

Qualys File Integrity Monitoring v2.x

Release Notes

Version 2.1

March 13, 2020

Here's what's new in Qualys FIM 2.1!

[Correlation Rule Wizard Layout Changed to a Single Page](#)

[Query Library Support](#)

[Group Events by Various Filters to Get Count of Events](#)

[Improvements in Inclusion/Exclusion Filters](#)

[Search Queries Created in All Events or Events Review tab to Show in both the Tabs](#)

[Message Shown for Invalid Search Tokens](#)

[Rules tab Renamed to Responses](#)

[Activated Monitoring Profile to Contain at least One Rule or Section](#)

[Event Details Page to Show Incident Details](#)

[Renamed the option to Import Library Profile](#)

[Create Alert Rule and Create Correlation Rule Options Available in All Events and Event Review tabs](#)

**Qualys FIM 2.1 brings you many more
Improvements and updates! [Learn more](#)**

Correlation Rule Wizard Layout Changed to a Single Page

Correlation rule wizard is now simplified to show a single page for creating rules instead of tab based multiple pages. This means the user does not have to switch between forms when creating or modifying a correlation rule as all the information will be available for view at one place. We have also updated few field labels in the form to make them crisper and more meaningful.

The process of creating correlation rules is going to be same. You need to provide a rule name and description, rule query to specify for which events you want to create incidents, a schedule to indicate when and how often you want to run the rule to create incidents for the events matching the rule query and choose how you want to review and close the incident.

← Create Correlation Rule

Correlation Rule Details

Rule Name

Required

Incidents for create events

Reviewer : quays_sb1

Description

Optional

Enter Description

Rule Query

Required

X action:Create

Saved Searches | Queries

Schedule Management

☐ Recurring Job

Fix Date

02/06/2020

Start Time

11:00am

End Time

11:59pm

Schedule : February 6th 2020 from 11.00 AM to 11.59 PM

Approval Type

Required

MANUAL

Cancel

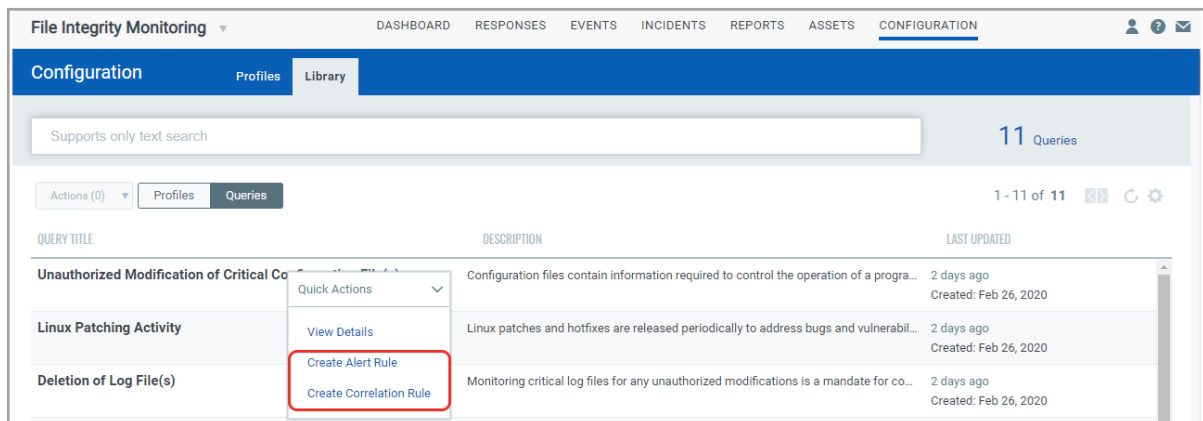
Save

Save & Create Alerting Rule

Query Library Support

We are providing a library of QQL queries under Configuration > Library > Queries, which will contain predefined queries for creating complex rules. For each query, we will show you its name, description and the last updated date.

Use Quick Actions menu to view what the query does, create alert and correlation rules. To create an Alert and Correlation rule, choose a query and from Quick Actions menu, select "Create Alert Rule" or "Create Correlation rule". You will be navigated to the appropriate rule wizard.



You can also access Query library when you create a new correlation rule.

← Create Correlation Rule

Correlation Rule Details

Rule Name Required

Rule Name

Reviewer : quays_hs

Description Optional

Enter Description

Rule Query Required

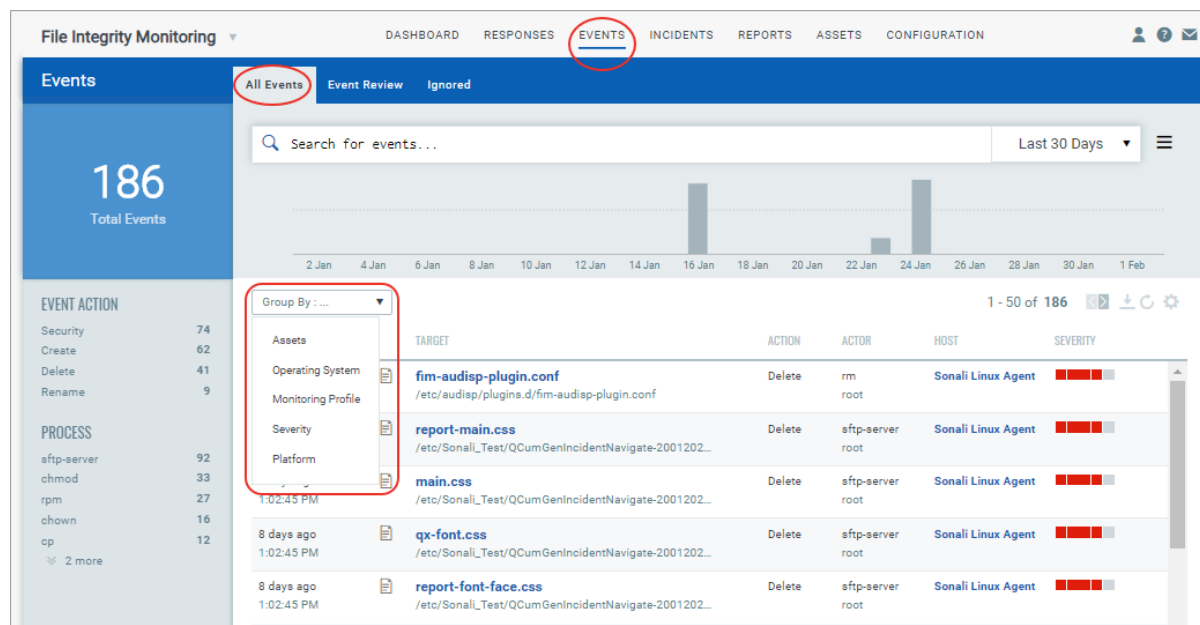
Search...

Saved Searches **Queries**

Schedule Management ☐ Recurring Job

Group Events by Various Filters to Get Count of Events

You can now view the total number of events created by Assets, Operating System, Monitoring Profile, Severity and Platform in the All Events tab. To view the count of FIM events by any of the filters, go to Events > All Events tab, select a date range and select a filter from Group By drop-down.



The screen shows total event count by assets.

The screenshot shows the 'File Integrity Monitoring' dashboard with the 'EVENTS' tab selected. The 'All Events' sub-tab is active, displaying a total of 186 events. The 'Group By' dropdown menu is set to 'Assets'. The table shows a single entry for 'Sonali Linux Agent' with 186 total events.

ASSET NAME	OPERATING SYSTEM	TOTAL EVENTS
Sonali Linux Agent cc501fd2-cd79-4454-96be-32afe1130223	CentOS Linux 7.5.1804	186

Improvements in Inclusion/Exclusion Filters

In the Monitoring Profile Rule wizard, we will now show you the base directory path when you add a relative path to include or exclude a file or directory. You will see the base directory path before the path text box. When you save the rule, the base path is appended to the relative path.

We have made another improvement. Earlier, when specifying file/directory paths for inclusion/exclusion filters for both Linux and Windows, the path after comma is treated as new file/directory filter. This is an issue if the file/directory name has comma in it. We now support file and directory names with comma by not creating a new filter if a comma is found in a file/directory path.

If you want to specify more than one file or directory, then add a new path or create a new filter and add path for each new file/directory filter.

← Create New: Monitoring Profile Rule

Monitoring Rule Parameters

Rule Type: Directory Severity: Severity 3

Directory Path: C:\Windows Required

Depth: None

Monitor the directory structure for: ☐ All

☐ Directory Name Changes ☐ Changes to Attributes

☐ Directory Removal ☐ Changes to Security Settings

☐ Directory Creation

Monitor files within the directory structure for: ☐ All

☒ Name Changes ☐ File Content Changes

☐ File Removal ☐ Changes to Attributes

☐ File Creation ☐ Changes to Security Settings

Advanced Options

Filter: 1

Type: Include Targeting: Files

Please enter relative path(s) here:

C:\Windows\ system32*.txt Delete

C:\Windows\ system32\boot1,boot2.txt Delete

Base directory path

Relative path with comma in file name is considered as a single filter

Add another path

Search Queries Created in All Events or Events Review tab to Show in both the Tabs

Queries saved in the All Events tab and Events Review tab will appear in both the tabs as Saved Searches.

File Integrity Monitoring

DASHBOARD RESPONSES **EVENTS** INCIDENTS REPORTS ASSETS CONFIGURATION

Events

41 Total Events

PROCESS

sftp-server 40

rm 1

All Events Event Review Ignored

action:Delete

Last 30 Days

Recent Searches

Save this Search Query

Manage Saved Searches

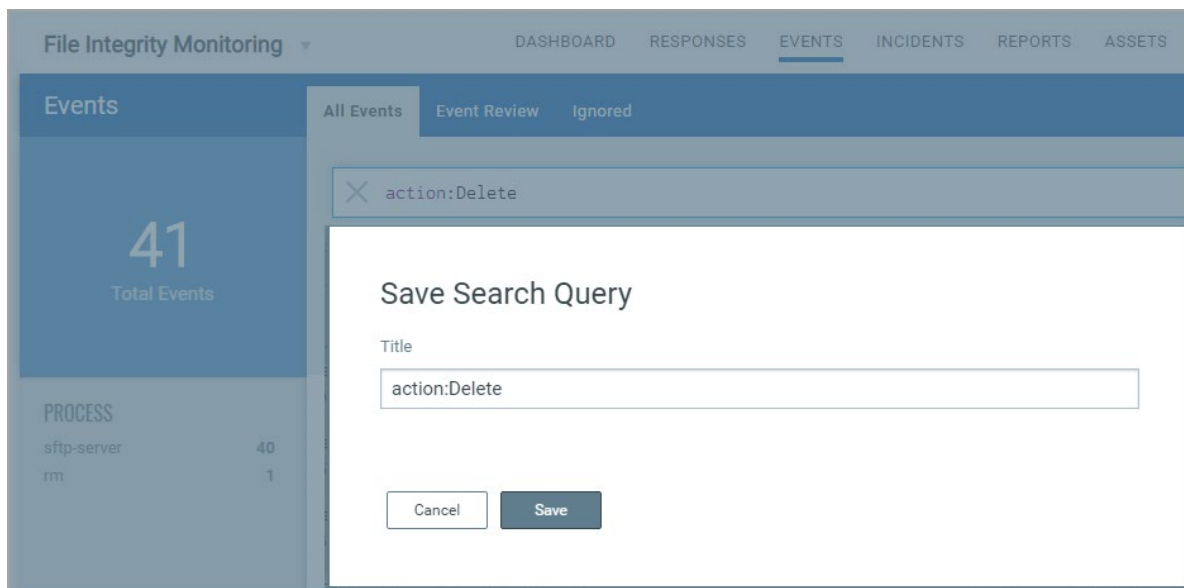
Create Alert Rule from Search Query

Create Correlation Rule from Search Query

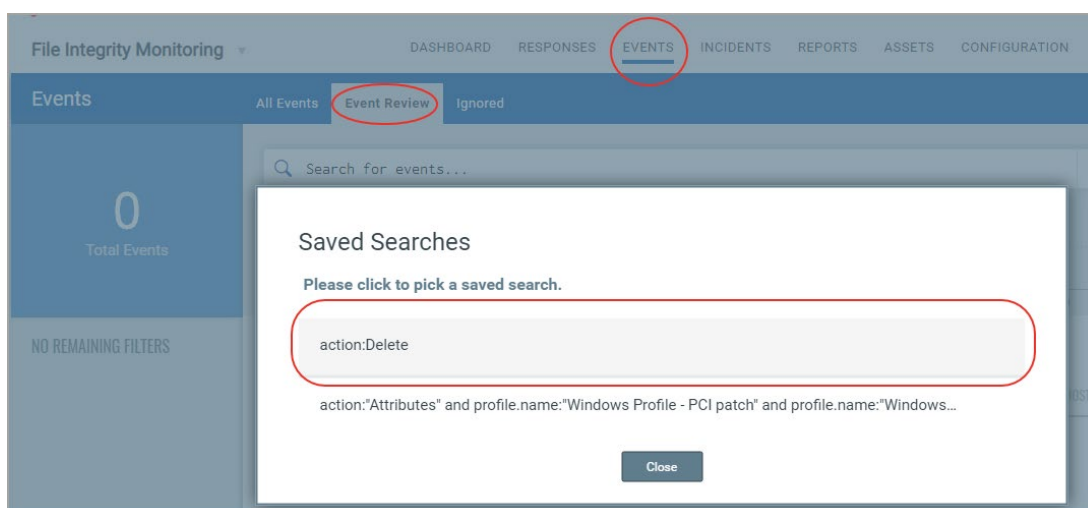
Group By: ...

TIME	TARGET	ACTION	ACTOR	HOS
10 days ago 3:18:00 PM	fim-audisp-plugin.conf /etc/audisp/plugins.d/fim-audisp-plugin.conf	Delete	rm root	Sonali Linux Agent

When you save a search query in the “All Events” tab, the same query will be available in the “Event Review” tab when you go to the Manage Save Searches > Save Searches screen.

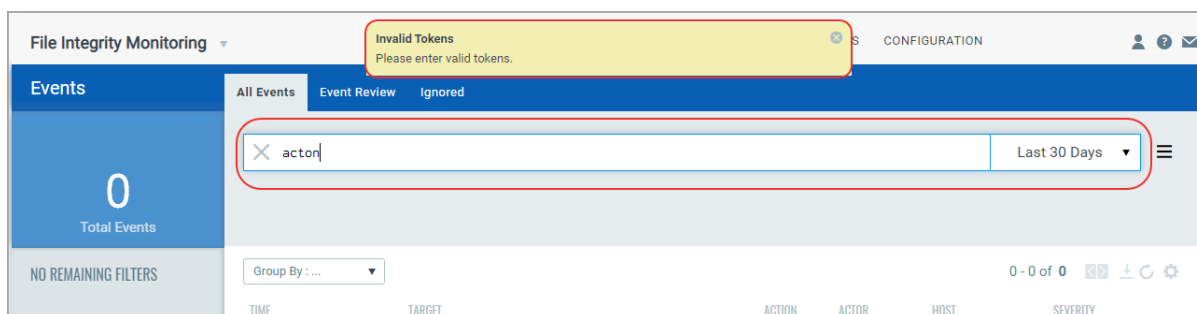


The query “action:Delete” that is created in the “All Events” tab is listed in the “Saved Searches” screen in the “Event Review” tab.



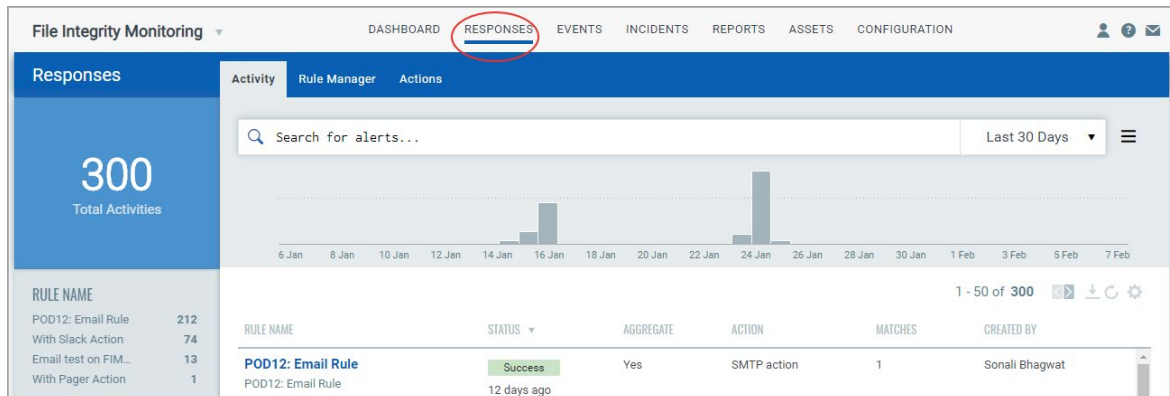
Message Shown for Invalid Search Tokens

We now validate QQL tokens when you manually type the search tokens in the search box in all the tabs except Responses tab. FIM shows an Invalid Token message if the token is not valid. Note that values are not validated. This message is shown also if values are not provided for tokens that required input values.



Rules tab Renamed to Responses

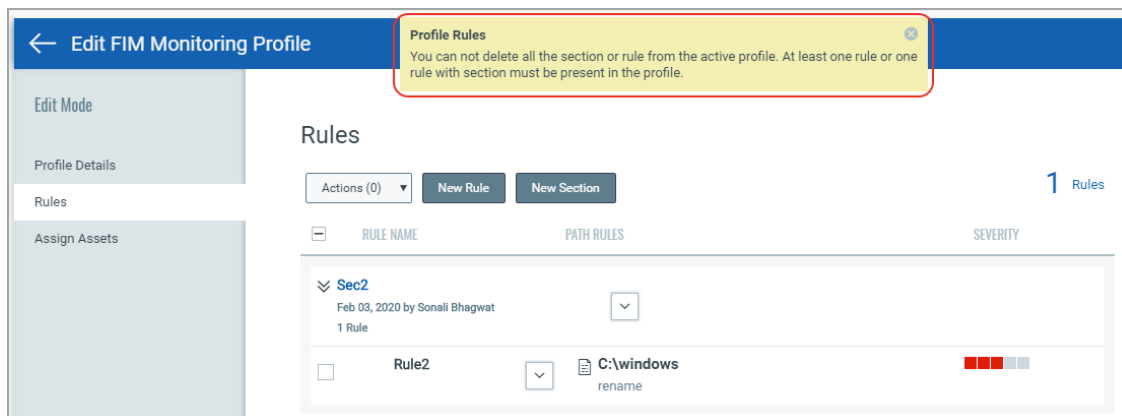
We renamed Rules tab to Responses. The tab will provide the same functionality that is to create and manage alert rules.



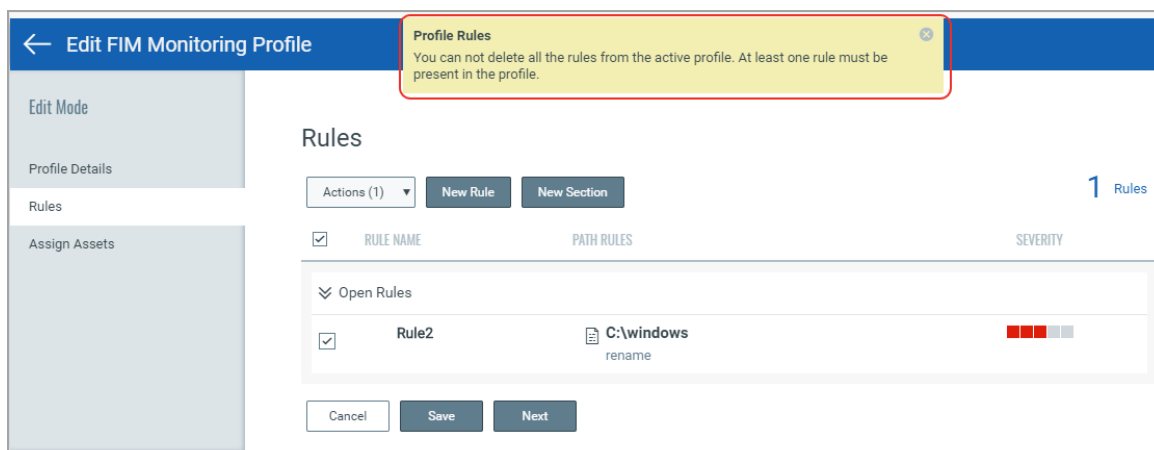
Activated Monitoring Profile to Contain at least One Rule or Section

We have made it mandatory for activated profiles to have at least one Rule or a Section with a rule in it. We show an error message if you try to 1) activate a profile that has no rule or section with a rule in it, 2) delete the only rule in the profile, and 3) remove the only section with rule.

The error message is shown when the user tries to delete the only section with a rule in it.



The error message is shown when the user tries to delete the only rule in the monitoring profile.



Event Details Page to Show Incident Details

You can now see the incident details of an event that is associated with an Incident. Incident details are shown for the event on the Event Details page.

The screenshot shows the 'View Details: FIM-AUDISP-PLUGIN.CONF' page. The main section is titled 'Event Alert: File Delete'. It includes a file icon, the filename 'fim-audisp-plugin.conf', and details: 'Deleted On: 11 days ago Jan 24, 2020 at 3:18:00 PM', 'Category: 2-0-2 testing', 'By user: root', 'File Path: /etc/audisp/plugins.d/fim-audisp-plugin.conf', and 'By process: /usr/bin/rm'. A red box highlights the message 'fim-audisp-plugin.conf was Deleted'. Below this, the 'Triggers' section shows 'Monitoring Profile: 2.0.2 Testing' and 'Section and Rules: 2.0.2 testing: 1'. A red box highlights the 'Associated Incident' section, which contains a table with incident details.

Associated Incident	
Created On:	November 10th, 2019 05:39 pm
Incident Name:	Manual review incident-20191110-120900
Type:	AUTOMATED
Incident Status:	OPEN
Assignee:	quays_sb1
Disposition Category:	Not Available
Change Type:	Not Available
Approval Status:	Not Available

The right sidebar contains 'ABOUT ASSET' for 'Sonali Linux Agent' (CentOS Linux 7.5.1804) and 'Identification' details like DNS Hostname, NetBIOS Name, IP addresses, Agent ID, and Host ID. It also shows 'Activity' with login and boot timestamps.

Renamed the Option to Import Library Profile

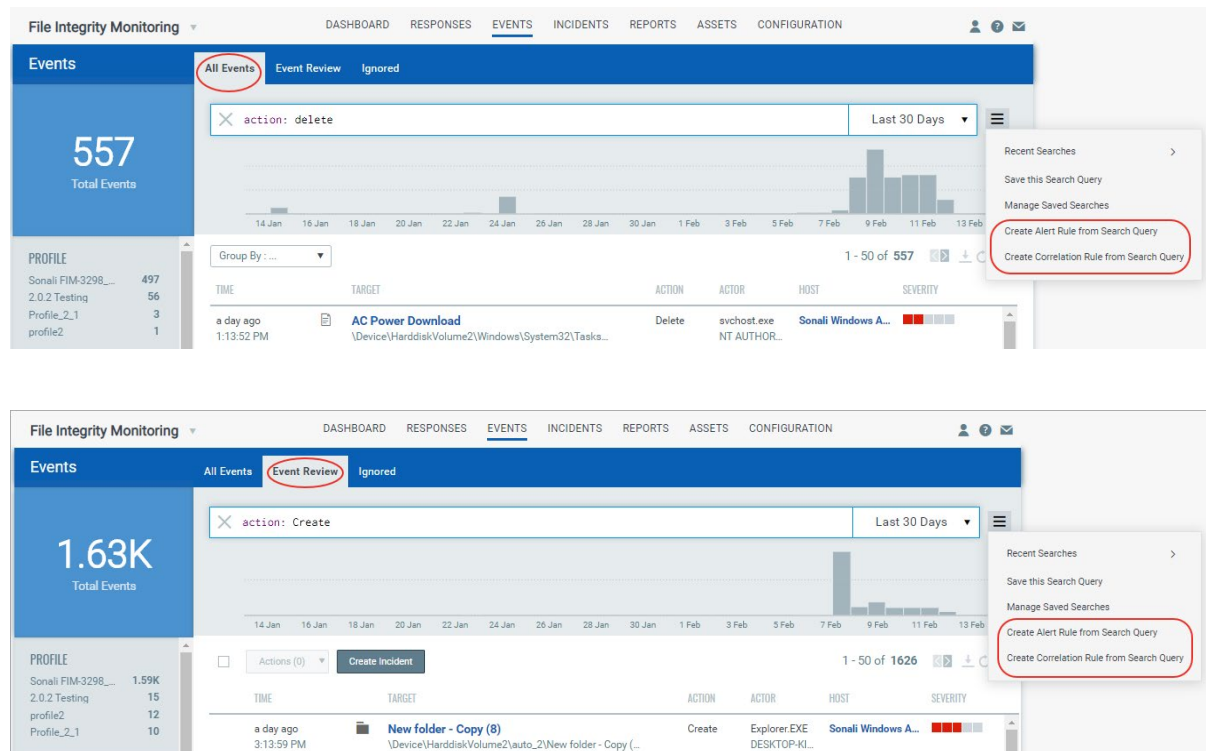
We have renamed the option to import library profile from “Import and Use as Active Profile” to “Import to Profile”. Earlier name was suggesting that the imported profile will be active. But the profile needs to be activated after it is imported.

The screenshot shows the 'File Integrity Monitoring' configuration page, specifically the 'Library' tab. It displays a table of profiles with columns: PROFILE TITLE, LAST UPDATED, CATEGORY, and PROFILE TYPE. The first profile is 'Lightweight Monitoring Profile for Windows Version 2.0'. A dropdown menu is open for the first profile, showing options: 'Quick Actions', 'View Details', and 'Import to Profiles' (highlighted with a red box). The table lists four profiles, all created on Sep 30, 2019, with categories PCI and profile types WINDOWS or LINUX.

PROFILE TITLE	LAST UPDATED	CATEGORY	PROFILE TYPE
☒ Lightweight Monitoring Profile for Windows Version 2.0	4 days ago Created: Sep 30, 2019	PCI	WINDOWS
Monitoring Profile for Linux Version 2.0	4 days ago Created: Sep 30, 2019	PCI	LINUX
Lightweight Monitoring Profile for Linux Version 2.0	4 days ago Created: Sep 30, 2019	PCI	LINUX
Monitoring Profile for IIS Version 2.0	4 days ago Created: Sep 30, 2019	PCI	WINDOWS

Create Alert Rule and Create Correlation Rule Options Available in All Events and Event Review tabs

You can now create both alert rule and correlation rule from the “All Events” and “Events Review tab”. Go to Events > All Event tab or Events > Event Review tab. Enter a search query in the search box and press Enter. Click  menu button next to search box and select "Create Rule from Search Query". When you create an alert rule, the search query provided on the page is copied to the new rule.



Issues Addressed

- Now incidents will get created for an autocorrelation rule when an event is created that matches the incident criteria specified in the rule.
- We have fixed an issue where it was not possible to download the Events list.
- UI is improved in terms of look and feel.
- In Approval Status field for Autocorrelation Rules, NA option is removed as it was ambiguous.
- By default, Events are displayed in descending order of Event time.
- All types of FIM supported Linux agents were not available in the list in Profile > Assign Asset tab. Now it is possible to add assets of all supported Linux versions from Profile > Assign Asset page.
- Through autocorrelation rules, incidents will get created when there is an Event created that matches the Incident criteria.
- We fixed the issue with 'Ignore All Matching Events' option.
- Ignore/ Ignore and Whitelist option is made available on the Event Details page.