview is not seen after uninstallation.
5. Now install the app from Extension Management. See Installation.

## General Troubleshooting

**Problem:** If you encounter a problem that is not described in this document, follow these steps:

1. Click on System and License Management in the Admin Panel.
2. Select the host on which the Illumio App is installed.
3. In the top panel, click Actions, and select Collect Log Files. The Log File Collection window opens.
4. Click Advanced Options.
5. Click these checkboxes:
   - Include Debug Logs
   - Application Extension Logs
   - Setup Logs (Current Version)
6. For data input, select 2 days.
7. Click Collect Log Files.
8. Click the link "Click here to download files." This will download all the logs in a single zip file on your local machine.
9. Create a support case with Illumio and attach the zipped-up log files.

-- END OF DOCUMENT--