Qualys FIM for QRadar - QRadar 7.3.3 FP12+/7.4.3 FP6+/7.5.0 UP2+

User Guide

Version 2.0.0

February 17, 2023
# Table of Contents

Introduction to Qualys FIM for QRadar - 7.3.3 FP12+/7.4.3 FP6+/7.5.0 UP2+ .......... 4

- Features ......................................................................................................................... 4
- Prerequisites .................................................................................................................. 4

Installing the App ............................................................................................................. 4

Validating Dependencies ................................................................................................. 4

DSM Editor ......................................................................................................................... 5
- Qualys FIM JSON ............................................................................................................. 5
- Qualys FIM INCIDENTS ................................................................................................. 6
- Log Source Event Mapping ............................................................................................. 7

Log Source ........................................................................................................................ 11
- Qualys FIM JSON ............................................................................................................. 11
- Qualys FIM INCIDENTS ................................................................................................. 13
- Custom Event Properties ............................................................................................... 15

Configuring the App ........................................................................................................... 17

- Qualys API Configurations ........................................................................................... 17
- Settings ......................................................................................................................... 17
- FIM Events .................................................................................................................. 18
- FIM Ignored Events ....................................................................................................... 19
- FIM Incidents ................................................................................................................ 20
- Advanced .................................................................................................................... 21
- Advanced Configuration ............................................................................................... 21
- Index Management ........................................................................................................ 21

How Qualys App works? .................................................................................................. 23

- What happens after configuration? ................................................................................ 23
- How does data get into QRadar? .................................................................................... 23
- Raw Data ..................................................................................................................... 23
- Input Logs ..................................................................................................................... 24
  - For FIM Events and FIM Ignored Events ...................................................................... 24
  - For FIM Incidents and Incident Events ....................................................................... 25

Dashboard .......................................................................................................................... 27

Reports ............................................................................................................................... 31

Search ................................................................................................................................ 34

Uninstalling the app .......................................................................................................... 36

Troubleshooting ................................................................................................................ 37

- If user is not able to pull data without proxy ................................................................. 37
- If user is not able to pull data with proxy ...................................................................... 37
- If Token returned is Null ............................................................................................... 37
- If Log Source error occurs ............................................................................................ 37
- If you get errors for AQL ............................................................................................... 38
- If you get “[Errno 111] Connection refused” error ...................................................... 38
- If widgets are taking time to load/display data .............................................................. 38

Qualys Support ................................................................................................................ 38

Appendix ............................................................................................................................. 39
Introduction to Qualys FIM for QRadar - 7.3.3 FP12+/7.4.3 FP6+/7.5.0 UP2+

Use the Qualys FIM for QRadar – QRadar 7.3.3 FP12+/7.4.3 FP6+/7.5.0 UP2+ to ingest your Qualys FIM Events, FIM Ignored Events and FIM Incidents into QRadar. To view the data, go to QRadar’s Log Activity tab or the application Dashboard. All you need to do is install the app, configure the app and schedule the sync. The Qualys FIM App continuously pull your event delta. Want to visualize historical data? Just use date-time pickers given in the QRadar’s Activity log or application Dashboard to check the useful information.

Features

- Fetch the FIM events, ignored events and FIM incidents from Qualys to ingest into QRadar
- Search the ingested data in the QRadar using Log Activity tab or use the Dashboard with different widgets to view the data.

Prerequisites

Make sure you have:
- A valid Qualys subscription
- API access to Qualys FIM module
- Internet access and your Qualys API server must be reachable from QRadar

Note: This app is compatible with these versions only- QRadar 7.3.3 FP12+/7.4.3 FP6+/7.5.0 UP2+

Installing the App

1. Log in to QRadar and go to the Admin tab > Extensions Management and click Add.
2. Select the extensions .zip file for FIM app.
   - Before installing the app, check if the Content of the app is correct.
   - Confirm whether you want to replace/skip any existing contents with those coming from the extension and click Install.

   Note: If the user is using QRadar version 7.4.x, then it is mandatory to select the Start a default instance of each app check-box before clicking the Install.
3. Once installation is completed, refresh your QRadar user interface.
4. After installation of the app, check if all the details appear as required for the following settings:
   - Admin > Custom Event Properties
   - Admin > Log Source
   - Admin > Log Source Extensions
   - Admin > DSM Editor
5. User must perform the DSM Editor steps before configuring the App.
6. Then configure the Qualys FIM app.

Validating Dependencies

Please go through each of the sections listed below. You need to carry out the following steps manually, right after you install the app and before you start using it.
Note: Some sections may not be applicable in your case, and you may need to skip them.

DSM Editor

Qualys FIM JSON

In Configuration tab, check if the following fields are set with values as mentioned in the following:

1. Select Log Source Type (Qualys FIM JSON) > Configuration > Log Source Autodetection Configuration > Enable Log Source Autodetection: enabled

2. Click Show Advanced Options, and set the following as mentioned:
   - Minimum Successful Events for Autodetection: 2
   - Minimum Success Rate for Autodetection: 100
   - Attempted Parse Limit: as it is
   - Consecutive Failed Parse Limit: as it is
Qualys FIM INCIDENTS

In Configuration tab, check if the following fields are set with values as mentioned in the following:

1. Select Log Source Type (Qualys FIM INCIDENT) > Configuration > Log Source Autodetection Configuration > Enable Log Source Autodetection: enabled

2. Click Show Advanced Options, and set the following as mentioned:
   - Minimum Successful Events for Autodetection: 1
   - Minimum Success Rate for Autodetection: 100
   - Attempted Parse Limit: as it is
   - Consecutive Failed Parse Limit: as it is
Log Source Event Mapping

Qualys FIM JSON

1. Go to Admin > DSM Editor.
2. In Select Log Source Type, search for “Qualys FIM JSON” and click Select.

3. From the Qualys FIM JSON screen, go to Event Mappings tab. You can view mapping for FIM_EVENTS, FIM_IGNORED_EVENTS and FIM_INCIDENT_EVENTS.
If you don't see mapping for FIM_EVENTS, FIM_IGNORED_EVENTS and FIM INCIDENT_EVENTS create new (refer below steps).

4. Click the Choose QID link.
   - High Level Category: Any
   - Low Level Category: Any
   - Log Source Type: Any
   - QID/Name: In this text box, user must search for Qualys FIM, click Search.

   Search results will be displayed based on the QID/Name entered.

5. Click + icon to add a new mapping. The “Create a new Event Mapping” pop-up opens. Set Event ID as “FIM_EVENTS, FIM_IGNORED_EVENTS and FIM_INCIDENT_EVENTS” (without quotes) and Category as “FIM_EVENTS, FIM_IGNORED_EVENTS and FIM_INCIDENT_EVENTS” (without quotes).

6. Choose the option Qualys FIM Events/Qualys FIM Ignored Events/Qualys FIM Incidents based on your requirement.
7. Click **OK**. Create a new Event Mapping window is displayed.
8. Click **Create**. Event Mappings window is displayed. You can verify the new event mapping created.
9. Click **Save** and close the window.

**Qualys FIM INCIDENTS**

1. Go to **Admin > DSM Editor**.
2. In **Select Log Source Type**, search for “Qualys FIM INCIDENT” and click **Select**.
3. From the Qualys FIM INCIDENTS screen, go to **Event Mappings** tab. You can view mapping for FIM _INCIDENT_EVENTS_. If you don’t see mapping for FIM _INCIDENT_EVENTS_ create new (refer below steps).

4. Click + icon to add a new mapping. The “Create a new Event Mapping” pop-up opens. Set **Event ID** as “FIM_INCIDENT_EVENTS” (without quotes) and **Category** as “FIM_INCIDENT_EVENTS” (without quotes).
5. Click the **Choose QID** link.
   - High Level Category: Any
Search results will be displayed based on the QID/Name entered.

6. Choose the option Qualys FIM Incidents.
7. Click OK.
   Create a new Event Mapping window is displayed.
8. Click Create.
   Event Mappings window is displayed.
   You can verify the new event mapping created.
9. Click Save and close the window.
Log Source

Qualys FIM JSON

When you install app, it will create a new Log Source named “QualysFimMultiline”. Check if the log source is created and correctly configured after the installation. If the log source is not created, the following error is displayed.

You need to create/edit the custom log source for the Qualys app using the following steps. Keep the configuration of custom log source same as that mentioned below:-

1. Qualys FIM will send the data to QRadar console only. The user will not be able to use the app for distributed setup.
2. On your console UI, go to Admin → Data Sources → Log Sources and click Add.
3. Add the details shown below to the form to Create QualysFimMultiline Log Source. All fields marked with an asterisk (*) are mandatory. Make sure your Log Source Name and Log Source Identifier have same value.

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Name*</td>
<td>QualysFimMultiline (Customizable)</td>
</tr>
<tr>
<td>Log Source Description</td>
<td>QualysFimMultiline</td>
</tr>
<tr>
<td>Log Source Type*</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>Protocol Configuration*</td>
<td>TCP Multiline Syslog</td>
</tr>
<tr>
<td>Log Source Identifier*</td>
<td>QualysFimMultiline (Customizable, but same as Log Source Name)</td>
</tr>
<tr>
<td>Listen Port</td>
<td>12400 (Customizable)</td>
</tr>
<tr>
<td>Aggregation Method*</td>
<td>Start/End Matching</td>
</tr>
</tbody>
</table>
| Event Start Pattern*            | [A-Z][a-z][a-z]\d\d\s\d\d\d:]d:d:s
<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event End Pattern</td>
<td>qualys_event_ends</td>
</tr>
<tr>
<td>Event Formatter</td>
<td>No Formatting</td>
</tr>
<tr>
<td>Show Advance Option</td>
<td>Yes</td>
</tr>
<tr>
<td>Use Custom Source Name</td>
<td>Unchecked</td>
</tr>
<tr>
<td>Use As A Gateway Log Source</td>
<td>Checked</td>
</tr>
<tr>
<td>Flatten Multiline Events Into Single Line</td>
<td>Checked</td>
</tr>
<tr>
<td>Retain Entire Lines During Event Aggregation</td>
<td>Checked</td>
</tr>
<tr>
<td>Enabled</td>
<td>Checked</td>
</tr>
<tr>
<td>Credibility</td>
<td>5</td>
</tr>
<tr>
<td>Target Event Collector</td>
<td>&lt;default/your choice&gt;</td>
</tr>
<tr>
<td>Coalescing Events</td>
<td>Unchecked</td>
</tr>
<tr>
<td>Store Event Payload</td>
<td>Checked</td>
</tr>
<tr>
<td>Log Source Extension</td>
<td>QualysFIMJSONCustom_ext</td>
</tr>
</tbody>
</table>

**Note:** If you see the fields (listed below), which are not mandatory Qualys FIM app’s log source while editing or creating the custom Qualys log source.

Enable and then disable the "Use Custom Source Name" option. As a result, QRadar removes those fields from mandatory fields.

Once you confirm the specified configurations are added or verified properly, click **Save**.

With the above steps, you may create the required log source if it is not exist or edit the existing one, if its values are not configured as required. Then, go to **Admin > Advance** and click **Deploy Full Configuration**.
**Qualys FIM INCIDENTS**

When you install app, it will create a new Log Source named “QualysFimIncidents”. Check if the log source is created and correctly configured after the installation. If the log source is not created, the following error is displayed.

You need to create/edit the custom log source for the Qualys app using the following steps. Keep the configuration of custom log source same as that mentioned below:-

1. Qualys FIM will send the data to QRadar console only. The user will not be able to use the app for distributed setup.
2. On your console UI, go to Admin → Data Sources → Log Sources and click Add.
3. Add the details shown below to the form to Create QualysFimIncidents Log Source. All fields marked with an asterisk (*) are mandatory. Make sure your Log Source Name and Log Source Identifier have same value.

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Source Name</td>
<td>QualysFimIncidents(Customizable)</td>
</tr>
<tr>
<td>Log Source Description</td>
<td>QualysFimIncidents</td>
</tr>
<tr>
<td>Log Source Type</td>
<td>Qualys FIM INCIDENTS</td>
</tr>
<tr>
<td>Protocol Configuration</td>
<td>TCP Multiline Syslog</td>
</tr>
<tr>
<td>Log Source Identifier*</td>
<td>QualysFIMIncidents (Customizable, but same as Log Source Name)</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------------------------------------------------------</td>
</tr>
<tr>
<td>Listen Port</td>
<td>12400 (Customizable)</td>
</tr>
<tr>
<td>Aggregation Method*</td>
<td>Start/End Matching</td>
</tr>
<tr>
<td>Event Start Pattern*</td>
<td>[A-Z][a-z][a-z][d:d[d:d[d:d[d:d]s</td>
</tr>
<tr>
<td>Event End Pattern*</td>
<td>qualys_event_ends</td>
</tr>
<tr>
<td>Event Formatter*</td>
<td>No Formatting</td>
</tr>
<tr>
<td>Show Advance Option*</td>
<td>Yes</td>
</tr>
<tr>
<td>Use Custom Source Name*</td>
<td>Unchecked</td>
</tr>
<tr>
<td>Use As A Gateway Log Source*</td>
<td>Checked</td>
</tr>
<tr>
<td>Flatten Multiline Events Into Single Line*</td>
<td>Checked</td>
</tr>
<tr>
<td>Retain Entire Lines During Event Aggregation*</td>
<td>Checked</td>
</tr>
<tr>
<td>Enabled*</td>
<td>Checked</td>
</tr>
<tr>
<td>Credibility</td>
<td>5</td>
</tr>
<tr>
<td>Target Event Collector</td>
<td>&lt;default/your choice&gt;</td>
</tr>
<tr>
<td>Coalescing Events*</td>
<td>Unchecked</td>
</tr>
<tr>
<td>Store Event Payload*</td>
<td>Checked</td>
</tr>
<tr>
<td>Log Source Extension*</td>
<td>QualysFIMINCIDENTCustom_ext</td>
</tr>
</tbody>
</table>

**Note:** If you see the fields (listed below), which are not mandatory Qualys FIM app’s log source while editing or creating the custom Qualys log source.

Enable and then disable the "Use Custom Source Name" option. As a result, QRadar removes those fields from mandatory fields.

4. Once you confirm the specified configurations are added or verified properly, click **Save**.

With the above steps, you may create the required log source if it is not exist or edit the existing one, if its values are not configured as required. Then, go to **Admin > Advance** and click **Deploy Full Configuration**.
Custom Event Properties

1. Go to Admin > Log Sources and confirm that QualysFimMultiline and QualysFIMIncidents Log Sources are Enabled. If it is disabled, please enable it.

2. Go to Admin > Custom Event Properties and confirm that all 51 Qualys related properties are Enabled and are linked to “Qualys FIM JSON” and “Qualys FIM INCIDENTS” log source type.

Note: As per IBM QRadar’s upgrade to QRadar® 7.4.3, some Custom Event Properties are renamed and merged default custom properties

Refer to Alias properties created for custom properties

Qualys related properties are:

<table>
<thead>
<tr>
<th>Field name</th>
<th>Expression</th>
<th>Log Source Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Absolute File Path</td>
<td>/&quot;fullPath&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>Absolute Process Path</td>
<td>/&quot;actor&quot;/&quot;imagePath&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>Action</td>
<td>/&quot;action&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>Agent Version</td>
<td>/&quot;asset&quot;/&quot;agentVersion&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>Asset Interfaces</td>
<td>/&quot;assetInterfaces&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>Asset Name</td>
<td>/&quot;asset&quot;/&quot;name&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>Asset Tags</td>
<td>/&quot;asset&quot;/&quot;tags&quot;[]</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>Attribute New</td>
<td>/&quot;attributes&quot;/&quot;new&quot;[]</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>Attribute Old</td>
<td>/&quot;attributes&quot;/&quot;old&quot;[]</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>Category name</td>
<td>/&quot;profiles&quot;[0]/&quot;category&quot;/&quot;name&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>Event Alert</td>
<td>/&quot;name&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>Event Incident Id</td>
<td>/&quot;incidentId&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>Event Incident Name</td>
<td>/&quot;incidentName&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>Event UUID</td>
<td>/&quot;id&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>Event Type</td>
<td>/&quot;type&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>File Certificate Hash</td>
<td>/&quot;fileCertificateHash&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>File Hash</td>
<td>/&quot;fileContentHash&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>File Reputation Status</td>
<td>/&quot;reputationStatus&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>File Trust Status</td>
<td>/&quot;trustStatus&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>Incident Approval Status</td>
<td>/&quot;approvalStatus&quot;</td>
<td>Qualys FIM INCIDENTS</td>
</tr>
<tr>
<td>Incident Approval Type</td>
<td>/&quot;approvalType&quot;</td>
<td>Qualys FIM INCIDENTS</td>
</tr>
<tr>
<td>Incident Assignee</td>
<td>/&quot;reviewers&quot;[]</td>
<td>Qualys FIM INCIDENTS</td>
</tr>
<tr>
<td>Incident Change Type</td>
<td>/&quot;changeType&quot;</td>
<td>Qualys FIM INCIDENTS</td>
</tr>
<tr>
<td>Incident Correlation Rule ID</td>
<td>/&quot;ruleId&quot;</td>
<td>Qualys FIM INCIDENTS</td>
</tr>
<tr>
<td>Incident Correlation Rule Name</td>
<td>/&quot;ruleName&quot;</td>
<td>Qualys FIM INCIDENTS</td>
</tr>
<tr>
<td>Incident Disposition Category</td>
<td>/&quot;dispositionCategory&quot;</td>
<td>Qualys FIM INCIDENTS</td>
</tr>
<tr>
<td>Incident ID</td>
<td>/&quot;id&quot;</td>
<td>Qualys FIM INCIDENTS</td>
</tr>
<tr>
<td>Incident Name</td>
<td>/&quot;name&quot;</td>
<td>Qualys FIM INCIDENTS</td>
</tr>
<tr>
<td>Incident Status</td>
<td>/&quot;status&quot;</td>
<td>Qualys FIM INCIDENTS</td>
</tr>
<tr>
<td>Incident Type</td>
<td>/&quot;type&quot;</td>
<td>Qualys FIM INCIDENTS</td>
</tr>
<tr>
<td>Monitoring Profile</td>
<td>/&quot;profiles&quot;[0]/&quot;name&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>New Content</td>
<td>/&quot;newContent&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>New Registry Value Content</td>
<td>/&quot;newRegistryValueContent&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>New Registry Value Type</td>
<td>/&quot;newRegistryValueType&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>Field name</td>
<td>Expression</td>
<td>Log Source Type</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>Old Content</td>
<td>/&quot;oldContent&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>Old Registry Value Content</td>
<td>/&quot;oldRegistryValueContent&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>Old Registry Value Type</td>
<td>/&quot;oldRegistryValueType&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>Platform</td>
<td>/&quot;platform&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>Process ID</td>
<td>/&quot;actor&quot;/&quot;processID&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>Process Name</td>
<td>/&quot;actor&quot;/&quot;process&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>Registry Name</td>
<td>/&quot;registryName&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>Registry Path</td>
<td>/&quot;registryPath&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>Rules ID</td>
<td>/&quot;profiles&quot;[0]&quot;rules&quot;[0]&quot;id&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>Rules name</td>
<td>/&quot;profiles&quot;[0]&quot;rules&quot;[0]&quot;name&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>Section ID</td>
<td>/&quot;profiles&quot;[0]&quot;rules&quot;[0]&quot;section&quot;/&quot;id&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>Section Name</td>
<td>/&quot;profiles&quot;[0]&quot;rules&quot;[0]&quot;section&quot;/&quot;name&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>Source Host Name (for 7.3.3 QRadar family)</td>
<td>/&quot;asset&quot;/&quot;interfaces&quot;[0]/&quot;hostname&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>Source Hostname (for 7.4.3 and above QRadar family)</td>
<td>/&quot;asset&quot;/&quot;interfaces&quot;[0]/&quot;hostname&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>User ID</td>
<td>/&quot;actor&quot;/&quot;userID&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>Qradar Data Type</td>
<td>/&quot;qradarDataType&quot;</td>
<td>Qualys FIM INCIDENTS</td>
</tr>
<tr>
<td>Qradar Event Type</td>
<td>/&quot;qradarEventType&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
<tr>
<td>Severity Level</td>
<td>/&quot;severity&quot;</td>
<td>Qualys FIM JSON</td>
</tr>
</tbody>
</table>

For the Qualys related properties, complete these checks:

1. If any property is disabled, enable it.
2. If any property does not belong to the Qualys FIM JSON/Qualys FIM Incidents log source type, please open it to edit and select Qualys FIM JSON or Qualys FIM Incidents as the log source type.
3. Do not select any specific Log source, select **All** in the drop-down option.
4. Select the Category, with **High Level Category** as System and **Low Level Category** as Information.
5. Provide **JSON** or Incident expression from the above table in the **Extraction using** section.
6. Finally, save the properties.

For any change in Custom Event Properties, it is recommended to do Deploy Full Configuration.
Configuring the App

Qualys API Configurations

1. Log in to QRadar and go to the Admin tab.
2. Scroll to “Apps” section and click Qualys FIM App Settings. A pop-up window opens.

Settings

QRadar Authorization token is used while interacting securely with QRadar. You can obtain this token from Admin > User Management > Authorized Service.

To generate the authentication token follow the steps:

1. Go to Authorized Services in Admin tab
2. Click Add Authorized Service.
3. Enter the desired Service Name.
4. Select User Role as Admin.
5. Select Security Profile as Admin.
6. Set the expiry date as required.
7. Click Create Service and then click Deploy changes.

After providing the Authorization Token, under the settings tab, click Save to Proceed.

1. Use the Settings tab to configure your Qualys credentials. Enter your Qualys API server, username and password in the appropriate fields.

Log Source

Select Log Source for Events as QualysFimMultiline
Select Log Source for Incidents as QualysFimIncidents
Proxy Configuration
If you want Qualys app to use proxy while calling the API, configure proxy details.
Select the check box to enable proxy.
Add your proxy server and proxy port in `<proxy server>:<proxy port>` format.
If your proxy needs authentication, add proxy user and proxy password along with server and port, in `<proxy user>:<proxy password>@<proxy server>:<proxy port>` format.

FIM Events
Use the FIM Events tab to configure and enable Fetch FIM Events.

1) Tick the "Enable FIM Events Fetch" checkbox to enable this data input.
2) In the "Cron Schedule" field, enter a valid cron format entry. This is a mandatory field if the "Enable FIM Events" checkbox is checked. [Learn about cron expressions...](#)
3) In the "Start Date-Time" field, enter the date-time from which you want to fetch the FIM events data from the Qualys.
• This is an optional field.
• The date-time format should be 'YYYY-MM-DDTHH:MM:SS.MSZ. e.g. '2019-02-25T18:30:00.000Z.
• If the value is not provided, then FIM events will be fetched from the current date of the browser. The start date shouldn’t be less than 2017-01-01T00:00:00.000Z.

4) In the "Filter" field, enter filter criteria to filter the FIM events.
• This is an optional field.
• The filter fields should be in Elastic Search Query format.

5) From the Select log level drop-down menu, select the required log level out of the following options:
• INFO
• DEBUG
• WARNING
• ERROR

FIM Ignored Events

Use the FIM Ignored Events tab to configure and enable Fetch FIM Ignored Events.

2. Tick the "Enable FIM Ignored Events Fetch" checkbox to enable this data input.
3. In the "Cron Schedule" field, enter a valid cron format entry. This is a mandatory field if the "Enable FIM Ignored Events" checkbox is checked.
4. In the "Start Date-Time" field, enter the date-time from which you want to fetch the FIM Ignored events data from the Qualys.
• This is an optional field.
• The date-time format should be 'YYYY-MM-DDTHH:MM:SS.MSZ. e.g. '2019-02-25T18:30:00.000Z.
• If the value is not provided, then FIM events will be fetched from the current date of the browser. The start date shouldn’t be less than 2017-01-01T00:00:00.000Z.

5. In the "Filter" field, enter extra filter criteria to filter the FIM Ignored events.
• This is an optional field.
• The filter fields should be in Elastic Search Query format.

6. From the Select log level drop-down menu, select the required log level out of the following options:
• INFO
• DEBUG
• WARNING
• ERROR
FIM Incidents

Use the **FIM Incidents** tab to configure and enable Fetch FIM Incidents.

1. Tick the "Enable FIM Incidents Fetch" checkbox to enable this data input.
2. In the "Cron Schedule" field, enter a valid cron format entry. This is a mandatory field if the "Enable FIM Events" checkbox is checked. [Learn about cron expressions](#).
3. In the "Start Date-Time" field, enter the date-time from which you want to fetch the FIM events data from the Qualys.
   - This is an optional field.
   - The date-time format should be 'YYYY-MM-DDTHH:MM:SS.MSZ'. e.g. '2019-02-25T18:30:00.000Z'.
   - If the value is not provided, then FIM events will be fetched from the current date of the browser. The start date shouldn’t be less than 2017-01-01T00:00:00.000Z.
4. In the "Filter" field, enter filter criteria to filter the FIM events.
   - This is an optional field.
   - The filter fields should be in Elastic Search Query format.
5. From the Select log level drop-down menu, select the required log level out of the following options:
   - INFO
   - DEBUG
   - WARNING
   - ERROR

---

Qualys FIM for QRadar
Advanced

Use Advanced tab to see the last success and last failure for FIM Events, FIM Ignored Events, and FIM Incidents.

![Advanced Tab](image)

Advanced Configuration

These are the advanced and optional configurations which provides you additional benefits while using Qualys FIM for QRadar - QRadar 7.3.3 FP12+/7.4.3 FP6+/7.5.0 UP2+

Index Management

From the QRadar Console, you can use the Index Management tool to control database indexing on event and flow properties. By adding an indexed field in your search query, it helps to improve the speed of searches in QRadar by narrowing the overall data. Learn how to modify database indexing in the Index Management tool by making use of statistics before and after you enable or disable indexing on multiple properties.

Steps to enable indexing for the specific custom event properties:

1. On the navigation menu, click Admin and then click Index Management in the System Configuration section.
2. Search, select and click Enable Index for the required properties. Once you click Enable Index, Indexed column shows (green bubble) for the indexed property.
3. Click **Save**.
4. For more information, refer [Index management](#).
How Qualys App works?

What happens after configuration?

Once you configure and enable FIM Events, Ignored Events, FIM Incidents, the application bundled with this extension will start fetching your FIM data. By default, it will pull 1000 events at a time. This value is set to such a small number to make sure the app can process your data without hitting the memory limit governed by QRadar. For first run, it might take some time depending on your scan volume. After that, subsequent pulls are incremental ones - fetching only new/changed data.

How does data get into QRadar?

Whenever cron runs any job (based on the cron schedule you defined), it makes outbound API call to Qualys, get the event JSON and sends it to the QRadar over socket using TCP port configured in “QualysFimMultiline/QualysFimIncidents” Log Source. Using DSM editor and “Qualys FIM JSON/Qualys FIM INCIDENTS” Log Source Type provided with this extension, QRadar then puts this data into the “events” table in Ariel database.

Raw Data

There may be times when you want to see the raw data. Follow these steps:

1. Go to Log Activity tab and go to Advance Search field.
2. In the Advance Search field, post the sample AQL below. (Tip - For more AQLs please check the Troubleshooting section in this guide.)

   Note: As per IBM QRadar’s upgrade to QRadar® 7.4.3, some Custom Event Properties are renamed and merged default custom property. Refer to Alias properties created for custom properties

   Use the following query if your QRadar version is 7.4.3 and above QRadar family:

   ```
   ```
"Absolute File Path" from events WHERE LOGSOURCENAME(logsourceid) = 'QualysFimMultiline'

Use the following query if your QRadar version is 7.3.3 QRadar family:

```
```

3. Select the date range for which you want to see the data.
4. Click Search.

Depending on the results, you may want to change the date-time range to widen/shorten your search span. You can also execute your own AQL queries to find more appropriate data. Please refer to fields in "Qualys FIM JSON" or "Qualys FIM INCIDENTS" log source type of DSM editor to know the Qualys fields.

**Input Logs**

While running, host detection input sends its log to QRadar over syslog. To see them, you can use the following AQL in Log Activity > Advance Search.
Follow the same steps mentioned above with below AQL:

**For FIM Events and FIM Ignored Events**

This AQL has all the fields which the app parses.

**Note:** As per IBM QRadar's upgrade to QRadar® 7.4.3, some custom event properties are renamed and merged default custom property. Refer to [Alias properties created for custom properties](#).

Use the following query if your QRadar version is 7.4.3 and above QRadar family:

AQL:
```
"Log Source Time" FROM events WHERE LOGSOURCENAME(logsourceid) = 'QualysFimMultiline'
```

Use the following query if your QRadar Version is 7.3.3 QRadar family:

AQL:
```
"Log Source Time" FROM events WHERE LOGSOURCENAME(logsourceid) = 'QualysFimMultiline'
```

To fetch FIM Events specific data add this option at the end of the AQL:

AND "Qradar Event Type"= 'FIM_EVENTS'

To fetch FIM Ignored Events specific data add this option at the end of the AQL:

AND "Qradar Event Type"= 'FIM_IGNORED_EVENTS'

For FIM Incidents and Incident Events

This AQL has all the fields which the app parses.

SELECT "Incident ID" , "Incident Name" , "Incident Status" , "Incident Type" , "Incident Approval Type" , "Incident Approval Status" , "Incident Assignee" , "Incident Change Type" , "Incident Correlation Rule ID" , "Incident Correlation Rule Name" , "Incident Disposition Category" from events where LOGSOURCENAME(logsourceid) = 'QualysFimIncidents' and "Qradar Data Type"='FIM_INCIDENTS'

Note: As per IBM QRadar's upgrade to QRadar® 7.4.3, some Custom Event Properties are renamed and merged with the default custom property. Refer to Alias properties created for custom properties

Use the following query if your QRadar version is 7.4.3 and above QRadar family:

Use the following query if your QRadar version is 7.3.3 QRadar family:

```sql
```
Dashboard
QRadar displays a dashboard with 11 widgets. These widgets display different details with option to select a date range.
Go to Qualys FIM > Dashboard > Select a date range for which you want to view the changes.
The different widgets of dashboard are:

**Total Event Count** – Displays count of total FIM Events in the selected date range.

309.19K

**Total Incident Count** – Displays count of total FIM Incidents in the selected date range.

9

**Events by Profile** – Displays profile wise distribution of events. On mouse hover, the name of the profile and the count of events is displayed.

**Top Changes by User** – Top changes done by user in FIM events are displayed here.
**Top Changes by Process** – Top changes done by process in FIM events are displayed here.

**Events by Severity** – Displays severity wise distribution of all FIM Events in the selected date range. By hovering over the mouse, the severity bars shows the count of events.

**File Changes by Change Action** – FIM Events for the file changes by their change action are displayed here. Top 10 actions for file changes are presented with their count.
**Directory Changes by Change Action** – Graphical display of directory changes by change action in the selected date range.

**Top 5 Incidents Based on Event Count** – Graphical display of top 5 incidents based on event count in the selected date range.

**Incidents by Status** – Graphical display of incidents by their status in the selected date range.
**Incidents by Approval Status** – Graphical display of incidents by their approval status in the selected date range.

**Ignored Events** – Graphical display of total FIM Ignored Events in the selected date range. Information in bar chart is displayed according to:

- If the start and end date difference is in the year(s), then show the bar chart year-wise.
- Else if the start and end date difference is in the month(s), then show the bar chart month-wise.
- Else if the start and end date difference is in the day(s), then show the bar chart day-wise.
- Else if the start and end date difference is in the hour(s), then show the bar chart hour-wise.
- Else if the start and end date difference is in the minute(s), then show the bar chart minute-wise.

Note - If the date difference is > 30 days, then it is converted to month.
Reports

Reports Tab has different criteria for the user to view the reports.

Incident Status
Displays reports based on status of the Incidents.
1. Select a required date range.
2. Select Status as Open/Closed/Reopened.
3. Click Search to view the reports.

Events by Severity
Displays reports based on severity of the Incidents.
1. Select a required date range.
2. Select Severity as 1, 2, 3, 4, or 5.
3. Click Search to view the reports.

Ignored Events
Displays reports of ignored events.
1. Select a required date range.
2. Click Search to view the required reports.

File Changes by Change Action
Displays reports based on change actions of the incidents.
1. Select a required date range.
2. Select Action as Security, Attributes, Delete, Rename, Create, or Content.
3. Click Search to view the reports.

Changes by Type
Displays reports based on change by type of the incidents.
1. Select a required date range and Type as File, Directory, Key, or Value.
2. Click Search to view the reports.
**Note:** Maximum 20 rows are displayed in one page. To view rest of the pages, use pagination option.
Search
Search Tab provides different search criteria for users to search the events.

Incident Based Events
To search for incident based events:
1. Select a required date range.
2. Select either Incident ID(s) or incident Name(s) from the drop-down option.
3. If Incident ID(s) is selected: Add single or multiple incident Ids in the **Contains** field.
   If Incident Name(s) is selected: Add single or multiple incident names in the **Contains** field.
4. Click Search to view the results.

User Based Events
To search for user based events:
1. Select a required date range.
2. Add a username or multiple usernames in the text field provided to search for the required incident.
3. Click Search to view the results.

Process Based Events
To search for process based events:
1. Select a required date range.
2. Select either Process Name(s) or Absolute Process Path(s) from the drop-down option.
3. If Process Name(s) is selected: Add single or multiple names in the **Contains** field.
If Absolute Process Path is selected: Add single or multiple paths in the **Contains** field.
4. Click **Search** to view the results.

**File Based Events**
To search for file based events:
1. Select a required date range.
2. Select either File Name(s) or Absolute File Path(s) from the drop-down option.

3. If File Name(s) is selected: Add single or multiple names in the **Contains** field.
If Absolute File Path is selected: Add single or multiple paths in the **Contains** field.
4. Click **Search** to view the results.

**Asset Based Events**
To search for asset based events:
1. Select a required date range.
2. Select Asset Name(s) or Asset Tag ID from the drop-down option.

3. If Asset Name(s) is selected: Add an asset name or multiple asset names in the text field provided to search for the required incident.
If Asset Tag ID is selected: Add a Tag Id. Note: You can add only single tag since one tag may contain multiple assets.
4. Click **Search** to view the results.
Uninstalling the app

1. Uninstall the FIM app from Admin > Extension management. If you are asked to Remove or Preserve, then remove everything.
2. Check if all the CEPs are deleted for "Qualys FIM JSON" and "Qualys FIM Incidents" (whichever is required) log source type in Admin > Custom Event Properties.
3. Delete the FIM app related:
   4. Admin > Log Source
   5. Admin > Log Source Extensions
   6. Open the Admin > DSM Editor
      • Select the "Qualys FIM JSON" log source type. Check if all the custom fields are deleted and override fields are not override in the Properties tab.
      • Select the "Qualys FIM INCIDENTS" log source type. Check if all the custom fields are deleted and override fields are not override in the Properties tab.
      • Delete the Event mapping(s) related to the FIM app.
      • Disable:
        Configuration > Log Source Autodetection
        Configuration > Enable Log Source Autodetection.

7. Then delete the "Qualys FIM JSON" and "Qualys FIM Incidents" log source type in Admin > DSM Editor.
8. Log out.

While uninstalling the app in unfortunate cases, it should be done cleanly. Any leftover artifacts can potentially interfere with next installation attempt creating unstable state.
When app gets installed following components will get installed in QRadar, so to uninstall completely following components also need to be removed.
**Troubleshooting**

If any error (example: socket connection on the port xxxx configured for FIM log sources is refused) is displayed on application log or in app configuration under the Advanced tab > Last Failure

Perform the following steps:

1. Disable all the data inputs from the application configuration, then:
2. Admin > Advanced drop-down > Deploy Full Configuration
3. Admin > Advanced drop-down > Restart Event Collection Service
4. Enable the required data inputs

**Note:** Please wait for the Event Collection Service to restart before enabling the FIM job.

---

**If user is not able to pull data without proxy**

If the user is not able to pull the data without proxy, please check with your networking team and the team responsible for providing the QRadar host machine.

**If user is not able to pull data with proxy**

If the user is not able to pull the data with HTTP proxy and not HTTPS proxy and vice versa, please check with your networking team and the team responsible for providing the QRadar host machine.

**If Token returned is Null**

If the user observes that the ETL says "Received auth token from API Gateway Server" and then the process terminates. It means the Token returned is None. Please run the curl to verify the same in the app container from /opt/app-root/app directory

- If the proxy is not needed remove the --proxy option and proxy:
  ```
  curl --location --request POST '<gateway api>/auth' --proxy '<proxy>' --header 'Content-Type: application/x-www-form-urlencoded' --data-urlencode 'username=<POD username>' --data-urlencode 'password=<POD password>' --data-urlencode 'token=true'
  ```
- If the JWT token is not returned please check with your networking team or the team responsible for providing the QRadar host machine for proxy or firewall-related issues.
- If the JWT token is returned, please contact Qualys support.

**If Log Source error occurs**

If the Log source shows this message, “This log source uses an undocumented protocol. IBM Support cannot troubleshoot problems with receiving event data. Events received by an undocumented protocol may be in a format unrecognized by the DSM. Use the DSM Editor to resolve any parsing issues.” please refer to these links from IBM:

If you get errors for AQL

- If you get N/A for any field value, this means the payload which has these fields will show the data and if the fields are not present it will show N/A. N/A is provided by QRadar if the field is not available in the payload.
- If you get this error in the Activity Log tab "Field '<field name>' does not exist in catalog 'events'. Please manually type the field name to get the exact match for that value.

If you get “[Errno 111] Connection refused” error

Following error messages will be displayed for different cases:
ERROR: Socket connection on port 12400 configured for 'QualysFimMultiline' log source is refused, 'Deploy Full Configuration'. Error while connecting to socket: [Errno 111] Connection refused This error occurs when the Listen port is not LISTENING. You need to do the Deploy Full Configuration on QRadar box to resolve this issue.
Verify the following points:
- https://www.ibm.com/support/pages/node/6395080 is performed or not
- Can be verified as > if the license is patched user can see Live Events under Log Activity otherwise no events are visible to the user
- Verify user performed the 'Deploy Changes' after the application installation
  This is the last step that could be authorized by QRadar Admin > Do 'Full Deployment'
- If the above steps do not work for a user then they should contact Qualys Support

If widgets are taking time to load/display data

Try loading each widget separately. After selecting a date range, the widgets might take time to fetch the data, hence try to refresh each widget separately.

Qualys Support

If you tried the troubleshooting steps but still need help, please contact Qualys Support at https://www.qualys.com/support/

Provide the following information to Qualys Support:
- Qualys App version number
- QRadar version number, including the patch number
- Steps to reproduce the issue
- Note any manual changes done to Qualys app’s code
- Note any manual changes done to Qualys app’s container
- Please download the logs from Admin > Qualys FIM App Settings page and attach them to your support case.
Appendix

User will get this information under Application Configuration → Advanced tab.

<table>
<thead>
<tr>
<th>Error code</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>QRFIM-100</td>
<td>The /opt/app-root/store/qradar_fim_app.db is either missing or is in read-only mode as it must have been updated by another file. In that case please provide permission to write.</td>
</tr>
<tr>
<td>QRFIM-101</td>
<td>Not able to connect to the qualys_fim_config table in The /opt/app-root/store/qradar_fim_app.db file, please check if the table is available in the db file.</td>
</tr>
<tr>
<td>QRFIM-102</td>
<td>The configuration key-value is not available in the qualys_fim_config table.</td>
</tr>
<tr>
<td>QRFIM-103</td>
<td>Some error encountered while adding or updating the qualys_fim_checkpoint table.</td>
</tr>
<tr>
<td>QRFIM-104</td>
<td>Some error is encountered while adding or updating the qualys_fim_config table.</td>
</tr>
<tr>
<td>QRFIM-105</td>
<td>Some error encountered while getting the data from the qualys_fim_checkpoint table.</td>
</tr>
<tr>
<td>QRFIM-106</td>
<td>Some error is encountered while adding or updating the qualys_fim_job_status table.</td>
</tr>
<tr>
<td>QRFIM-200</td>
<td>To make the REST API call to QRadar, we use HTTP headers. Some issue is encountered for creating the headers. Please check the job logs.</td>
</tr>
<tr>
<td>QRFIM-201</td>
<td>While making the QRadar REST API call we encountered an error that is not parsable. Please check the job logs.</td>
</tr>
<tr>
<td>QRFIM-202</td>
<td>We did not find the 'Qualys FIM JSON' Log source Type in the DSM Editor. Please reinstall the app.</td>
</tr>
<tr>
<td>QRFIM-203</td>
<td>We did not find the 'QualysFimMultiline' Log source Type in the DSM Editor. Please create a log source or reinstall the app.</td>
</tr>
<tr>
<td>QRFIM-204</td>
<td>We could not connect with the QRadar REST API server. Please check with IBM support. If there is an issue with the QRadar host machine.</td>
</tr>
<tr>
<td>QRFIM-205</td>
<td>While fetching the Log source information we encountered an error please check the job logs.</td>
</tr>
<tr>
<td>QRFIM-206</td>
<td>Please update a correct QRadar Auth token on Qualys FIM app settings page.</td>
</tr>
<tr>
<td>QRFIM-207</td>
<td>Got an error from QRadar REST API. Please contact IBM support.</td>
</tr>
<tr>
<td>QRFIM-208</td>
<td>No Log source information available in QRadar for a selected Log Source Id.</td>
</tr>
<tr>
<td>QRFIM-209</td>
<td>We encountered an error while validating the Qradar related settings before starting the job process. Please check the job logs for more information.</td>
</tr>
<tr>
<td>QRFIM-210</td>
<td>Connection with QRadar host machine over socket is lost. Please check if the DSM PORT is open on the QRadar host machine. Restart the job process.</td>
</tr>
<tr>
<td>QRFIM-211</td>
<td>Could not connect with QRadar host machine over the socket. Please check if the DSM PORT is open on the QRadar host machine.</td>
</tr>
<tr>
<td>QRFIM-212</td>
<td>We encountered an exception while trying a socket connection to QRadar. Please check the job logs for more information.</td>
</tr>
<tr>
<td>QRFIM-213</td>
<td>Events and Incidents Listen port does not match.</td>
</tr>
<tr>
<td>QRFIM-214</td>
<td>FIM log source is not configured correctly. Please provide proper log source identifier and listen port.</td>
</tr>
<tr>
<td>QRFIM-300</td>
<td>There is some error with the saved Qualys JWT Auth token. However, do not worry we will generate a new token.</td>
</tr>
<tr>
<td>QRFIM-301</td>
<td>Could not get Qualys JWT Auth token. Please check job logs for more information.</td>
</tr>
<tr>
<td>QRFIM-302</td>
<td>We were not able to get a valid response from Qualys API. Please check the job logs.</td>
</tr>
<tr>
<td>QRFIM-303</td>
<td>Qualys REST API concurrency limit reached. We will retry to fetch the data. If you need to improve the job process speed, please increase the concurrency limit for your account.</td>
</tr>
<tr>
<td>QRFIM-304</td>
<td>You are unauthorized to make Qualys JWT Auth token call. Please check with Qualys support for more information.</td>
</tr>
<tr>
<td>QRFIM-305</td>
<td>Saved Qualys JWT Auth token is expired. Do not worry we will generate a new token.</td>
</tr>
<tr>
<td>QRFIM-306</td>
<td>We got an unexpected response while getting Qualys JWT Auth token. However, do not worry we will generate a new token.</td>
</tr>
<tr>
<td>Code</td>
<td>Message</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
</tr>
<tr>
<td>QRFIM-307</td>
<td>Invalid Qualys POD details provided. Please provide the correct information.</td>
</tr>
<tr>
<td>QRFIM-308</td>
<td>Check if Qualys POD credentials are correct.</td>
</tr>
<tr>
<td>QRFIM-309</td>
<td>Socket error during Qualys REST API request. Please check with Qualys support for more information.</td>
</tr>
<tr>
<td>QRFIM-310</td>
<td>Unknown exception during Qualys REST API request. Please check the job logs.</td>
</tr>
<tr>
<td>QRFIM-311</td>
<td>Server URL or Username or Password should not be empty. Please update them from the app settings page.</td>
</tr>
<tr>
<td>QRFIM-312</td>
<td>exception while validating the Start Date for Job. Please provide the Date-Time format as YYYY-MM-DDTHH:MM:SS.msZ &amp; greater than 2017-01-01T00:00:00.000Z.</td>
</tr>
<tr>
<td>QRFIM-313</td>
<td>Invalid Start Date for Job. Please provide the Date-Time format as YYYY-MM-DDTHH:MM:SS.msZ &amp; greater than 2017-01-01T00:00:00.000Z.</td>
</tr>
<tr>
<td>QRFIM-314</td>
<td>We encountered an exception while validating the Qualys app configuration. Please check the job logs.</td>
</tr>
<tr>
<td>QRFIM-315</td>
<td>An invalid proxy is provided on the app settings page. Please validate if the proxy details provided are valid.</td>
</tr>
<tr>
<td>QRFIM-316</td>
<td>Got None in the API response. Qualys JWT Auth Token not received. Please check with Qualys support if the POD details are correct and authorized for FIM API.</td>
</tr>
<tr>
<td>QRFIM-317</td>
<td>There was an ambiguous exception that occurred while handling your API request.</td>
</tr>
<tr>
<td>QRFIM-318</td>
<td>Got ConnectionError while API request.</td>
</tr>
<tr>
<td>QRFIM-319</td>
<td>API request timeout reached. Will retry once.</td>
</tr>
<tr>
<td>QRFIM-320</td>
<td>Received 401 unauthorized from JWT auth token API response.</td>
</tr>
<tr>
<td>QRFIM-321</td>
<td>Received 403 forbidden from JWT auth token API response.</td>
</tr>
<tr>
<td>QRFIM-400</td>
<td>We did not get any count from Qualys API for your POD. No new event in the subscription.</td>
</tr>
<tr>
<td>QRFIM-401</td>
<td>We found some errors in the JSON data we received from Qualys API. Please check the job logs and the JSON file for the API request for more information.</td>
</tr>
<tr>
<td>QRFIM-402</td>
<td>Could not get the FIM data from Qualys REST API for the job.</td>
</tr>
<tr>
<td>QRFIM-403</td>
<td>Not able to parse the incomplete JSON data in file.</td>
</tr>
<tr>
<td>QRFIM-500</td>
<td>Please check the job logs for more information on which database file is required to run the job.</td>
</tr>
<tr>
<td>QRFIM-501</td>
<td>Log source not selected. Please select a valid Log source on the app settings page.</td>
</tr>
<tr>
<td>QRFIM-502</td>
<td>We were not able to decrypt the proxy password. Please check with Qualys Support.</td>
</tr>
<tr>
<td>QRFIM-503</td>
<td>Please provide a valid proxy host on the app settings page.</td>
</tr>
<tr>
<td>QRFIM-504</td>
<td>We were not able to decrypt the API password. Please check with Qualys Support.</td>
</tr>
<tr>
<td>QRFIM-505</td>
<td>Due to some exceptions, we are not able to rename the Qualys REST API response JSON file. Please check job logs for more information.</td>
</tr>
<tr>
<td>QRFIM-506</td>
<td>Due to some exceptions, we are not able to remove the Qualys REST API response JSON file. Please check job logs for more information.</td>
</tr>
<tr>
<td>QRFIM-507</td>
<td>Due to some exceptions, we are not able to save the Qualys REST API response JSON file. Please check job logs for more information.</td>
</tr>
<tr>
<td>QRFIM-508</td>
<td>You are trying to run the job which is already running. Please do not run another job manually.</td>
</tr>
<tr>
<td>QRFIM-509</td>
<td>While cleaning the JSON files we encountered an exception. Please check the job logs.</td>
</tr>
<tr>
<td>QRFIM-510</td>
<td>FIM Incidents log source not selected. Please select a valid Log source on the app settings page.</td>
</tr>
</tbody>
</table>