Qualys File Integrity Monitoring v2.x

Release Notes

Version 2.3
July 17, 2020

Here's what's new in Qualys FIM 2.3!

Performance Improvements

Download Events Reports

UI Enhancements

Performance Improvements

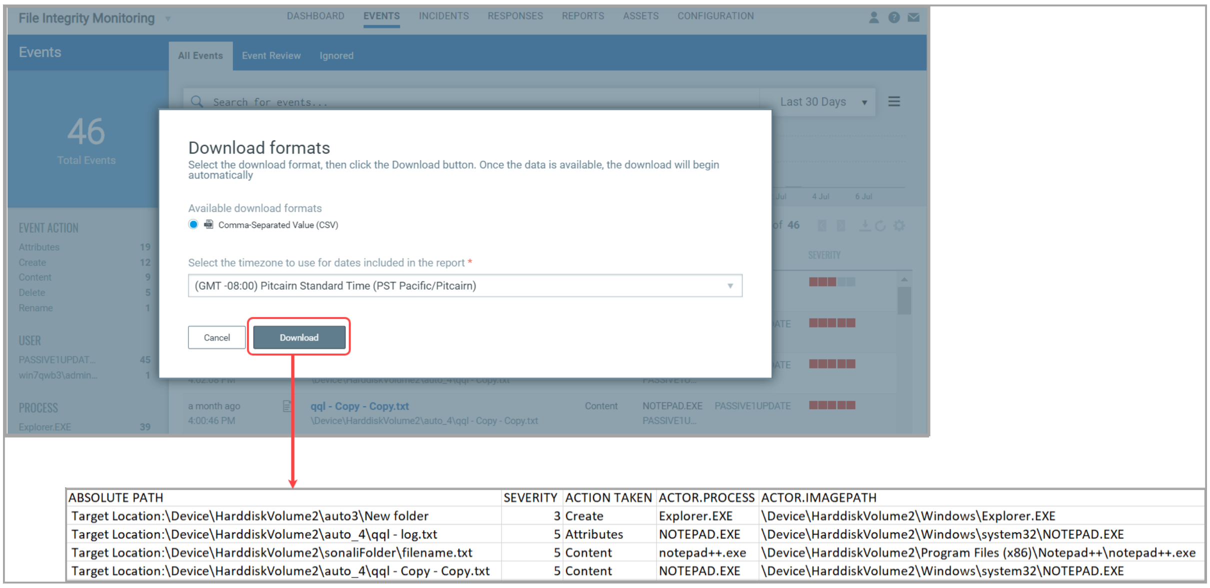
For better performance and reliability, we have made the following improvement to FIM:

- Refactored the manifest service to address the timing issues in the manifest generation.
- Improved the reliability of our correlation engine for a better incident generation.

Download Events Reports

We have made the following changes to the Events Report:

- The ABSOLUTE PATH column will now display the path of the file/directory where the change is detected.
- The ACTOR.IMAGEPATH column will now display the path to the application because of which the change is detected.



Download formats

Select the download format, then click the Download button. Once the data is available, the download will begin automatically

Available download formats

● Comma-Separated Value (CSV)

Select the timezone to use for dates included in the report *

(GMT -08:00) Pitcairn Standard Time (PST Pacific/Pitcairn)

ABSOLUTE PATH	SEVERITY	ACTION TAKEN	ACTOR.PROCESS	ACTOR.IMAGEPATH
Target Location:\Device\HarddiskVolume2\auto3\New folder	3	Create	Explorer.EXE	\Device\HarddiskVolume2\Windows\Explorer.EXE
Target Location:\Device\HarddiskVolume2\auto_4\qql - log.txt	5	Attributes	NOTEPAD.EXE	\Device\HarddiskVolume2\Windows\system32\NOTEPAD.EXE
Target Location:\Device\HarddiskVolume2\sonaliFolder\filename.txt	5	Content	notepad++.exe	\Device\HarddiskVolume2\Program Files (x86)\Notepad++\notepad++.exe
Target Location:\Device\HarddiskVolume2\auto_4\qql - Copy - Copy.txt	5	Content	NOTEPAD.EXE	\Device\HarddiskVolume2\Windows\system32\NOTEPAD.EXE

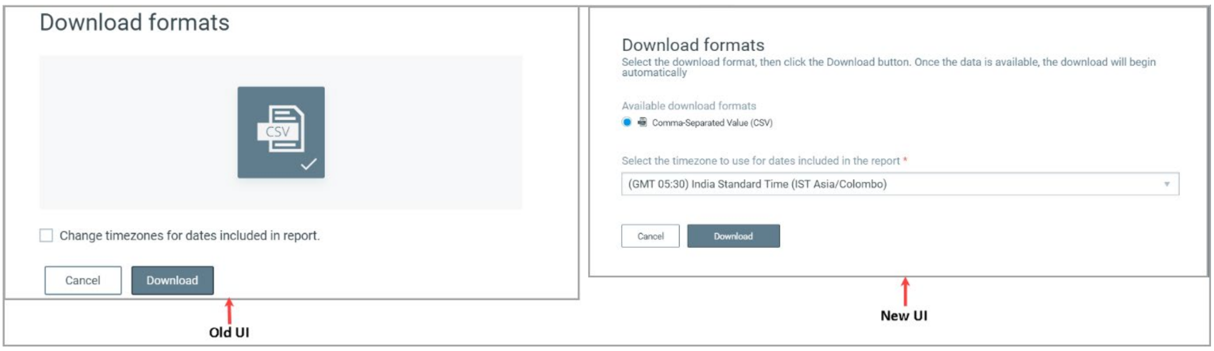
You can download the Events report from the following locations:

1. From the **Events** tab:
   - Select **All Events** tab and then click on the download option.
   - Select **Events Review** tab and then click on the download option.
   - Select **Ignored** tab and then click on the download option.
2. From the **Incidents** tab, select the required incident and click **Quick Action > View Details**. On the **Incidents Details** page, select the **Events** tab and then click on the download option.

UI Enhancements

For better usability and customer experience, we have made the following changes to the FIM UI:

1. Revamped the Download formats window.



Download formats

□ Change timezones for dates included in report.

Download formats

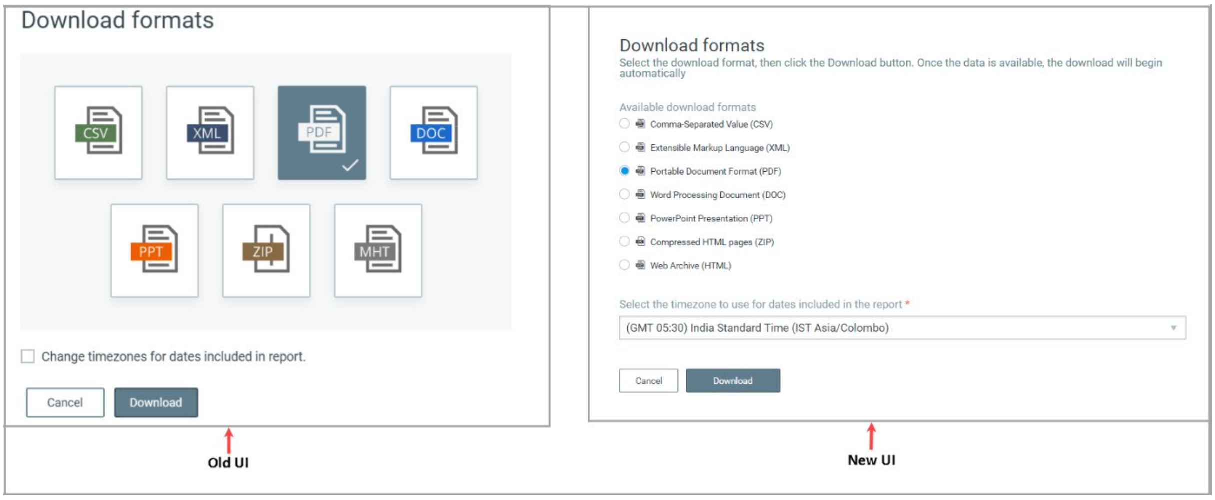
Select the download format, then click the Download button. Once the data is available, the download will begin automatically

Available download formats

● Comma-Separated Value (CSV)

Select the timezone to use for dates included in the report *

(GMT 05:30) India Standard Time (IST Asia/Colombo)



Download formats

□ Change timezones for dates included in report.

Download formats

Select the download format, then click the Download button. Once the data is available, the download will begin automatically

Available download formats

○ Comma-Separated Value (CSV)

○ Extensible Markup Language (XML)

● Portable Document Format (PDF)

○ Word Processing Document (DOC)

○ PowerPoint Presentation (PPT)

○ Compressed HTML pages (ZIP)

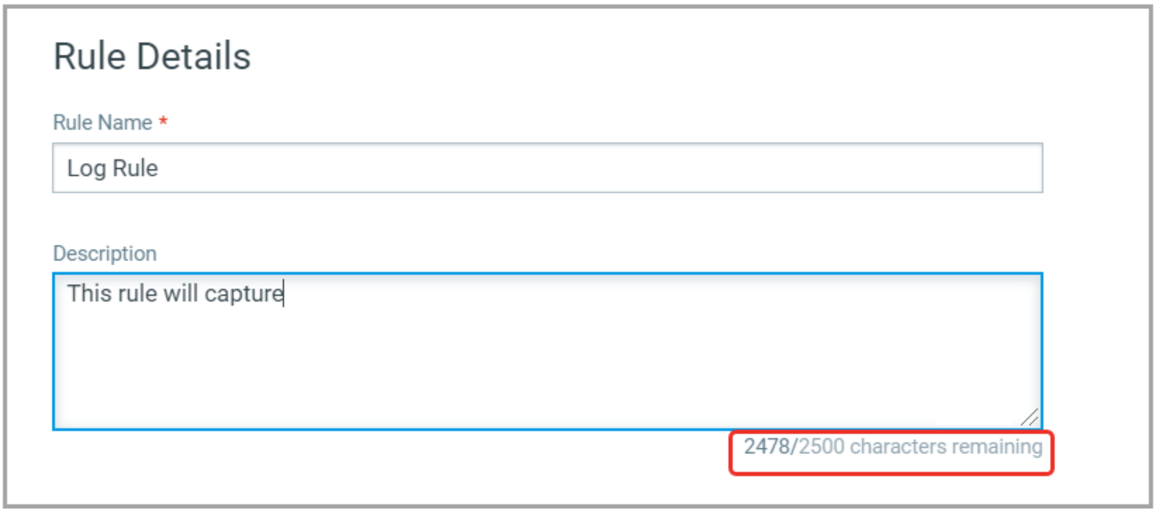
○ Web Archive (HTML)

Select the timezone to use for dates included in the report *

(GMT 05:30) India Standard Time (IST Asia/Colombo)

2. The Description option now displays a counter for the number of characters pending and the permissible character limit.

   Example: In the following screenshot, 2478 characters are pending from the permissible limit of 2500 characters.



Rule Details

Rule Name *

Log Rule

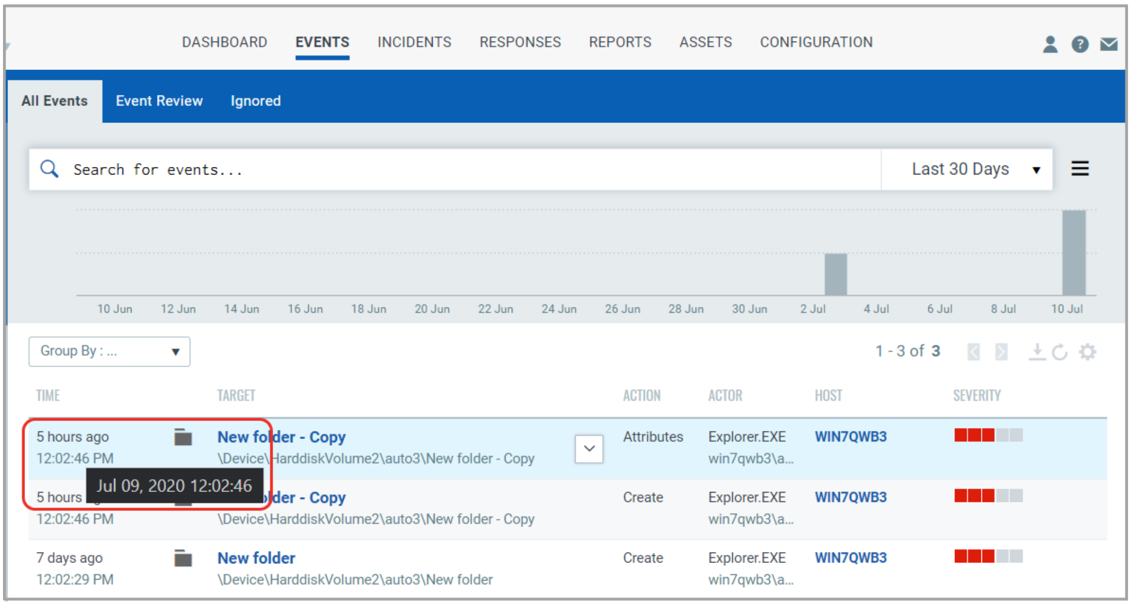
Description

This rule will capture

2478/2500 characters remaining

3. The exact date and time are now displayed when you hover the mouse over the relative time entry.

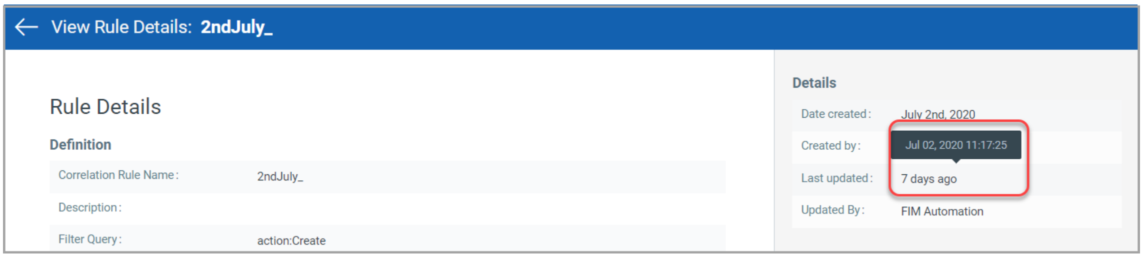
   Example 1: When you hover the mouse on “5 hours ago”, the exact date and time for the event is displayed in the pop-up.



TIME	TARGET	ACTION	ACTOR	HOST	SEVERITY
5 hours ago 12:02:46 PM	New folder - Copy \Device\HarddiskVolume2\auto3\New folder - Copy	Attributes	Explorer.EXE win7qwb3\a...	WIN7QWB3	🟥🟥🟥⬜⬜
5 hours ago 12:02:46 PM	New folder - Copy \Device\HarddiskVolume2\auto3\New folder - Copy	Create	Explorer.EXE win7qwb3\a...	WIN7QWB3	🟥🟥🟥⬜⬜
7 days ago 12:02:29 PM	New folder \Device\HarddiskVolume2\auto3\New folder	Create	Explorer.EXE win7qwb3\a...	WIN7QWB3	🟥🟥🟥⬜⬜

Jul 09, 2020 12:02:46

   Example 2: When you hover the mouse on “7 days ago”, the exact date and time for the rule last updated is displayed in the pop-up.


View Rule Details: **2ndJuly_**

Rule Details

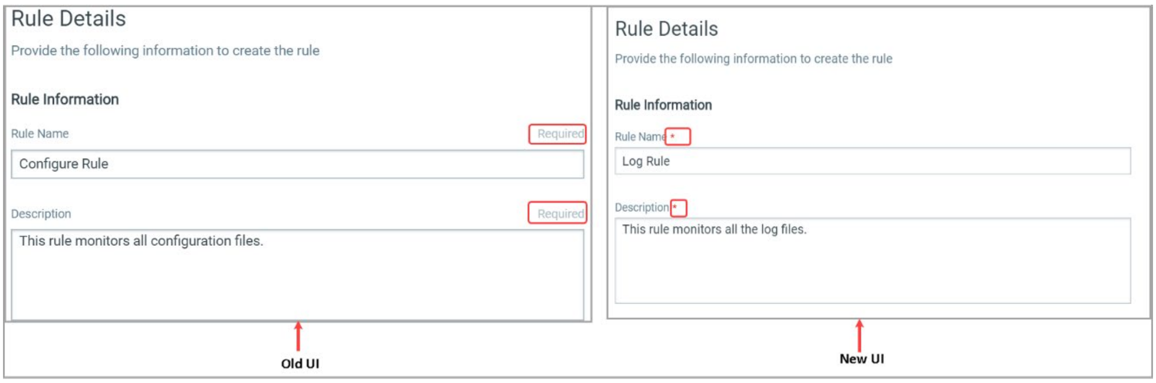
Definition

Correlation Rule Name:	2ndJuly_
Description:	
Filter Query:	action:Create

Details

Date created:	July 2nd, 2020
Created by:	Jul 02, 2020 11:17:25
Last updated:	7 days ago
Updated By:	FIM Automation

4. The required fields are now marked with a red Asterisk sign against the field name.


Rule Details

Provide the following information to create the rule

Rule Information

Rule Name Required

Configure Rule

Description Required

This rule monitors all configuration files.

Old UI

Rule Details

Provide the following information to create the rule

Rule Information

Rule Name *

Log Rule

Description *

This rule monitors all the log files.

New UI