Qualys File Integrity Monitoring (FIM)

Release Notes

Version 3.6.1

January 11, 2023

What's New!

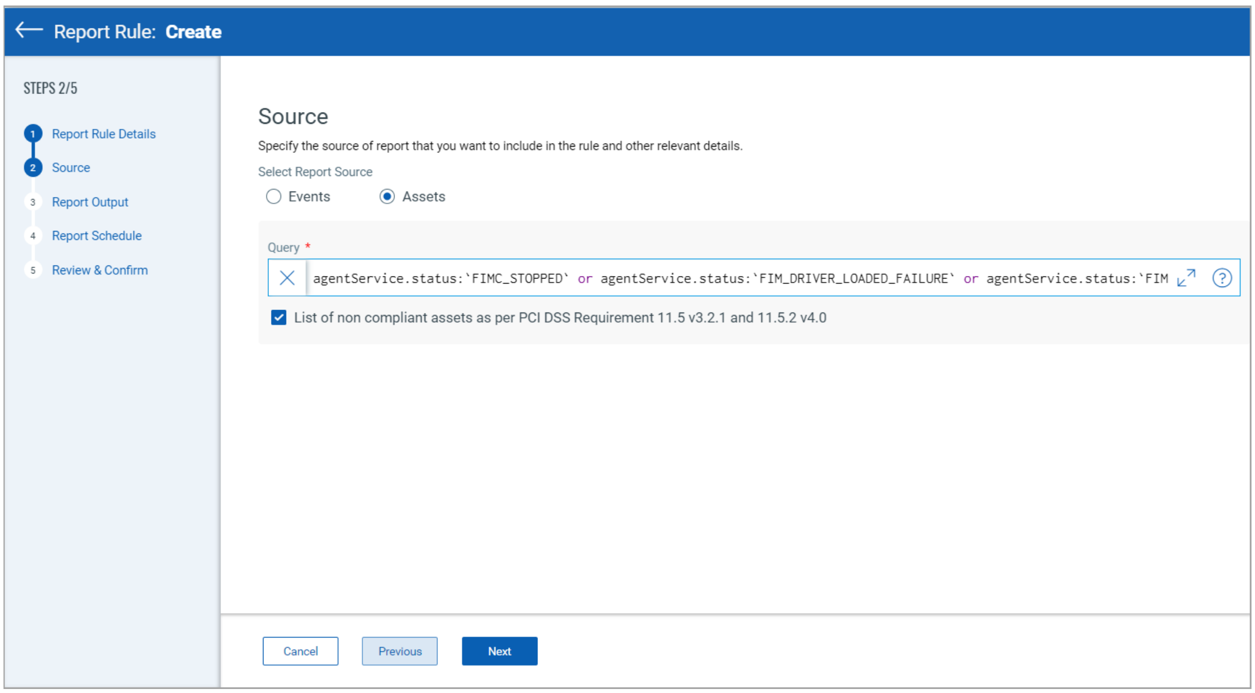
New Features

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 reards to FIM; thus, empowering you to be always audit-ready.



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*.

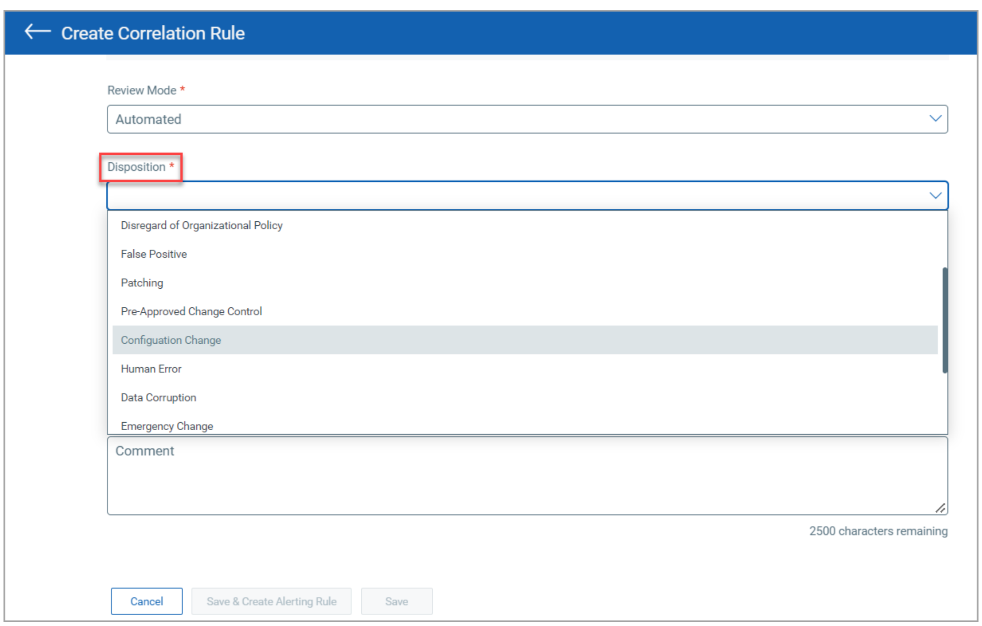
Enhancements

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.

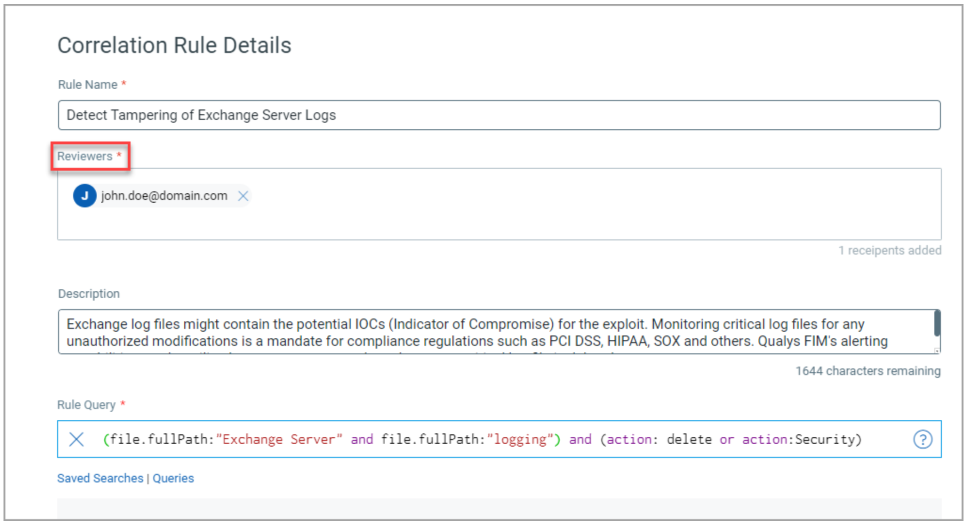


Improvements to Incident Creation Workflow

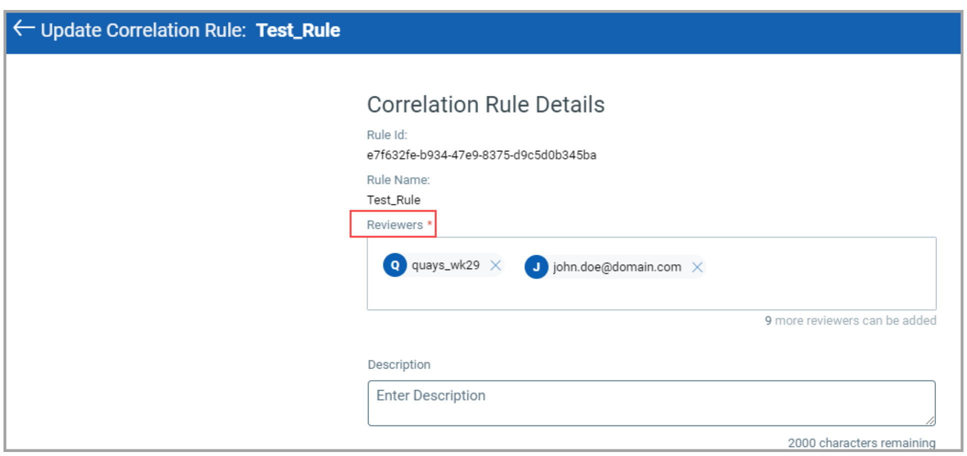
Earlier, when an incident was created, it used to get assigned to the logged in user. With this release, you can now add one or more reviewers (maximum limit is 10) for incident generation.

You can add the reviewer in

- Create Correlation Rule page

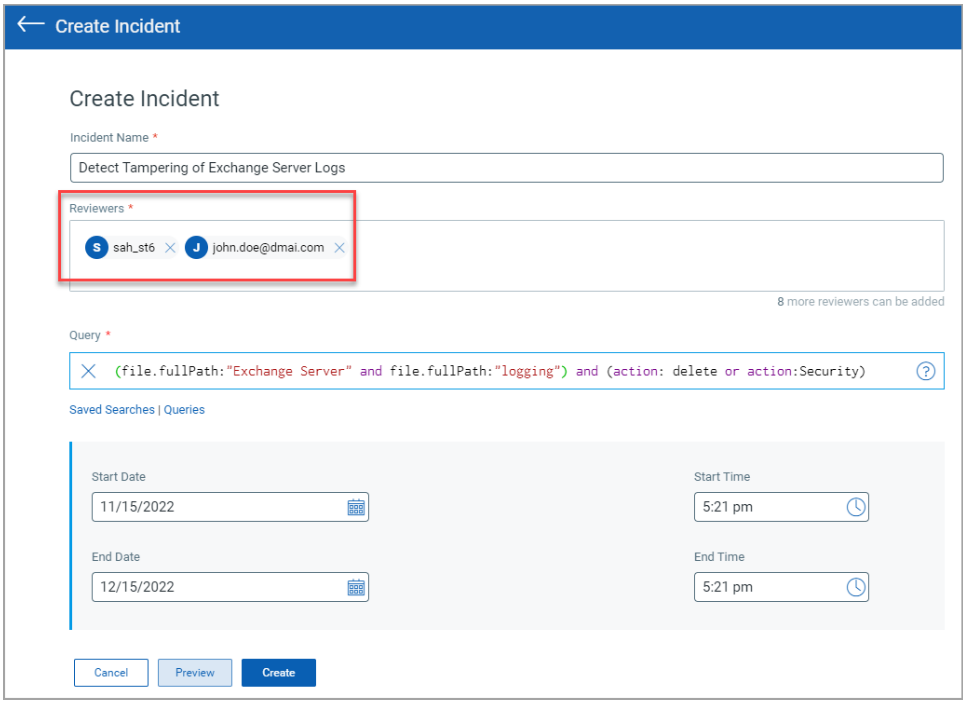


- Update Correlation Rule page



- Create Default/Manual Incident

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



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.