Qualys File Integrity Monitoring v2.x

Release Notes

Version 2.0
July 10, 2019

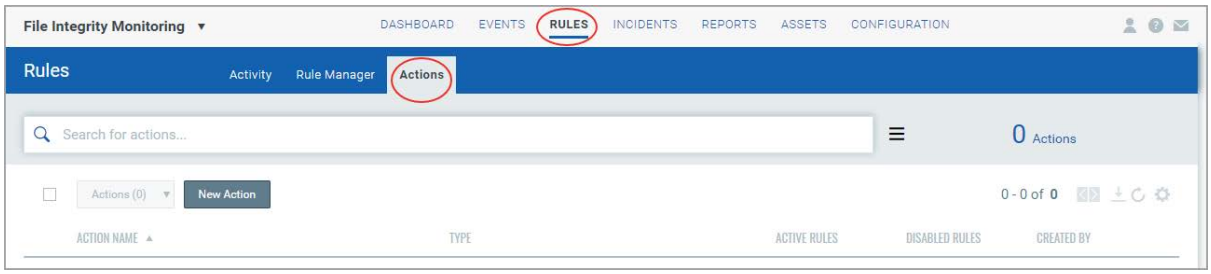
Here's what's new in Qualys FIM 2.0!

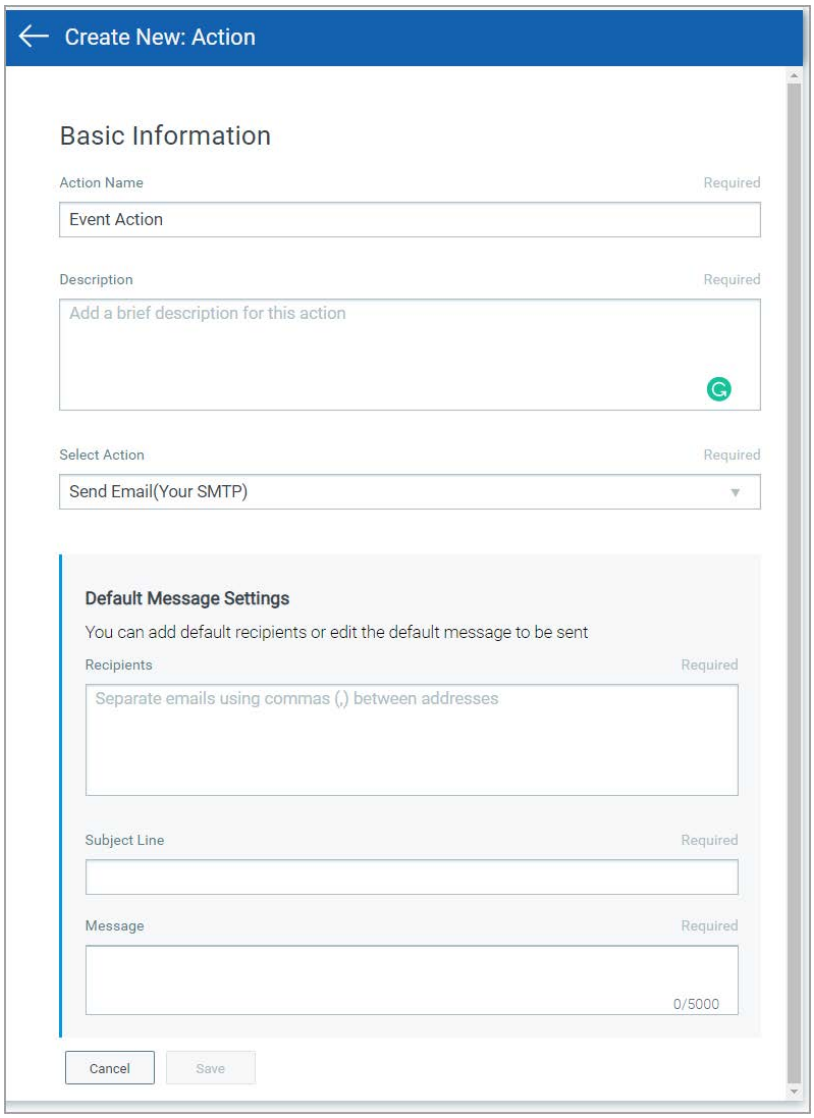
Configure Rule-Based Alerts for Events and Incidents

You can now configure FIM to monitor critical events/incidents based on the conditions specified in a rule and send you alert messages by a specified messaging system if events/incidents matching the condition is found. The alert message will have the events/incidents details. For FIM to send alerts, you need to first configure a rule action to specify what action to be taken when events matching a condition is detected. FIM will use the rule action settings to send you the alerts. Finally, create an alert rule to specify the conditions for triggering the rule and select rule actions that you have configured earlier for sending the alert message when a rule is triggered.

Create a New Action

Create a new action to define a mode of communication such as Email, PagerDuty or Post to Slack to be used for sending alert messages. To create an action, go to Rules > Actions > New Action.





Provide required details in the respective sections to create a new action:

- In the Basic Information section, provide name and description of the action in the Action name and Description fields respectively.

- Select an action from the Select Action drop-down and provide the settings for configuring the messaging system that FIM will use to send alerts.

- We support these three actions: Send Email (Via Qualys)/Send Email (Your SMTP),
Post to Slack and Send to Pager Duty for alerts.

a) Select “Send Email (Via Qualys)”/”Send Email (Your SMTP)” to receive email alerts. Specify the recipients’ email ID who will receive the alerts, subject of the alert message and the customized alert message. Note that based on the configuration settings you will see either of the two options.

b) Select “Send to PagerDuty” to send alerts to your PagerDuty account. Provide the service key that FIM will require to connect to your PagerDuty account. In Default Message Settings, specify the subject and the customized alert message.

c) Select “Post to Slack” to post alert messages to your Slack account. Provide the Webhook URI that FIM will use to connect to your slack account to post alert messages. In Default Message Settings, specify the subject of the alert message and the customized alert message.

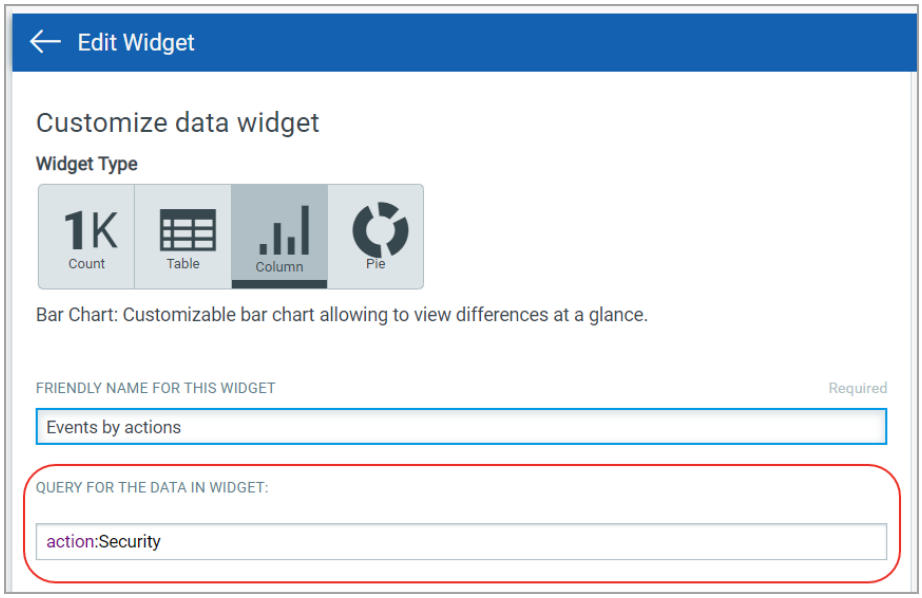
Create a New Alert Rule

You can create a new rule from the following pages:

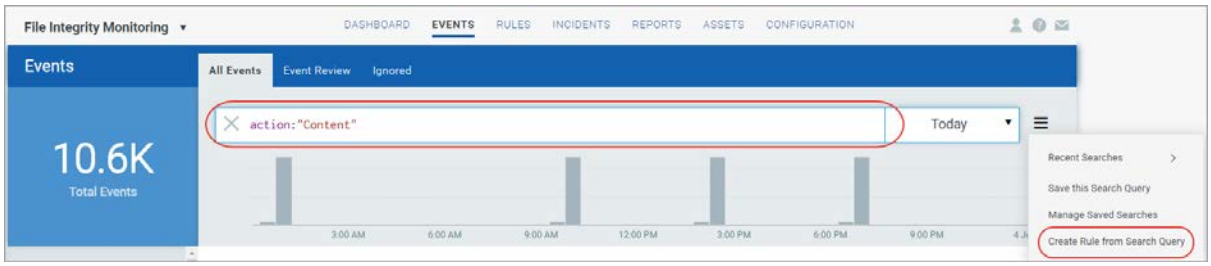
1) Go to Rules > Rule Manager and click New Rule.

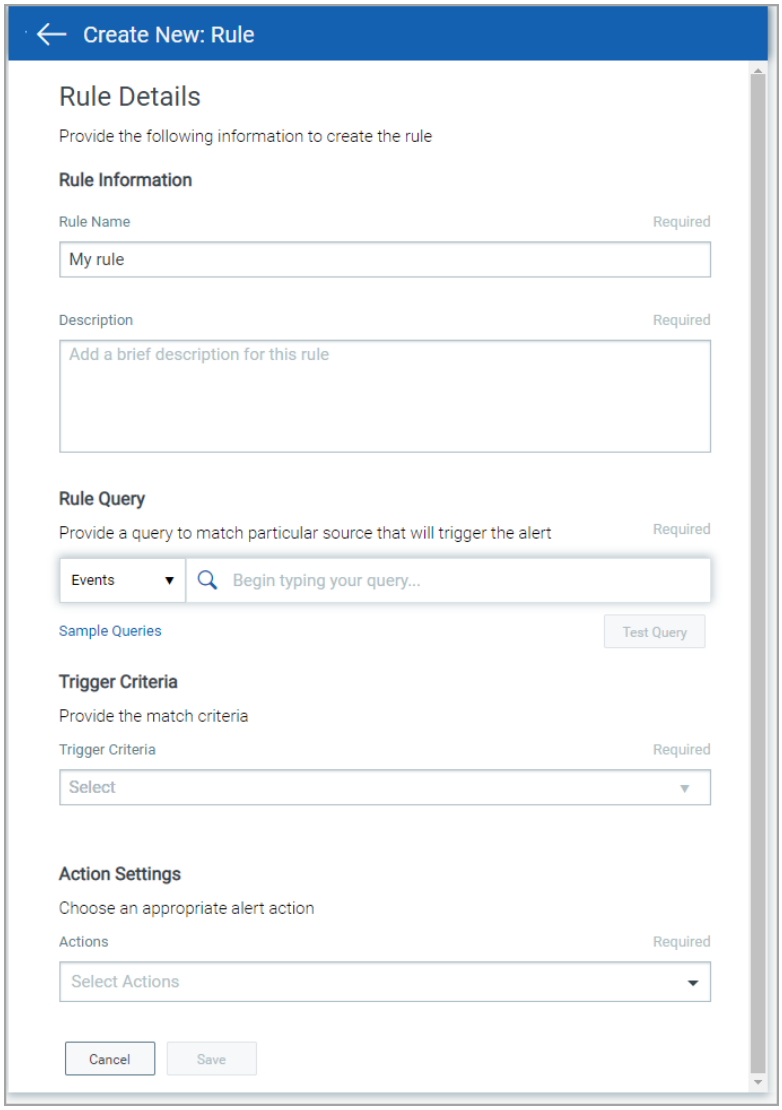
2) Go to the Dashboard tab and choose a widget that is using a customized query for fetching the widget data. Then select the Widget menu and choose “Create Rule from this Widget” to create alert rules based on the customized query that you used for creating the widget.

Note that a search query is required in the "Query for the data in the widget" field to create a rule from a widget.



3) Go to the Events > All Events tab. On the Events List page, enter a search query in the event search box. Then select “Create Rule from Search Query” from the Actions menu.





Provide required details in the respective sections to create a new rule:

- In the Rule Information section, provide a name and description of the new rule in the Rule Name and Description.

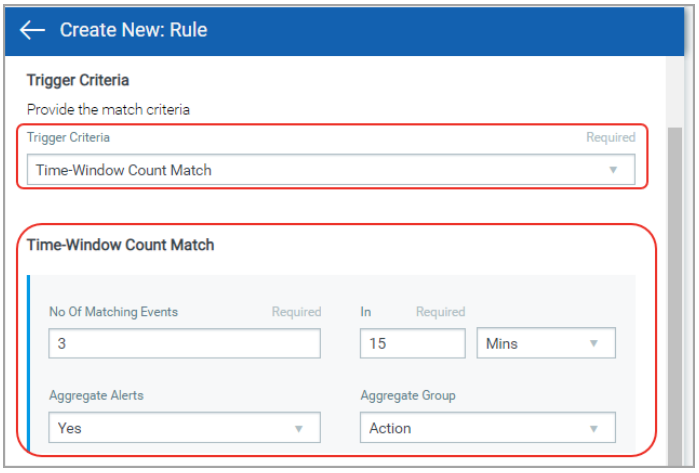
- In the Rule Query section, choose Events or Incidents and specify a query for the rule. The system uses this query to search for events/incidents. Use the Test Query button to test your query. Click the "Sample Queries" link to select from predefined queries.

- In the Trigger Criteria section, choose from 3 trigger criteria that work in conjunction with the rule query. The trigger criteria are: Single Match, Time-Window Count Match and Time-Window Scheduled Match. See Trigger Criteria.

- In the Action Settings section, choose the actions that you want the system to perform when an alert is triggered.

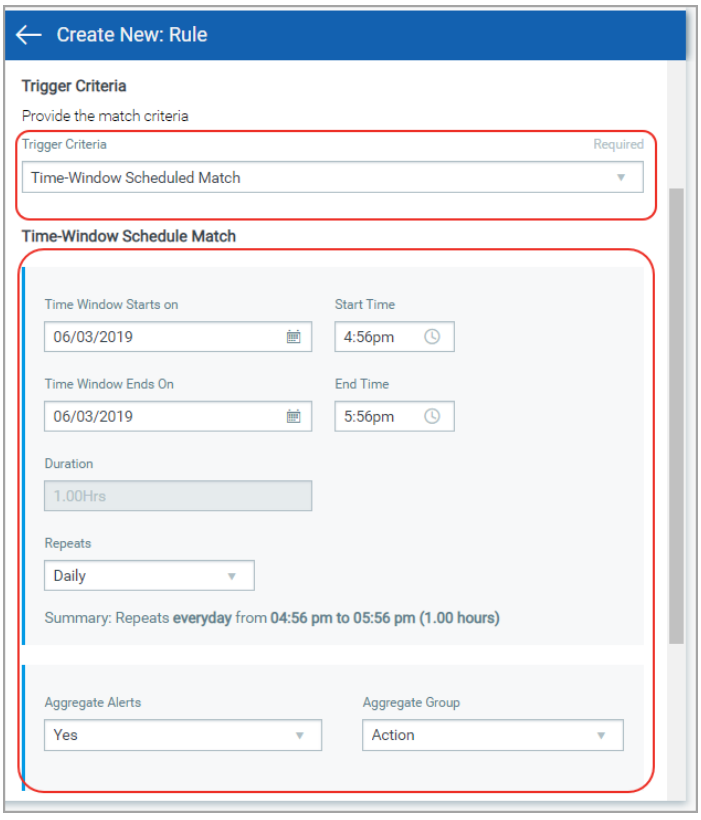
Trigger Criteria

- Select “Single Match” if you want the system to generate an alert each time the system detects an event/incident matching your search query.



- Select “Time-Window Count Match” when you want to generate alerts based on the number of events/incidents returned by the search query in a fixed time interval.

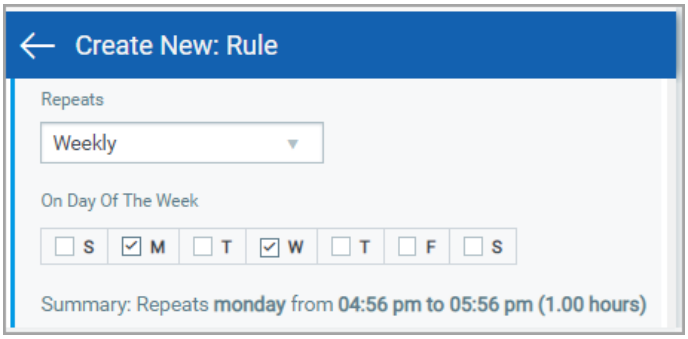
For example, an alert will be sent when three matching events are found within 15 minutes window.



- Select “Time-Window Scheduled Match” when you want to generate alerts for matching events or incidents found during a scheduled time. The rule will be triggered only when an event/incident matching your search criteria is found during the time specified in the schedule.

Choose a date and time range for creating a schedule and specify how often you want to run the schedule for example, daily, weekly and monthly.

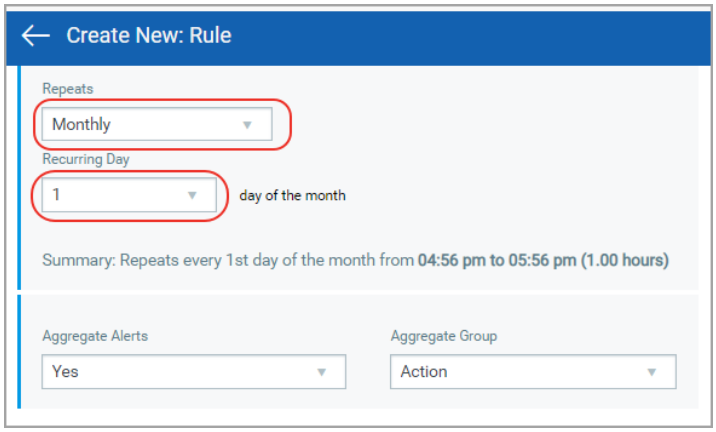
For example, send daily alerts with all matches in a scheduled window between 4.56 pm and 5.56 pm.



For the Weekly option, select the days of the week on which the rule will run.

For example, send weekly alerts with all matches generated between 4.56 pm and 5.56 pm every Monday and Wednesday.

For the Monthly option, specify the day of the month on which the the rule will run. For example, send monthly alerts on the first day of every month.



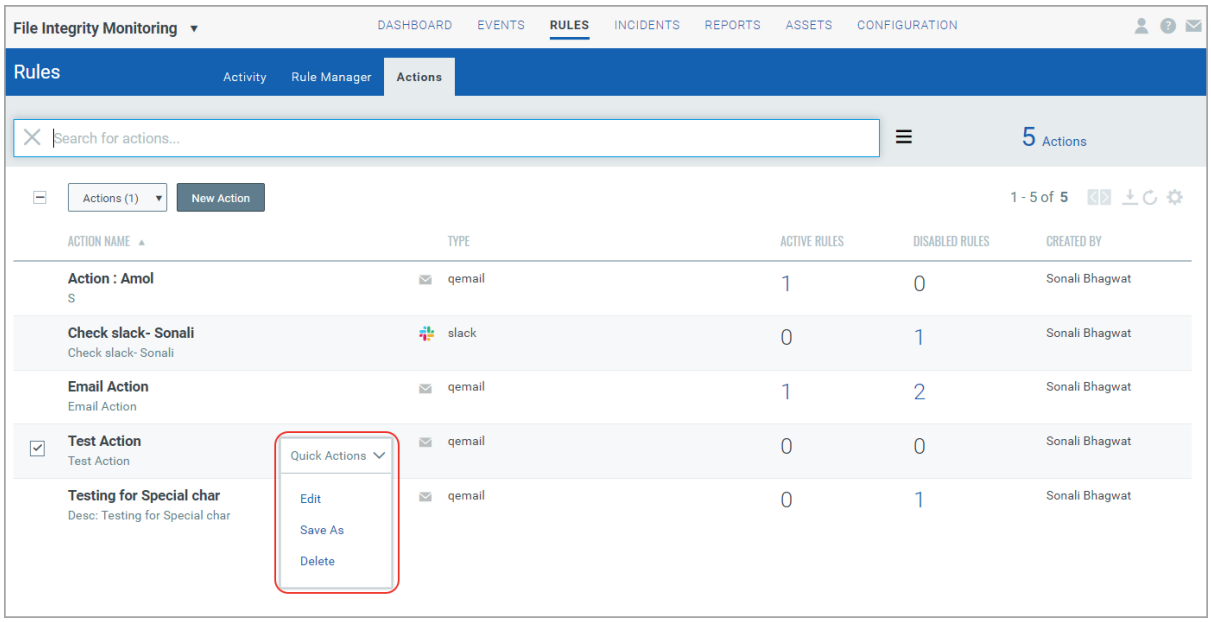
For “Time-Window Count Match” and “Time-Window Scheduled Match”, you have the option to aggregate the alerts by aggregate groups such as based on action, asset host name and so on.

When you choose an aggregate alert option as "Yes" for a rule, FIM combines all the alerts generated during a schedule under a selected aggregate group and when the schedule ends, FIM sends a single alert message that contains all the alerts. If you select aggregate alerts option as “No”, then FIM sends you an alert message for each alert generated between the start and end of a specified schedule.

Manage Actions

View the newly created actions in the Actions tab with the details such as name of the action, type of the action, the number of rules for which this action is chosen are active or inactive and the user who created the rule. You can use the Actions menu or Quick Actions menu to edit, delete actions and save an existing action along with its configuration to create a new action with a new name. Use the search bar to search for actions using the search tokens.

Note that you can delete an action only if it is not associated with any active or disabled rules.

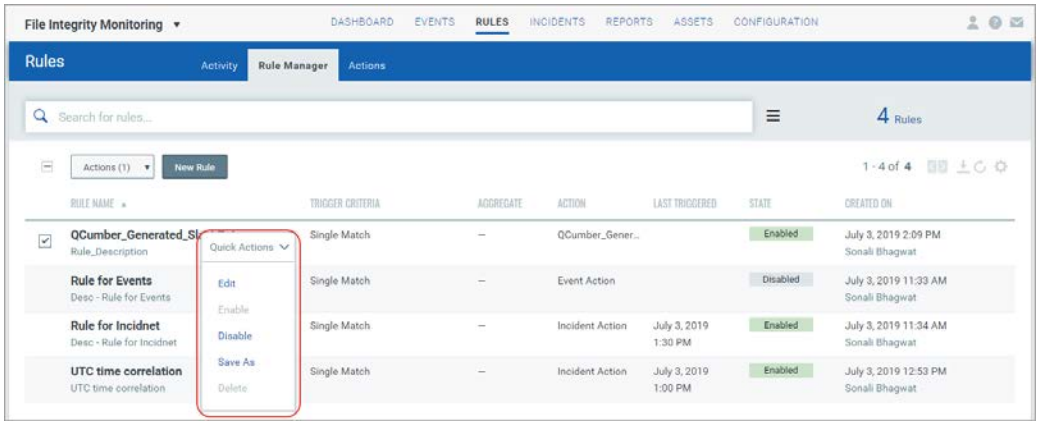


Manage Alert Rules

Rule Manager tab lists all the rules that you have created with rule name, trigger criteria selected for the rule, alert message aggregating enabled or disabled for the rule, action chosen for the rule, date and time when the rule is last triggered and state of the rule, whether the rule is enabled or disabled and created date and time of the rule.

You can use the Actions menu or Quick Actions menu to edit, enable, disable, delete rules and save an existing rule along with its configuration to create a new rule with a new name. Use the search bar to search for rules using the search tokens.

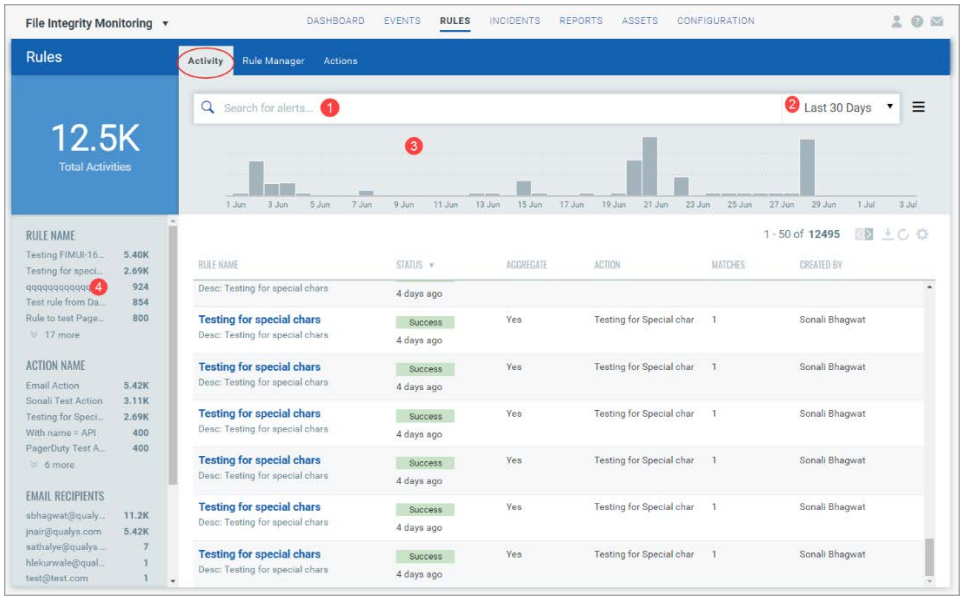
Note that Last Triggered value for a rule is shown after the rule is triggered.



Manage Alerts

Activity tab lists all the alerts. Here you will see for each alert, rule name, alert status to indicate whether sending of the alert is success, error or retrying (if the attempt to send the alert is not success), aggregate enabled (Yes) or aggregate disabled (No) for the rule, action chosen for the rule, matches found for the rule and the user who created the rule.

Search for alerts using our search tokens (1), select a period to view the rules triggered during that time frame (2), click any bar to jump to the alerts triggered in a certain timeframe (3), use these filters to group the alerts by rule name, action name, email recipients and status (4).



Configure Correlation Rules to Auto-Create Incidents

FIM can help you automate the creation of incidents based on certain criteria defined in a correlation rule. To help you create correlation rules, FIM provides a Correlation Rule wizard. In the wizard, define a query to specify for which events you want to create incidents and a schedule to indicate when and how often you want to run the rule to create incidents for the matching events.

On running a correlation rule, if no events matching the query are found then FIM still creates an incident to indicate that no events are generated during the specified time interval. The correlation rule wizard also provides you an option to create alerts for the incidents that are created for this rule. See "Create an alerting rule for incidents".

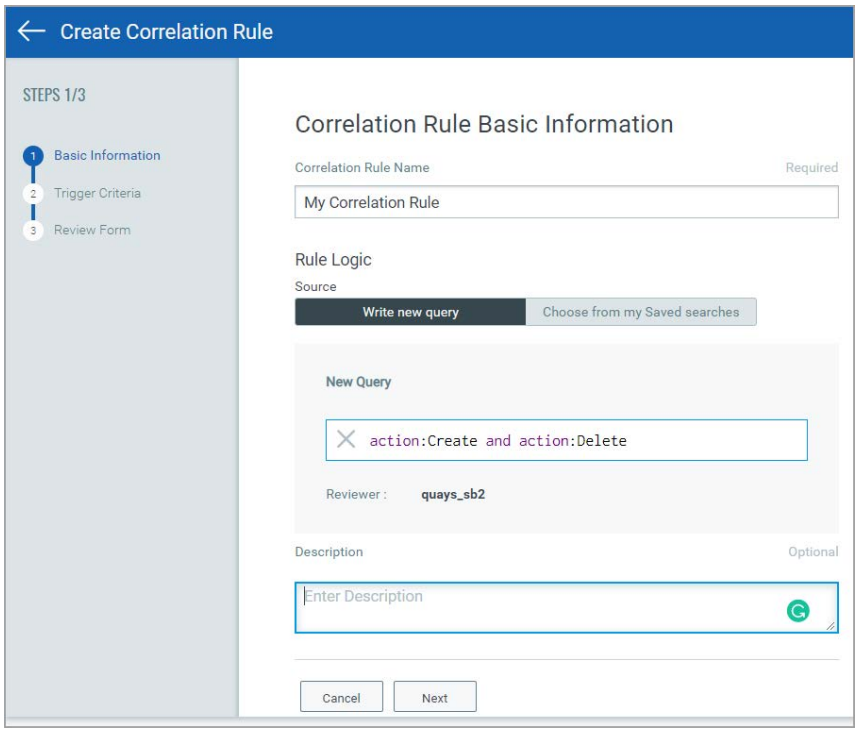
You can access the correlation wizard from the following pages:

1) Go to Incidents > Correlation Rules tab.

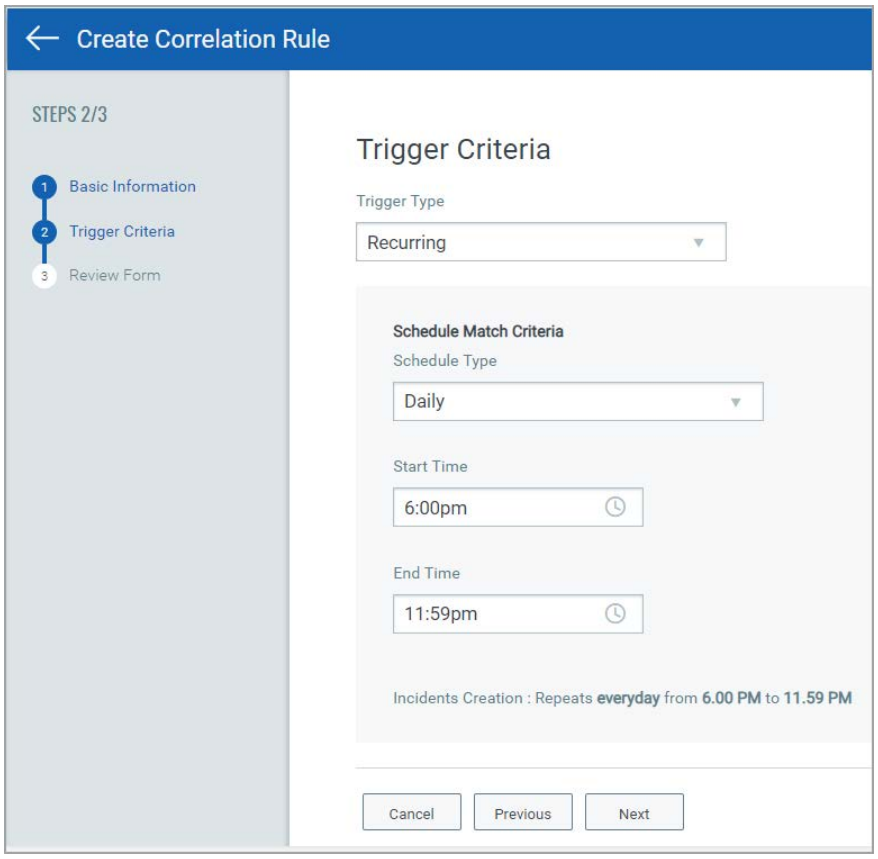
2) Go to Events > Event Review tab. Enter a search query in the search box and from the Actions menu select "Create Correlation Rule from Search Query". When you create a correlation rule from the Event Review page, the search query provided on the page is copied to the new correlation rule.

3) Go to the Assets tab, select an asset and from the Quick Actions menu select "Create Correlation Rule" to create a correlation rule for an asset. When you create a correlation rule for an asset, the agent ID of the asset is copied to the new correlation rule.
Use the operators "and/or" to customize your search query.

Create a Correlation Rule Using Correlation Rule Wizard



Provide the correlation rule name. Enter a search query to find events that you want FIM to add in the incidents. Optionally, use the Choose from my saved searches option to select a search query. Enter a description of the rule and click Next.



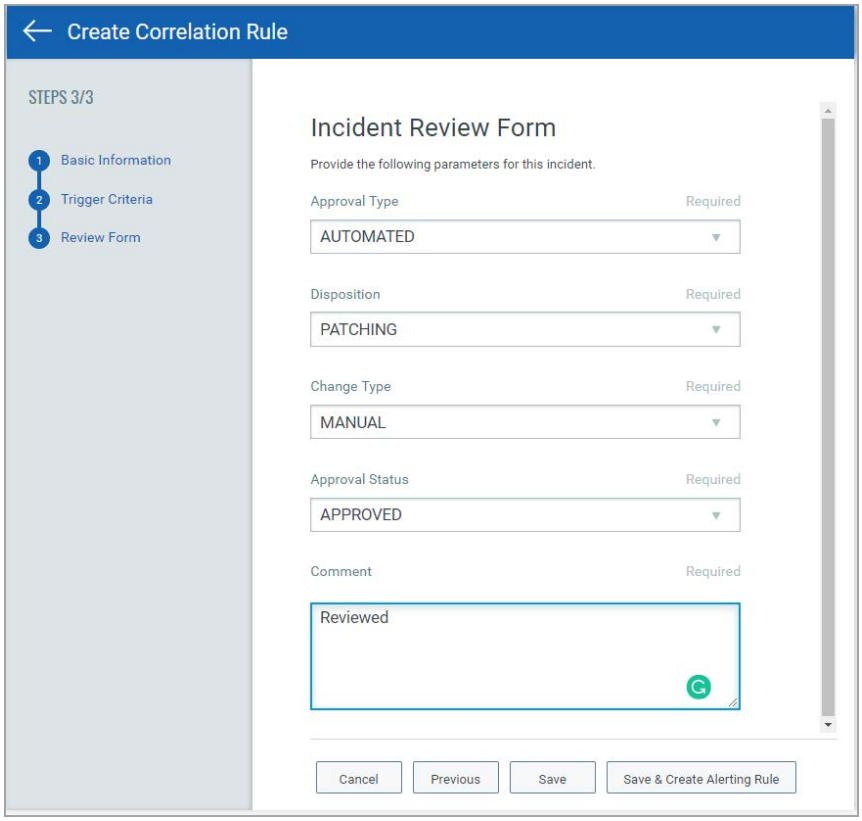
Next, select the trigger criteria for the rule. Select One Time or Recurring to indicate how often you want to run the rule. To run the rule only once select One Time as

Trigger Type and choose a date and a start and end time. Choose Recurring to schedule the rule to run daily between a specified time, every week on the chosen days between a specified time or every month on a chosen day between a specified time period.

FIM also supports cross date scheduling. Correlation can start at 10 pm on day 1 and end at 2 am on day 2 (effective schedule of 4 hours). If the end time is less than or equal to start time, the end time is considered as the time of next day. There is no end date for the schedule. User can deactivate or delete a correlation rule to stop creating incidents for the rule.

The scheduler runs every 5 minutes to pick up new jobs. Hence, it is recommended that while creating a schedule, you choose a "Start Time" greater than 10 minutes from the current time for a job to get picked up. If you choose a Start Time less than 10 minutes, it is possible that by the time you have created the rule, the scheduler has already picked up the job. In such a case your job will be picked up in the next scheduled cycle. This means One Time rule will never run as the time set for running the rule has already passed and if it is a Recurring rule, it will run at the next schedule.

When the correlation rule is run during the scheduled time, FIM will pick up all the events that are raised during the scheduled time and that match the search query provided in the rule. All these events are then added to the newly created incident. The naming convention used for incidents is correlation rule name followed by incident creation date and time. Note that you cannot change the Trigger criteria of a correlation rule in the edit mode.



Finally, select an approval type to indicate if you want to automate the review process for the incident or manually review the incident.

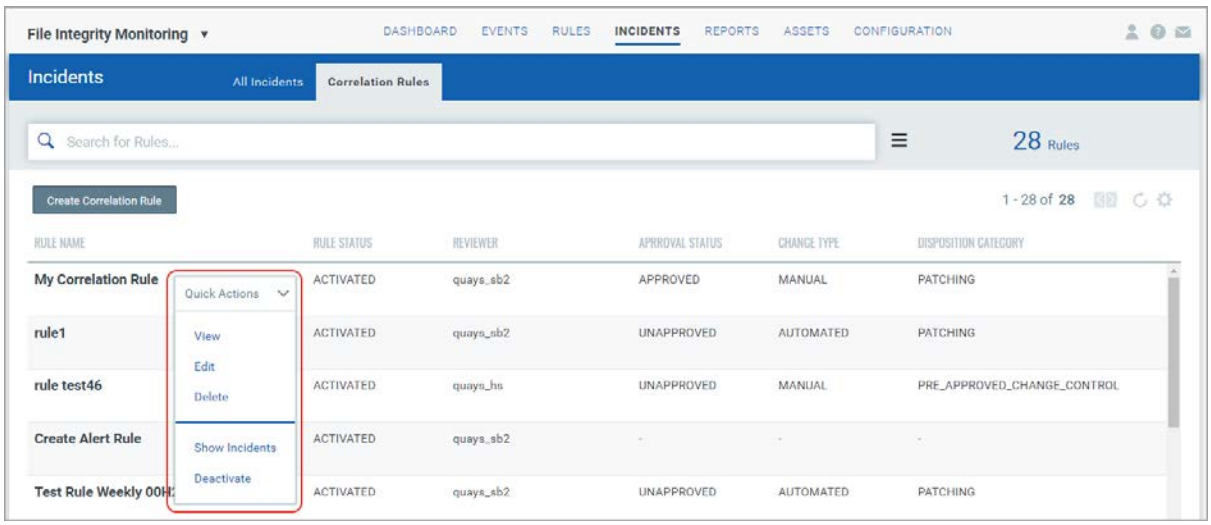
For Automated approval type, select a disposition category for reporting and classification, choose whether the incident resulted from a manual or automated change, mark the incident Approved, Unapproved Change or Policy Violation and provide a comment.

Click Save to create the correlation rule.

Manage Correlation Rules

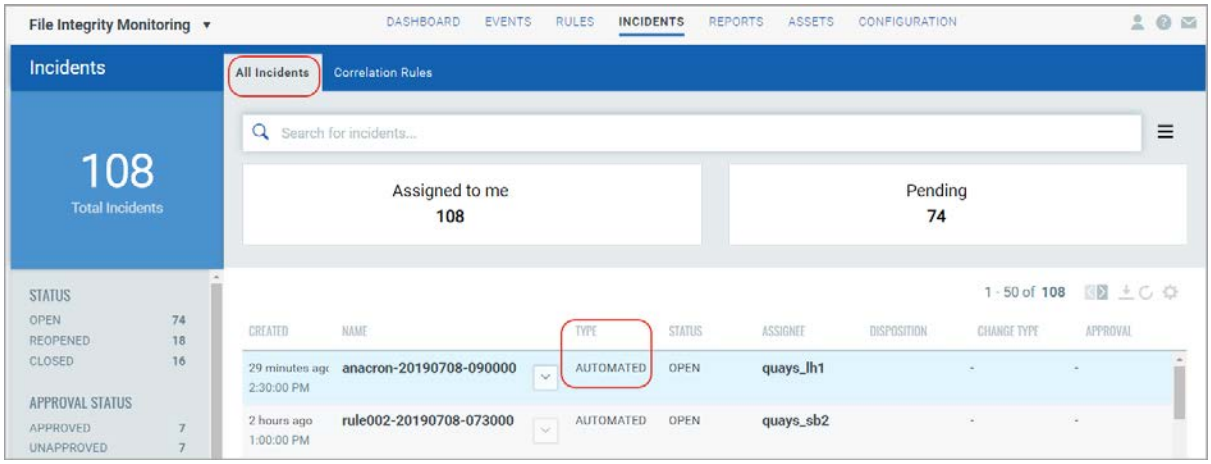
The Correlations Rules tab lists all the correlation rules. The page show details such as the name of the rule, whether the rule is currently active or deactivated, reviewer of the incident. The page also shows approval status, change type and disposition category values for approval type selected as Manual for incidents when creating/editing the rule. The Quick Actions menu on the page provides you options to view, edit, delete, activate/deactivate a rule and view the incidents of a rule.

Note that activate/deactivate option will be available for correlation rule that has a recurring schedule.

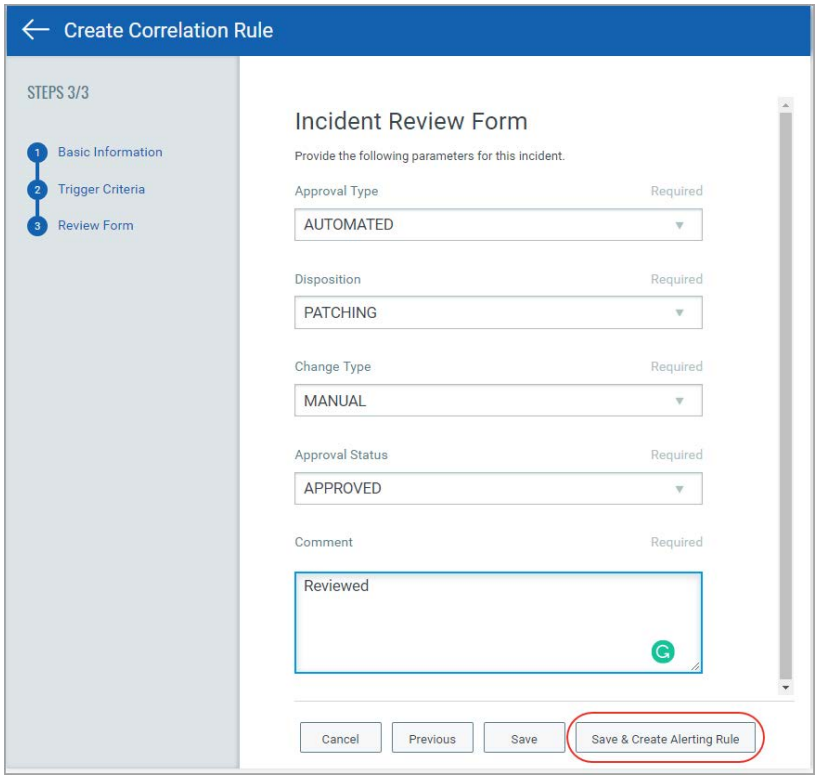


Manage Incidents

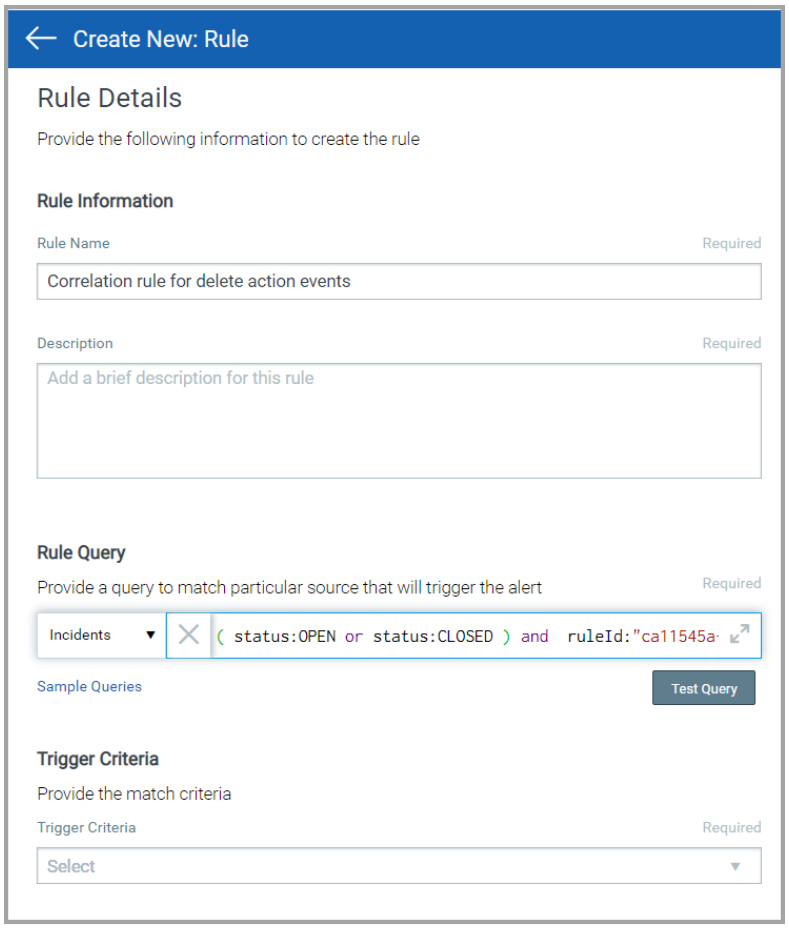
All the incidents generated for a correlation rule are listed in the All Incidents tab with type as "Automated". Note that you cannot delete an incident that is generated for a correlation rule.



Create an Alerting Rule for Incidents Generated for a Rule



While saving a correlation rule, the Correlation rule wizard gives you an option to create alerts for the incidents created for a correlation rule.



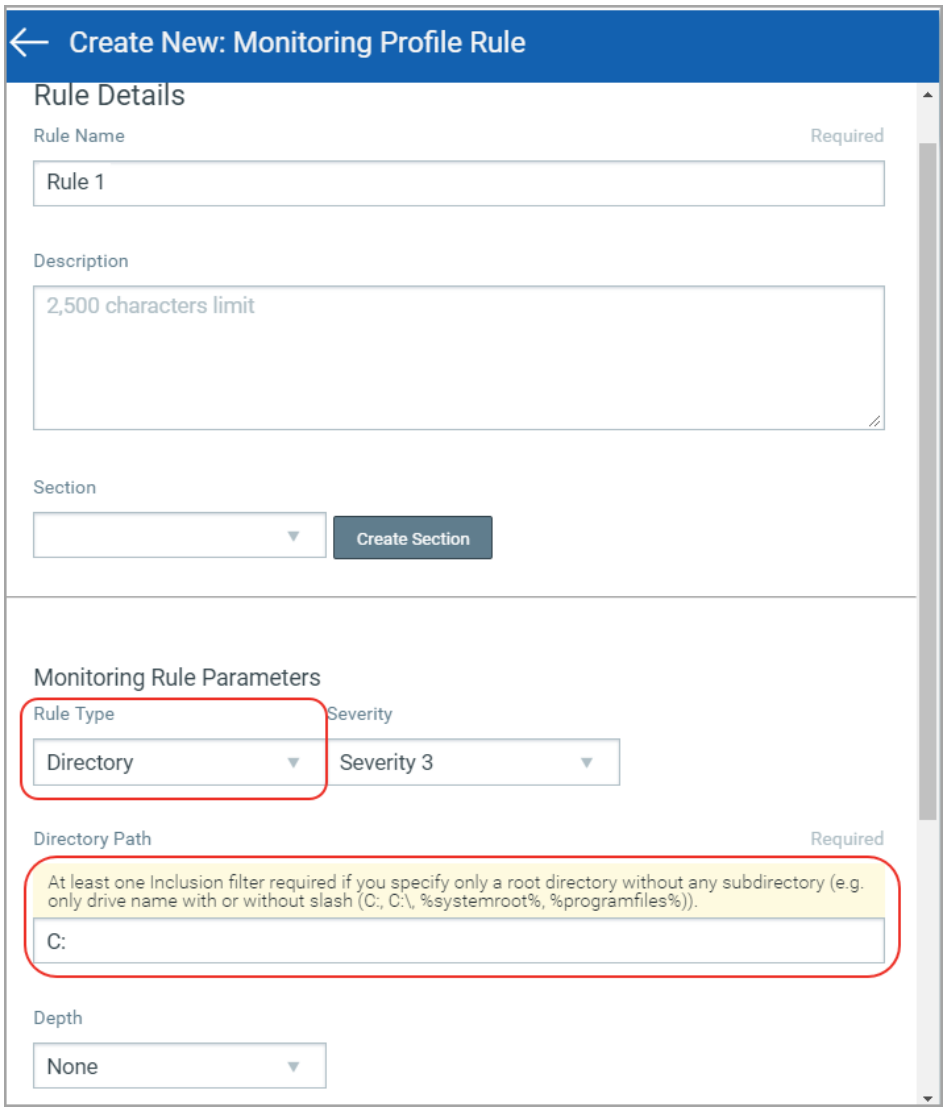
When you choose the option to create a rule, FIM opens the Alert Rule wizard to help you configure the alert rule. The new alert rule name and description will be the same as the correlation rule name and description from which the alert rule is created.
The search query for the alert rule will default to Incidents and a query is created with incident status open or closed and correlation rule ID.

Note that the option to create an alerting rule is available only when you create a new correlation rule.

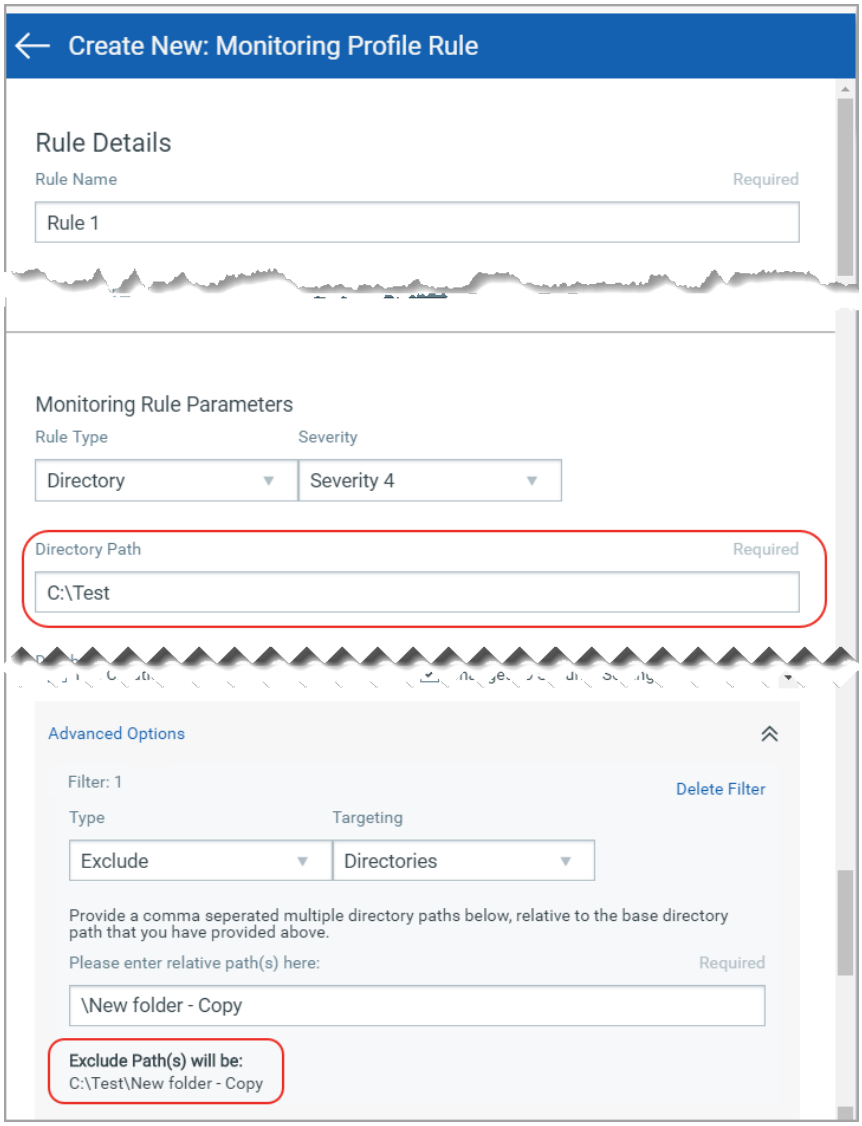
New Validations Added for Creating Directory Rules

Now while creating a new Monitoring Profile Rule, if you select "Directory" rule type and in the Directory path if you specify only a Windows root directory without any subdirectory (e.g. only drive names with or without slash (C:, D:, C:\, D:\, %systemroot%, %programfiles%) in Directory Path then you will be prompted to specify at least one Inclusion filter.

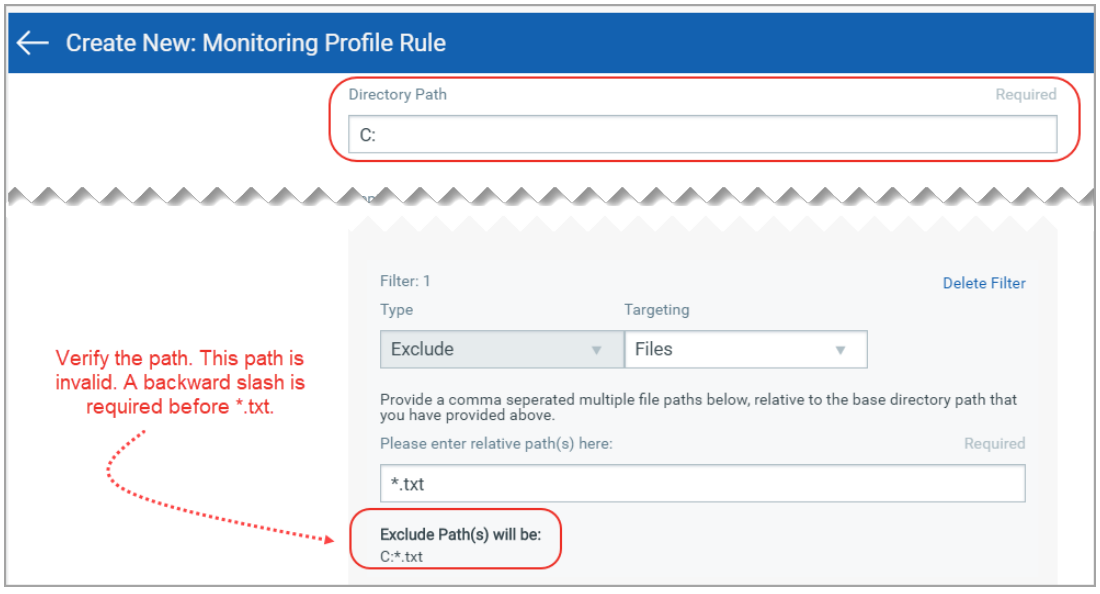
Similarly, if you specify only a Linux root directory without any subdirectory (e.g. /, /root, /var, /opt, /usr) then at least one Inclusion filter is required.



In Advance Options, now when you apply inclusion and exclusion filter to include/exclude files or directories, you need to enter a directory path relative to the base directory path mentioned in the Rule. UI now shows the base directory path while adding include/exclude path so that the user will be able to enter further relative path.



Verify that the path shown under the exclude/include filters is valid. The screen below shows an example of an invalid path.



Issues Addressed

- We fixed an issue where the include/exclude filters for a rule were not working to give the desired results. Now this issue is fixed. The user needs to enter a directory path relative to the base path mentioned in the Rule. UI now shows the base path while adding include/exclude path so that user will be able to enter further relative path.
- On the Assets Details page, we fixed an issue where the graph legends were overlapping the graph. Now the legends do not overlay on the graph but are displayed alongside the graph.
- We fixed an issue where FIM configuration profiles were not loading and Assets were not visible in the FIM asset tab. Now FIM configuration profiles and Assets in the Asset tab are visible.
- We fixed an issue where FIM was showing the status “No FIM Profile found” for an asset with an activated profile assigned to it. Now, FIM shows “Matching FIM profile found” status for assets with an activated profile.