Qualys FIM for QRadar - QRadar 7.3.3 FP6+/7.4.1 FP2+/7.4.2 GA+

User Guide

Version 1.1.0

December 1, 2021

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

Table of Contents

Introduction to Qualys FIM for QRadar - QRadar 7.3.3 FP6+/7.4.1 FP2+/7.4.2 GA+

Use the Qualys FIM for QRadar 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 will 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 FP6, 7.4.1 FP2, 7.4.2GA+

Install 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 button.
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.

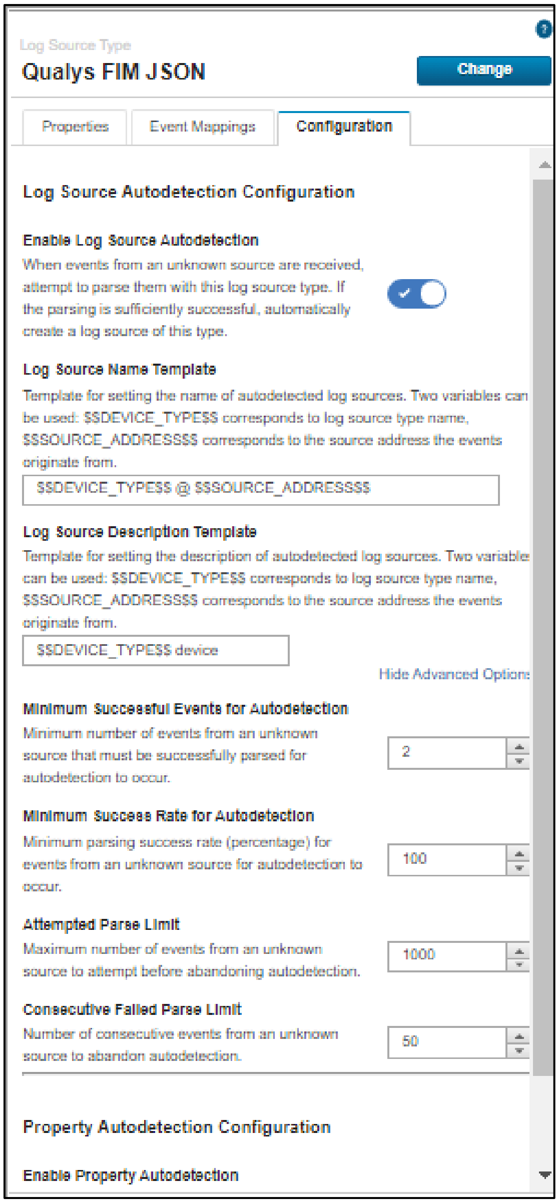
DSM Editor

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 JSON

Log Source Autodetection Configuration

Enable Log Source Autodetection

When events from an unknown source are received, attempt to parse them with this log source type. If the parsing is sufficiently successful, automatically create a log source of this type.

Log Source Name Template

Template for setting the name of autodetected log sources. Two variables can be used: $$DEVICE_TYPE$$ corresponds to log source type name, $$SOURCE_ADDRESS$$ corresponds to the source address the events originate from.

$$DEVICE_TYPE$$ @ $$SOURCE_ADDRESS$$

Log Source Description Template

Template for setting the description of autodetected log sources. Two variable can be used: $$DEVICE_TYPE$$ corresponds to log source type name, $$SOURCE_ADDRESS$$ corresponds to the source address the events originate from.

$$DEVICE_TYPE$$ device

Minimum Successful Events for Autodetection

Minimum number of events from an unknown source that must be successfully parsed for autodetection to occur.

2

Minimum Success Rate for Autodetection

Minimum parsing success rate (percentage) for events from an unknown source for autodetection to occur.

100

Attempted Parse Limit

Maximum number of events from an unknown source to attempt before abandoning autodetection.

1000

Consecutive Failed Parse Limit

Number of consecutive events from an unknown source to abandon autodetection.

50

Property Autodetection Configuration

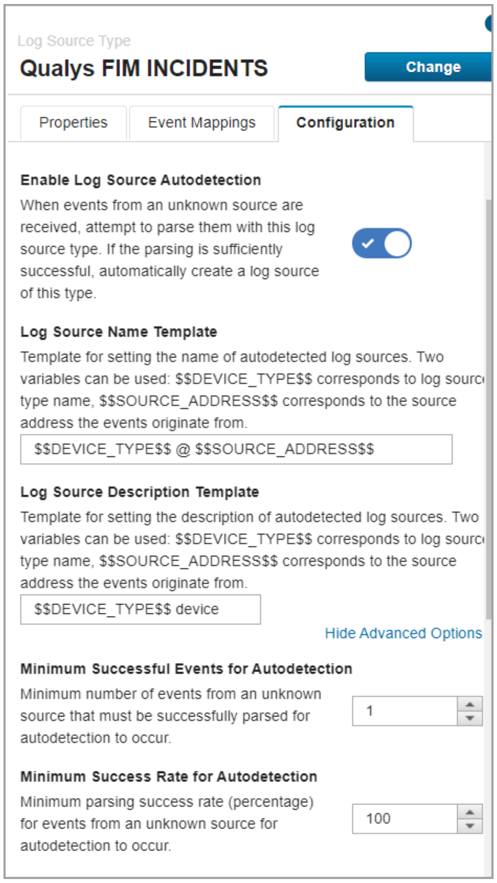
Enable Property Autodetection

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 Type

Qualys FIM INCIDENTS

Enable Log Source Autodetection

When events from an unknown source are received, attempt to parse them with this log source type. If the parsing is sufficiently successful, automatically create a log source of this type.

Log Source Name Template

Template for setting the name of autodetected log sources. Two variables can be used: $$DEVICE_TYPE$$ corresponds to log sourc type name, $$SOURCE_ADDRESS$$ corresponds to the source address the events originate from.

$$DEVICE_TYPE$$ @ $$SOURCE_ADDRESS$$

Log Source Description Template

Template for setting the description of autodetected log sources. Two variables can be used: $$DEVICE_TYPE$$ corresponds to log sourc type name, $$SOURCE_ADDRESS$$ corresponds to the source address the events originate from.

$$DEVICE_TYPE$$ device

Hide Advanced Options

Minimum Successful Events for Autodetection

Minimum number of events from an unknown source that must be successfully parsed for autodetection to occur.

1

Minimum Success Rate for Autodetection

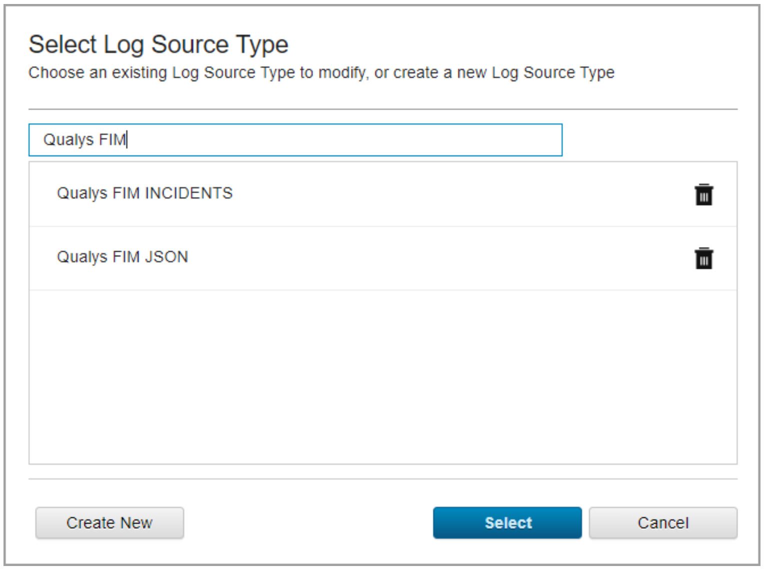
Minimum parsing success rate (percentage) for events from an unknown source for autodetection to occur.

100

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**.



Select Log Source Type

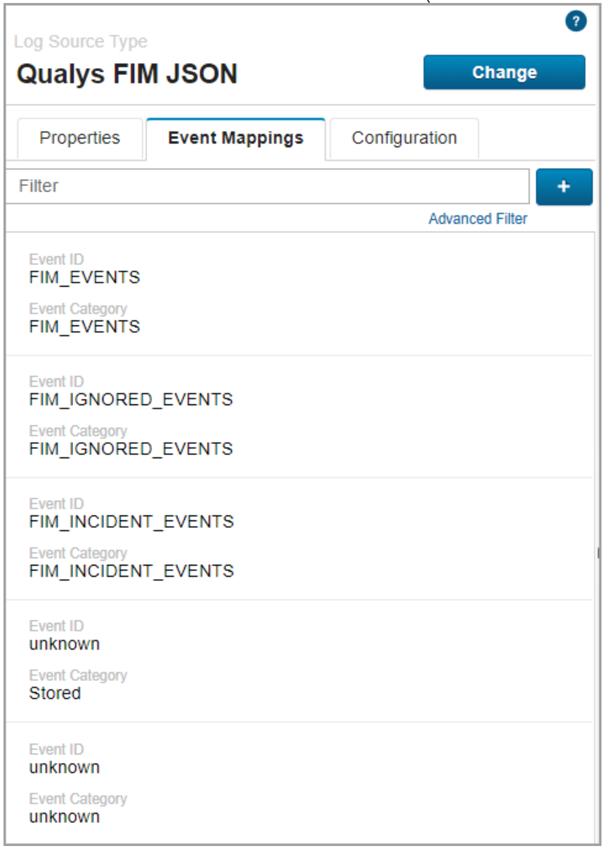
Choose an existing Log Source Type to modify, or create a new Log Source Type

Qualys FIM

Qualys FIM INCIDENTS

Qualys FIM JSON

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).



Log Source Type

Qualys FIM JSON

Event ID
FIM_EVENTS
Event Category
FIM_EVENTS

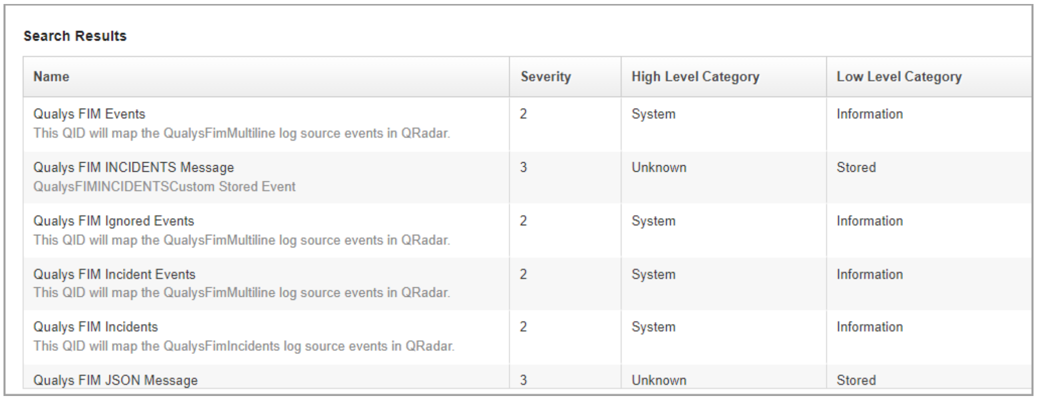
Event ID
FIM_IGNORED_EVENTS
Event Category
FIM_IGNORED_EVENTS

Event ID
FIM_INCIDENT_EVENTS
Event Category
FIM_INCIDENT_EVENTS

Event ID
unknown
Event Category
Stored

Event ID
unknown
Event Category
unknown

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

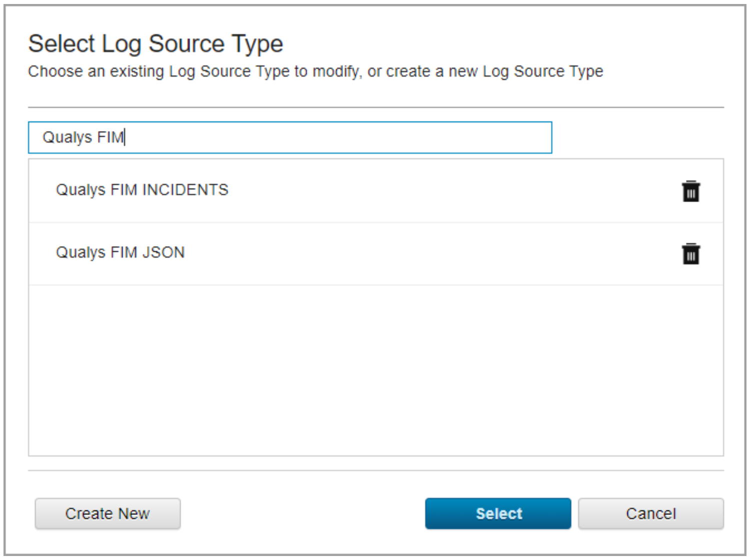
Name	Severity	High Level Category	Low Level Category
Qualys FIM Events This QID will map the QualysFimMultiline log source events in QRadar.	2	System	Information
Qualys FIM INCIDENTS Message QualysFIMINCIDENTSCustom Stored Event	3	Unknown	Stored
Qualys FIM Ignored Events This QID will map the QualysFimMultiline log source events in QRadar.	2	System	Information
Qualys FIM Incident Events This QID will map the QualysFimMultiline log source events in QRadar.	2	System	Information
Qualys FIM Incidents This QID will map the QualysFimIncidents log source events in QRadar.	2	System	Information
Qualys FIM JSON Message	3	Unknown	Stored

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**.
   This takes you back to "Create a new Event Mapping" window.
8) Click **Create**. This will take you back to "Event Mappings" window.
   You can verify the new event mapping created.
9) Finally, 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**.



Select Log Source Type

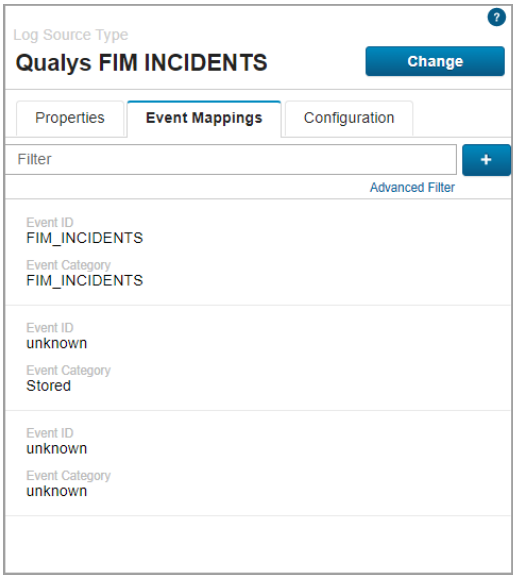
Choose an existing Log Source Type to modify, or create a new Log Source Type

Qualys FIM

Qualys FIM INCIDENTS

Qualys FIM JSON

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).



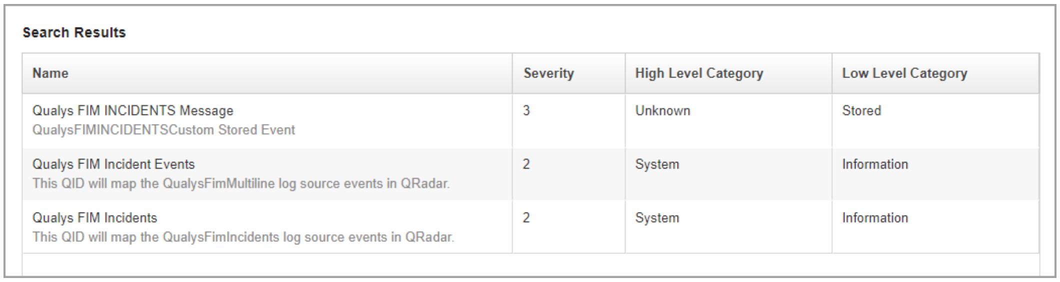
Log Source Type
Qualys FIM INCIDENTS

Event ID
FIM_INCIDENTS
Event Category
FIM_INCIDENTS

Event ID
unknown
Event Category
Stored

Event ID
unknown
Event Category
unknown

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
    - Low Level Category: Any
    - Log Source Type: Any
    - QID/Name: In this text box, user must search for Qualys FIM, click **Search**.



Search Results

Name	Severity	High Level Category	Low Level Category
Qualys FIM INCIDENTS Message QualysFIMINCIDENTSCustom Stored Event	3	Unknown	Stored
Qualys FIM Incident Events This QID will map the QualysFimMultiline log source events in QRadar.	2	System	Information
Qualys FIM Incidents This QID will map the QualysFimIncidents log source events in QRadar.	2	System	Information

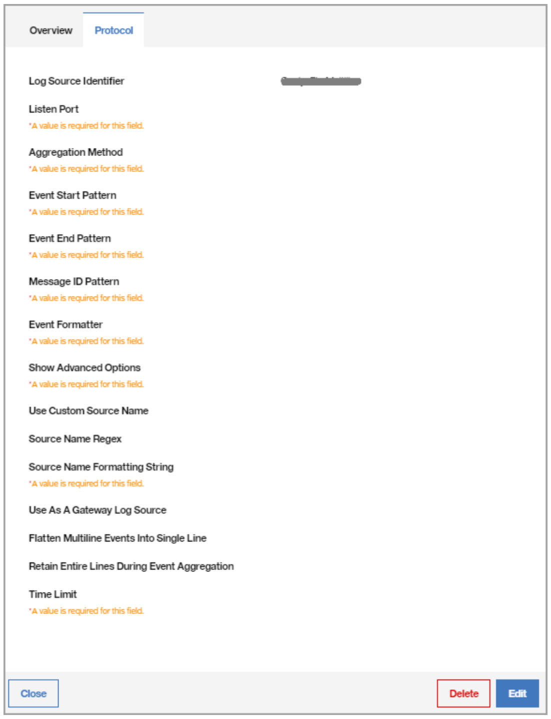
Search results will be displayed based on the QID/Name entered.

6) Choose the option Qualys FIM Incidents.
7) Click **OK**.
   This takes you back to “Create a new Event Mapping” window.
8) Click **Create**. This will take you back to “Event Mappings” window.
   You can verify the new event mapping created.
9) Finally, 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.



Log Source Identifier [redacted]

Listen Port
*A value is required for this field.

Aggregation Method
*A value is required for this field.

Event Start Pattern
*A value is required for this field.

Event End Pattern
*A value is required for this field.

Message ID Pattern
*A value is required for this field.

Event Formatter
*A value is required for this field.

Show Advanced Options
*A value is required for this field.

Use Custom Source Name

Source Name Regex

Source Name Formatting String
*A value is required for this field.

Use As A Gateway Log Source

Flatten Multiline Events Into Single Line

Retain Entire Lines During Event Aggregation

Time Limit
*A value is required for this field.

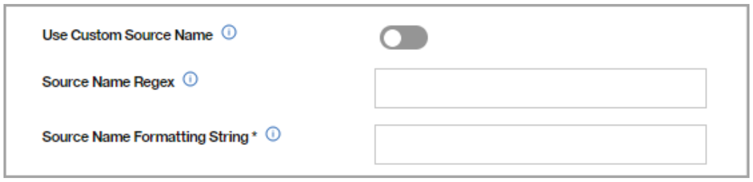
You need to create/edit the custom log source for the Qualys app using the following steps. Keep the configuration of custom log source same as that mentioned below:-

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.

Property	Value
Log Source Name*	QualysFimMultiline (Customizable)
Log Source Description	QualysFimMultiline
Log Source Type*	Qualys FIM JSON
Protocol Configuration*	TCP Multiline Syslog
Log Source Identifier*	QualysFimMultiline (Customizable, but same as Log Source Name)
Listen Port	12400 (Customizable)
Aggregation Method*	Start/End Matching
Event Start Pattern*	[A-Z][a-z][a-z]\s\d\d\s\d\d:\d\d:\d\d\s

Event End Pattern*	qualys_event_ends
Event Formatter*	No Formatting
Show Advance Option*	Yes
Use Custom Source Name*	Unchecked
Use As A Gateway Log Source*	Checked
Flatten Multiline Events Into Single Line*	Checked
Retain Entire Lines During Event Aggregation*	Checked
Enabled*	Checked
Credibility	5
Target Event Collector	<default/your choice>
Coalescing Events*	Unchecked
Store Event Payload*	Checked
Log Source Extension*	QualysFIMJSONCustom_ext

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.



Use Custom Source Name

Source Name Regex

Source Name Formatting String *

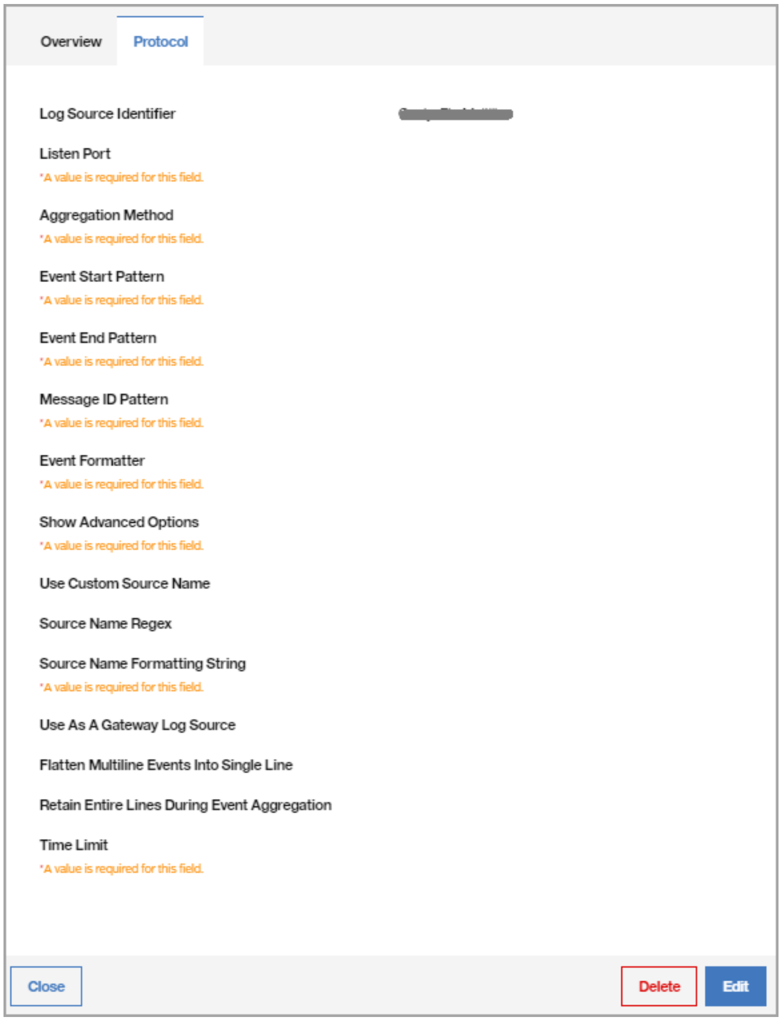
Enable and then disable the "Use Custom Source Name" option. As a result, QRadar removes those fields from mandatory fields.

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.



Log Source Identifier [redacted]

Listen Port
*A value is required for this field.

Aggregation Method
*A value is required for this field.

Event Start Pattern
*A value is required for this field.

Event End Pattern
*A value is required for this field.

Message ID Pattern
*A value is required for this field.

Event Formatter
*A value is required for this field.

Show Advanced Options
*A value is required for this field.

Use Custom Source Name

Source Name Regex

Source Name Formatting String
*A value is required for this field.

Use As A Gateway Log Source

Flatten Multiline Events Into Single Line

Retain Entire Lines During Event Aggregation

Time Limit
*A value is required for this field.

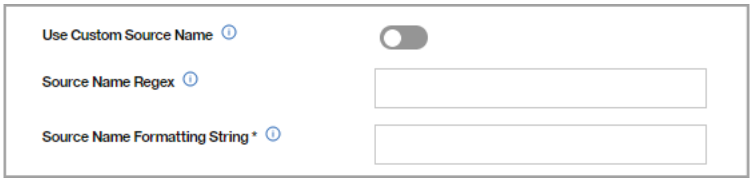
You need to create/edit the custom log source for the Qualys app using the following steps. Keep the configuration of custom log source same as that mentioned below:-

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.

Property	**Value**
Log Source Name*	QualysFimIncidents(Customizable)
Log Source Description	QualysFimIncidents
Log Source Type*	Qualys FIM INCIDENTS
Protocol Configuration*	TCP Multiline Syslog

Log Source Identifier*	QualysFimIncidents (Customizable, but same as Log Source Name)
Listen Port	12400 (Customizable)
Aggregation Method*	Start/End Matching
Event Start Pattern*	[A-Z][a-z][a-z]\s\d\d\s\d\d:\d\d:\d\d\s
Event End Pattern*	qualys_event_ends
Event Formatter*	No Formatting
Show Advance Option*	Yes
Use Custom Source Name*	Unchecked
Use As A Gateway Log Source*	Checked
Flatten Multiline Events Into Single Line*	Checked
Retain Entire Lines During Event Aggregation*	Checked
Enabled*	Checked
Credibility	5
Target Event Collector	<default/your choice>
Coalescing Events*	Unchecked
Store Event Payload*	Checked
Log Source Extension*	QualysFIMINCIDENTCustom_ext

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.



Use Custom Source Name ⓘ

Source Name Regex ⓘ

Source Name Formatting String * ⓘ

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.

   Qualys related properties are:

Field name	Expression	Log Source Type
Absolute File Path	/"fullPath"	Qualys FIM JSON
Absolute Process Path	/"actor"/"imagePath"	Qualys FIM JSON
Action	/"action"	Qualys FIM JSON
Agent Version	/"asset"/ "agentVersion"	Qualys FIM JSON
Asset Interfaces	/"assetInterfaces"	Qualys FIM JSON
Asset Name	/"asset"/"name"	Qualys FIM JSON
Asset Tags	/"asset"/"tags"[]	Qualys FIM JSON
Attribute New	/"attributes"/"new"[]	Qualys FIM JSON
Attribute Old	/"attributes"/"old"[]	Qualys FIM JSON
Category name	/"profiles"[0]/"category"/"name"	Qualys FIM JSON
Event Alert	/"name"	Qualys FIM JSON
Event Incident Id	/"incidentId"	Qualys FIM JSON
Event Incident Name	/"incidentName"	Qualys FIM JSON
Event UUID	/"id"	Qualys FIM JSON
Event Type	/"type"	Qualys FIM JSON
File Certificate Hash	/"fileCertificateHash"	Qualys FIM JSON
File Hash	/"fileContentHash"	Qualys FIM JSON
File Reputation Status	/"reputationStatus"	Qualys FIM JSON
File Trust Status	/"trustStatus"	Qualys FIM JSON
Incident Approval Status	/"approvalStatus"	Qualys FIM INCIDENTS
Incident Approval Type	/"approvalType"	Qualys FIM INCIDENTS
Incident Assignee	/"reviewers"[]	Qualys FIM INCIDENTS
Incident Change Type	/"changeType"	Qualys FIM INCIDENTS
Incident Correlation Rule ID	/"ruleId"	Qualys FIM INCIDENTS
Incident Correlation Rule Name	/"ruleName"	Qualys FIM INCIDENTS
Incident Disposition Category	/"dispositionCategory"	Qualys FIM INCIDENTS
Incident ID	/"id"	Qualys FIM INCIDENTS
Incident Name	/"name"	Qualys FIM INCIDENTS
Incident Status	/"status"	Qualys FIM INCIDENTS
Incident Type	/"type"	Qualys FIM INCIDENTS
Monitoring Profile	/"profiles"[0]/"name"	Qualys FIM JSON
New Content	/"newContent"	Qualys FIM JSON
New Registry Value Content	/"newRegistryValueContent"	Qualys FIM JSON
New Registry Value Type	/"newRegistryValueType"	Qualys FIM JSON
Old Content	/"oldContent"	Qualys FIM JSON
Old Registry Value Content	/"oldRegistryValueContent"	Qualys FIM JSON
Old Registry Value Type	/"oldRegistryValueType"	Qualys FIM JSON
Platform	/"platform"	Qualys FIM JSON
Process ID	/"actor"/"processID"	Qualys FIM JSON

Field name	Expression	Log Source Type
Process Name	/"actor"/"process"	Qualys FIM JSON
Registry Name	/"registryName"	Qualys FIM JSON
Registry Path	/"registryPath"	Qualys FIM JSON
Rules ID	/"profiles"[0]/"rules"[0]/"id"	Qualys FIM JSON
Rules name	/"profiles"[0]/"rules"[0]/"name"	Qualys FIM JSON
Section ID	/"profiles"[0]/"rules"[0]/"section"/"id"	Qualys FIM JSON
Section Name	/"profiles"[0]/"rules"[0]/"section"/"name"	Qualys FIM JSON
Source Host Name	/"asset"/"interfaces"[0]/"hostname"	Qualys FIM JSON
User ID	/"actor"/"userID"	Qualys FIM JSON
Qradar Data Type	/"qradarDataType"	Qualys FIM INCIDENTS
Qradar Event Type	/"qradarEventType"	Qualys FIM JSON
Severity Level	/"severity"	Qualys FIM JSON

For the Qualys related properties, complete these checks:

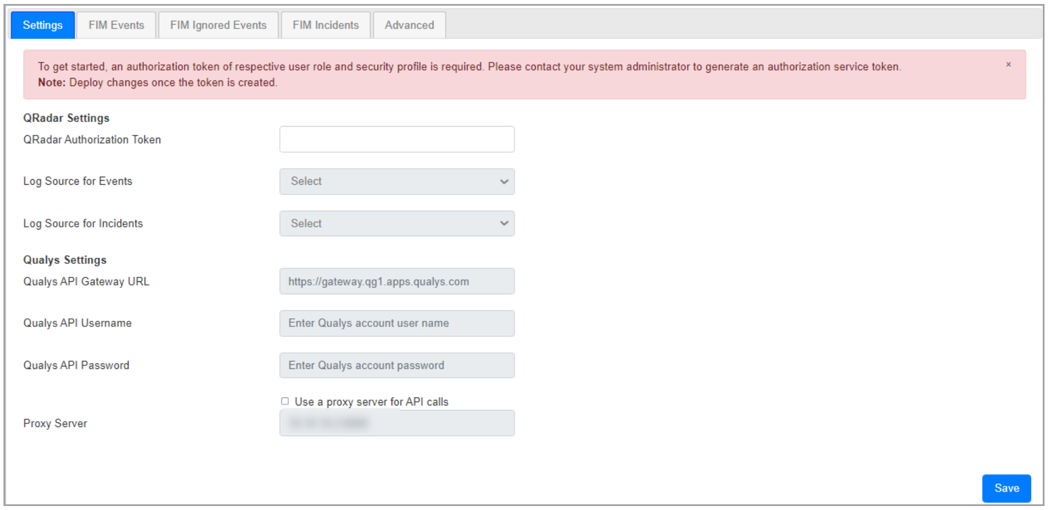
1) If any property is disabled, enable it.
2) If any property does not belong to the Qualys FIM JSON/Qualys FIM Incidents log source type, please open it to edit and select Qualys FIM JSON or Qualys FIM Incidents as the log source type.
3) Do not select any specific Log source, select **All** in the 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.

Configure 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.



To get started, an authorization token of respective user role and security profile is required. Please contact your system administrator to generate an authorization service token.
Note: Deploy changes once the token is created.

QRadar Settings

QRadar Authorization Token

Log Source for Events: Select

Log Source for Incidents: Select

Qualys Settings

Qualys API Gateway URL: https://gateway.qg1.apps.qualys.com

Qualys API Username: Enter Qualys account user name

Qualys API Password: Enter Qualys account password

□ Use a proxy server for API calls

Proxy Server: [redacted]

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:

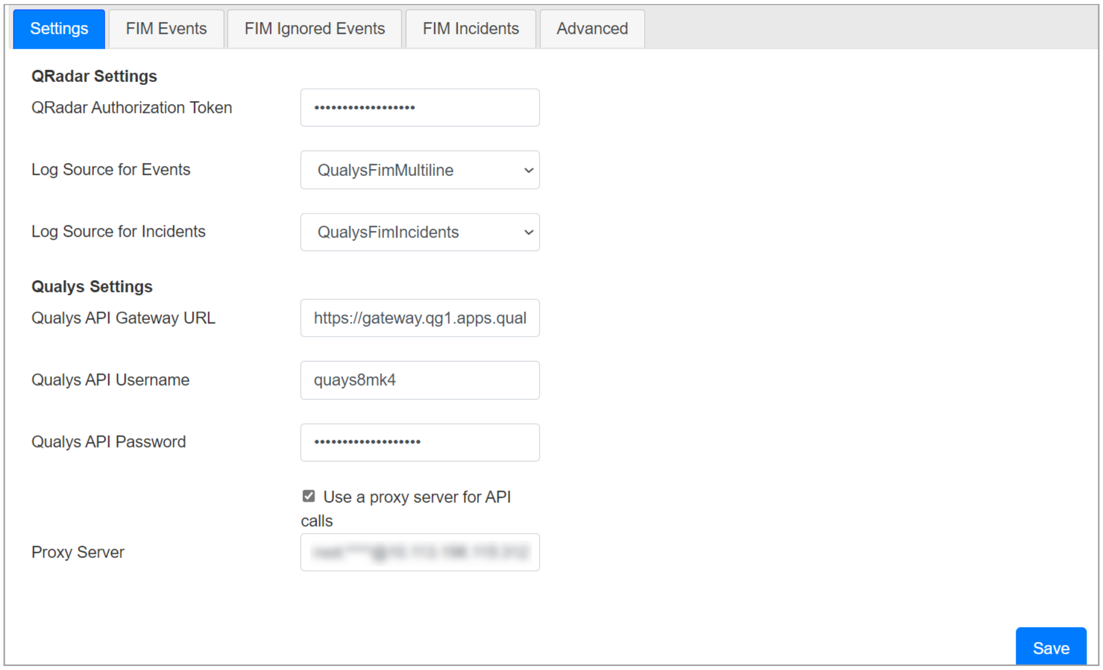
1) Go to **Authorized Services** in Admin tab
2) Click **Add Authorized Service.**
3) Enter the desired **Service Name.**
4) Select **User Role** as *Admin.*
5) Select **Security Profile** as *Admin.*
6) Set the expiry date as required.
7) Click **Create Service** and then click **Deploy changes**.

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

8) 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



QRadar Settings

QRadar Authorization Token	••••••••••••••••••
Log Source for Events	QualysFimMultiline
Log Source for Incidents	QualysFimIncidents

Qualys Settings

Qualys API Gateway URL	https://gateway.qg1.apps.qual
Qualys API Username	quays8mk4
Qualys API Password	•••••••••••••••••••
	☑ Use a proxy server for API calls
Proxy Server	[redacted]

Proxy Configuration

If you want Qualys app to use proxy while calling the API, configure proxy details.

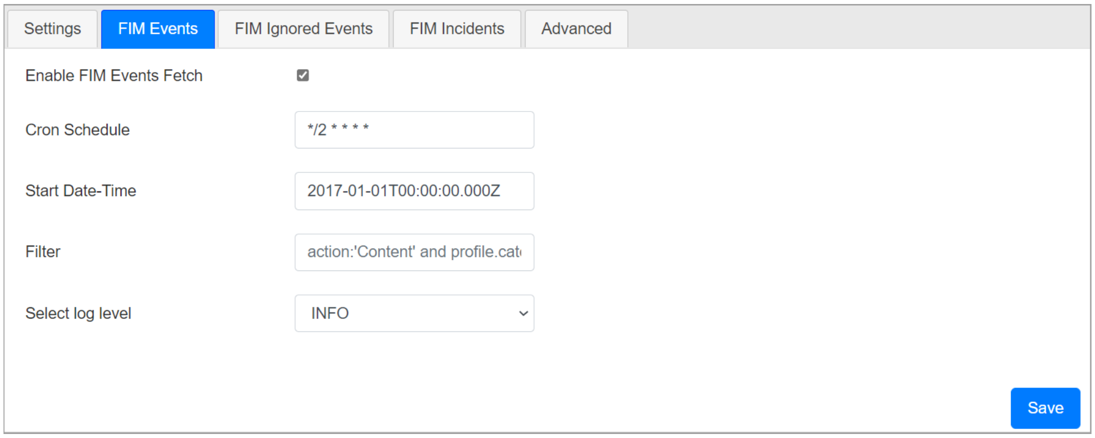
Select the check box to enable proxy.

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.



Enable FIM Events Fetch	☑
Cron Schedule	*/2 * * * *
Start Date-Time	2017-01-01T00:00:00.000Z
Filter	action:'Content' and profile.cat
Select log level	INFO

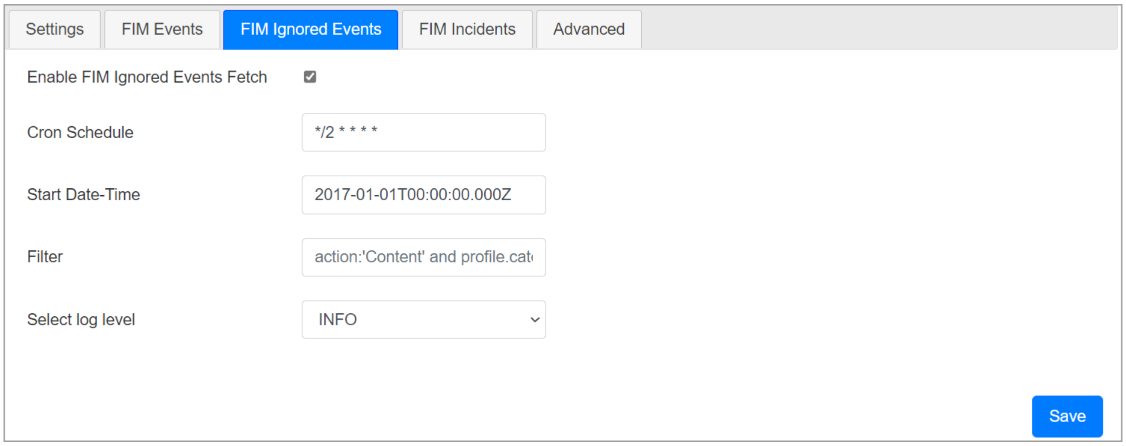
1) Tick the "Enable FIM Events Fetch" checkbox to enable this data input.
2) In the "Cron Schedule" field, enter a valid cron format entry. This is a mandatory field if the "Enable FIM Events" checkbox is checked. Learn about cron expressions…
3) In the "Start Date-Time" field, enter the date-time from 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.



Enable FIM Ignored Events Fetch ☑

Cron Schedule: */2 * * * *

Start Date-Time: 2017-01-01T00:00:00.000Z

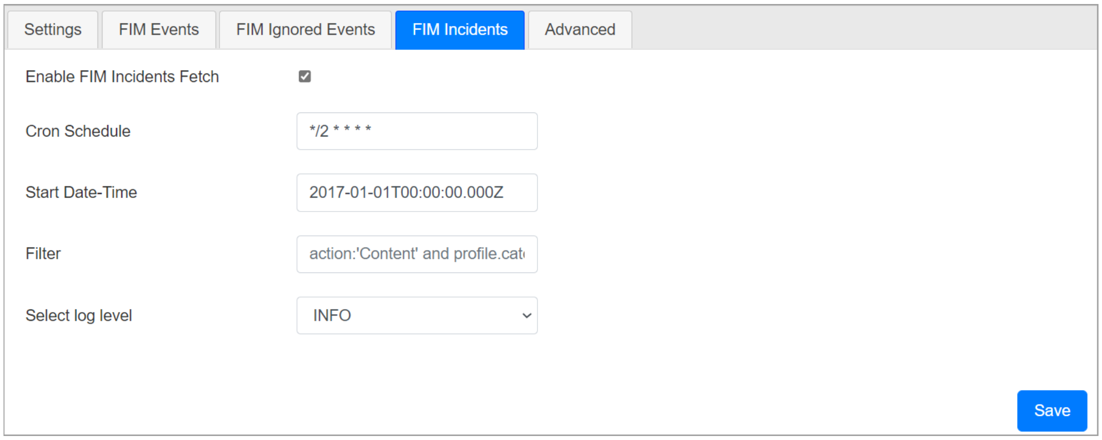
Filter: action:'Content' and profile.cat

Select log level: INFO

1) Tick the "Enable FIM Ignored 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 Ignored Events" checkbox is checked.
3) 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.
4) 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.
5) 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.

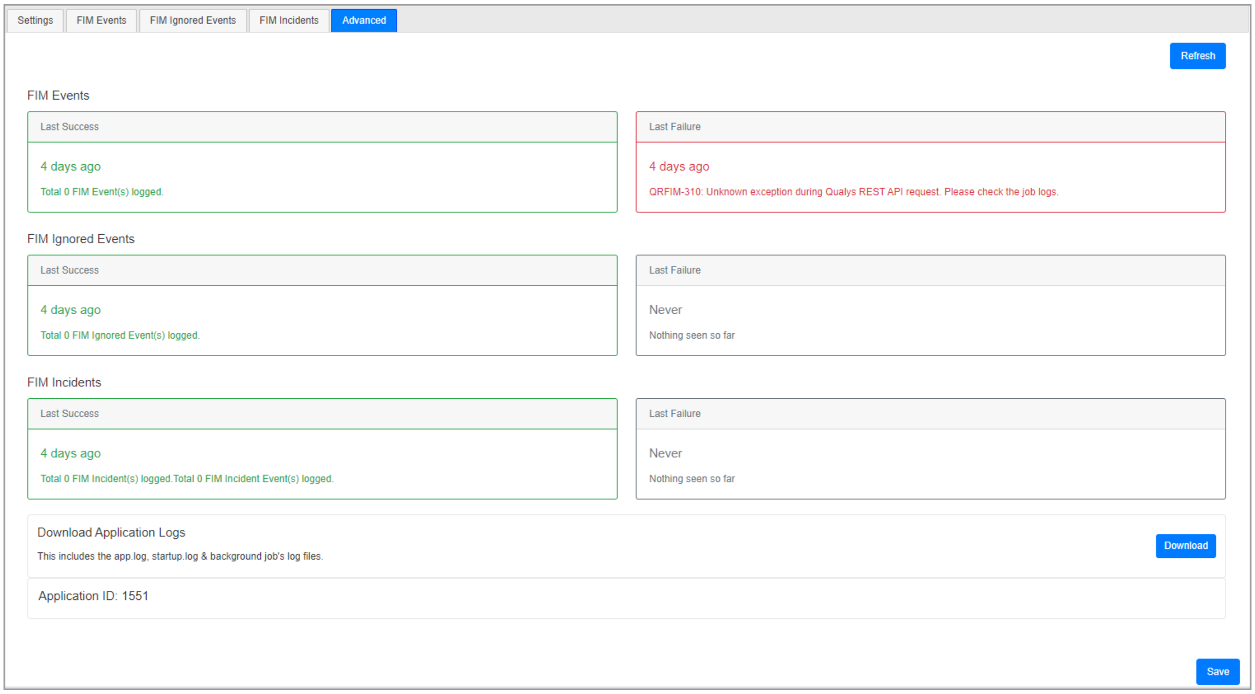


Enable FIM Incidents Fetch	☑
Cron Schedule	*/2 * * * *
Start Date-Time	2017-01-01T00:00:00.000Z
Filter	action:'Content' and profile.cat
Select log level	INFO

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

Advanced

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



FIM Events

Last Success	Last Failure
4 days ago Total 0 FIM Event(s) logged.	4 days ago QRFIM-310: Unknown exception during Qualys REST API request. Please check the job logs.

FIM Ignored Events

Last Success	Last Failure
4 days ago Total 0 FIM Ignored Event(s) logged.	Never Nothing seen so far

FIM Incidents

Last Success	Last Failure
4 days ago Total 0 FIM Incident(s) logged.Total 0 FIM Incident Event(s) logged.	Never Nothing seen so far

Download Application Logs

This includes the app.log, startup.log & background job's log files.

Application ID: 1551

Advanced Configuration

These are the advanced and optional configurations which provides you additional benefits while using Qualys FIM for QRadar - QRadar 7.3.3 FP6+/7.4.1 FP2+/7.4.2 GA+!

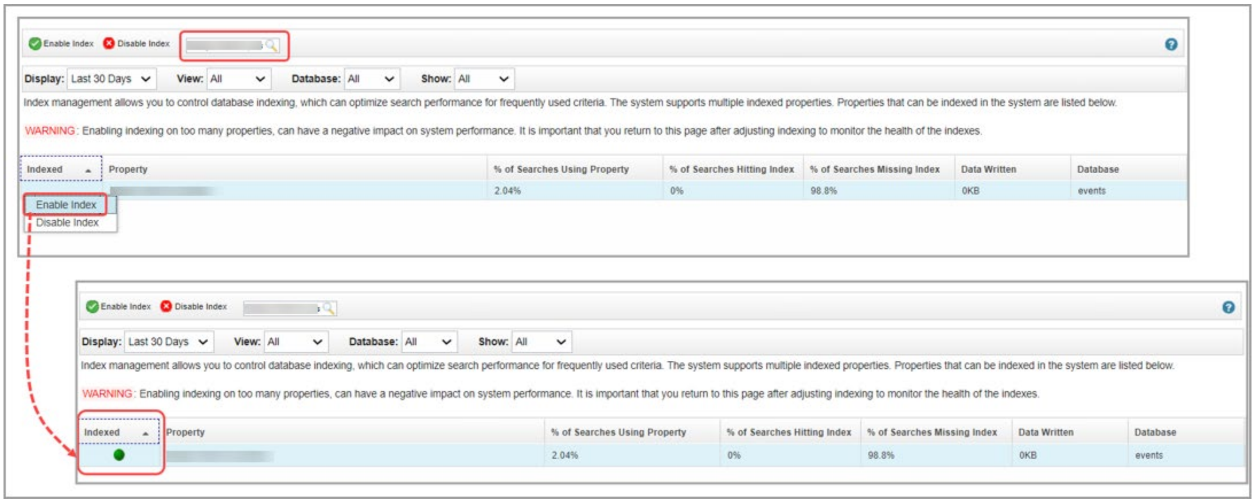
Index Management

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.



Display: Last 30 Days View: All Database: All Show: All

Index management allows you to control database indexing, which can optimize search performance for frequently used criteria. The system supports multiple indexed properties. Properties that can be indexed in the system are listed below.

WARNING: Enabling indexing on too many properties, can have a negative impact on system performance. It is important that you return to this page after adjusting indexing to monitor the health of the indexes.

Indexed	Property	% of Searches Using Property	% of Searches Hitting Index	% of Searches Missing Index	Data Written	Database
	[redacted]	2.04%	0%	98.8%	0KB	events

Display: Last 30 Days View: All Database: All Show: All

Index management allows you to control database indexing, which can optimize search performance for frequently used criteria. The system supports multiple indexed properties. Properties that can be indexed in the system are listed below.

WARNING: Enabling indexing on too many properties, can have a negative impact on system performance. It is important that you return to this page after adjusting indexing to monitor the health of the indexes.

Indexed	Property	% of Searches Using Property	% of Searches Hitting Index	% of Searches Missing Index	Data Written	Database
●	[redacted]	2.04%	0%	98.8%	0KB	events

3) Click **Save**.

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.)

```
select "User ID" , "Source Host Name" , "Asset Name" , "Event UUID" , "Event
Alert" , "Severity Level" , "Process Name" , "Process Id" , "Absolute File
Path" from events WHERE LOGSOURCENAME(logsourceid) = 'QualysFimMultiline'
```

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.

AQL: select "Absolute File Path" , "Absolute Process Path" , "Action" , "Agent Version" , "Asset Interfaces" , "Asset Name" , "Asset Tags" , "Attribute New" , "Attribute Old" , "Category Name" , "Event Alert" , "Event Type" , "Event UUID", "File Certificate Hash" , "File Reputation Status" , "File Trust Status", "Monitoring Profile" , "New Content" , "New Registry Value Content" , "New Registry Value Type","Old Content", "New Registry Value Content", "New Registry Value Type" , "Platform", "Process Id", "Process Name", "Qradar Event Type", "Registry Name", "Registry Path", "Rules ID" , "Rule Name", "Section ID", "Section Name", "Severity Level", "Source Host Name" , "User ID", DATEFORMAT(devicetime,'yyyy-MM- dd h:m:ss:SSS z')as "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.

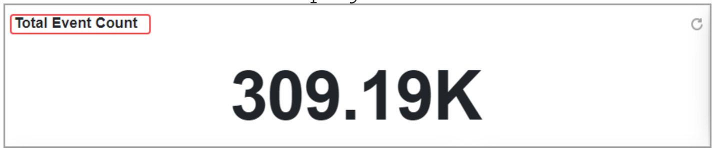
```
SELECT "Incident ID" , "Incident Name" , "Incident Status" , "Incident Type"
, "Incident Approval Type", "Incident Approval Status" , "Incident Assignee"
, "Incident Change Type" , "Incident Correlation Rule ID" , "Incident
Correlation Rule Name" , "Incident Disposition Category" from events where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

```
SELECT "Absolute File Path" , "Absolute Process Path" , "Action" , "Agent
Version" , "Asset Interfaces" , "Asset Name" , "Asset Tags" , "Attribute New"
, "Attribute Old" , "Category Name" , "Event Alert" , "Event Type" , "Event
UUID" , "File Certificate Hash" , "File Hash" , "File Reputation Status" ,
"File Trust Status" , "Monitoring Profile" , "New Content" , "New Registry
Value Content" , "New Registry Value Type" , "Old Content" , "Old Registry
Value Content" , "Old Registry Value Type" , "Platform" , "Process Id",
"Process Name" , "Qradar Event Type", "Registry Name" , "Registry
Path","Rules ID", "Rules Name", "Section ID", "Section Name", "Severity
Level", "Source Host Name", "User ID", DATEFORMAT(devicetime,'yyyy-MM-  dd
h:m:ss:SSS z')as "Log Source Time" FROM events WHERE
LOGSOURCENAME(logsourceid) = 'QualysFimMultiline' AND "Qradar Event Type"=
'FIM_INCIDENT_EVENTS'
```

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:

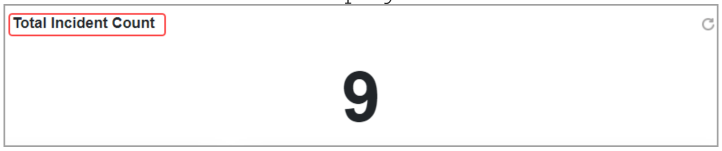
Total Event Count – Displays count of total FIM Events in the selected date range.



Total Event Count

309.19K

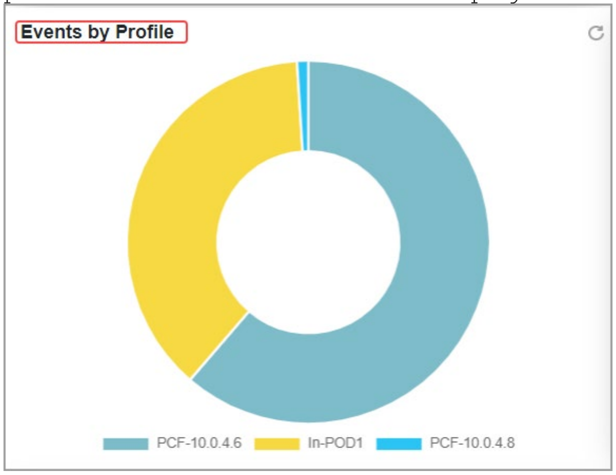
Total Incident Count – Displays count of total FIM Incidents in the selected date range.



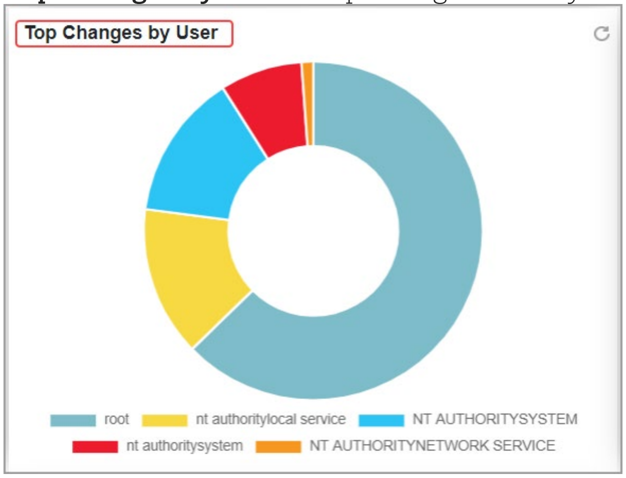
Total Incident Count

9

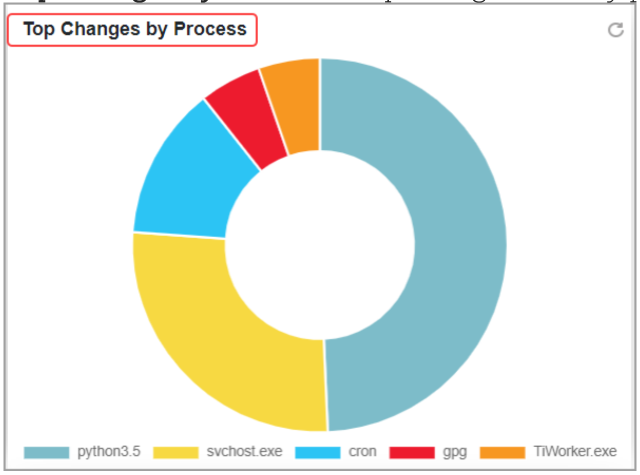
Events by Profile – Displays profile wise distribution of events. On mouse hover, the name of the profile and the count of events is displayed.



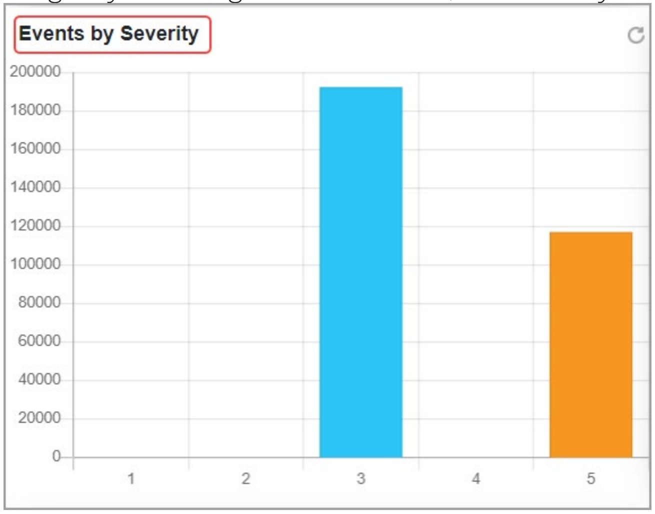
Top Changes by User – Top changes done by user in FIM events are displayed here.



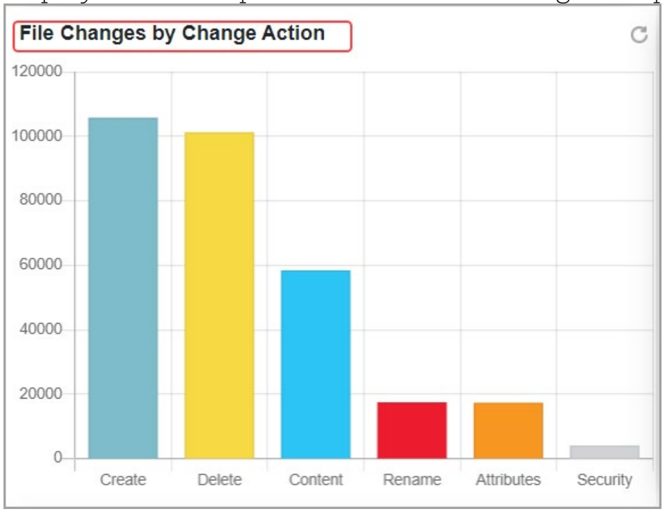
Top Changes by Process – Top changes done by process in FIM events are displayed here.



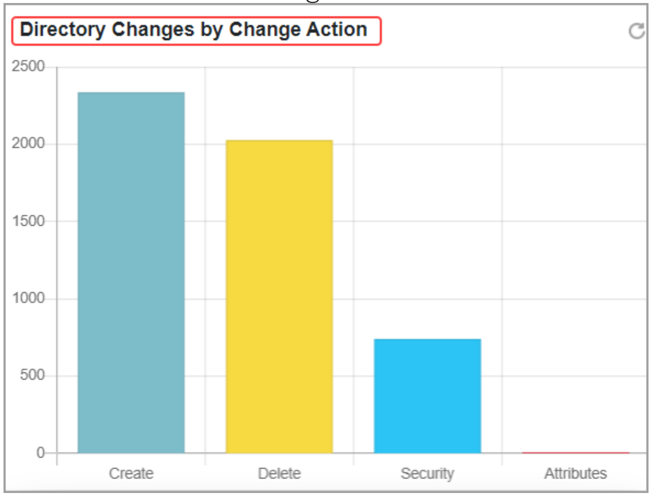
Events by Severity – Displays severity wise distribution of all FIM Events in the selected date range. By hovering over the mouse, the severity bars shows the count of events.



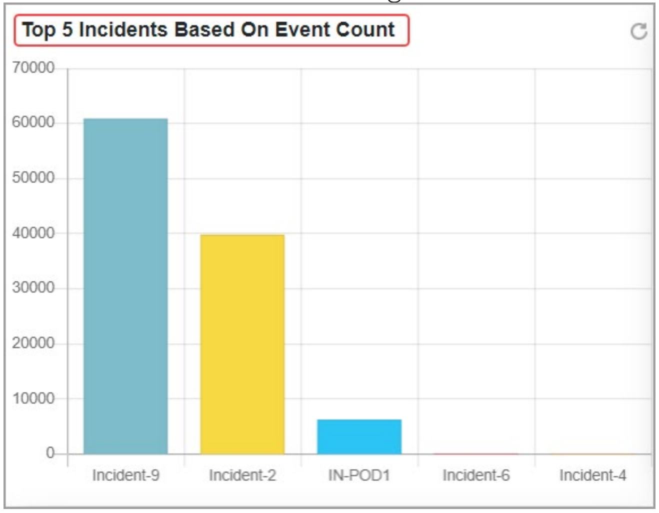
File Changes by Change Action – FIM Events for the file changes by their change action are displayed here. Top 10 actions for file changes are presented with their count.



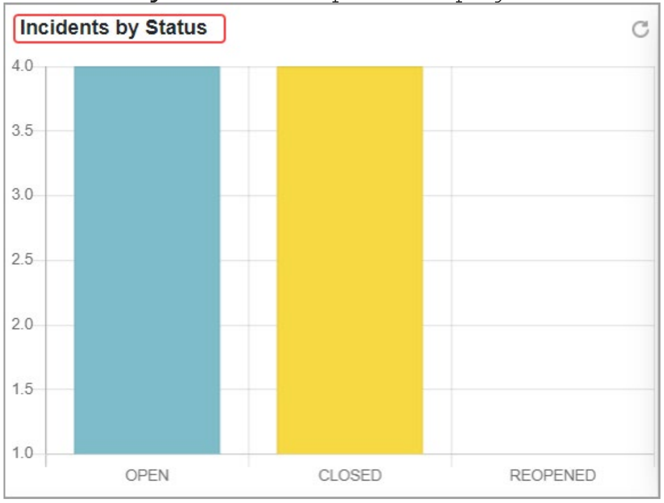
Directory Changes by Change Action – Graphical display of directory changes by change action in the selected date range.



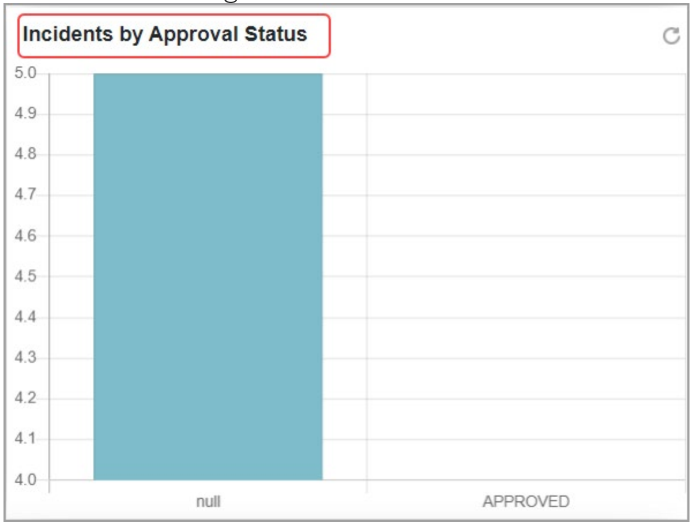
Top 5 Incidents Based on Event Count – Graphical display of top 5 incidents based on event count in the selected date range.



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



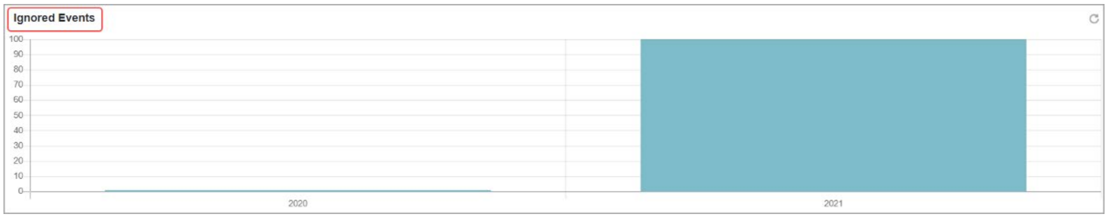
Incidents by Approval Status – Graphical display of incidents by their approval status in the selected date range.



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

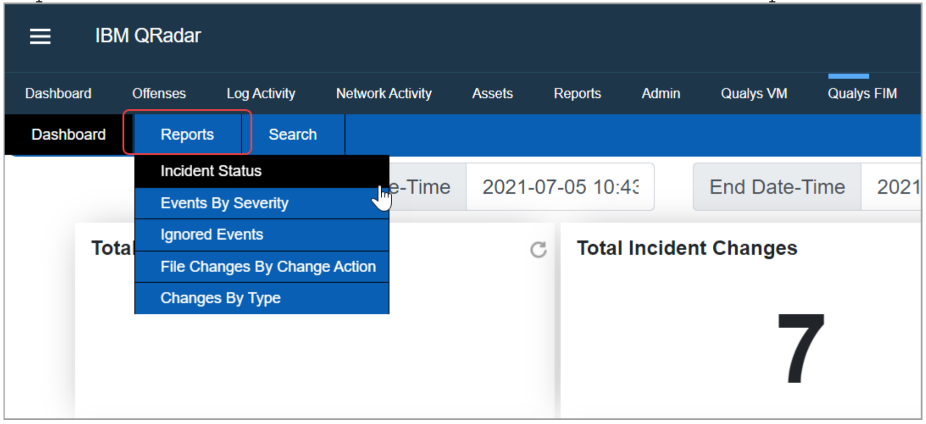
- If the start and end date difference is in the year(s), then show the bar chart year-wise.
- Else If the start and end date difference is in the month(s), then show the bar chart month-wise.
- Else If the start and end date difference is in the day(s), then show the bar chart day-wise.
- Else If the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

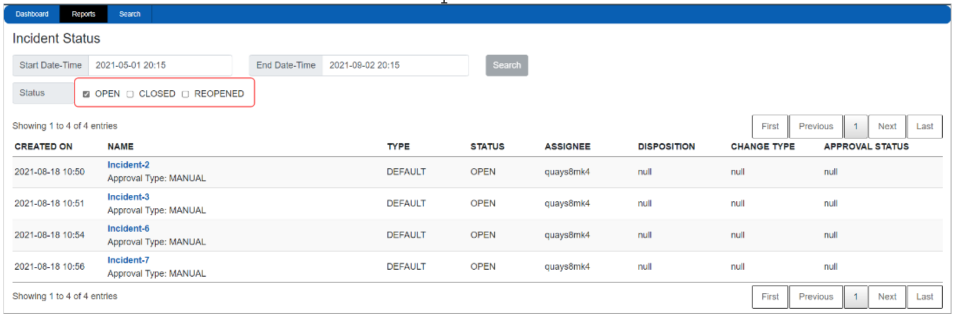
Reports Tab has different criteria for the user to view the reports.



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.



Incident Status

Start Date-Time 2021-05-01 20:15

End Date-Time 2021-09-02 20:15

Status ☑ OPEN ☐ CLOSED ☐ REOPENED

Showing 1 to 4 of 4 entries

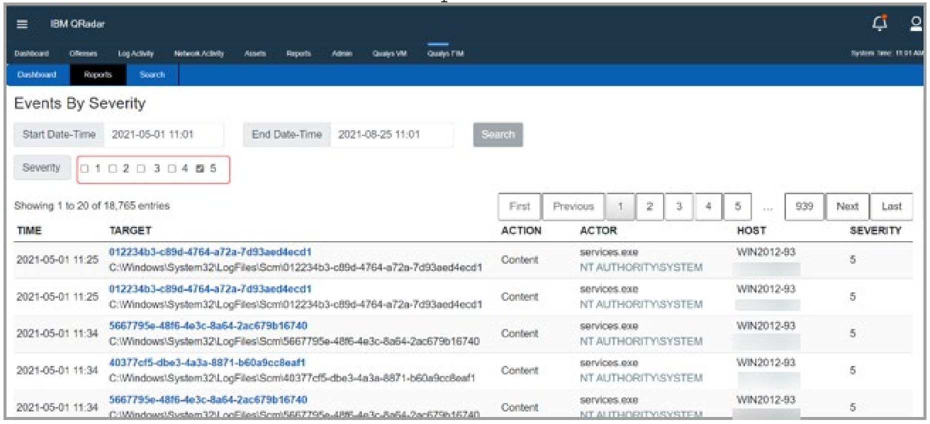
CREATED ON	NAME	TYPE	STATUS	ASSIGNEE	DISPOSITION	CHANGE TYPE	APPROVAL STATUS
2021-08-18 10:50	Incident-2 Approval Type: MANUAL	DEFAULT	OPEN	quays8mk4	null	null	null
2021-08-18 10:51	Incident-3 Approval Type: MANUAL	DEFAULT	OPEN	quays8mk4	null	null	null
2021-08-18 10:54	Incident-6 Approval Type: MANUAL	DEFAULT	OPEN	quays8mk4	null	null	null
2021-08-18 10:56	Incident-7 Approval Type: MANUAL	DEFAULT	OPEN	quays8mk4	null	null	null

Showing 1 to 4 of 4 entries

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.



Events By Severity

Start Date-Time 2021-05-01 11:01

End Date-Time 2021-08-25 11:01

Severity ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☑ 5

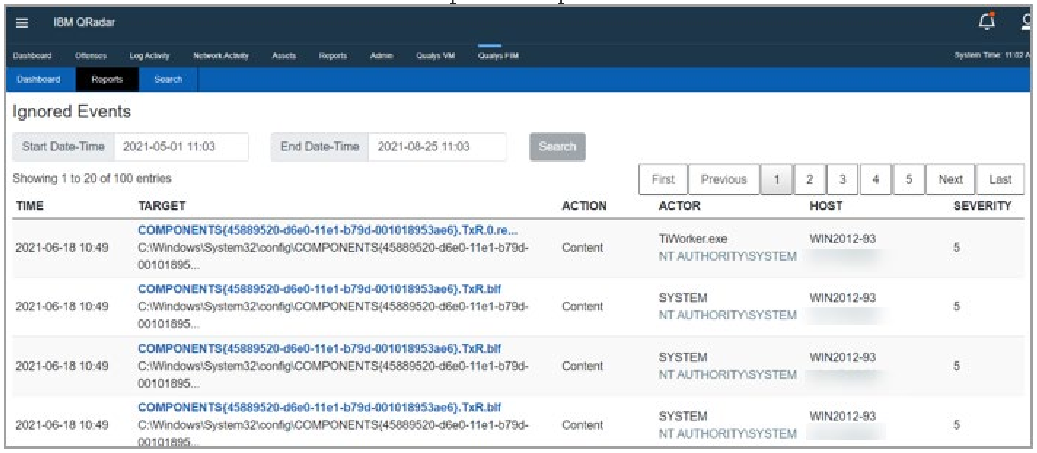
Showing 1 to 20 of 18,765 entries

TIME	TARGET	ACTION	ACTOR	HOST	SEVERITY
2021-05-01 11:25	012234b3-c89d-4764-a72a-7d93aed4ecd1 C:\Windows\System32\LogFiles\Scm\012234b3-c89d-4764-a72a-7d93aed4ecd1	Content	services.exe NT AUTHORITY\SYSTEM	WIN2012-93 [redacted]	5
2021-05-01 11:25	012234b3-c89d-4764-a72a-7d93aed4ecd1 C:\Windows\System32\LogFiles\Scm\012234b3-c89d-4764-a72a-7d93aed4ecd1	Content	services.exe NT AUTHORITY\SYSTEM	WIN2012-93 [redacted]	5
2021-05-01 11:34	5667795e-48f6-4e3c-8a64-2ac679b16740 C:\Windows\System32\LogFiles\Scm\5667795e-48f6-4e3c-8a64-2ac679b16740	Content	services.exe NT AUTHORITY\SYSTEM	WIN2012-93 [redacted]	5
2021-05-01 11:34	40377cf5-dbe3-4a3a-8871-b60a9cc8eaf1 C:\Windows\System32\LogFiles\Scm\40377cf5-dbe3-4a3a-8871-b60a9cc8eaf1	Content	services.exe NT AUTHORITY\SYSTEM	WIN2012-93 [redacted]	5
2021-05-01 11:34	5667795e-48f6-4e3c-8a64-2ac679b16740 C:\Windows\System32\LogFiles\Scm\5667795e-48f6-4e3c-8a64-2ac679b16740	Content	services.exe NT AUTHORITY\SYSTEM	WIN2012-93 [redacted]	5

Ignored Events

Displays reports of ignored events.

1. Select a required date range.
2. Click Search to view the required reports.



Ignored Events

Start Date-Time 2021-05-01 11:03 End Date-Time 2021-08-25 11:03 Search

Showing 1 to 20 of 100 entries

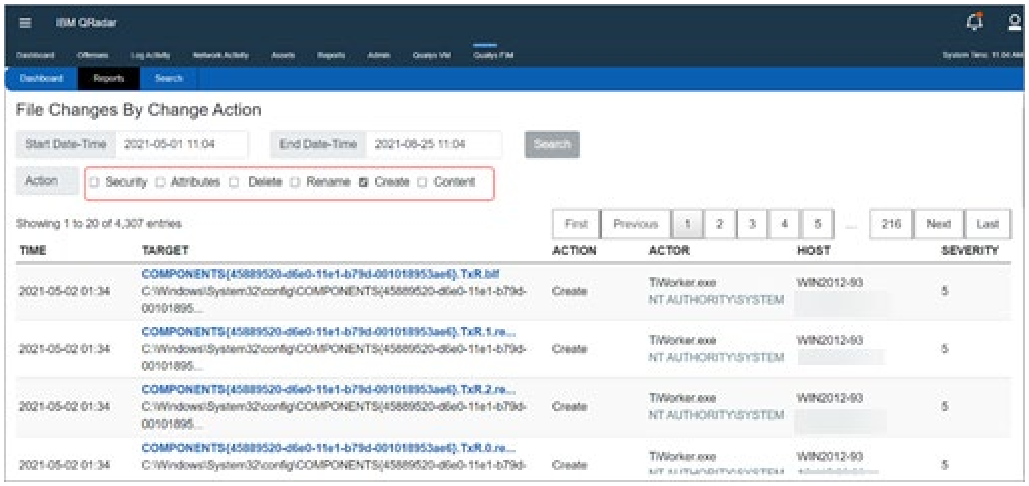
First Previous 1 2 3 4 5 Next Last

TIME	TARGET	ACTION	ACTOR	HOST	SEVERITY
2021-06-18 10:49	COMPONENTS{45889520-d6e0-11e1-b79d-001018953ae6}.TxR.0.re... C:\Windows\System32\config\COMPONENTS{45889520-d6e0-11e1-b79d-00101895...	Content	TiWorker.exe NT AUTHORITY\SYSTEM	WIN2012-93 [redacted]	5
2021-06-18 10:49	COMPONENTS{45889520-d6e0-11e1-b79d-001018953ae6}.TxR.blf C:\Windows\System32\config\COMPONENTS{45889520-d6e0-11e1-b79d-00101895...	Content	SYSTEM NT AUTHORITY\SYSTEM	WIN2012-93 [redacted]	5
2021-06-18 10:49	COMPONENTS{45889520-d6e0-11e1-b79d-001018953ae6}.TxR.blf C:\Windows\System32\config\COMPONENTS{45889520-d6e0-11e1-b79d-00101895...	Content	SYSTEM NT AUTHORITY\SYSTEM	WIN2012-93 [redacted]	5
2021-06-18 10:49	COMPONENTS{45889520-d6e0-11e1-b79d-001018953ae6}.TxR.blf C:\Windows\System32\config\COMPONENTS{45889520-d6e0-11e1-b79d-00101895...	Content	SYSTEM NT AUTHORITY\SYSTEM	WIN2012-93 [redacted]	5

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.



File Changes By Change Action

Start Date-Time 2021-05-01 11:04 End Date-Time 2021-08-25 11:04 Search

Action □ Security □ Attributes □ Delete □ Rename ☒ Create □ Content

Showing 1 to 20 of 4,307 entries

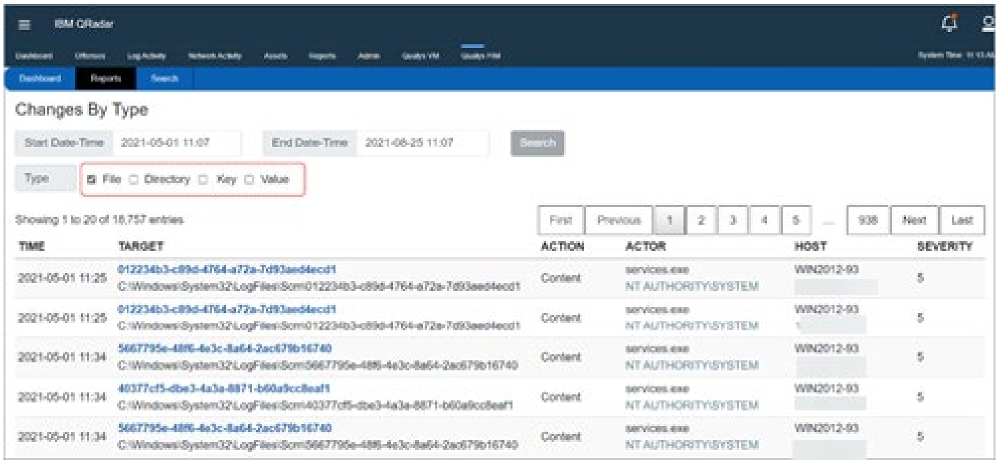
First Previous 1 2 3 4 5 ... 216 Next Last

TIME	TARGET	ACTION	ACTOR	HOST	SEVERITY
2021-05-02 01:34	COMPONENTS{45889520-d6e0-11e1-b79d-001018953ae6}.TxR.blf C:\Windows\System32\config\COMPONENTS{45889520-d6e0-11e1-b79d-00101895...	Create	TiWorker.exe NT AUTHORITY\SYSTEM	WIN2012-93 [redacted]	5
2021-05-02 01:34	COMPONENTS{45889520-d6e0-11e1-b79d-001018953ae6}.TxR.1.re... C:\Windows\System32\config\COMPONENTS{45889520-d6e0-11e1-b79d-00101895...	Create	TiWorker.exe NT AUTHORITY\SYSTEM	WIN2012-93 [redacted]	5
2021-05-02 01:34	COMPONENTS{45889520-d6e0-11e1-b79d-001018953ae6}.TxR.2.re... C:\Windows\System32\config\COMPONENTS{45889520-d6e0-11e1-b79d-00101895...	Create	TiWorker.exe NT AUTHORITY\SYSTEM	WIN2012-93 [redacted]	5
2021-05-02 01:34	COMPONENTS{45889520-d6e0-11e1-b79d-001018953ae6}.TxR.0.re... C:\Windows\System32\config\COMPONENTS{45889520-d6e0-11e1-b79d-	Create	TiWorker.exe NT AUTHORITY\SYSTEM	WIN2012-93 [redacted]	5

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.



Changes By Type

Start Date-Time 2021-05-01 11:07 End Date-Time 2021-08-25 11:07

Type ☒ File □ Directory □ Key □ Value

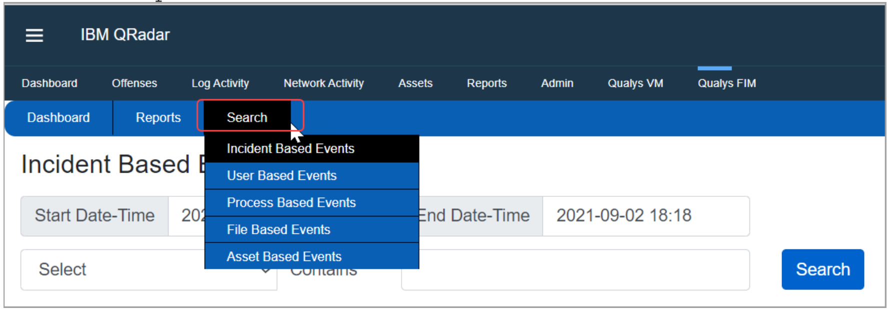
Showing 1 to 20 of 18,757 entries

TIME	TARGET	ACTION	ACTOR	HOST	SEVERITY
2021-05-01 11:25	012234b3-c89d-4764-a72a-7d93aed4ecd1 C:\Windows\System32\LogFiles\Scm\012234b3-c89d-4764-a72a-7d93aed4ecd1	Content	services.exe NT AUTHORITY\SYSTEM	WIN2012-93 [redacted]	5
2021-05-01 11:25	012234b3-c89d-4764-a72a-7d93aed4ecd1 C:\Windows\System32\LogFiles\Scm\012234b3-c89d-4764-a72a-7d93aed4ecd1	Content	services.exe NT AUTHORITY\SYSTEM	WIN2012-93 [redacted]	5
2021-05-01 11:34	5667795e-48f6-4e3c-8a64-2ac679b16740 C:\Windows\System32\LogFiles\Scm\5667795e-48f6-4e3c-8a64-2ac679b16740	Content	services.exe NT AUTHORITY\SYSTEM	WIN2012-93 [redacted]	5
2021-05-01 11:34	40377cf5-dbe3-4a3a-8871-b60a9cc8eaf1 C:\Windows\System32\LogFiles\Scm\40377cf5-dbe3-4a3a-8871-b60a9cc8eaf1	Content	services.exe NT AUTHORITY\SYSTEM	WIN2012-93 [redacted]	5
2021-05-01 11:34	5667795e-48f6-4e3c-8a64-2ac679b16740 C:\Windows\System32\LogFiles\Scm\5667795e-48f6-4e3c-8a64-2ac679b16740	Content	services.exe NT AUTHORITY\SYSTEM	WIN2012-93 [redacted]	5

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 E

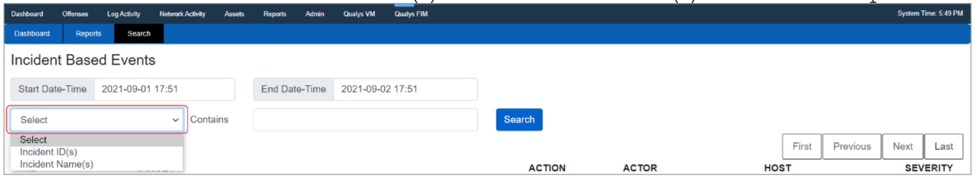
Start Date-Time 202

End Date-Time 2021-09-02 18:18

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.



Incident Based Events

Start Date-Time 2021-09-01 17:51

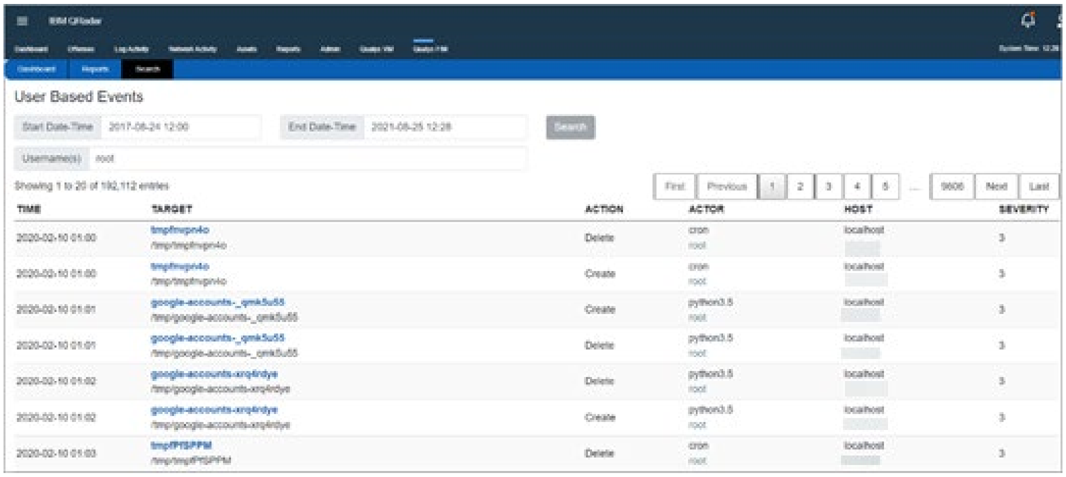
End Date-Time 2021-09-02 17:51

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.



User Based Events

Start Date-Time 2017-08-24 12:00

End Date-Time 2021-08-25 12:28

Username(s) root

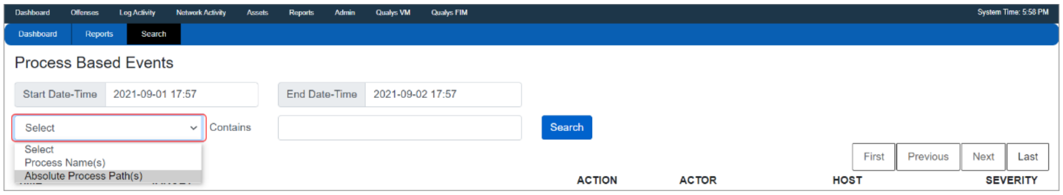
Showing 1 to 20 of 192,112 entries

TIME	TARGET	ACTION	ACTOR	HOST	SEVERITY
2020-02-10 01:00	tmpfmvpn4o /tmp/tmpfmvpn4o	Delete	cron root	localhost [redacted]	3
2020-02-10 01:00	tmpfmvpn4o /tmp/tmpfmvpn4o	Create	cron root	localhost [redacted]	3
2020-02-10 01:01	google-accounts-_qmk5u55 /tmp/google-accounts-_qmk5u55	Create	python3.5 root	localhost [redacted]	3
2020-02-10 01:01	google-accounts-_qmk5u55 /tmp/google-accounts-_qmk5u55	Delete	python3.5 root	localhost [redacted]	3
2020-02-10 01:02	google-accounts-xrq4rdye /tmp/google-accounts-xrq4rdye	Delete	python3.5 root	localhost [redacted]	3
2020-02-10 01:02	google-accounts-xrq4rdye /tmp/google-accounts-xrq4rdye	Create	python3.5 root	localhost [redacted]	3
2020-02-10 01:03	tmpfPfSPPM /tmp/tmpfPfSPPM	Delete	cron root	localhost [redacted]	3

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.



Process Based Events

Start Date-Time 2021-09-01 17:57

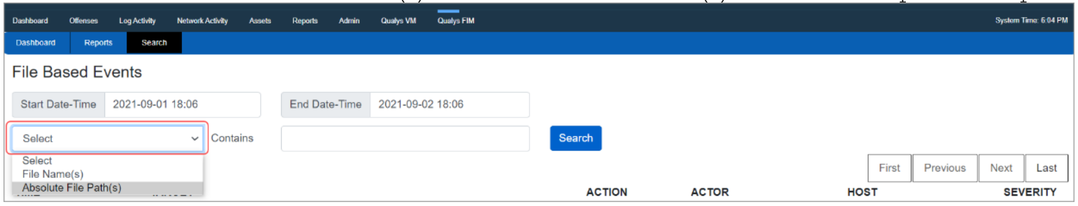
End Date-Time 2021-09-02 17:57

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.



File Based Events

Start Date-Time 2021-09-01 18:06

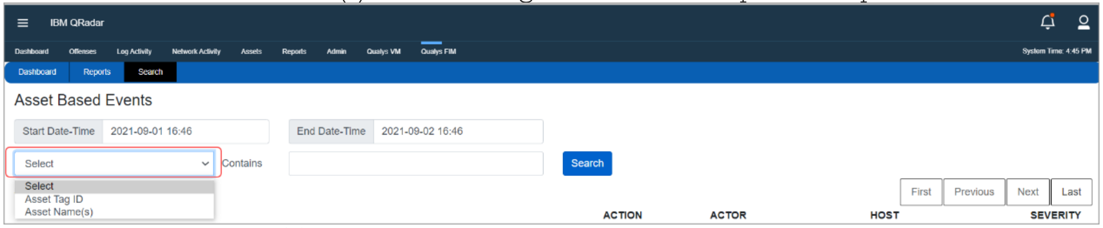
End Date-Time 2021-09-02 18:06

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.

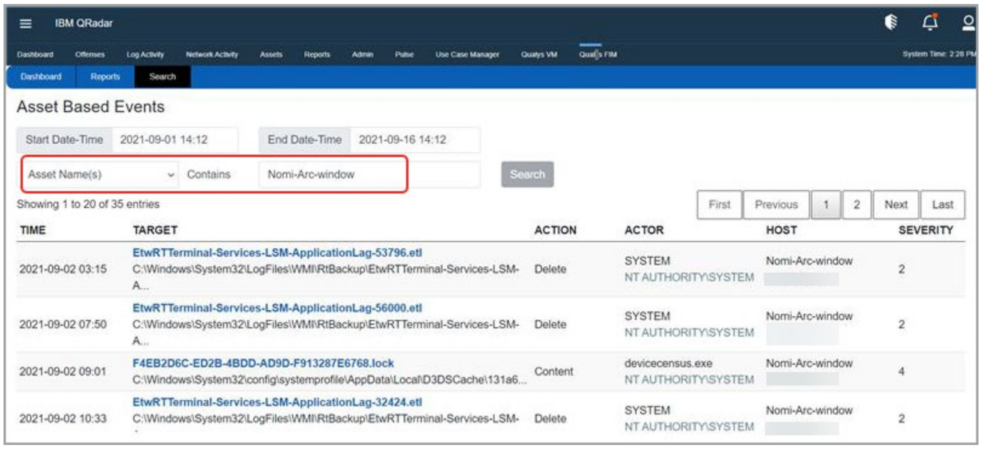


Asset Based Events

Start Date-Time 2021-09-01 16:46

End Date-Time 2021-09-02 16:46

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.



Asset Based Events

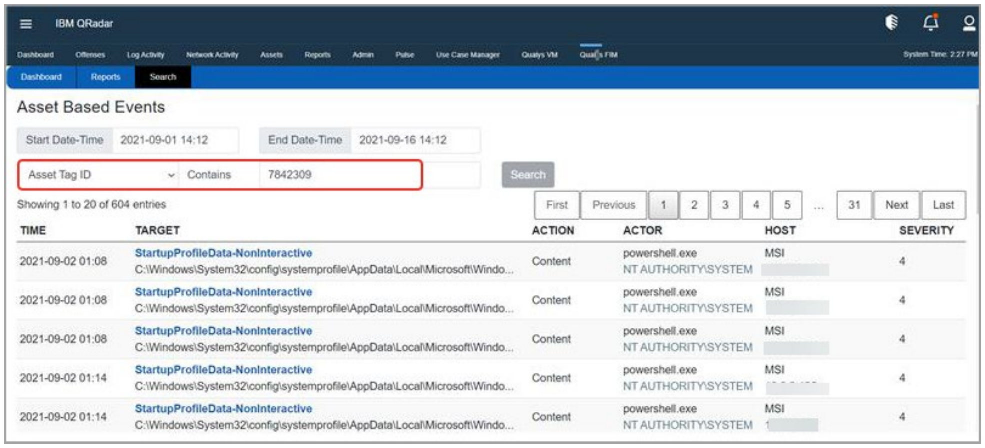
Start Date-Time 2021-09-01 14:12

End Date-Time 2021-09-16 14:12

Asset Name(s) Contains Nomi-Arc-window

Showing 1 to 20 of 35 entries

TIME	TARGET	ACTION	ACTOR	HOST	SEVERITY
2021-09-02 03:15	EtwRTTerminal-Services-LSM-ApplicationLag-53796.etl C:\Windows\System32\LogFiles\WMI\RtBackup\EtwRTTerminal-Services-LSM-A...	Delete	SYSTEM NT AUTHORITY\SYSTEM	Nomi-Arc-window [redacted]	2
2021-09-02 07:50	EtwRTTerminal-Services-LSM-ApplicationLag-56000.etl C:\Windows\System32\LogFiles\WMI\RtBackup\EtwRTTerminal-Services-LSM-A...	Delete	SYSTEM NT AUTHORITY\SYSTEM	Nomi-Arc-window [redacted]	2
2021-09-02 09:01	F4EB2D6C-ED2B-4BDD-AD9D-F913287E6768.lock C:\Windows\System32\config\systemprofile\AppData\Local\D3DSCache\131a6...	Content	devicecensus.exe NT AUTHORITY\SYSTEM	Nomi-Arc-window [redacted]	4
2021-09-02 10:33	EtwRTTerminal-Services-LSM-ApplicationLag-32424.etl C:\Windows\System32\LogFiles\WMI\RtBackup\EtwRTTerminal-Services-LSM-	Delete	SYSTEM NT AUTHORITY\SYSTEM	Nomi-Arc-window [redacted]	2



Asset Based Events

Start Date-Time 2021-09-01 14:12 End Date-Time 2021-09-16 14:12

Asset Tag ID Contains 7842309

Showing 1 to 20 of 604 entries

TIME	TARGET	ACTION	ACTOR	HOST	SEVERITY
2021-09-02 01:08	StartupProfileData-NonInteractive C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windo...	Content	powershell.exe NT AUTHORITY\SYSTEM	MSI [redacted]	4
2021-09-02 01:08	StartupProfileData-NonInteractive C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windo...	Content	powershell.exe NT AUTHORITY\SYSTEM	MSI [redacted]	4
2021-09-02 01:08	StartupProfileData-NonInteractive C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windo...	Content	powershell.exe NT AUTHORITY\SYSTEM	MSI [redacted]	4
2021-09-02 01:14	StartupProfileData-NonInteractive C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windo...	Content	powershell.exe NT AUTHORITY\SYSTEM	MSI [redacted]	4
2021-09-02 01:14	StartupProfileData-NonInteractive C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windo...	Content	powershell.exe NT AUTHORITY\SYSTEM	MSI [redacted]	4

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:
   - **Admin > Log Source**
   - **Admin > Log Source Extensions**
4) 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.
     AND
   - 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**.
5) Then delete the "Qualys FIM JSON" and "Qualys FIM Incidents" log source type in **Admin > DSM Editor**.
6) 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.

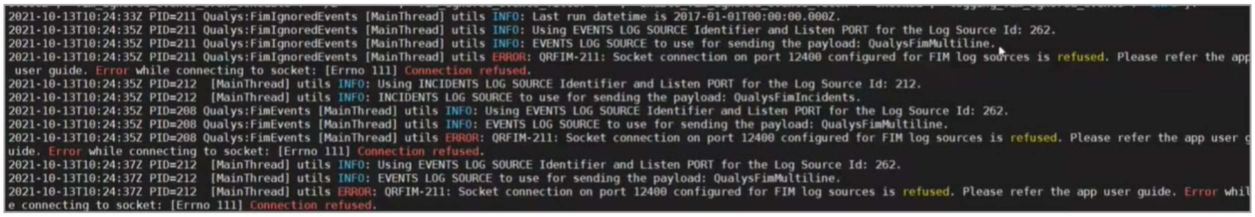
Troubleshooting

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.



```
2021-10-13T10:24:33Z PID=211 Qualys:FimIgnoredEvents [MainThread] utils INFO: Last run datetime is 2017-01-01T00:00:00.000Z.
2021-10-13T10:24:35Z PID=211 Qualys:FimIgnoredEvents [MainThread] utils INFO: Using EVENTS LOG SOURCE Identifier and Listen PORT for the Log Source Id: 262.
2021-10-13T10:24:35Z PID=211 Qualys:FimIgnoredEvents [MainThread] utils INFO: EVENTS LOG SOURCE to use for sending the payload: QualysFimMultiline.
2021-10-13T10:24:35Z PID=211 Qualys:FimIgnoredEvents [MainThread] utils ERROR: QRFIM-211: Socket connection on port 12400 configured for FIM log sources is refused. Please refer the app
 user guide. Error while connecting to socket: [Errno 111] Connection refused.
2021-10-13T10:24:35Z PID=212  [MainThread] utils INFO: Using INCIDENTS LOG SOURCE Identifier and Listen PORT for the Log Source Id: 212.
2021-10-13T10:24:35Z PID=212  [MainThread] utils INFO: INCIDENTS LOG SOURCE to use for sending the payload: QualysFimIncidents.
2021-10-13T10:24:35Z PID=208 Qualys:FimEvents [MainThread] utils INFO: Using EVENTS LOG SOURCE Identifier and Listen PORT for the Log Source Id: 262.
2021-10-13T10:24:35Z PID=208 Qualys:FimEvents [MainThread] utils INFO: EVENTS LOG SOURCE to use for sending the payload: QualysFimMultiline.
2021-10-13T10:24:35Z PID=208 Qualys:FimEvents [MainThread] utils ERROR: QRFIM-211: Socket connection on port 12400 configured for FIM log sources is refused. Please refer the app user g
uide. Error while connecting to socket: [Errno 111] Connection refused.
2021-10-13T10:24:37Z PID=212  [MainThread] utils INFO: Using EVENTS LOG SOURCE Identifier and Listen PORT for the Log Source Id: 262.
2021-10-13T10:24:37Z PID=212  [MainThread] utils INFO: EVENTS LOG SOURCE to use for sending the payload: QualysFimMultiline.
2021-10-13T10:24:37Z PID=212  [MainThread] utils ERROR: QRFIM-211: Socket connection on port 12400 configured for FIM log sources is refused. Please refer the app user guide. Error whil
e connecting to socket: [Errno 111] Connection refused.
```

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:

- https://www.ibm.com/docs/en/dsm?topic=configuration-undocumented-protocols

- https://www.ibm.com/docs/en/qradar-common?topic=app-undocumented-protocols

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.

Error code	Meaning
QRFIM-100	The /opt/app-root/store/qradar_fim_app.db is either missing or is in read-only mode as it must have updated by another file. In that case please provide permission to write.
QRFIM-101	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.
QRFIM-102	The configuration key-value is not available in the qualys_fim_config table
QRFIM-103	Some error is encountered while adding or updating the qualys_fim_checkpoint table.
QRFIM-104	Some error is encountered while adding or updating the qualys_fim_config table.
QRFIM-105	Some error is encountered while getting the data from the qualys_fim_checkpoint table.
QRFIM-106	Some error is encountered while adding or updating the qualys_fim_job_status table.
QRFIM-200	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.
QRFIM-201	While making the QRadar REST API call we encountered an error that is not parsable. Please check the job logs.
QRFIM-202	We did not found the 'Qualys FIM JSON' Log source Type in the DSM Editor. Please reinstall the app.
QRFIM-203	We did not found the 'QualysFimMultiline' Log source Type in the DSM Editor. Please create a log source or reinstall the app.
QRFIM-204	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.
QRFIM-205	While fetching the Log source information we encountered an error please check the job logs.
QRFIM-206	Please update a correct QRadar Auth token on Qualys FIM app settings page.
QRFIM-207	Got an error from QRadar REST API. Please contact IBM support.
QRFIM-208	No Log source information available in QRadar for a selected Log Source Id.
QRFIM-209	We encountered an error while validating the Qradar related settings before starting the job process. Please check the job logs for more information.
QRFIM-210	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.
QRFIM-211	Could not connect with QRadar host machine over the socket. Please check if the DSM PORT is open on the QRadar host machine.
QRFIM-212	We encountered an exception while trying a socket connection to QRadar. Please check the job logs for more information.
QRFIM-213	Events and Incidents Listen port does not match.
QRFIM-214	FIM log source is not configured correctly. Please provide proper log source identifier and listen port.
QRFIM-300	There is some error with the saved Qualys JWT Auth token. However, do not worry we will generate a new token.
QRFIM-301	Could not get Qualys JWT Auth token. Please check job logs for more information.
QRFIM-302	We were not able to get a valid response from Qualys API. Please check the job logs.
QRFIM-303	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.
QRFIM-304	You are unauthorized to make Qualys JWT Auth token call. Please check with Qualys support for more information.
QRFIM-305	Saved Qualys JWT Auth token is expired. Do not worry we will generate a new token.
QRFIM-306	We got an unexpected response while getting Qualys JWT Auth token. However, do not worry we will generate a new token.

QRFIM-307	Invalid Qualys POD details provided. Please provide the correct information.
QRFIM-308	Check if Qualys POD credentials are correct.
QRFIM-309	Socket error during Qualys REST API request. Please check with Qualys support for more information.
QRFIM-310	Unknown exception during Qualys REST API request. Please check the job logs.
QRFIM-311	Server URL or Username or Password should not be empty. Please update them from the app settings page.
QRFIM-312	exception while validating the Start Date for Job. Please provide the Date-Time format as YYYY-MM-DDTHH:MM:SS.msZ & greater than 2017-01-01T00:00:00.000Z.
QRFIM-313	Invalid Start Date for Job. Please provide the Date-Time format as YYYY-MM-DDTHH:MM:SS.msZ & greater than 2017-01-01T00:00:00.000Z.
QRFIM-314	We encountered an exception while validating the Qualys app configuration. Please check the job logs.
QRFIM-315	An invalid proxy is provided on the app settings page. Please validate if the proxy details provided are valid.
QRFIM-316	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.
QRFIM-317	There was an ambiguous exception that occurred while handling your API request.
QRFIM-318	Got ConnectionError while API request.
QRFIM-319	API request timeout reached. Will retry once.
QRFIM-320	Received 401 unauthorized from JWT auth token API response.
QRFIM-321	Received 403 forbidden from JWT auth token API response.
QRFIM-400	We did not get any count from Qualys API for your POD. No new event in the subscription.
QRFIM-401	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.
QRFIM-402	Could not get the FIM data from Qualys REST API for the job.
QRFIM-403	Not able to parse the incomplete JSON data in file
QRFIM-500	Please check the job logs for more information on which database file is required to run the job.
QRFIM-501	Log source not selected. Please select a valid Log source on the app settings page.
QRFIM-502	We were not able to decrypt the proxy password. Please check with Qualys Support.
QRFIM-503	Please provide a valid proxy host on the app settings page.
QRFIM-504	We were not able to decrypt the API password. Please check with Qualys Support.
QRFIM-505	Due to some exceptions, we are not able to rename the Qualys REST API response JSON file. Please check job logs for more information.
QRFIM-506	Due to some exceptions, we are not able to remove the Qualys REST API response JSON file. Please check job logs for more information.
QRFIM-507	Due to some exceptions, we are not able to save the Qualys REST API response JSON file. Please check job logs for more information.
QRFIM-508	You are trying to run the job which is already running. Please do not run another job manually.
QRFIM-509	While cleaning the JSON files we encountered an exception. Please check the job logs.
QRFIM-510	FIM Incidents log source not selected. Please select a valid Log source on the app settings page.