



Qualys File Integrity Monitoring (FIM)

Release Notes

Version 3.5.0

July 19, 2022

Here's what's new in Qualys File Integrity Monitoring 3.5.0!

New Features

- Granular Visibility Into Events Through the Event Insights Tab
- New Dashboard Layout for Enhanced Dashboarding Capabilities
- Support Added to Specify Event Source in Report Creation Flow
- Process and User-Based Event Exclusion for Windows Assets
- Option to Include Incidents While Creating a Widget

Enhancement

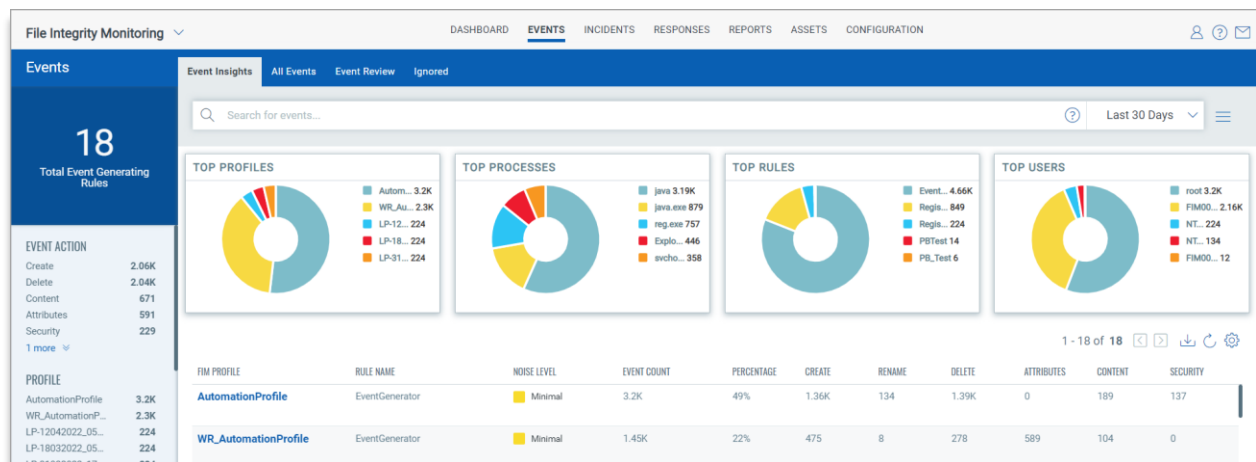
Fixed Issue

New Features

Granular Visibility Into Events Through the Event Insights Tab

This release introduces the new **Event Insights** sub-tab under the **Events** tab, which helps you have a thorough insight into the change events on your FIM console. The **Event Insights** tab includes a list of the FIM profiles that have generated the highest number of events as well as widgets with event data, which can be drilled down to access granular data.

The widgets in the **Event Insights** tab display specific data generated within the time frame that's selected from the time range selector. The widgets help you with a single-glance perception of the top event generators; thereby, enabling you to analyze your rules and pinpoint which rule in which profile has generated the maximum number of events.

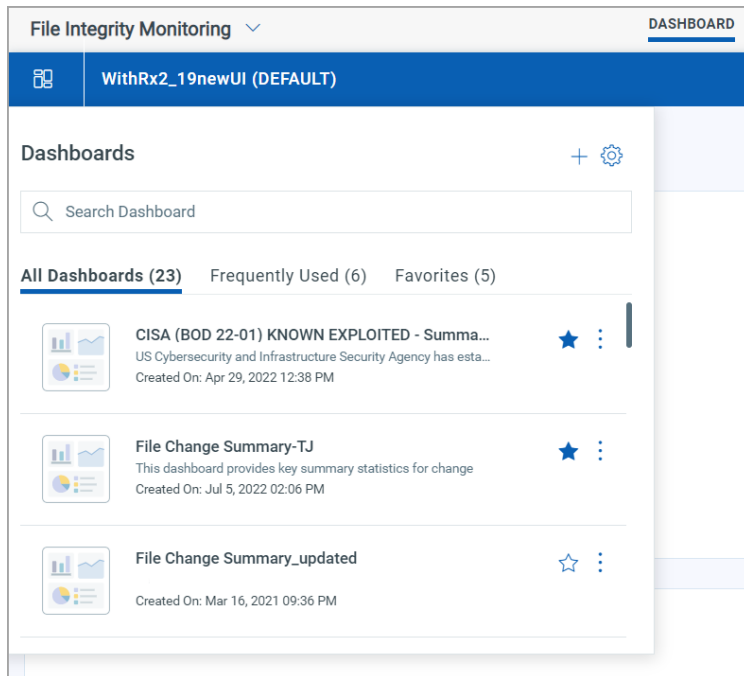


The event noise level is displayed as 'Minimal', 'Moderate' and 'Critical', where, 'Critical' indicates that the corresponding rule is generating more than 90% of the events. You can select a profile and fine-tune the rule to ensure reduced event noise.

New Dashboard Layout for Easy Access to the Dashboard Functions



You can now edit a dashboard or change the layout of the widgets in the dashboard.


Click  to open the **Dashboards** panel.



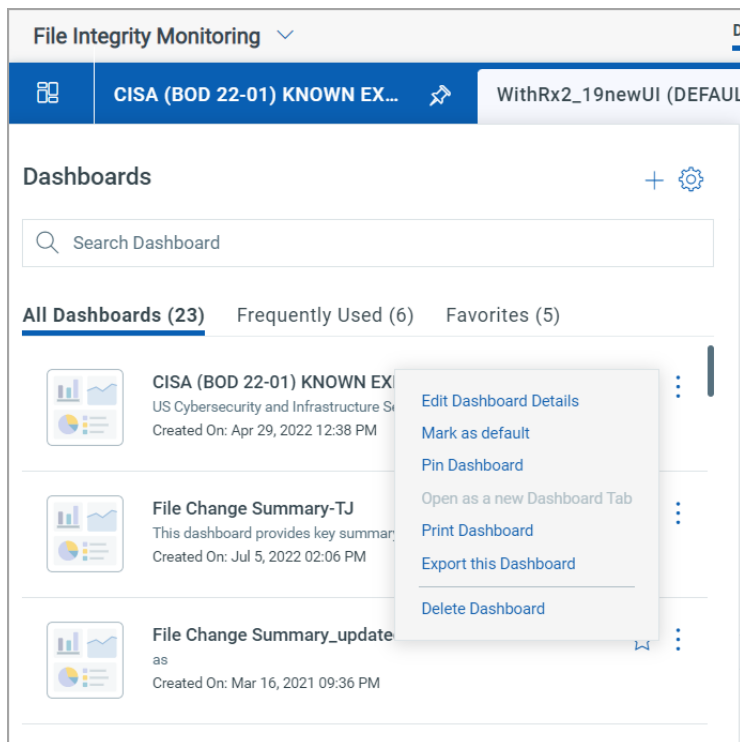
The **Dashboards** panel contains three tabs to let you do the following:

- View all the current dashboards
- View the frequently used dashboards
- View the favourite dashboards

You can click  to go to the **Add or Customize Dashboard templates** page. You can also click  to go to the **Manage Dashboards** page.

Select a dashboard and click  to perform any of the following actions:

- Edit the dashboard details.
- Mark the selected dashboard as the default dashboard.
- Pin the dashboard. The pinned dashboard is displayed on the dashboard panel even after you log out from your account or refresh the page.
- Open the selected dashboard as a new dashboard tab on the dashboard panel.
- Print the dashboard that you have selected.
- Export the selected dashboard.
- Delete the selected dashboard.



Support Added to Specify Event Source in Report Creation Flow

Previously in the report rule creation process, only custom queries were supported to specify event sources. This release adds several event sources that can just be selected from the drop-down list:

- Asset Tag
- Severity
- Action
- User
- Process
- File Path
- Monitoring Profile

← Report Rule: Create

STEPS 2/5

- 1 Report Rule Details
- 2 Event Source
- 3 Report Output
- 4 Report Schedule
- 5 Review & Confirm

Event Source

Specify the source of events that you want to include in the rule and other relevant details.

Event Source Type

- Asset Tag
- Severity
- Action
- User
- Process
- File Path
- Monitoring profile
- Custom Query

Cancel Previous Next

Process and User-Based Event Exclusion for Windows Assets

Starting this release, you can add profile exclusion filters to approve change events that are generated for trusted users and processes for Windows assets. The actions performed by users that you specify and events occurring from specified processes will always be excluded from the change events list in FIM. This new feature will allow you to control the event generation volume to a great extent.

To enable you to reduce event generation, the **Profile Exclusion** tab has been newly added to the configuration profile creation procedure. You can specify trusted users and approved processes in the **Users** and **Processes** list respectively.

Note: The profile exclusion option is only applicable for Windows assets.

Qualys Cloud Platform

← Create FIM Monitoring Profile

Edit Mode

- Profile Details
- Profile Exclusion
- Rules
- Assign Assets

Profile Exclusion

Profile level exclusion filter allows you to create an exclusion filter based on known good users and processes. This exclusion filter syncs with all the rules within the profile and suppresses event generation for whitelisted users and processes.

Maximum 10 filters should be applied for Users and Processes

Users

- FIMAdministrator

9 more users can be added

Processes

- java.exe
- explorer.exe

8 more process can be added

Cancel Save Next

Option to Include Incidents While Creating a Widget

You can now select the option to create a widget for FIM incidents as well. In the **Query Settings** page of the Widget Builder, select **Incidents** and do the following:

Enter the QQL token to specify the type of incidents and select one of the following change event types:

- Automated
- Compromise
- Manual
- Other

Optionally, select the time range for the incidents generated.

← Add Widget to Dashboard (FIM)

Widget Details

Query Settings

Advanced Settings

Display Settings

Query Search

Display results as:

☐ Events ☒ Incidents

Timeframe ⓘ ☒

Last 30 Days ▾

The newly created widget will include data for FIM incidents as per your specifications.

Enhancement

The following enhancement has been made in this release:

- **Limit on Inclusion and Exclusion filters and file paths:** The limit of inclusion and exclusion filters that can be applied to directories and files has been increased to a maximum of 15 filters. Similarly, the limit to add file paths to be monitored has been increased to 20.

Fixed Issue

Earlier, while creating a configuration profile, an error message used to be displayed when user entered a numerical value in the **Create New Category > Category Name** field in the **Profile Details** and **Section Details** pages. This issue is fixed and now the **Category Name** text box accepts alphanumeric characters.