Qualys FIM for QRadar

User Guide

Version 1.0.0

June 25, 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

Use the Qualys FIM for QRadar to ingest your Qualys FIM Events and FIM Ignored Events into QRadar and view the data in QRadar's Log Activity tab. 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 to check the useful information.

Info: For current version of Qualys FIM for QRadar, we do not have a separate Dashboard. User can see FIM Events and FIM Ignored Events through AQL using QRadar's Log Activity.

Features

- Fetch the FIM events and ignored events from Qualys to ingest into QRadar
- Search the ingested data in the QRadar using "Log Activity" tab

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) Click
    - **Admin > Advanced dropdown > Deploy Full Configuration**
    - **Admin > Advanced dropdown > Restart Event Collection Service**

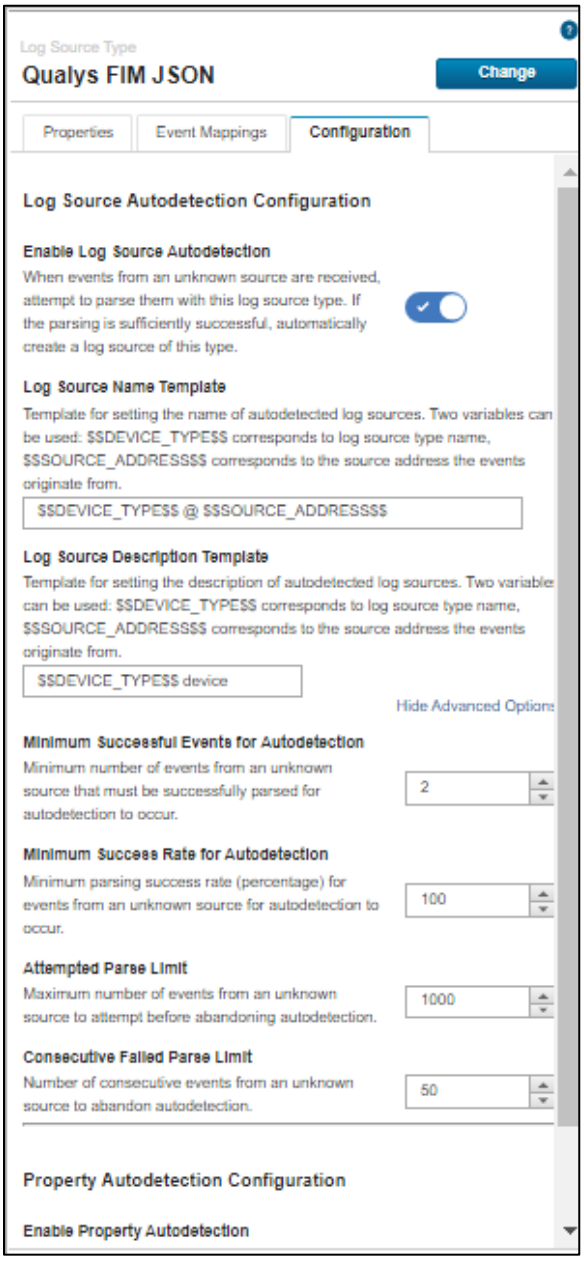
    Note: Please wait for the Event Collection Service to restart before enabling the FIM job.
6) User must perform the DSM Editor steps before configuring the App.
7) Then configure the Qualys FIM app.

DSM Editor

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

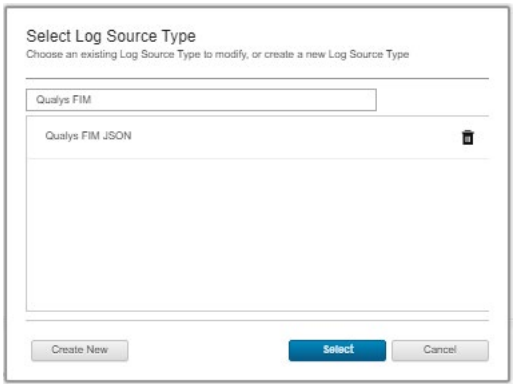


Validating Dependencies

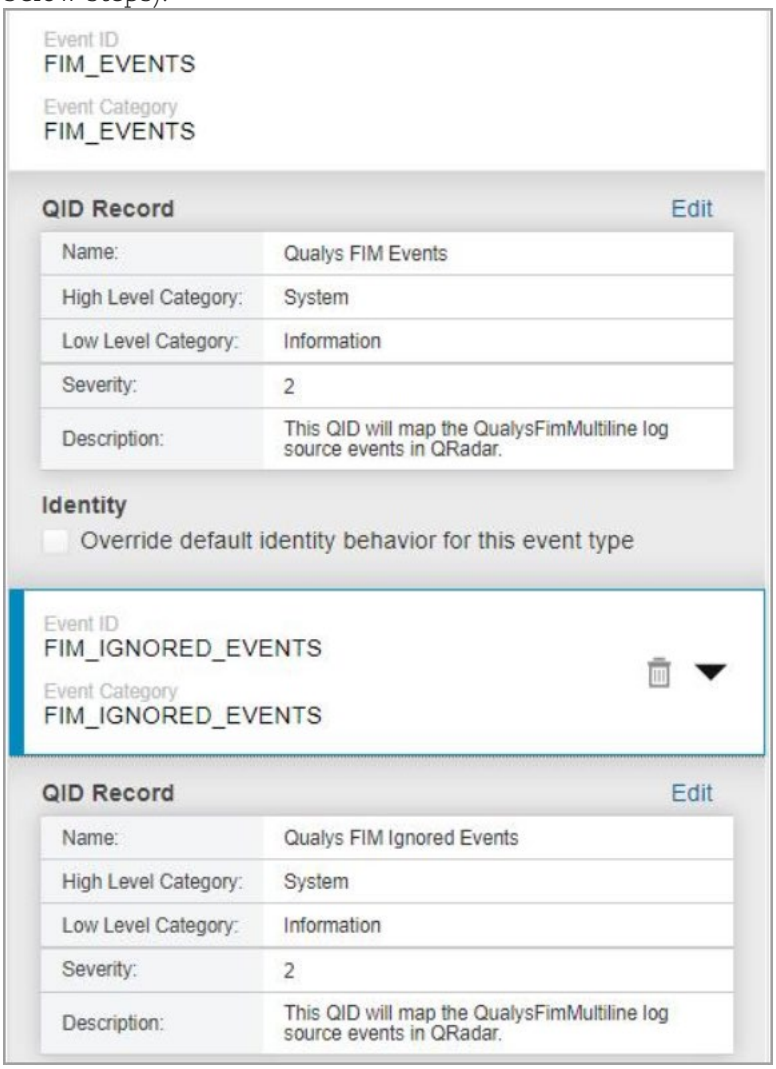
Please go through each of the sections listed below. You need to carry out the following steps manually, right after you install the app and before you start using it.
Note: Some sections may not be applicable in your case, and you may need to skip them.

Log Source Event Mapping

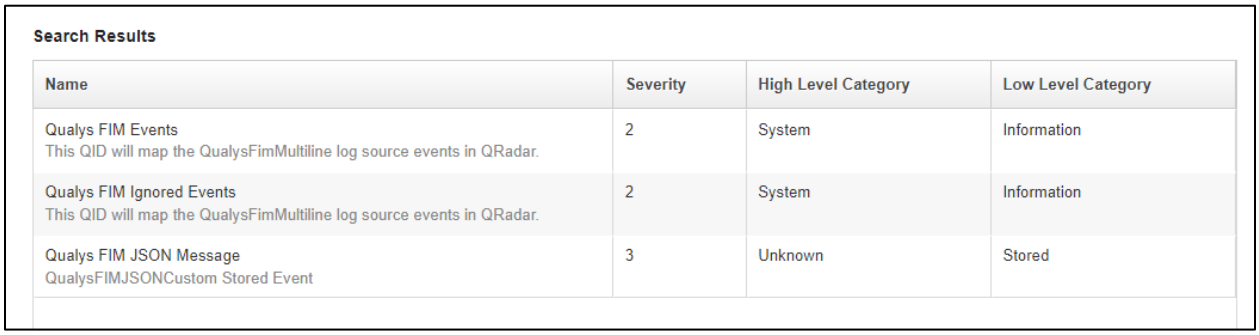
1) Go to **Admin** > **DSM Editor**.
2) In **Select Log Source Type**, search for "Qualys FIM JSON" and click **Select** button.



3) From the Qualys FIM JSON screen, go to **Event Mappings** tab. The requirement is that there should be mapping for FIM_EVENTS and FIM_IGNORED_EVENTS.
If you don't see mapping for FIM_EVENTS and FIM_IGNORED_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_EVENTS and FIM_IGNORED_EVENTS” (without quotes) and **Category** as “FIM_EVENTS and FIM_IGNORED_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 will be displayed based on the QID/Name entered.

6) Choose the option Qualys FIM Events/Qualys FIM Ignored Events 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.

Log Source

When you install app, it will create a new Log Source named “QualysFimMultiline”. Please check if it is created. You can also create the custom log source for the Qualys app with 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

4) Click **Save**.

If you need to create this new Log Source manually, you must do a full deployment. For that, please go to **Admin** > **Advance** and click **Deploy Full Configuration**.

Custom Event Properties

1) Go to **Admin** > **Log Sources** and confirm that QualysFimMultiline Log Source is Enabled. If it is disabled, please enable it.
2) Go to **Admin** > **Custom Event Properties** and confirm that all 36 Qualys related properties are Enabled and are linked to "Qualys FIM JSON" log source type.

   Qualys related properties are:

Field name	JSON keypath
Absolute File Path	/"fullPath"
Absolute Process Path	/"actor"/"imagePath"
Action	/"action"
Asset tags	/"asset"/"tags"[]
Attribute New	/"attributes"/"new"[]
Attribute Old	/"attributes"/"old"[]
Category name	/"profiles"[0]/"category"/"name"
Event Alert	/"name"
Event UUID	/"id"
Event type	/"type"
File Certificate Hash	/"fileCertificateHash"
File Hash	/"fileContentHash"
File Reputation Status	/"reputationStatus"

File Trust Status	/"trustStatus"
Monitoring Profile	/"profiles"[0]/"name"
New Content	/"newContent"
New Registry Value Content	/"newRegistryValueContent"
New Registry Value Type	/"newRegistryValueType"
Old Content	/"oldContent"
Old Registry Value Content	/"oldRegistryValueContent"
Old Registry Value Type	/"oldRegistryValueType"
Platform	/"platform"
Qualys Agent Version	/"asset"/"agentVersion"
Registry Name	/"registryName"
Registry Path	/"registryPath"
Rules ID	/"profiles"[0]/"rules"[0]/"id"
Rules name	/"profiles"[0]/"rules"[0]/"name"
Section ID	/"profiles"[0]/"rules"[0]/"section"/"id"
Section name	/"profiles"[0]/"rules"[0]/"section"/"name"
Source Host Name	/"asset"/"interfaces"[0]/"hostname"
User ID	/"actor"/"userID"
assetInterfaces	/"assetInterfaces"
processID	/"actor"/"processID"
processName	/"actor"/"process"
qradar_event_type	/"qradar_event_type"
severityLevel	/"severity"

For the Qualys related properties, complete these checks:

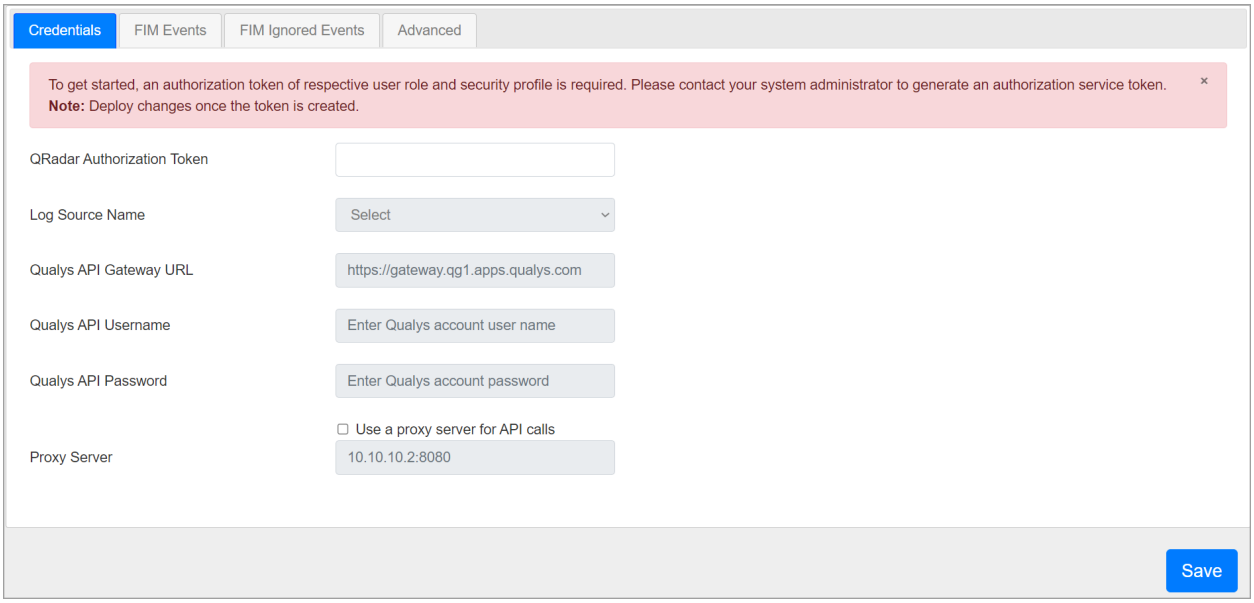
1) If any property is disabled, enable it.
2) If any property does not belong to the Qualys FIM JSON log source type, please open it to edit and select Qualys FIM JSON as the log source type.
3) Do not select any specific Log source, select **All** in the drop-down option.
4) Select the Category, with **High Level Category** as System and **Low Level Category** as Information.
5) Provide JSON keypath 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.



Credentials

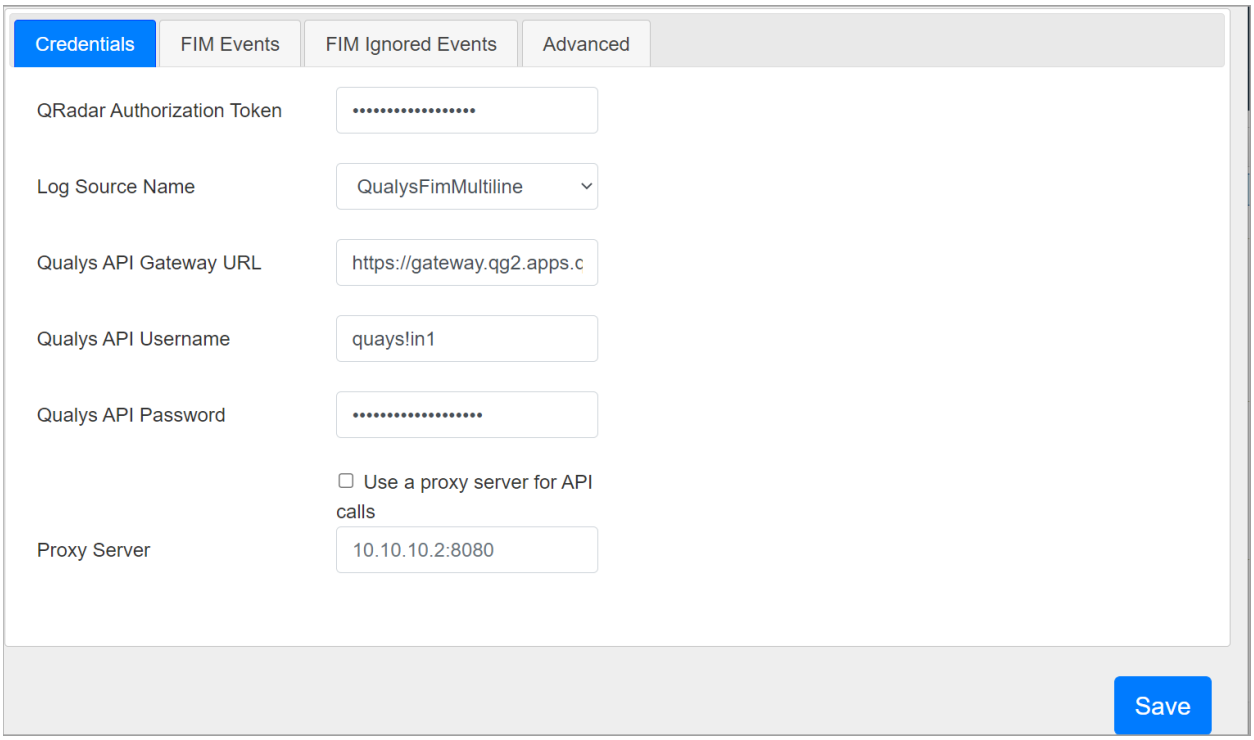
QRadar Authorization token is used while interacting securely with QRadar. You can obtain this token from **Admin** > **User Management** > **Authorized Service**.

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 credentials tab, click **Save** to Proceed.

8) Use the **Credentials** tab to configure your Qualys credentials. Enter your Qualys API server, username and password in the appropriate fields.



Proxy Configuration

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

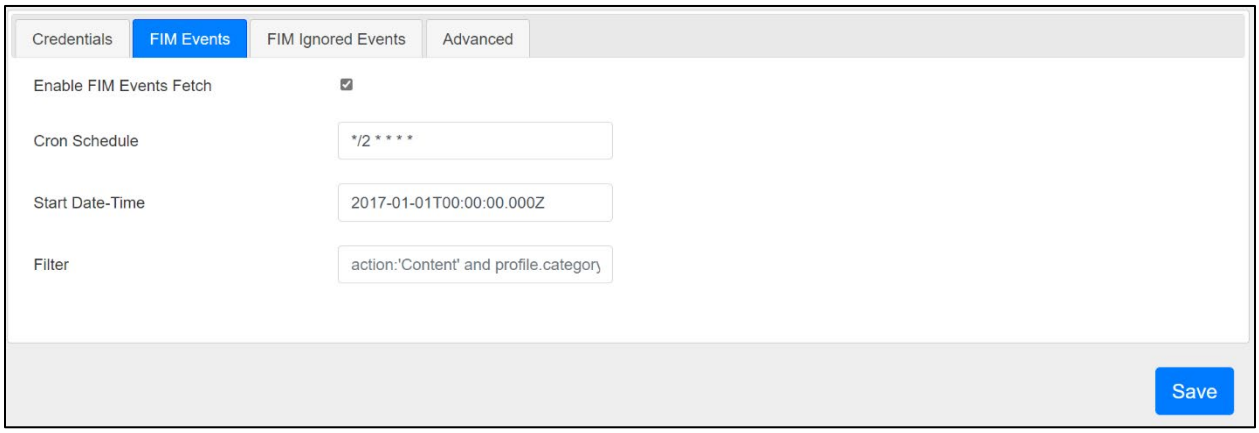
Select the check box to enable proxy.

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.

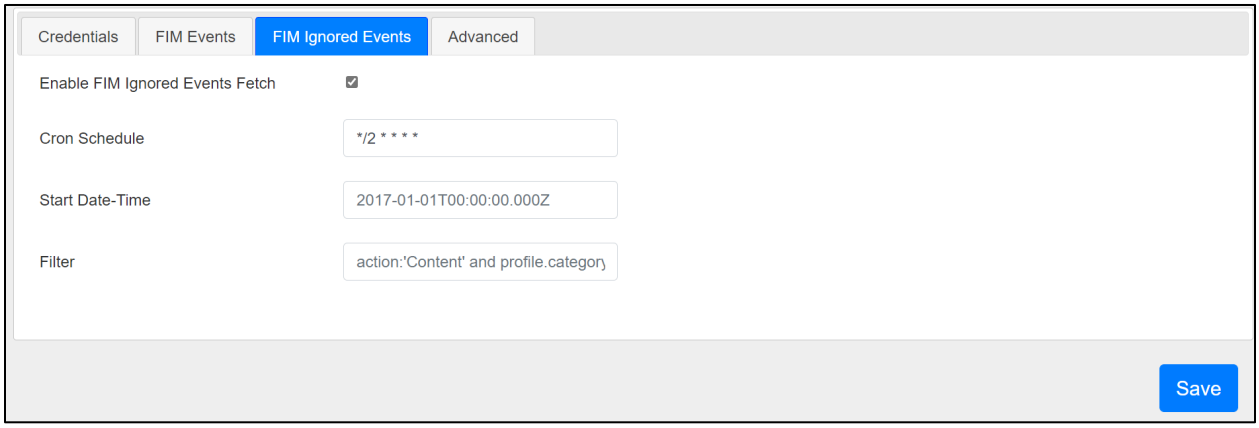


1) Tick the "Enable FIM Events" checkbox to enable this data input.

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.

FIM Ignored Events

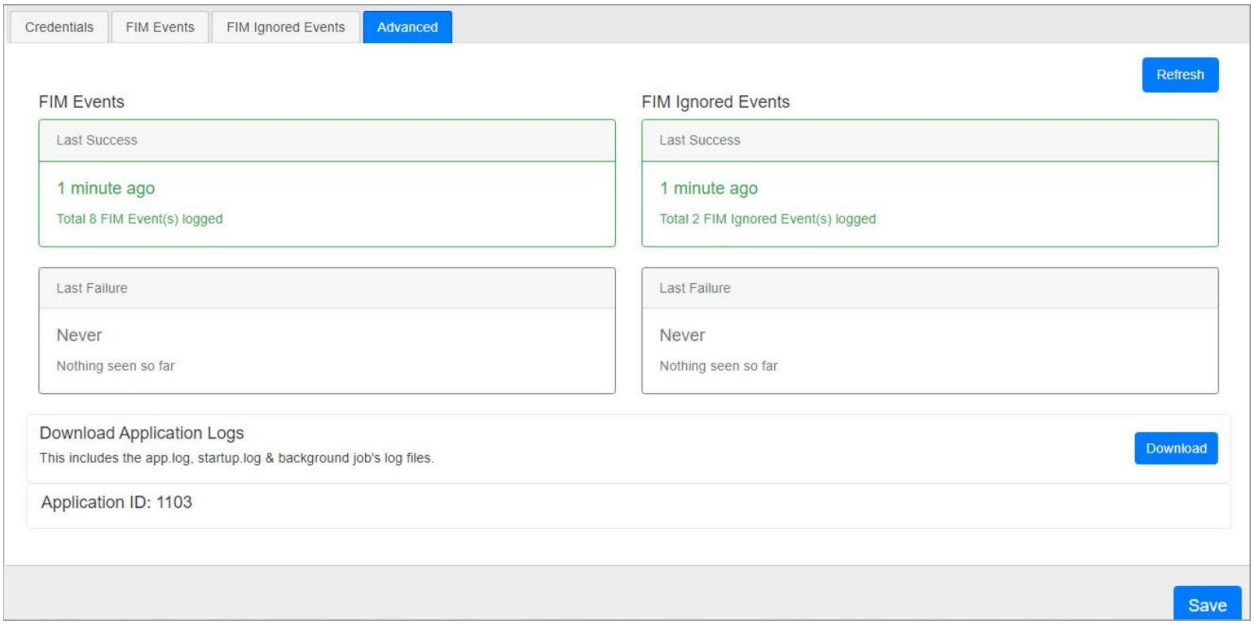
Use the **FIM Ignored Events** tab to configure and enable Fetch FIM Ignored Events.



1) Tick the "Enable FIM Ignored Events" 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.
4) 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.

Advanced

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



How Qualys App works?

What happens after configuration?

Once you configure and enable FIM Events or Ignored Events job, the application bundled with this extension will start fetching your FIM events 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" Log Source. Using DSM editor and "Qualys FIM JSON" 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 Username, "User ID", "Source Host Name", sourceip, sourcev6, "Event
UUID", "Event Alert", severityLevel, processName, processID, "Absolute
Process 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" 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:

This AQL has all the fields which the app parses.

AQL:
```
SELECT Username,DATEFORMAT(devicetime,'yyyy-MM-dd h:m:ss:SSS z') as "Log
Source Time",sourceip,sourcev6,assetInterfaces,"Source Host Name","Event
Alert", "User ID",severityLevel,processName,processID,"Absolute Process
Path",Action,"Absolute File Path","File Hash","File Reputation Status","File
Trust Status","File Certificate Hash","Category name","Event
type",Platform,"Monitoring Profile","Section name","Section ID","Rules
name","Rules ID","Asset tags","Registry Path","Qualys Agent Version","Event
UUID","Registry Name","Attribute Old","Attribute New","Old Content","New
```

```
Content","Old Registry Value Type","New Registry Value Type","Old Registry
Value Content","New Registry Value Content","qradar_event_type" 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'
```

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**" 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**
    - Then 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.
    - 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" 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 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

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-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-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-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.