



Qualys File Integrity Monitoring (FIM)

Release Notes

Version 3.6.1

January 11, 2023

What's New!

New Features

- Create Asset-based FIM Reports

Enhancements

- New Values for Incident Review Criteria

- Improvements to Incident Creation Workflow

- Provide Custom Subject in the Email Notification for Reports

New Features

Create Asset-based FIM Reports

With FIM 3.6 and earlier, report creation was restricted to events and incidents. This release adds support to create asset-based FIM reports.

As per PCI-DSS guidelines, all assets within your PCI scope for FIM must have a FIM solution actively running on them. If FIM is not running on scoped assets, such assets can be marked as non-compliant PCI assets.

You now have access to required asset information in real time and can generate on-demand or scheduled reports to detect non-compliant PCI assets with regards to FIM; thus, empowering you to be always audit-ready.

The screenshot shows the 'Report Rule: Create' interface. On the left, a sidebar lists five steps: 1. Report Rule Details, 2. Source (highlighted), 3. Report Output, 4. Report Schedule, and 5. Review & Confirm. The main area is titled 'Source' and contains the following elements:

- Instruction: 'Specify the source of report that you want to include in the rule and other relevant details.'
- Section: 'Select Report Source' with two radio buttons: 'Events' (unselected) and 'Assets' (selected).
- Query field: A text input box containing the query: `agentService.status:'FIM_STOPPED' or agentService.status:'FIM_DRIVER_LOADED_FAILURE' or agentService.status:'FIM`. The field has a search icon on the left and a help icon on the right.
- Checkbox: A checked checkbox labeled 'List of non compliant assets as per PCI DSS Requirement 11.5 v3.2.1 and 11.5.2 v4.0'.
- Navigation: At the bottom, there are three buttons: 'Cancel', 'Previous', and 'Next'.

To create a report on non-compliant assets, perform the following steps:

1. Go to **Reports > Report Rules > Create Report Rules**.
2. In the **Source** page, click **Assets**.
3. Select the **List of non-compliant assets as per PCI DSS Requirement 11.5 v3.2.1 and 11.5.2 v4.0** check box.
4. Click **Next** and provide the necessary inputs until you reach the **Review & Confirm** page.
5. Click **Create Report Rule**.

For more detailed help, refer to the *File Integrity Monitoring Online Help*.

Enhancements

New Values for Incident Review Criteria

This release introduces some new values for incident review process:

Incident Review Parameter	Description	Values
approvalStatus	The approval status of the incident created by the rule.	APPROVED, POLICY_VIOLATION, UNAPPROVED, PENDING .
changeType	Type of incidents created by the rule.	MANUAL, AUTOMATED, COMPROMISE, STANDARD_CHANGE , EMERGENCY_CHANGE , NORMAL_CHANGE , OTHER
dispositionCategory	The category of the incident created by the rule.	PATCHING, PRE_APPROVED_CHANGE_CONTROL, CONFIGURATION_CHANGE, HUMAN_ERROR, DATA_CORRUPTION, EMERGENCY_CHANGE, CHANGE_CONTROL_VIOLATION, GENERAL_HACKING, MALWARE, MALICIOUS_INTENT , UNAUTHORIZED_ACCESS , INAPPROPRIATE_USAGE_OR_FRAUD , DATA_LOSS_OR_THEFT , DISREGARD_OF_ORGANIZATIONAL_POLICY , FALSE_POSITIVE , OTHER

Note: The values in bold represent the new value added for the parameters.

The screenshot shows the 'Create Correlation Rule' interface. At the top, there is a blue header with a back arrow and the text 'Create Correlation Rule'. Below the header, there is a 'Review Mode' dropdown menu set to 'Automated'. Below that is a 'Disposition' dropdown menu, which is highlighted with a red box. The dropdown menu is open, showing a list of options: 'Disregard of Organizational Policy', 'False Positive', 'Patching', 'Pre-Approved Change Control', 'Configuration Change', 'Human Error', 'Data Corruption', and 'Emergency Change'. The 'Configuration Change' option is highlighted in grey. Below the dropdown menu is a 'Comment' text area with a character count of '2500 characters remaining'. At the bottom of the form, there are three buttons: 'Cancel', 'Save & Create Alerting Rule', and 'Save'.

Improvements to Incident Creation Workflow

Earlier, when an incident was created, it used to get assigned to the logged in user. With this release, you can now add one or more reviewers (maximum limit is 10) for incident generation.

You can add the reviewer in

- Create Correlation Rule page

Correlation Rule Details

Rule Name *
Detect Tampering of Exchange Server Logs

Reviewers *
john.doe@domain.com ×
1 recipients added

Description
Exchange log files might contain the potential IOCs (Indicator of Compromise) for the exploit. Monitoring critical log files for any unauthorized modifications is a mandate for compliance regulations such as PCI DSS, HIPAA, SOX and others. Qualys FIM's alerting
1644 characters remaining

Rule Query *
× (file.fullPath:"Exchange Server" and file.fullPath:"logging") and (action: delete or action: Security) ?

Saved Searches | Queries

- Update Correlation Rule page

← Update Correlation Rule: **Test_Rule**

Correlation Rule Details

Rule Id:
e7f632fe-b934-47e9-8375-d9c5d0b345ba

Rule Name:
Test_Rule

Reviewers *
quays_wk29 × john.doe@domain.com ×
9 more reviewers can be added

Description
Enter Description
2000 characters remaining

- Create Default/Manual Incident

You can also add reviewers when you manually create incidents from the **Incidents > All Incidents** page.

← Create Incident

Create Incident

Incident Name *

Reviewers *

S sah_st6 × J john.doe@dmai.com ×

8 more reviewers can be added

Query *

 ?

Saved Searches | Queries

Start Date	Start Time
<input type="text" value="11/15/2022"/> 📅	<input type="text" value="5:21 pm"/> 🕒
End Date	End Time
<input type="text" value="12/15/2022"/> 📅	<input type="text" value="5:21 pm"/> 🕒

Enhanced Alerting Workflow

With the new capability, incident reviewers will now get an alert notification (email) every time anyone creates, updates, approves, reopens, or deletes an incident. The reviewer can click on the provided link in the email notification and go to the specific incident and view the details.

Note: You must enter valid email IDs of the reviewers to ensure they receive the notification mails.

With this new alerting workflow, FIM deprecates the older way of creating alerting rules from the **Correlation Rule Creation** page.

Provide Custom Subject in the Email Notification for Reports

Earlier, the email notifications for reports used to have a default subject statement. Starting this release, you can provide a custom subject for the email notifications.

The screenshot shows the 'Report Rule: Create' interface. On the left, a sidebar lists the steps: 1. Report Rule Details, 2. Source, 3. Report Output (selected), 4. Report Schedule, and 5. Review & Confirm. The main content area is titled 'Report Output and Notification' and includes the instruction: 'Choose the format for your report output and specify if you want to notify users upon report generation.' Under 'Report Output', there are three radio buttons for 'Output Format': CSV (selected), PDF, and HTML. Below this is a question: 'Would you like to compress the generated report?' with 'Yes' and 'No' (selected) radio buttons. A red box highlights the 'Notification' checkbox, which is checked. Below it is the 'Notification Subject' field, which contains the text 'New Report Subject'. A tooltip is visible over this field, showing the text 'Qualys - Reporting - New Report Subject'. The 'To' field contains the email address 'john.doe@domain.com'. At the bottom, there are 'Cancel', 'Previous', and 'Next' buttons.