Qualys File Integrity Monitoring v2.x

Release Notes

Version 2.2
June 5, 2020

Here's what's new in Qualys FIM 2.2!

FIM Management APIs

Clone a Profile

Enhancement to the Incident Report

Delete a Profile

Enable Create Incident Option

Qualys FIM 2.2 brings you many more Improvements and updates! Learn more

FIM Management APIs

We are excited to introduce the following new set of APIs that enables you to:

- Automate the Alert and Incident functions.
- Create Profiles using Import and Export action.

For a detailed description of each API, refer to the FIM API Version V2 guide on the Documentation Portal.

FIM Alerting APIs

Alerting Action API	
Fetch all Alert Actions	/fim/v3/alert/actions/search
Fetch Alert Actions for an Action ID	/fim/v3/alert/actions/{actionId}
Alerting Rules API	
Fetch Alert Rules	/fim/v3/alert/rules/search
Fetch Details for Alert Rule	/fim/v3/alert/rules/{ruleId}
Enable Alert Rule	/fim/v3/alert/rules/{ruleId}/enable
Disable Alert Rule	/fim/v3/alert/rules/{ruleId}/disable
Delete Alert Rule	/fim/v3/alert/rules/{ruleId}/delete
Alerting Activities API	
Fetch the Generated Alerts for FIM	/fim/v3/alert/activities/search
Count Number of Alerts Generated for FIM	/fim/v3/alert/activities/count

FIM Incidents APIs

Fetch Incidents	/fim/v3/incidents/search
Create Manual Incident	/fim/v3/incidents/create
Approve an Incident	/fim/v3/incidents/{incidentId}/approve

FIM Correlation APIs

Fetch all Correlation Rules	/fim/v3/autocorrelation/rules/search
Fetch Correlation Rule Details for a Rule ID	/fim/v3/autocorrelation/rules/{autoCorrelationRuleId}
Fetch the Count of Correlation Rules	/fim/v3/autocorrelation/rules/count
Create Correlation Rules	/fim/v3/autocorrelation/rules/create

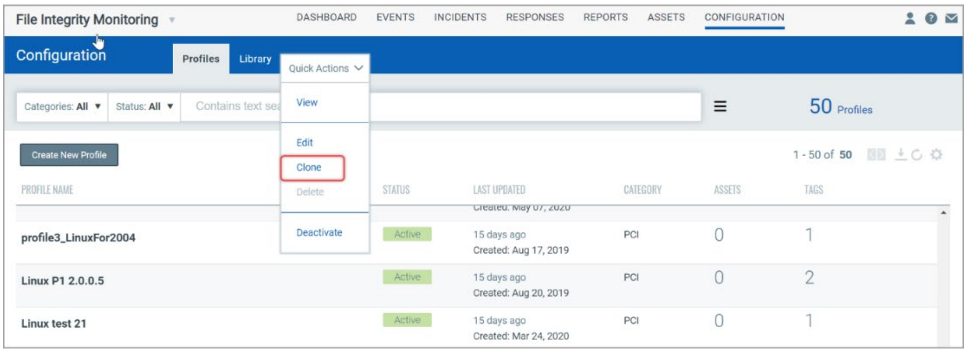
Update Correlation Rule	/fim/v3/autocorrelation/rules/{autoCorrelationRuleId}/update
Activate Correlation Rule	/fim/v3/autocorrelation/rules/{autoCorrelationRuleId}/activate
Deactivate Correlation Rule	/fim/v3/autocorrelation/rules/{autoCorrelationRuleId}/deactivate
Delete Correlation Rule	/fim/v3/autocorrelation/rules/{autoCorrelationRuleId}/delete

FIM Profile APIs

Search a Profile	/fim/v3/profiles/search
Activate a Profile	/fim/v3/profiles/{profileId}/activate
Assign an Asset to a Profile	/fim/v3/profiles/{profileId}/assets
Assign Tags to a Profile	/fim/v3/profiles/{profileId}/assettags
Export the Profile in XML Format	/fim/v3/profiles/{profileId}/exportxml
Export the Profile in JSON Format	/fim/v3/profiles/{profileId}/exportjson
Import a Profile from XML File Inputs	/fim/v3/profiles/importxml
Import a Profile from JSON File Inputs	/fim/v3/profiles/importjson
List the Profile Categories	/fim/v3/categories/search
Deactivate a Profile	/fim/v3/profiles/{profileId}/deactivate

Clone a Profile

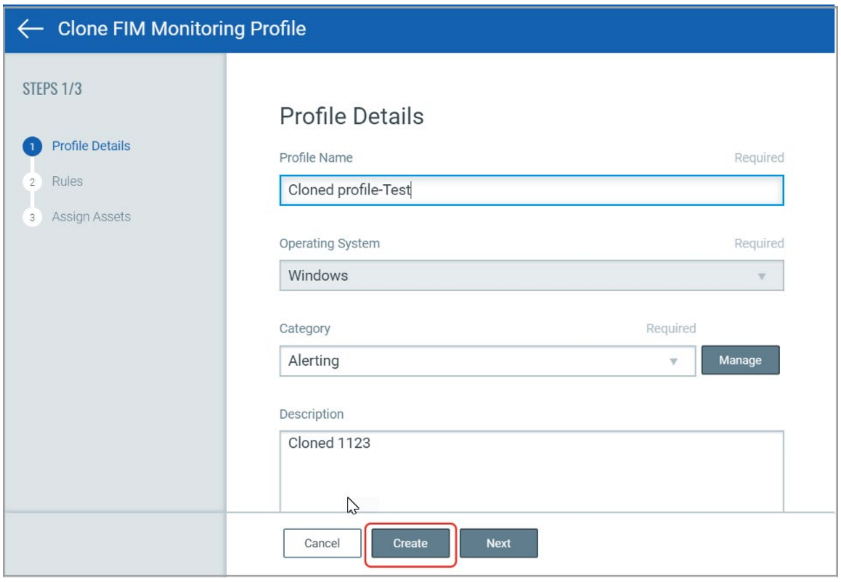
With this release, we introduce a feature that allows you to clone a profile along with its rules. To clone a profile, select an existing profile, and from the Quick Actions menu click Clone.



PROFILE NAME	STATUS	LAST UPDATED	CATEGORY	ASSETS	TAGS
		Created: May 07, 2020			
profile3_LinuxFor2004	Active	15 days ago Created: Aug 17, 2019	PCI	0	1
Linux P1 2.0.0.5	Active	15 days ago Created: Aug 20, 2019	PCI	0	2
Linux test 21	Active	15 days ago Created: Mar 24, 2020	PCI	0	1

The Clone FIM Monitoring Profile page is displayed and the Profile Name is prefixed with "Cloned profile". You can change the name, add Category and Description and then click Create to clone the profile along with its rules.

Note: You cannot change the Operating System of the cloned profile.



Profile Details

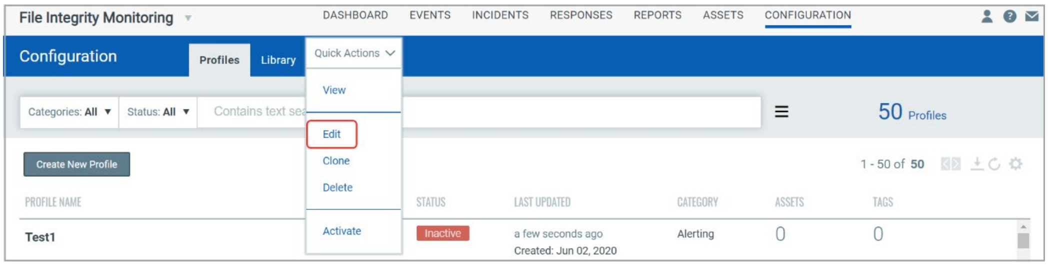
Profile Name (Required): Cloned profile-Test

Operating System (Required): Windows

Category (Required): Alerting

Description: Cloned 1123

After the profile is cloned, you must edit it to add the required details. Select the cloned profile and from the Quick Actions menu click Edit.



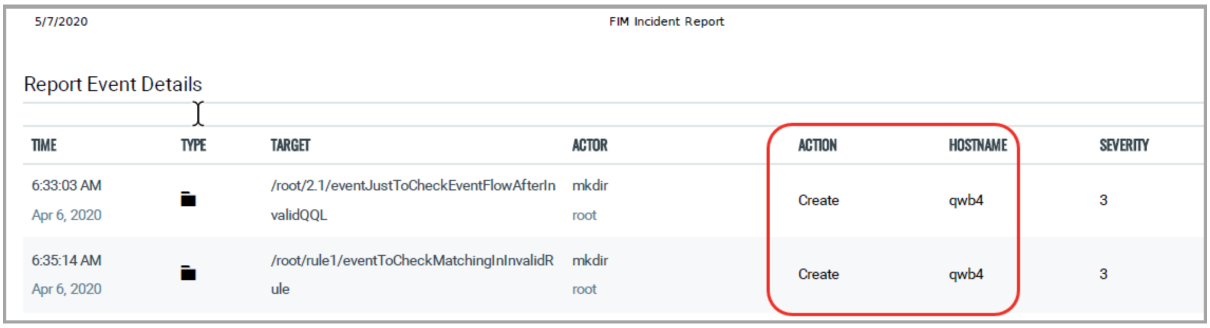
PROFILE NAME	STATUS	LAST UPDATED	CATEGORY	ASSETS	TAGS
Test1	Inactive	a few seconds ago Created: Jun 02, 2020	Alerting	0	0

On the Rules page, edit the rules if required and click Next. On the Assign Assets page, add tags, assets, and click Save. To use the profile for monitoring, activate the profile.

Enhancement to the Incident Report

For better clarity and understanding, we have added the following two columns in the Incident Report.

- Action: Registers the actions performed on the target.
- Hostname: Registers the name of the host that raised the event.



5/7/2020

FIM Incident Report

Report Event Details

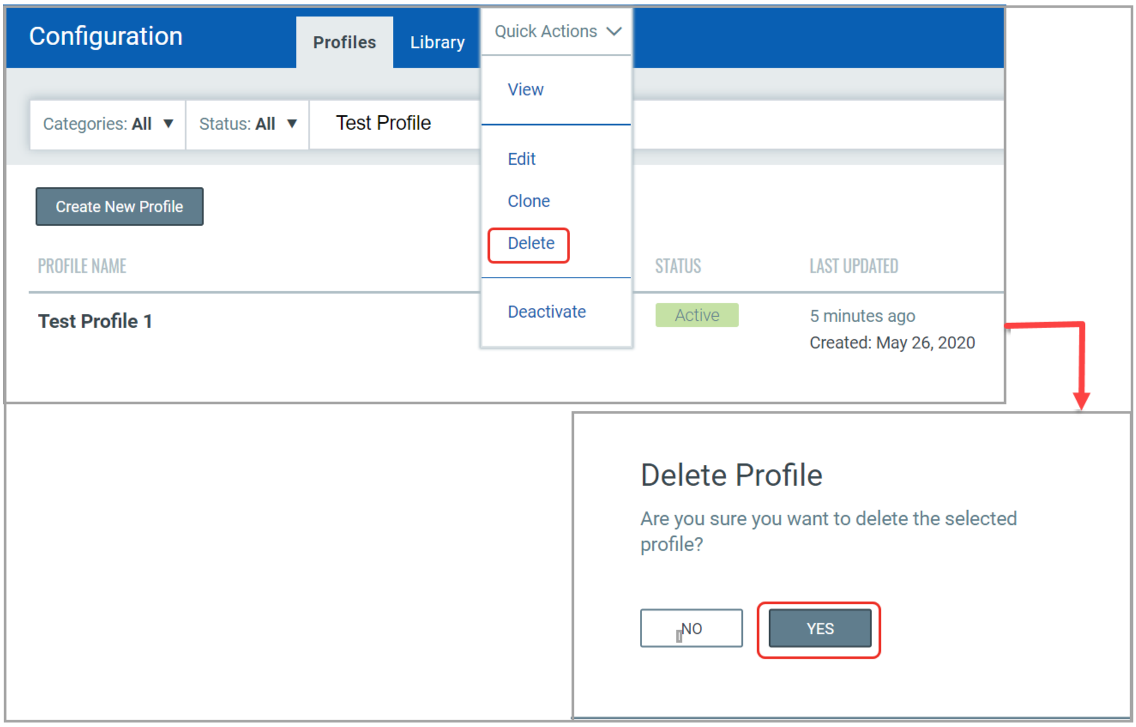
TIME	TYPE	TARGET	ACTOR	ACTION	HOSTNAME	SEVERITY
6:33:03 AM Apr 6, 2020	📁	/root/2.1/eventJustToCheckEventFlowAfterInvalidQQL	mkdir root	Create	qwb4	3
6:35:14 AM Apr 6, 2020	📁	/root/rule1/eventToCheckMatchingInInvalidRule	mkdir root	Create	qwb4	3

Delete a Profile

We have introduced a few alterations to the Delete profile feature. The changes are:

- You cannot delete an active profile that has tags or assets associated with it. To delete such profiles, you must deactivate the profile first.
- You can directly delete an inactive profile or an active profile that does not have tags or assets associated.

To delete a profile, select Delete from the Quick Actions menu and click Yes on the Delete Profile window.

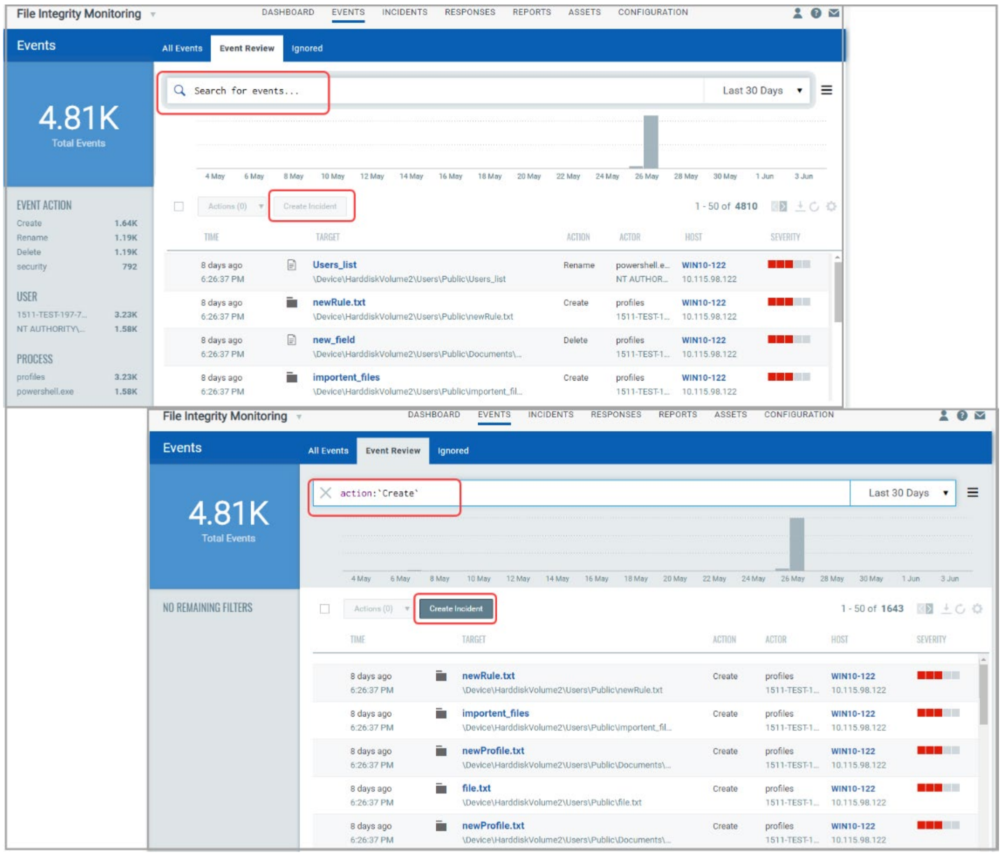


Delete Profile

Are you sure you want to delete the selected profile?

Enable Create Incident Option

The Create Incident option is enabled only after you enter a valid QQL query in the search bar.



Search for events...

Last 30 Days

EVENT ACTION	
Create	1.64K
Rename	1.19K
Delete	1.19K
security	792

USER	
1511-TEST-197-7...	3.23K
NT AUTHORITY\...	1.58K

PROCESS	
profiles	3.23K
powershell.exe	1.58K

1 - 50 of 4810

TIME	TARGET	ACTION	ACTOR	HOST	SEVERITY
8 days ago 6:26:37 PM	Users_list \Device\HarddiskVolume2\Users\Public\Users_list	Rename	powershell.e... NT AUTHOR...	WIN10-122 10.115.98.122	🟥🟥🟥⬜⬜
8 days ago 6:26:37 PM	newRule.txt \Device\HarddiskVolume2\Users\Public\newRule.txt	Create	profiles 1511-TEST-1...	WIN10-122 10.115.98.122	🟥🟥🟥⬜⬜
8 days ago 6:26:37 PM	new_field \Device\HarddiskVolume2\Users\Public\Documents\...	Delete	profiles 1511-TEST-1...	WIN10-122 10.115.98.122	🟥🟥🟥⬜⬜
8 days ago 6:26:37 PM	importent_files \Device\HarddiskVolume2\Users\Public\importent_fil...	Create	profiles 1511-TEST-1...	WIN10-122 10.115.98.122	🟥🟥🟥⬜⬜

action:`Create`

Last 30 Days

NO REMAINING FILTERS

1 - 50 of 1643

TIME	TARGET	ACTION	ACTOR	HOST	SEVERITY
8 days ago 6:26:37 PM	newRule.txt \Device\HarddiskVolume2\Users\Public\newRule.txt	Create	profiles 1511-TEST-1...	WIN10-122 10.115.98.122	🟥🟥🟥⬜⬜
8 days ago 6:26:37 PM	importent_files \Device\HarddiskVolume2\Users\Public\importent_fil...	Create	profiles 1511-TEST-1...	WIN10-122 10.115.98.122	🟥🟥🟥⬜⬜
8 days ago 6:26:37 PM	newProfile.txt \Device\HarddiskVolume2\Users\Public\Documents\...	Create	profiles 1511-TEST-1...	WIN10-122 10.115.98.122	🟥🟥🟥⬜⬜
8 days ago 6:26:37 PM	file.txt \Device\HarddiskVolume2\Users\Public\file.txt	Create	profiles 1511-TEST-1...	WIN10-122 10.115.98.122	🟥🟥🟥⬜⬜
8 days ago 6:26:37 PM	newProfile.txt \Device\HarddiskVolume2\Users\Public\Documents\...	Create	profiles 1511-TEST-1...	WIN10-122 10.115.98.122	🟥🟥🟥⬜⬜

Issues Addressed

- Now you can create a rule for Linux where filename can start with zero.
- When you are listing an inclusion or exclusion path, you need not start or end it with a slash. However, the base path should begin with a slash.