Proofpoint

Proofpoint on Demand Email Security App V2

V2.0.0

Contents

Architecture

IBM QRadar SIEM is a network security management platform that provides situational awareness and compliance support.

The PoD Logging service is a web service for Proofpoint on Demand customers that offers a real-time email processing log feed for use with Security Information and Event Management (SIEM) solutions

Proofpoint OnDemand Email Security ingests mail and message log into QRadar. The app consists of the following parts:

- Data collection
- Parsing
- Visualization(Dashboard)

Data Collection

- The PoD Logging Service production endpoint is wss://logstream.proofpoint.com/
- The API signature is /v1/stream?cid={clusterId}&type=[message|maillog]&sinceTime={sinceTime}&toTime={toTime}
- A web socket connection is created to receive data of mail and message log
- Make API calls to https://tap-api-v2.proofpoint.com/v2/siem/all?format=json&threatStatus=falsePositive&threatStatus=active&threatStatus=cleared&sinceTime=2019-06-17T13:49:15Z to fetch the TAP events
- For TAP integration, when a user is configured first time or deletes the configuration and reconfigured, in these cases it will collect data for the last 12 hours from the current UTC time.

Parsing

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

- **Protocol:** It defines how data gets into QRadar.
- **DSM:** 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.

Proofpoint OnDemand Email Security DSM

The custom DSM is used for correctly assigning event name and event categories to Proofpoint events. The event name and event categories are identified using QIDS. Following table lists Proofpoint events to QID mapping. All the events with event id other than one mentioned in the table below will have “Unknown” for event name and event category.

Event ID	QID Name	High-Level Category	Low-Level Category
message_log	Proofpoint Message Log	Application	Mail
mail_log	Proofpoint Mail Log	Application	Mail

Proofpoint TAP DSM

The custom DSM is used for correctly assigning event name and event categories to Proofpoint events. The event name and event categories are identified using QIDS. Following table lists Proofpoint TAP events to QID mapping. All the events with event id other than one mentioned in the table below will have “Unknown” for event name and event category.

Event ID	QID Name	High-Level Category	Low-Level Category
clicksBlocked	Clicks Blocked	Application	Mail
clicksPermitted	Clicks Permitted	Application	Mail
messageBlocked	Message Blocked	Application	Mail
messageDelivered	Message Delivered	Application	Mail

Custom Property Extraction

We have written a custom JSON key path to extract various Proofpoint properties. In QRadar we can associate particular custom property extraction to event name or event category. This will ensure that a particular field is extracted only for matching event names. The following table specifies a list of fields along the event name for which it will be extracted.

Custom Property	Expression
Action DKIMV	/"action_dkimv"[]
Action DMARC	/"action_dmarc"[]
Action SPF	/"action_spf"[]
Campaign Id	/"campaignID"
Campaign Id	/"campaignId"
Classification	/"classification"
Connection TLS Inbound Version	/"connection"/"tls"/"inbound"/"version"
Event Time	/"eventTime"
Event Type	/"eventType"
Filter Disposition	/"filter"/"disposition"
Filter Quarantine Folder	/"filter"/"quarantine"/"folder"
Filter Route Direction	/"filter"/"routeDirection"
Final Module	/"final_module"
Final Rule	/"final_rule"
GUID	/"GUID"
Impostor Score	/"impostorScore"
Labeled Name	/"msgParts"[0]/"labeledName"
Labeled Name 1	/"msgParts"[1]/"labeledName"
Labeled Name 2	/"msgParts"[2]/"labeledName"
Labeled Name 3	/"msgParts"[3]/"labeledName"
Labeled Name 4	/"msgParts"[4]/"labeledName"
Malware Score	/"malwareScore"

Message Header From	/"msg"/"header"/"from"[]
Message Header ID	/"msg"/"header"/"message-id"[]
Message Header Subject	/"msg"/"normalizedHeader"/"subject"[]
Message Header To	/"msg"/"header"/"to"[]
Message Time	/"messageTime"
MessageID	/"messageID"
Phish Score	/"phishScore"
Queue ID	/"QID"
Recipient	/"recipient"
Recipient	/"recipient"[]
Sender	/"sender"
Sender IP	/"senderIP"
Spam Score	/"spamScore"
Spam Type	/"SpamType"
Threat	/"threat"
Threat Type	/"threatType"

Upgrade

Upgrade app to v2.0.0

1. Users can upgrade only from the v1.1.3 app version published on XFE portal. Follow the same steps of installation to install the new version.
2. Clear the browser cache and refresh the page.
3. Follow the below steps to delete CEPs if Proofpoint app version older than v1.1.3 is installed.
4. Log on to the QRadar console.
5. Go to Admin → Custom Event Properties. In the search box enter the keyword “Proofpoint TAP”.
6. Delete below listed CEPs. (Make sure the associated log source type is “Proofpoint TAP”)
    a. Threat
    b. Classification

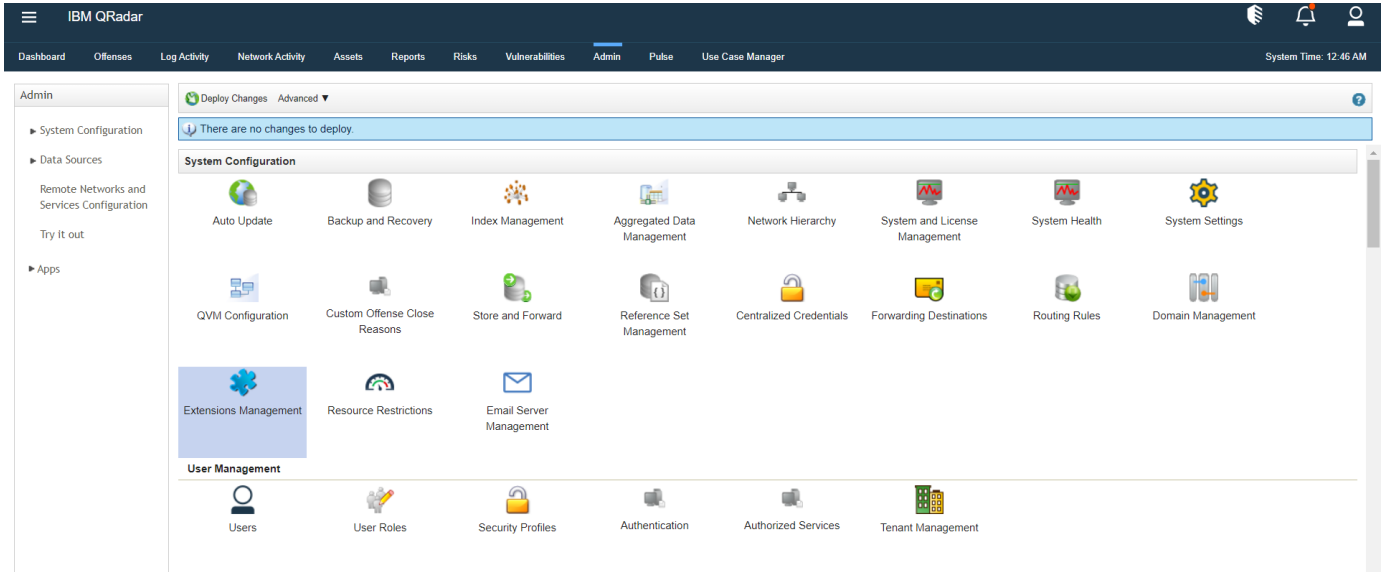
Installation

Prerequisites

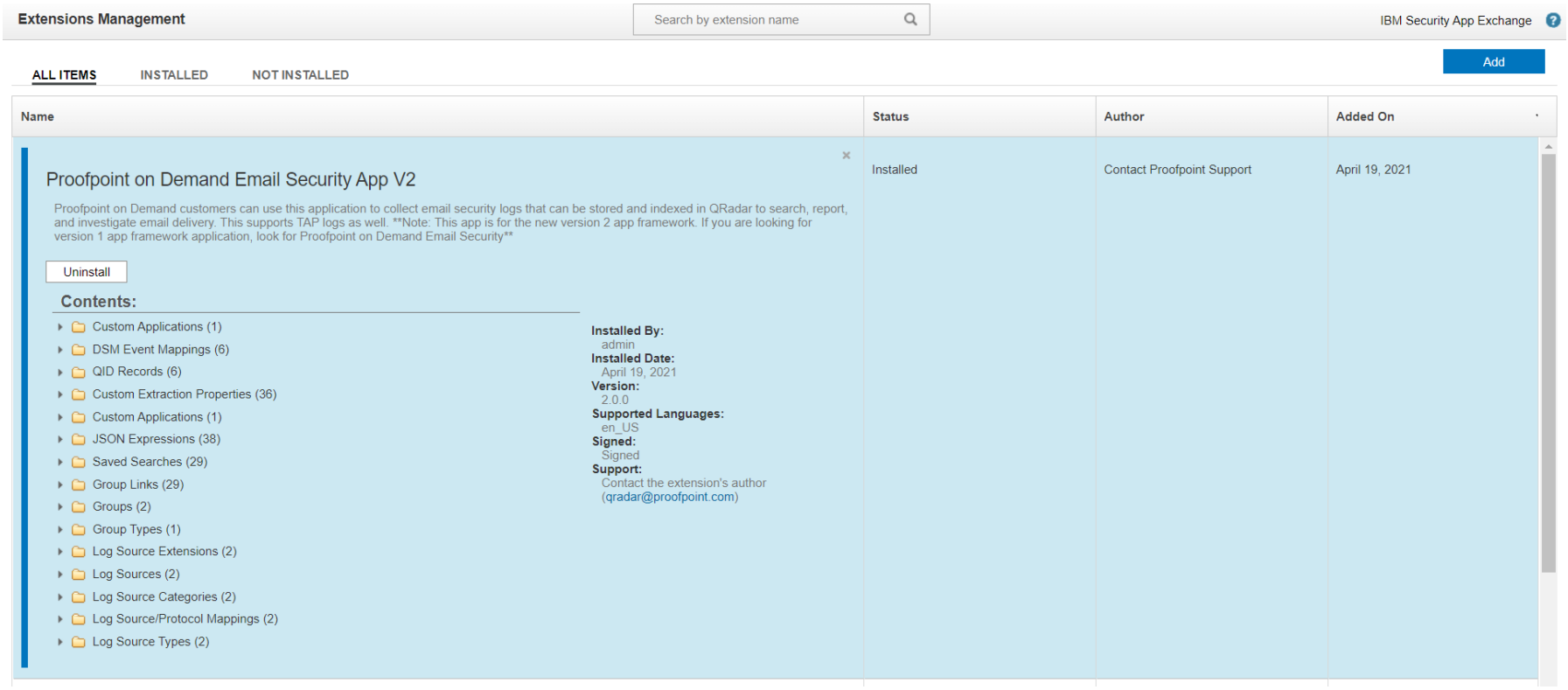
- QRadar version: 7.4.1 P2+

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

a. Login to QRadar console.
b. Go to Admin → Extension Management.



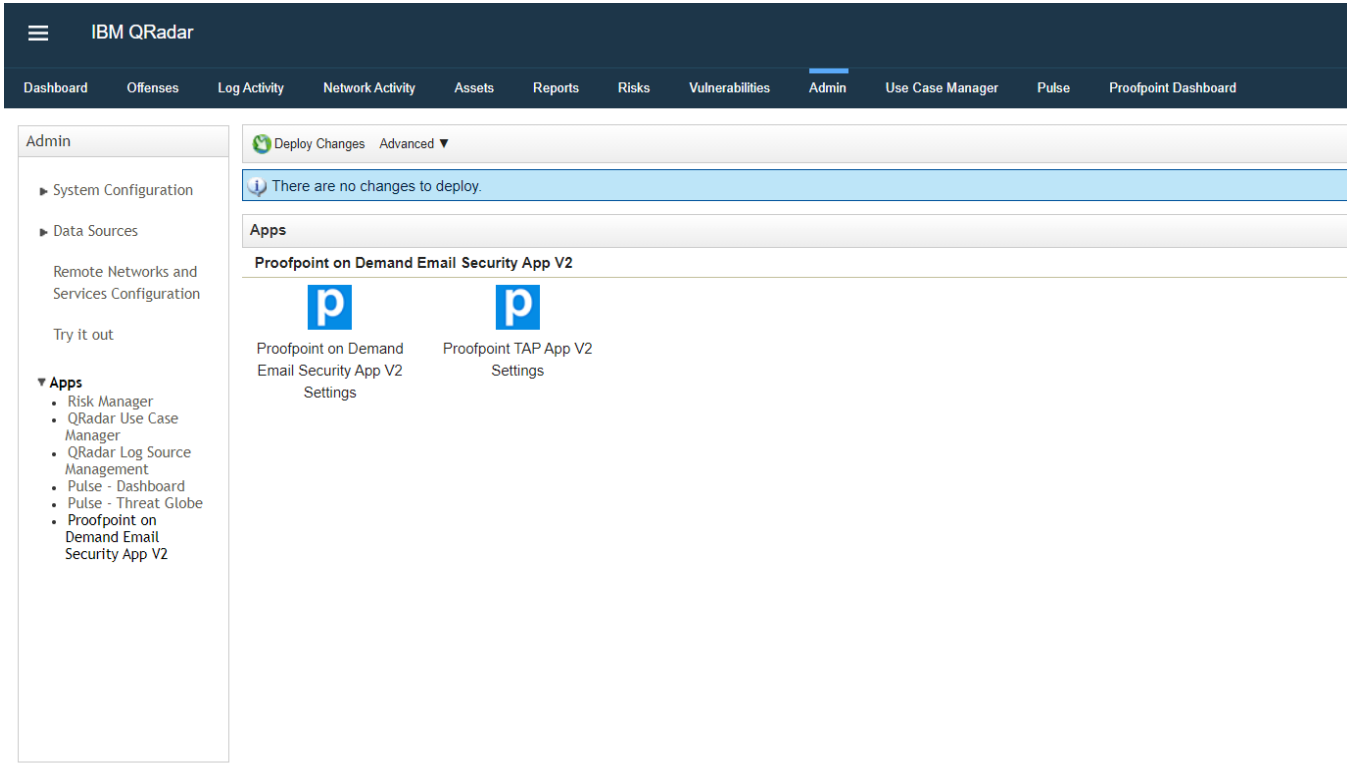
c. Choose the downloaded zip file by clicking on “Browse”.
d. The QRadar will prompt a list of changes being made by the app. Click on the “Install” button. After the Application is installed it will show all the components as shown below:



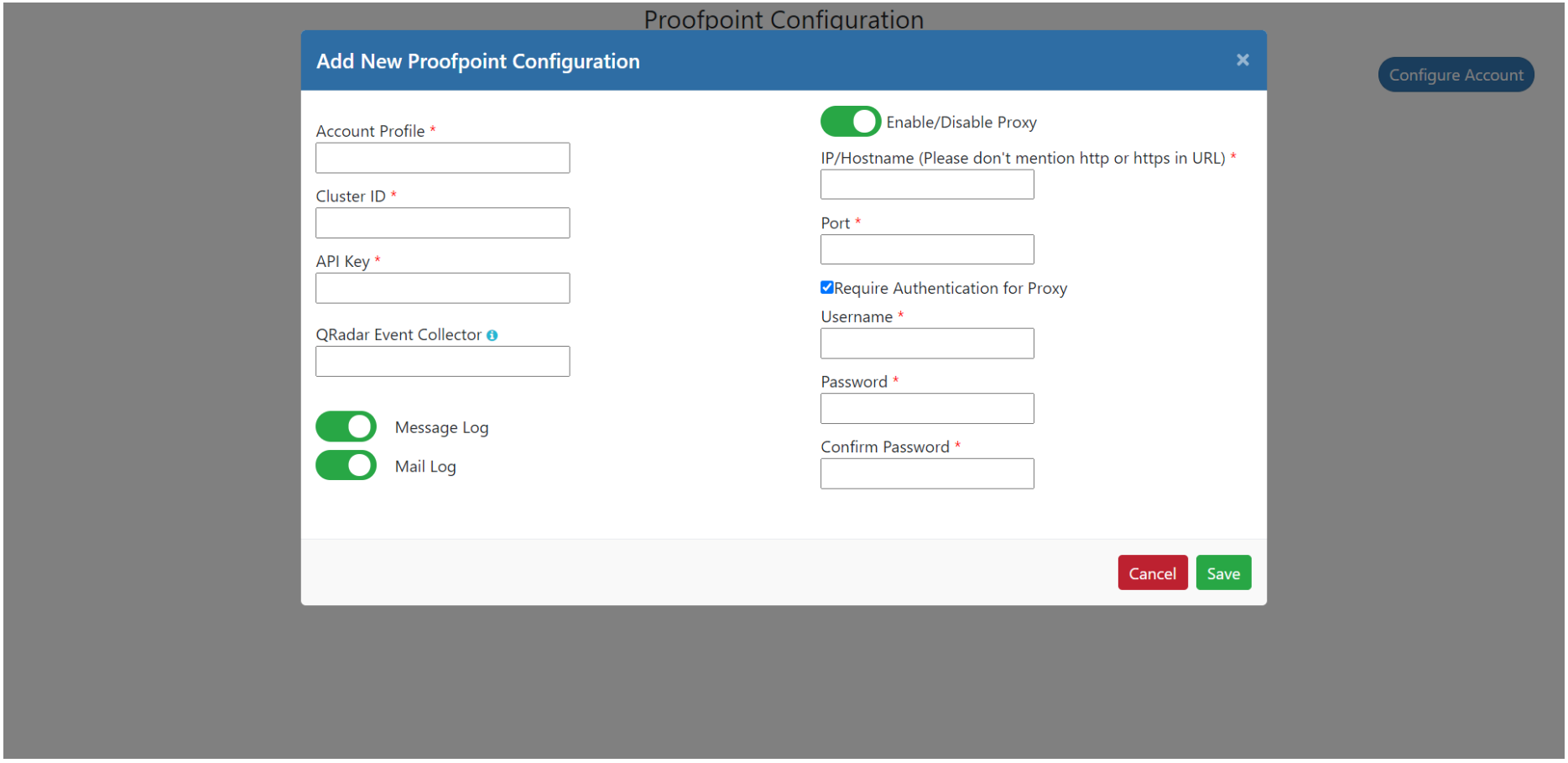
Configuration

In order for QRadar to start receiving data from Proofpoint data collection must be enabled. To enable data collection, perform the following steps:

a. Login to QRadar console.
b. Go to Admin → Apps → Proofpoint on Demand Email Security App V2



c. To configure Proofpoint On Demand Email settings, click on “Proofpoint on Demand Email Security App Settings” and enter the details:



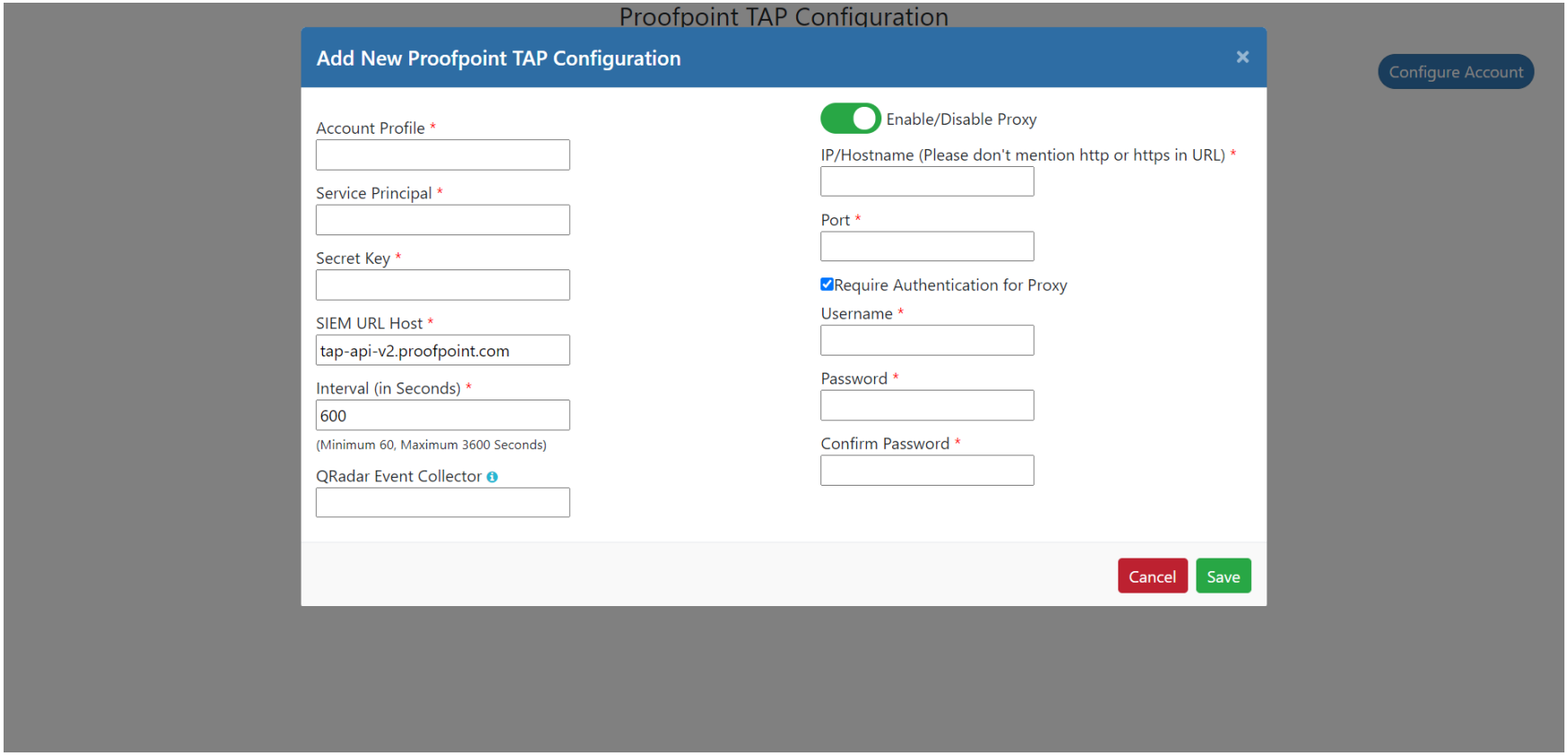
Configuration Fields:

- Account Profile: User should enter a Profile name.
- Cluster ID: User should enter Cluster ID.
- API Key: User should enter the On Demand API Key.

- QRadar Event Collector: If kept blank, it takes the default console IP address/hostname. User can enter the IP address/hostname of the Event Collector appliance.
  NOTE: The app does not verify whether the entered IP address/hostname is of Event Collector appliance.
- Enable/Disable proxy: It is a toggle to enable/disable proxy. The user should select its value depending on their environment.
- IP/Hostname: IP/Hostname of the proxy server without prefixing with http/https.
- Port: Port of the proxy server
- Require Authentication for Proxy: User should check this box if he is using Authenticated proxy.
- Username: Username of the Authentication proxy
- Password: Password of the Authentication proxy
- Confirm Password: Re-enter Password of the Authentication proxy

NOTE:
- The fields with asterisk (*) are mandatory

d. To configure the Proofpoint TAP, click on Proofpoint TAP App V2 settings and enter service principal and secret key.



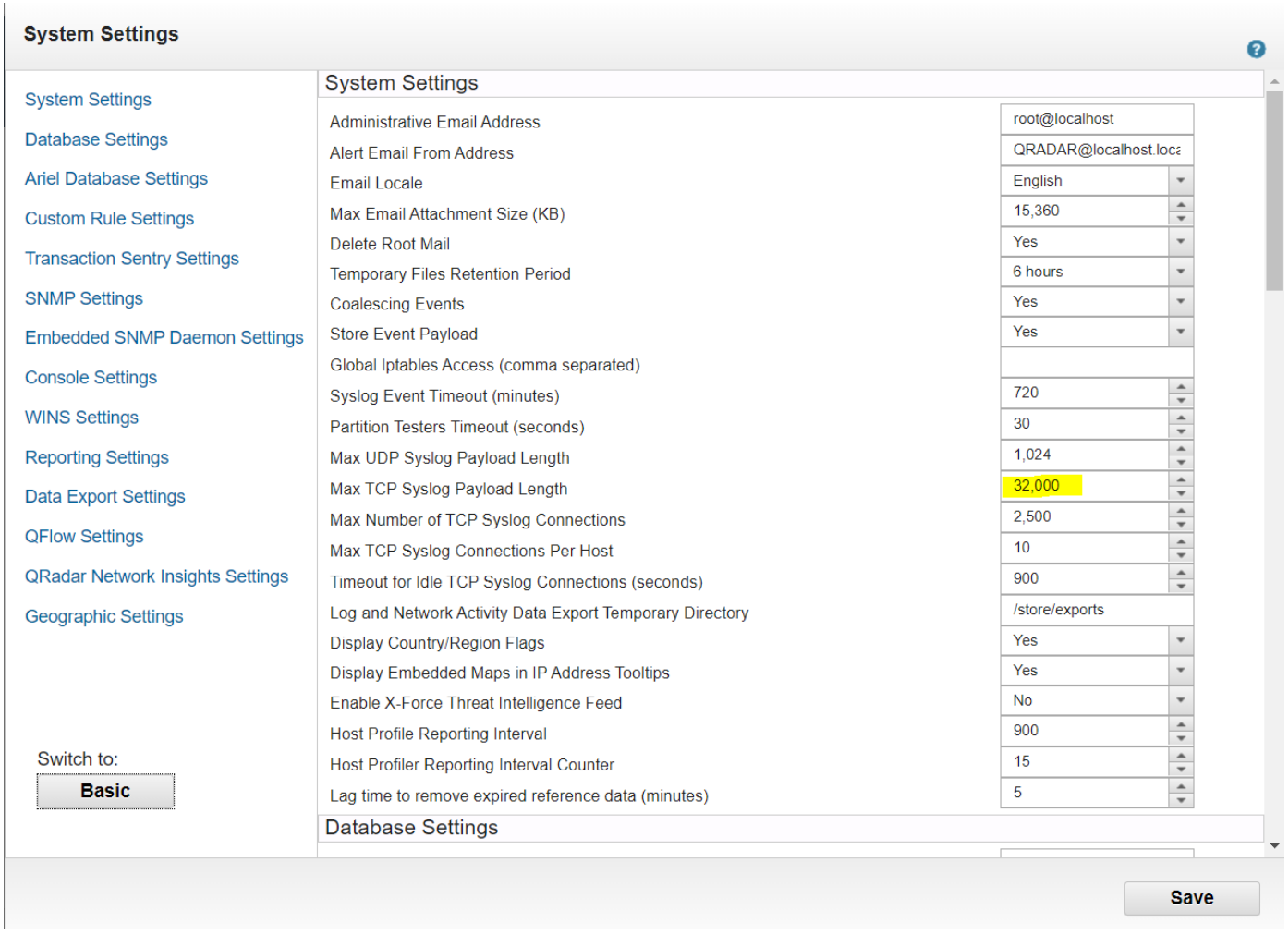
Configuration Fields:

- Account Profile: User should enter a Profile name of their choice.
- Service Principal: User should enter Service Principal.
- Secret Key: User should enter the TAP Secret Key.
- SIEM URL Host: API endpoint for collecting TAP data. Users cannot edit this field.
- Interval: It is the number of seconds after which API will be called every time during real time data collection. By default, it will be populated with 600 seconds.

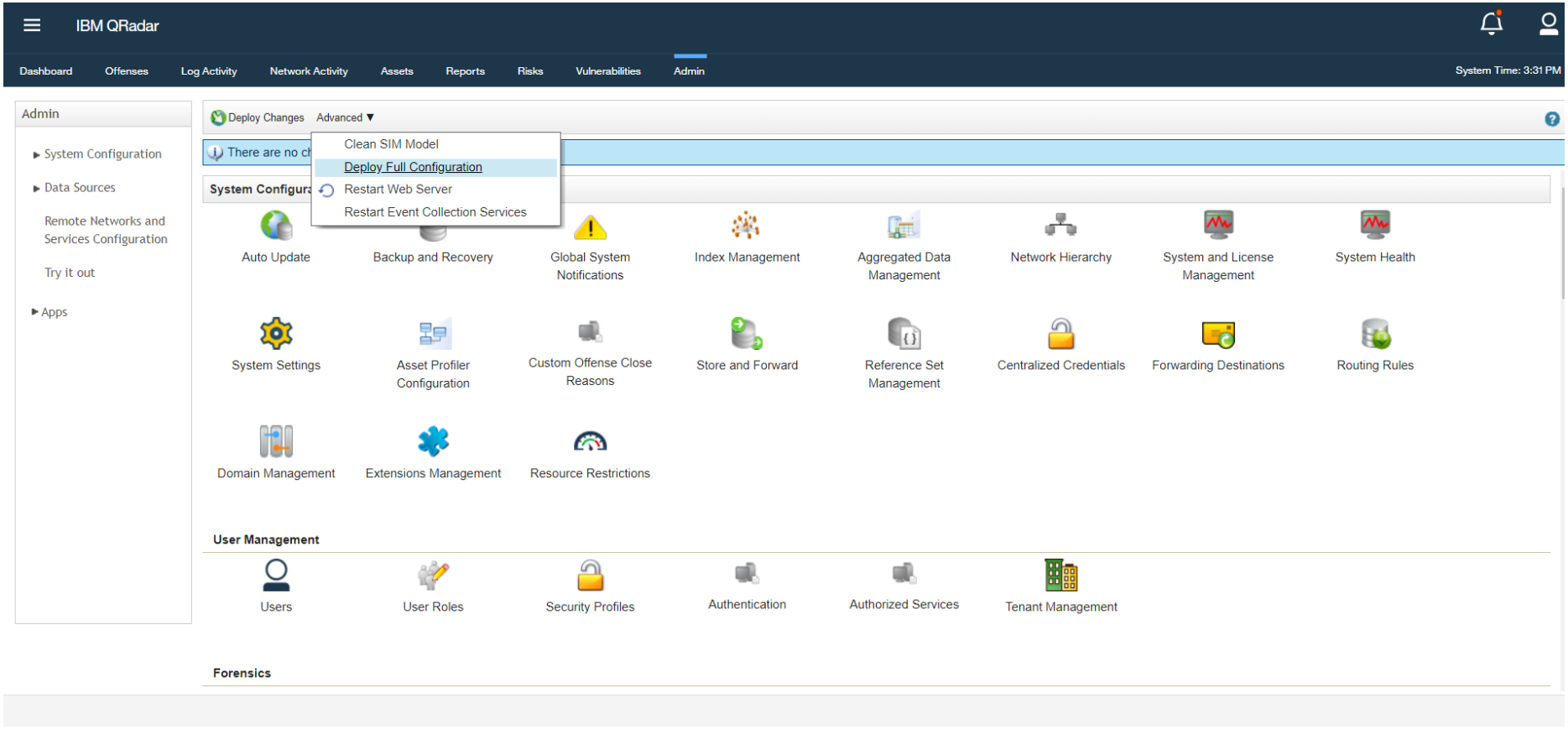
- QRadar Event Collector: User can enter the IP address/hostname of the Event Collector appliance. If kept blank, it takes the default console IP address/hostname.
  NOTE: The app does not verify whether the entered IP address/hostname is of Event Collector appliance.
- Enable/Disable proxy: It is a toggle to enable/disable proxy. The user should select its value depending on their environment.
- IP/Hostname: IP/Hostname of the proxy server without prefixing with http/https.
- Port: Port of the proxy server
- Require Authentication for Proxy: User should check this box if he is using Authenticated proxy.
- Username: Username of the Authentication proxy
- Password: Password of the Authentication proxy
- Confirm Password: Re-enter Password of the Authentication proxy

NOTE:
- The fields with asterisk (*) are mandatory

e. Now navigate to System Settings via Admin Panel .
f. Click on Advanced.
g. Change the value of Max TCP Payload Length from 4096 to 32000.



h. Click on Save.
i. Deploy Full Configuration and Restart Event Collection Services.


IBM QRadar
Dashboard
Offenses
Log Activity
Network Activity
Assets
Reports
Risks
Vulnerabilities
Admin
System Time: 3:31 PM
Admin
System Configuration
Data Sources
Remote Networks and Services Configuration
Try it out
Apps
Deploy Changes
Advanced
Clean SIM Model
Deploy Full Configuration
Restart Web Server
Restart Event Collection Services
There are no ch
System Configura
Auto Update
Backup and Recovery
Global System Notifications
Index Management
Aggregated Data Management
Network Hierarchy
System and License Management
System Health
System Settings
Asset Profiler Configuration
Custom Offense Close Reasons
Store and Forward
Reference Set Management
Centralized Credentials
Forwarding Destinations
Routing Rules
Domain Management
Extensions Management
Resource Restrictions
User Management
Users
User Roles
Security Profiles
Authentication
Authorized Services
Tenant Management
Forensics

Uninstalling the Application

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

1. Go to the Admin Page.
2. Open Extension Management.
3. Select Proofpoint on Demand Email Security App V2.
4. Click on Uninstall.

NOTE:

- On uninstalling the app, all the Custom Event Properties, Log source (included in app bundle), Saved search, and Dashboards will be removed.
- On uninstalling the app, removal of Log source type, Log source extension, DSM mapping(including QID) is not supported by QRadar yet.

Release Notes

v2.0.0

- Added support of QRadar App framework 2
- Code migration from python2 to python3
- Updated jQuery
- Added support for collecting Proofpoint events on the specific Event Collector Instance instead of the Console
- Changed Proofpoint logo on Configuration page and dashboards

Steps to check logs:

Users can go inside the application docker container. In the docker container user can see logs.

1. Follow steps for accessing the docker container of the Proofpoint App. Click here
2. cd /opt/app-root/store/log (For navigating to log directory)
3. ls (For getting list of all logs files)

Steps to access application Docker container:

Users can go inside the application docker container. In the docker container, users can see logs and configure some parameters.

1. Login into your QRadar Instance.
2. Go to the Admin panel.
3. Open any configuration page of Proofpoint App for QRadar.
4. From the URL of Configuration window of Proofpoint app, copy the app id, the number after /console/plugins/, e.g. suppose URL is: https://198.51.100.0/console/plugins/1062/app_proxy/index, Copy "1062".

Perform below command on your QRadar instance via SSH.

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

Now we are in the docker container.

Visualization

This application uses python's flask framework and various open source JavaScript frameworks to extend the capability of QRadar to visualize Proofpoint OnDemand Email Security events.

Dashboards:

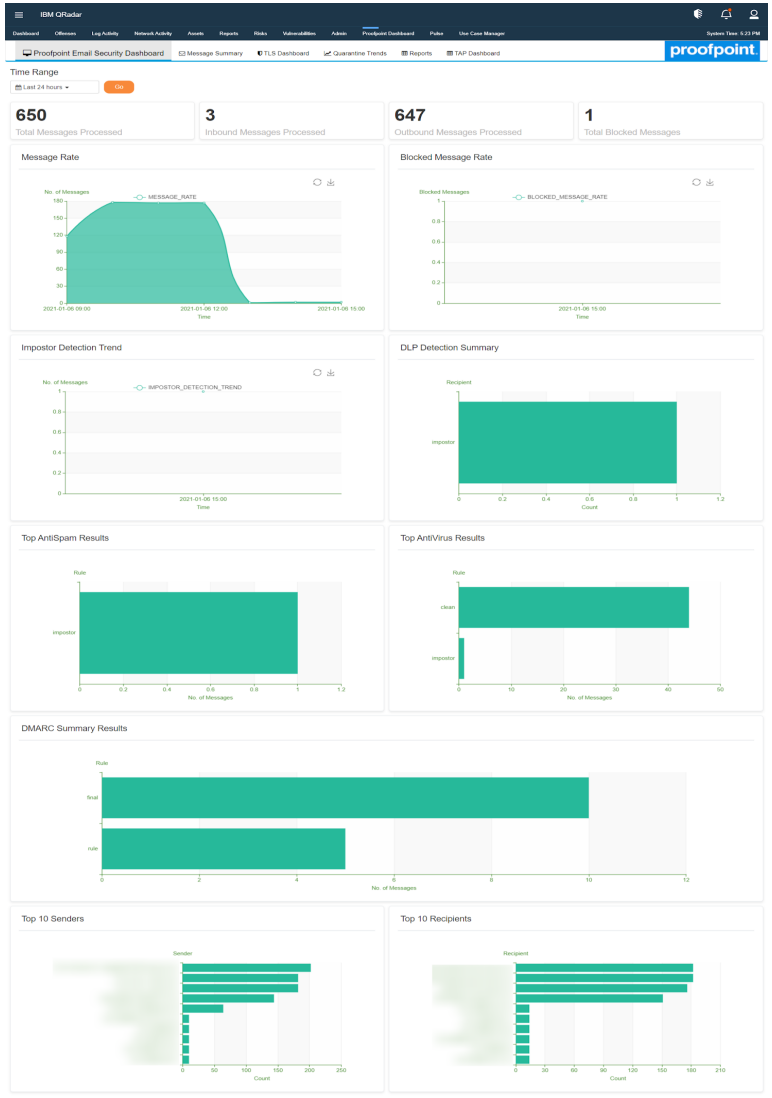
All the dashboards consist of individual panels which plot specific metrics related to the events from Proofpoint OnDemand Email Security server. All the dashboards allow the user to filter events by time. In addition, the Message Summary Dashboard also facilitates the user with Direction, Sender, Subject and Recipient to set as filters.

Drilldown functionality:

All the panels have drilldown functionality (except Tabular format panels). On clicking at any panels, it will redirect to the Log Activity Tab of QRadar. All the panels which are part of OnDemand email Security that will show Unique Message Header ID and their counts on drilldown whereas panels which are part of Proofpoint TAP that will show Raw event (Payload) on drilldown.

Proofpoint OnDemand Email Security

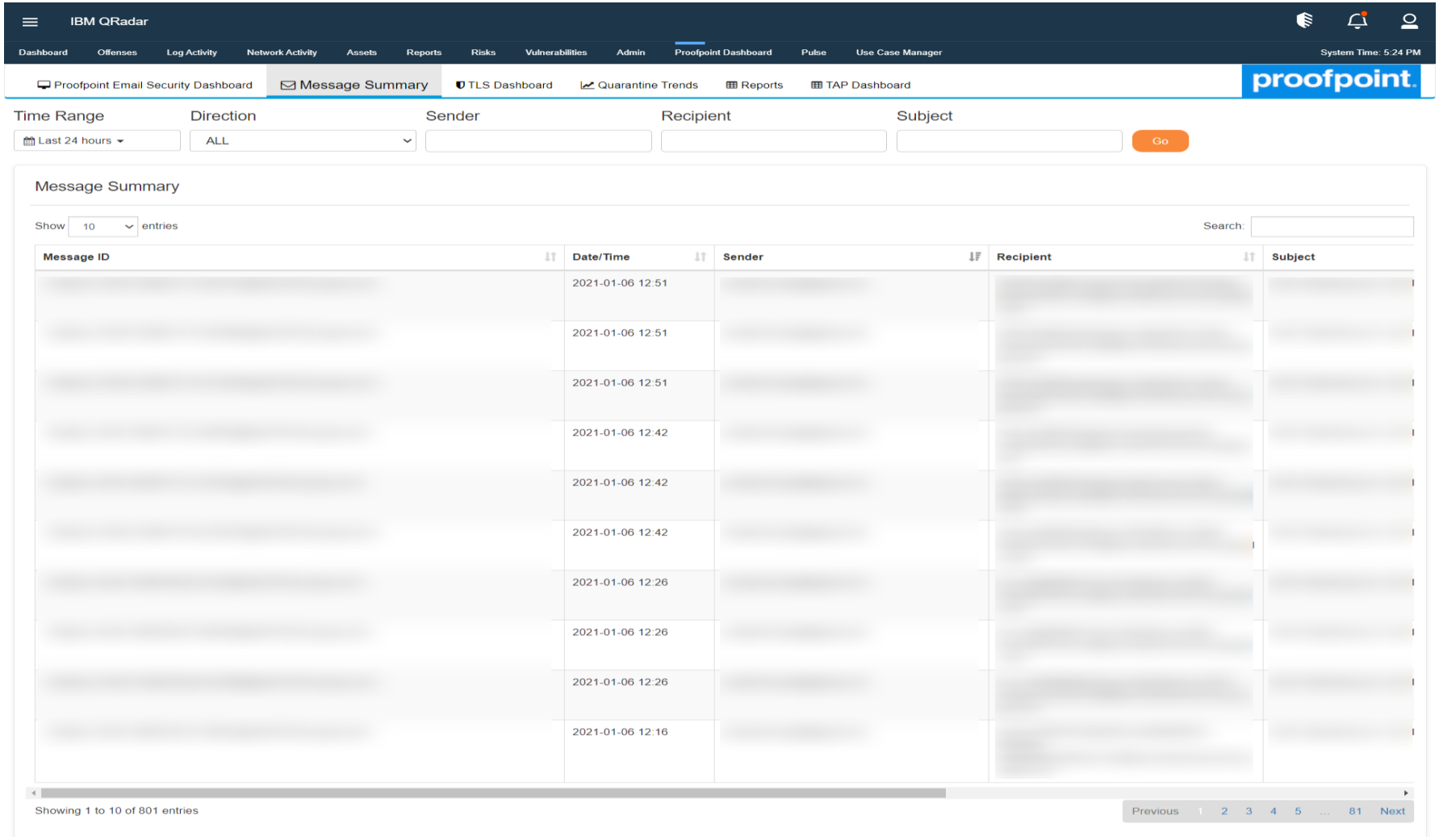
It shows the overall information of OnDemand email security.



Message Summary

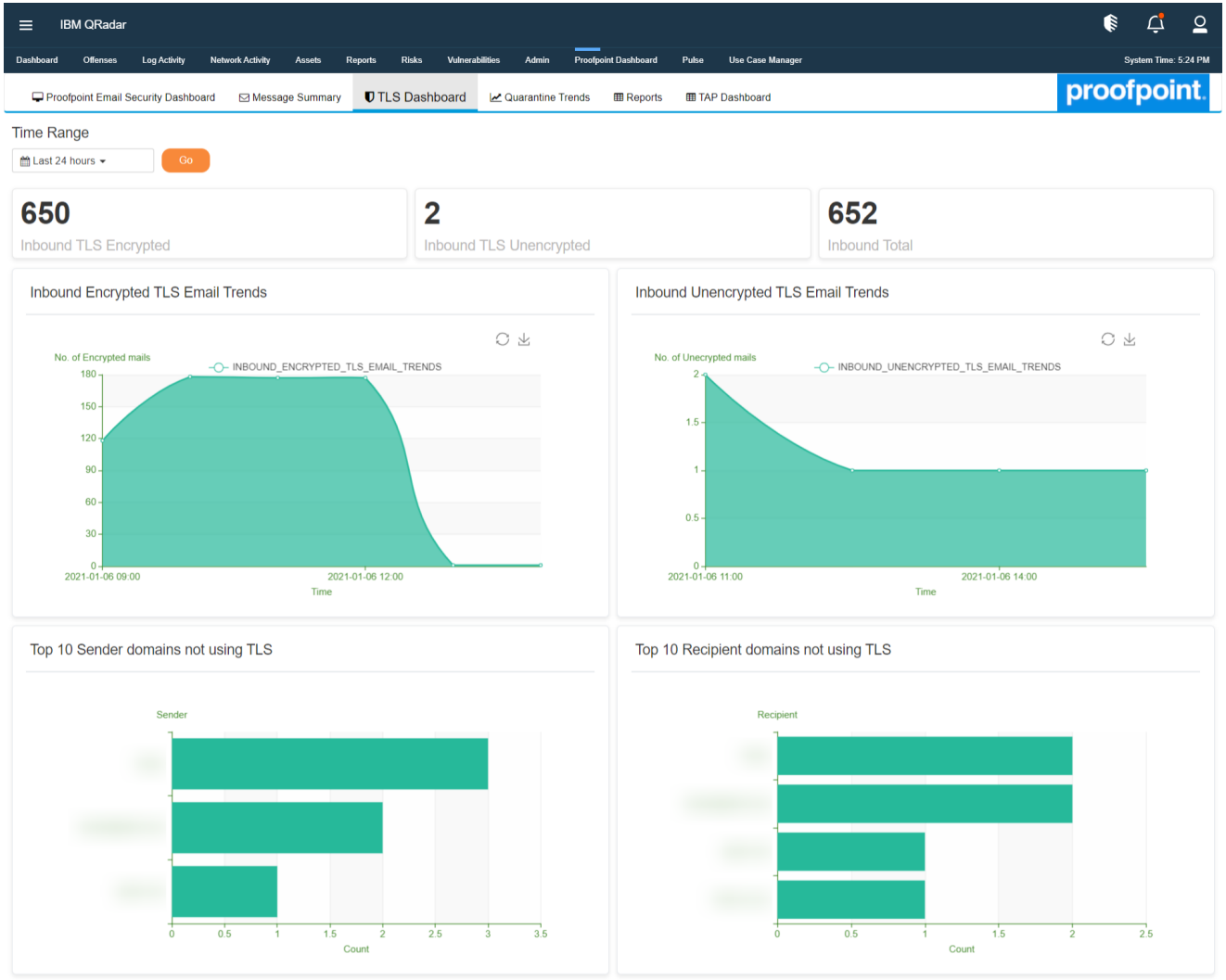
It shows the generic information about all the message types of events of OnDemand email security.

Note : In the search filters when a user enters special characters like **\",** it might show incorrect results on the dashboard.



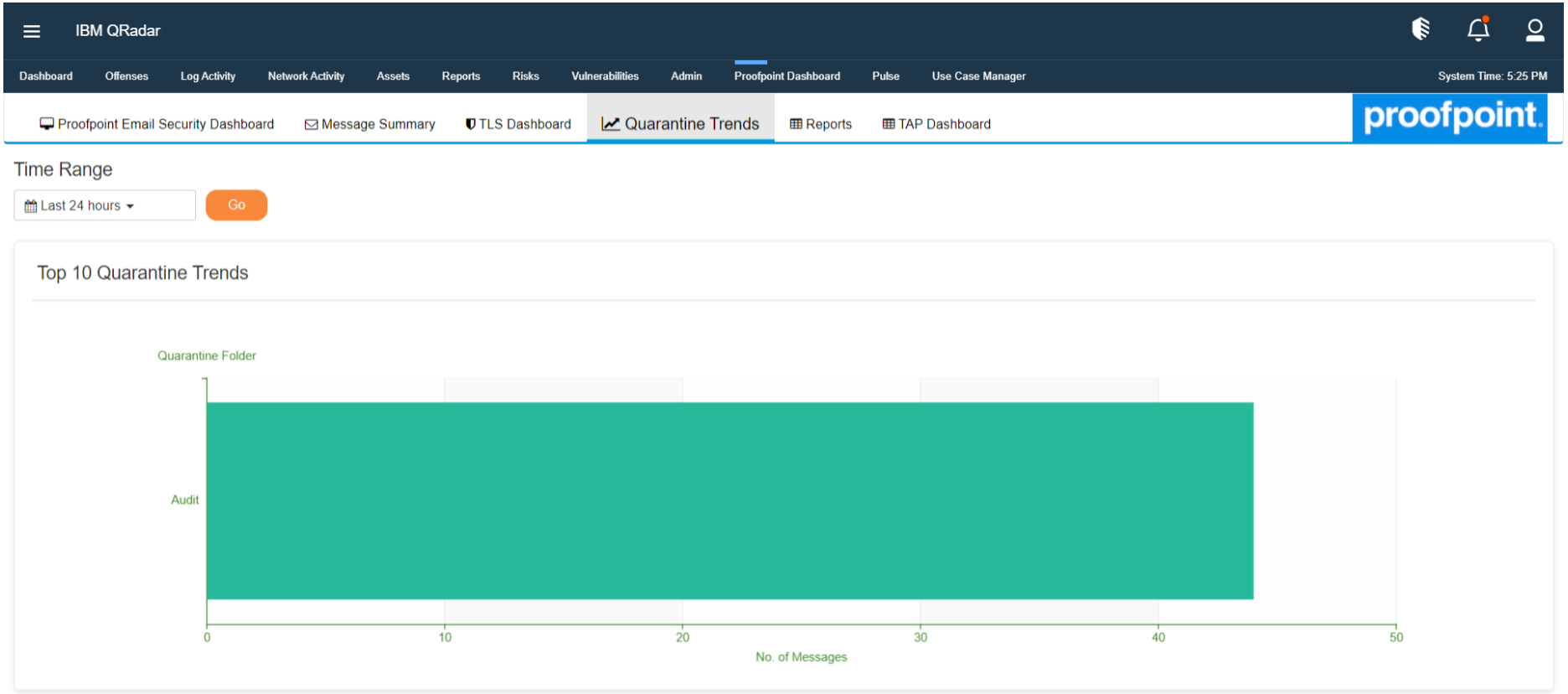
TLS Dashboard

It shows the information related to TLS encryption.



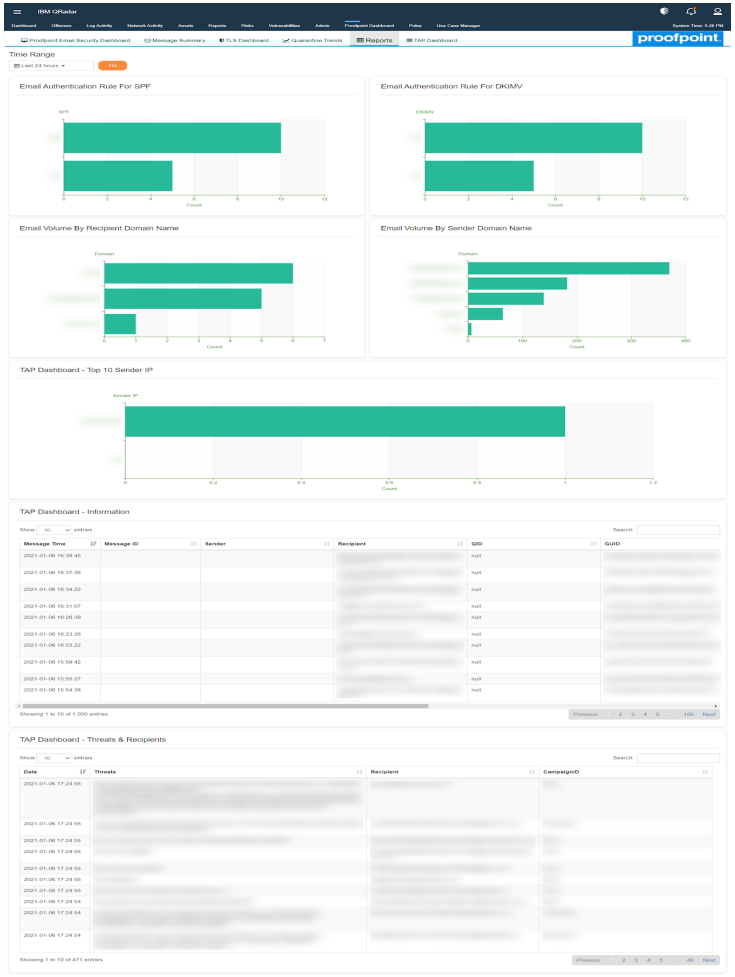
Quarantine Trends

It shows the messages according to type of email which are marked as quarantine.



Reports

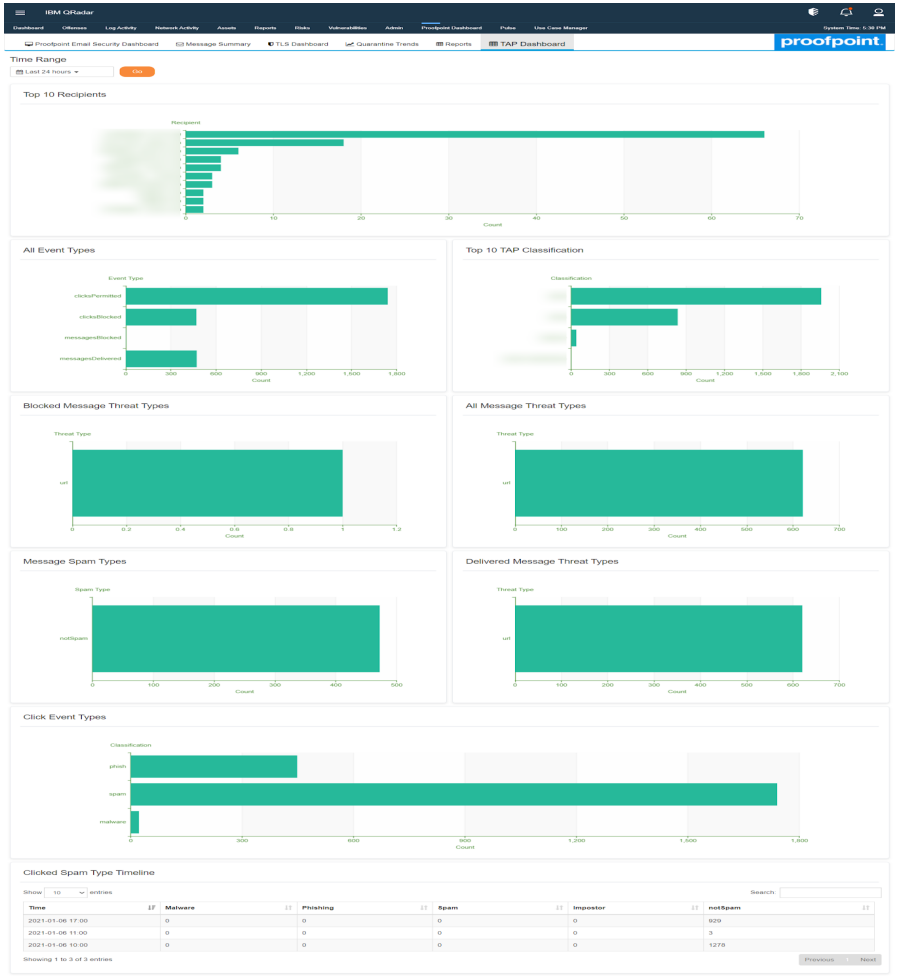
It shows the overall information of Reports.



TAP Dashboard

It shows the overall information of Proofpoint TAP.

Note: In this dashboard, for these 4 Panels, Top TAP Classification, Blocked Messages Threat Types, All Messages Threat Types, Delivered Messages Threat Type, it might be possible that drilldown count doesn't match with count on dashboard because it is possible that Threat Type and Classification Custom properties contain multiple values.



Troubleshooting

Case #1 – Data is not getting collected

Problem: This could happen for many reasons.

Troubleshooting Steps: Please follow below steps:

1. Click on System and License Management in the Admin Panel.
2. Select the host on which Proofpoint on Demand Email Security App V2 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 3 days as data input.
8. Click on "Click here to download the log files".
9. This will download all the log files in a single zip on your local machine.
10. Create a support case with Proofpoint and attach this log file.

Case #2 – UI related issues

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

Troubleshooting Steps: Please follow below 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 #3 – Re-installation of the app/Upgradation of the app

Problem: After upgrading from v1.1.3 (QRadar app framework v1 app) to v2.0.0 (QRadar app framework v2), data collection is stopped and in the backend, there are multiple errors which contain EncryptionError exception in the log files.

Troubleshooting Steps:

1. Go to the Admin tab of the QRadar console. Open configuration page and click on edit icon.
2. Save the configurations again.
3. If that also doesn't work, delete the configurations and save again.

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

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

4. Remove all custom properties and saved searches associated with the log source Proofpoint OnDemand Email Security and log source Proofpoint TAP.
5. Delete the log source named Proofpoint OnDemand Email Security and Proofpoint TAP by navigating to Log Sources via Admin panel.
6. Uninstall the app.
7. Refresh the page and check whether the Dashboard tab Proofpoint Email Security Dashboard is not seen after uninstallation.
8. Now install the app from Extension Management.

Case #4 – Payload gets truncated

Problem: If the input payload size is larger than the size specified in "Max TCP Syslog Payload Length", the payload will get split and only the specified size will be considered, and rest will get truncated. In such cases, those events will be treated as "Unknown Log Events". To solve this issue, increase the "Max TCP Syslog Payload Length" accordingly.

Troubleshooting Steps: To increase TCP payload size, please follow below steps.

1. Go to Admin Page → System Settings.
2. Switch to "Advanced".
3. Under "System Settings", increase the "Max TCP Syslog Payload Length" accordingly.
   (Preferably, size of "Max TCP Syslog Payload Length" is 32,000 bytes)

Case #5 – All other issues which are not a part of the Document

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

Troubleshooting Steps:

1. Click on System and License Management in the Admin Panel.
2. Select the host on which tab Proofpoint on Demand Email Security App V2 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 Log, 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 a support case with tab Proofpoint and attach this log file.