



Qualys File Integrity Monitoring v1.x

Release Notes

Version 1.9

March 26, 2019

Here's what's new in Qualys FIM 1.9!

[Monitoring Profile Rule: New Validations for Inclusion/Exclusion Filters](#)

[Create Sections to Group Rules](#)

[Configure Rule Name and Other Details while Creating a New Rule](#)

[Enhancements to Events](#)

[Closed Incidents can now be Reopened](#)

[View Reports for Incidents](#)

[Enhancements to Assets View](#)

Monitoring Profile Rule: New Validations for Inclusion/Exclusion Filters

We have added new rule validations for specifying files/directories to include or exclude from monitoring under Advanced Options.

Validations for Windows directories

- Multiple full directory paths must be comma separated (e.g. C:\windows\system32\temp\, D:\windows\temp).
- These special characters [] { } () * ? ' are allowed in directory paths. ? is a single character wildcard, and * is a multi-character wildcard.
- These special characters / " < > | are not allowed in directory paths.
- Each Directory path can have maximum 260 characters including [] { } () * ? characters, spaces, and slashes.

Validations for Windows files

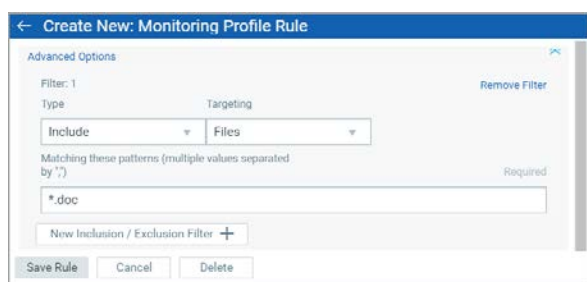
- Multiple file paths must be comma separated (e.g. *.doc, sample.txt).
- These special characters [] { } () * ? ' are allowed in file names. ? is a single character wildcard, and * is a multi-character wildcard.
- These special characters / " < > | are not allowed in file names.
- Each file name can have maximum 260 characters including spaces, and slashes.

Validations for Linux directories

- Multiple full directory paths must be comma separated (e.g. /user/tmp/demo, /user/tmp).
- These special characters [] { } () * ? ' are allowed in directory paths. ? is a single character wildcard, and * is a multi-character wildcard.
- These special characters \ " < > : | are not allowed in directory paths.
- Each Directory path can have maximum 4096 characters including [] { } () * ? characters, spaces, and slashes.

Validations for Linux files

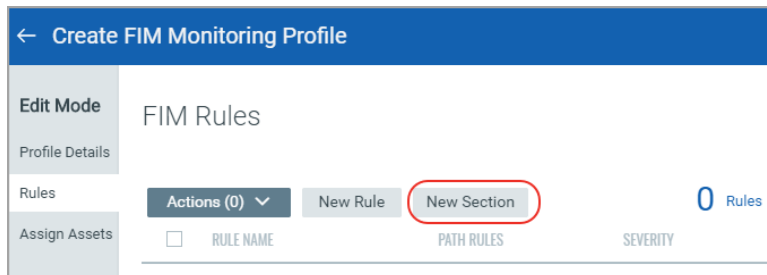
- Multiple file paths must be comma separated. (e.g. *.tmp, sample.tmp).
- These special characters [] { } () * ? ' are allowed in file names. ? is a single character wildcard, and * is a multi-character wildcard.
- These special characters \ " < > : | are not allowed in file names.
- Each file name can have maximum 255 characters including dot and extension.



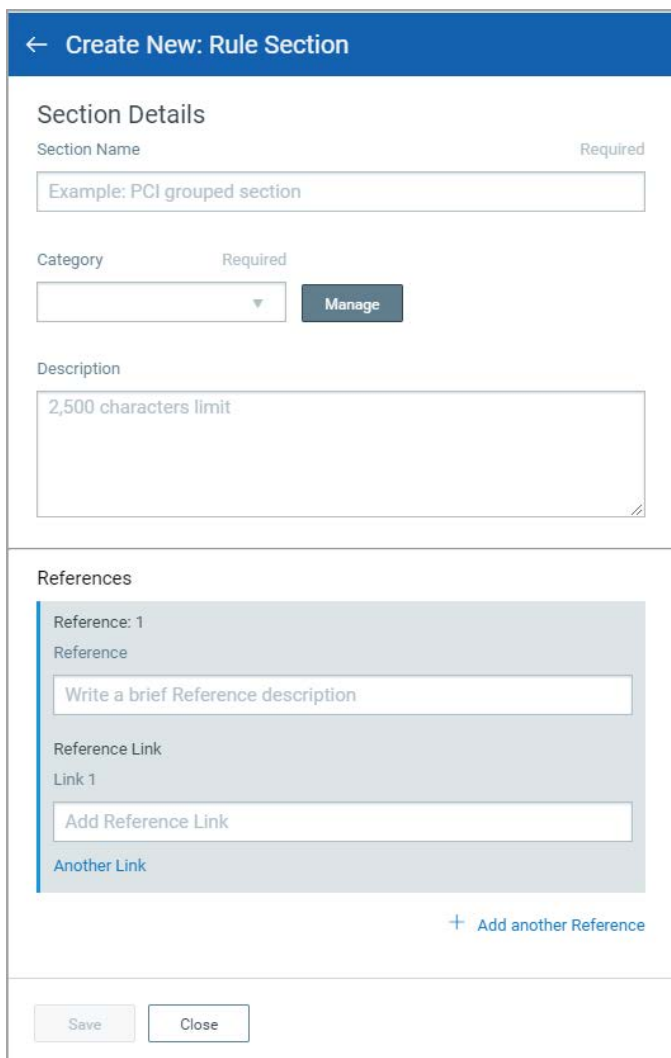
Create Sections to Group Rules

Now you can group rules in distinct categories using sections in a Windows/Linux profile. The section is available only in the profile in which it is created. A section once created cannot be deleted.

To create a new section, create/edit a profile, go to the Rules tab and click New Section.



The screenshot shows the 'Create FIM Monitoring Profile' interface. On the left is a sidebar with 'Edit Mode' selected. The main area is titled 'FIM Rules'. Below the title are buttons for 'Actions (0)', 'New Rule', and 'New Section' (which is circled in red). To the right of these buttons is a '0 Rules' indicator. Below the buttons is a table with columns for 'RULE NAME', 'PATH RULES', and 'SEVERITY'.



The screenshot shows the 'Create New: Rule Section' form. It has a 'Section Details' section with fields for 'Section Name' (with a 'Required' label), 'Category' (with a 'Required' label and a 'Manage' button), and 'Description' (with a '2,500 characters limit' label). Below this is a 'References' section with a table for adding references. The table has columns for 'Reference' and 'Reference Link'. The first row is labeled 'Reference: 1'. The 'Reference' column has a text input field with the placeholder 'Write a brief Reference description'. The 'Reference Link' column has a text input field with the placeholder 'Add Reference Link'. Below the table is a '+ Add another Reference' button. At the bottom of the form are 'Save' and 'Close' buttons.

Enter/select section name, description and category. Specify one or more references and reference links.

References provide information on grouping criteria of rules and links contain URLs to provide additional information. We are showing this information on the Event Details page.

Section category contains user-defined values. You can use the Manage button to add/ remove section categories.

Click Save.

← Create New: Monitoring Profile Rule

Rule Details

Rule Name Required

Example: System files rule

Description

2,500 characters limit

Section


▼ Create Section

Monitoring Rule Parameters

File ▼ ity 3

To add a rule to the section, select the section while creating or editing a rule.

Here you can also use the Create Section button to create a new section for the rule.

Click  icon to expand a section to show or hide the rules added to the section. The rules that are not part of any section are shown under Open rules.

← Edit FIM Monitoring Profile

Edit Mode

Profile Details

Rules

Assign Assets

FIM Rules

Actions (1) New Rule New Section 2 Rules

<input type="checkbox"/>	RULE NAME	PATH RULES	SEVERITY
<input checked="" type="checkbox"/>	Section Testing FIMUI-1474 Jan 23, 2019 by Sonali Bhagwat 1 Rule	▼	
<input checked="" type="checkbox"/>	Testing FIMUI-1474 1	C:\Test File: rename, modifyContent, delete, modifyMetadata, create, modifySecuritySettings Directory: rename, modifyMetadata, delete, modifySecuritySettings, create Additional filters: Exclude Directory: \Device\HarddiskVolume2\Test\New fo... 4 more...	■ ■ ■ ■
<input checked="" type="checkbox"/>	Open Rules		
<input checked="" type="checkbox"/>	Rule 2	C:\system.txt rename, delete	■ ■ ■ ■

← Edit FIM Monitoring Profile

Edit Mode

Profile Details

Rules

Assign Assets

FIM Rules

Actions (1) New Rule New Section

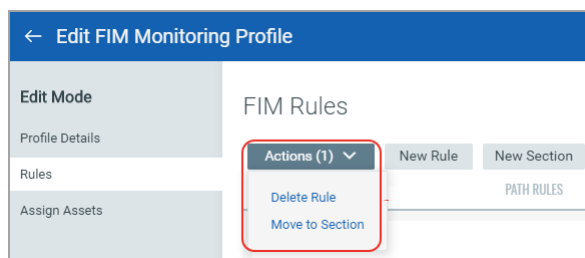
<input type="checkbox"/>	RULE NAME	PATH RULES
<input checked="" type="checkbox"/>	Section #2 Jan 25, 2019 by Sonali Bhagwat 1 Rule	▼
<input checked="" type="checkbox"/>	System 32 dir 1	C:\system32 File: rename, modifyContent, delete, modifyMetadata, create, modifySecuritySettings Directory: rename, modifyMetadata, delete, modifySecuritySettings, create Additional filters: Exclude Directory: \Device\HarddiskVolume2\New fo... 4 more...

Quick Actions ▼

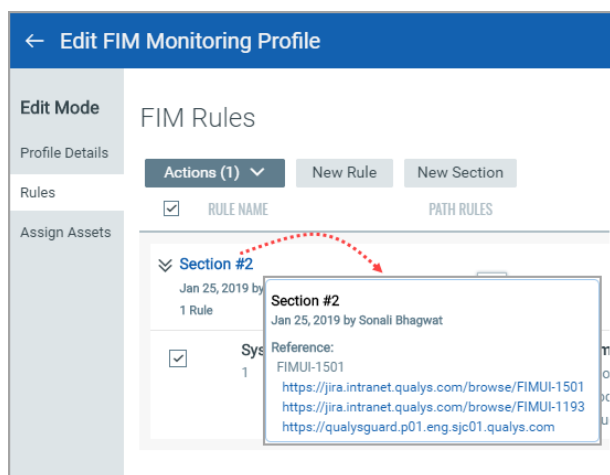
Delete

Delete option deletes the rules in the section.

We have provided an Actions menu to help you delete multiple selected rules using the Delete Rule option. You can not delete all the rules in an active profile. At least one rule must be present in the profile or else an error message is shown if you try to delete the rule.

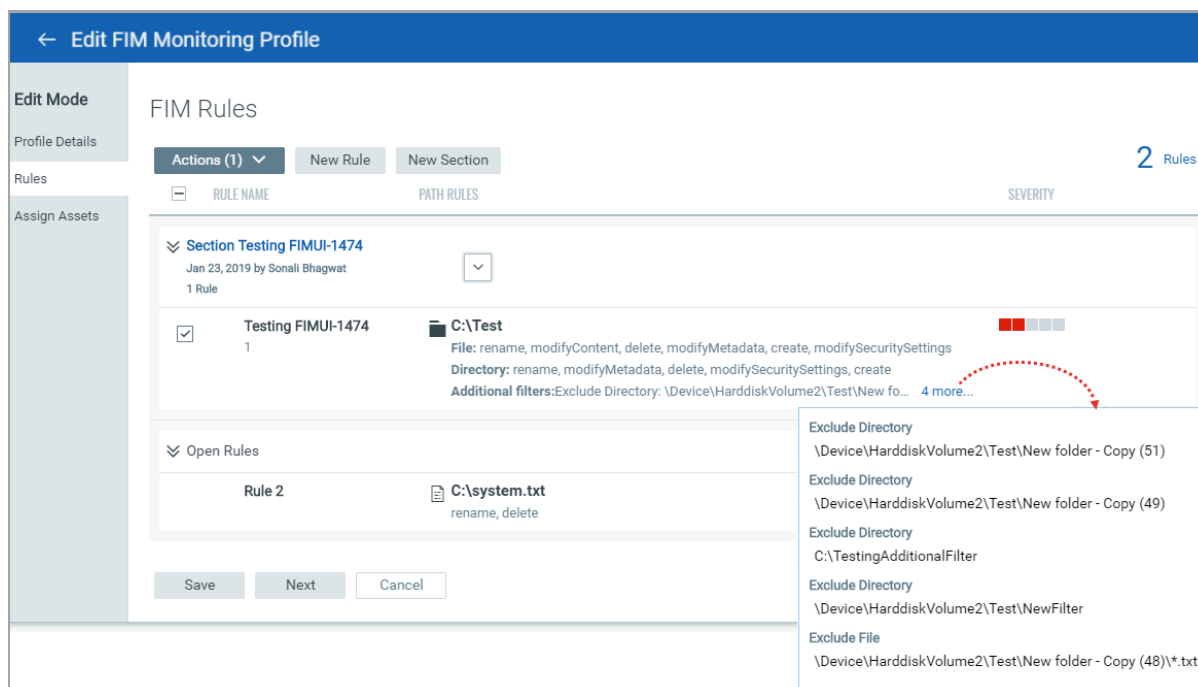


Move to Section lets you move the rule to another section.



Click the section name to view the references for the section.

Click “more” to view all the exclude or include filters applied on the rule.



Configure Rule Name and Other Details while Creating a New Rule

While creating a new monitoring profile rule, you can now specify rule name, description and group the rule under a section or create a new section for the rule.

Create New: Monitoring Profile Rule

Rule Details

Name Required
Directory Rule

Description
Directory Rule

Section
Directory Rule Section Create Section

Monitoring Rule Parameters

Rule Type Severity
Directory Severity 5

Directory Path Required
C:\Windows\System32

Depth
All

Monitor the directory structure for: ☒ All

☒ Directory Name Changes ☒ Changes to Attributes

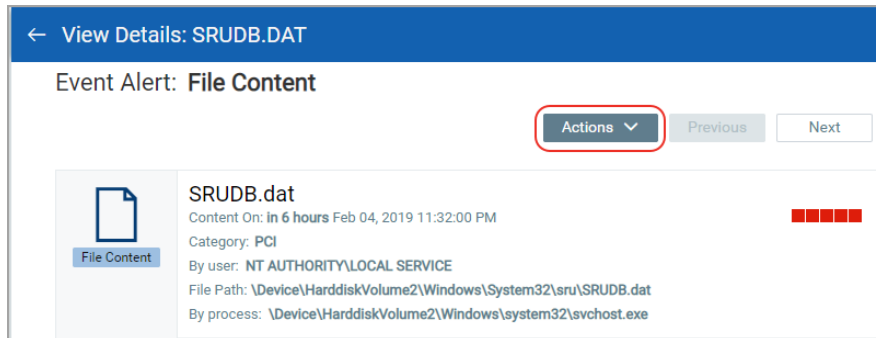
Save Rule Cancel Delete

Enhancements to Events

Actions Menu Moved to Event Details

We have moved the Actions Menu button, which contains Ignore Event option, from the Event List page to the Event Details page. The Event Details page show Ignore option only for events that are not added to any incident.

Go to the Event Review tab to ignore multiple events. The Event Review tab shows only events that are not included in an incident.

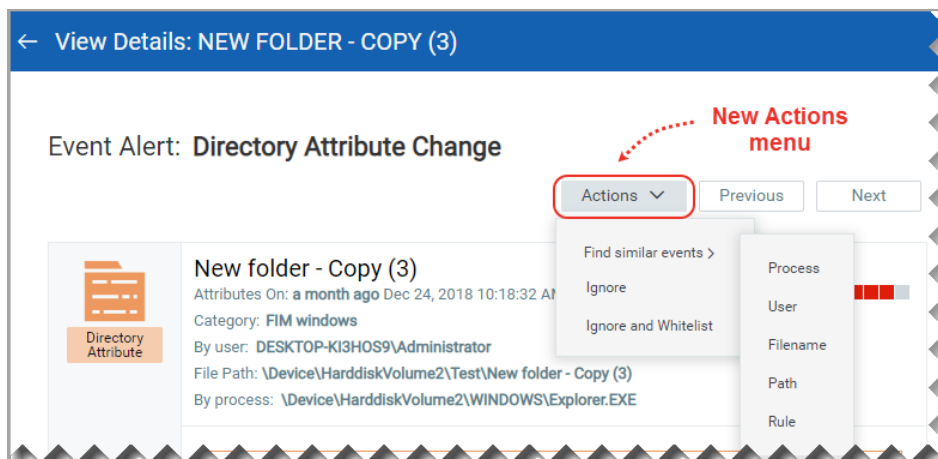



Enhancements to Event Details

The information on the Event Details page is now more organized and detailed.

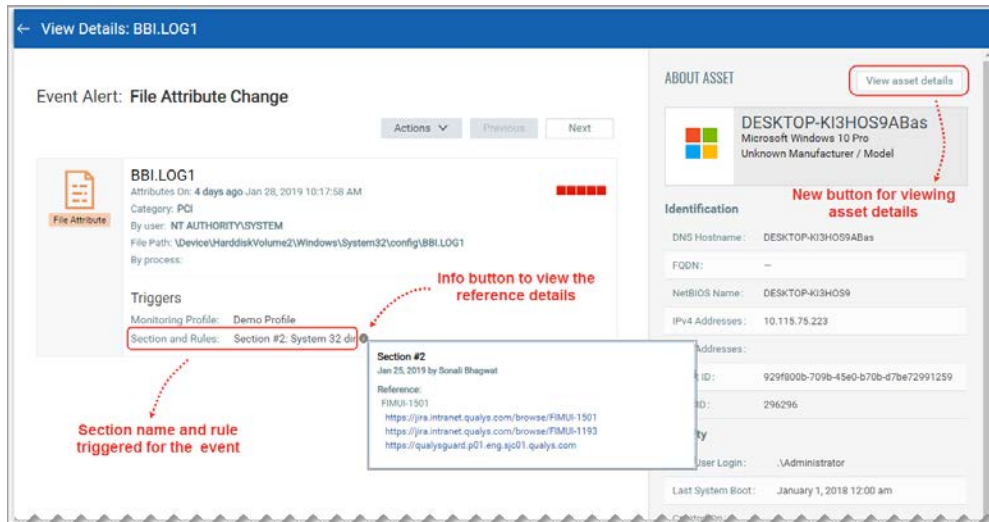
The Event details page now has Actions menu to search similar events, ignore an event and ignore and whitelist an event.

Find Similar Events allows you to search for events that are generated by the same process, user or for the same filename, file path or rule. Ignore only ignores the selected event. Ignore and Whitelist ignores the selected event and lets you apply on the triggered rules new exclude filters for target directories.

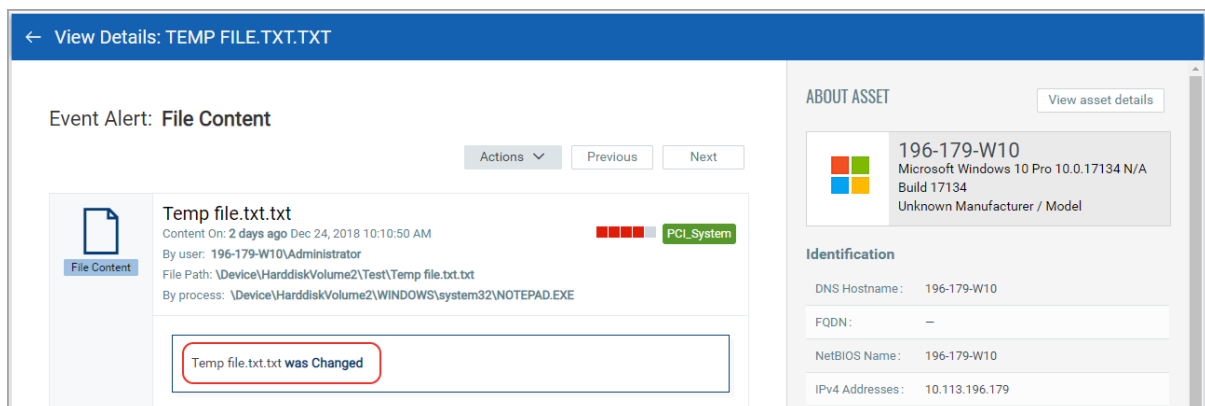


Triggers section now shows the section name, if rules are grouped in a section, and rule names that triggered the event. Click the info button  to view details of references, if added for the section.

Asset information on the right side is restructured to show DNS hostname, FQDN, IP address and other details of the asset. This detail is earlier available when you click on the host name. This section is renamed to About Asset and shows a View asset details button for viewing details of the asset.

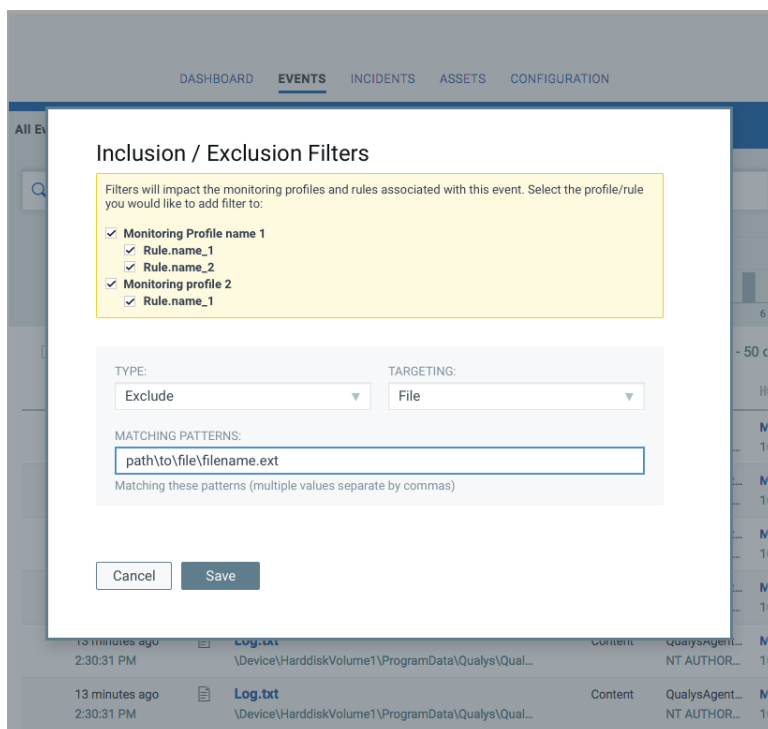
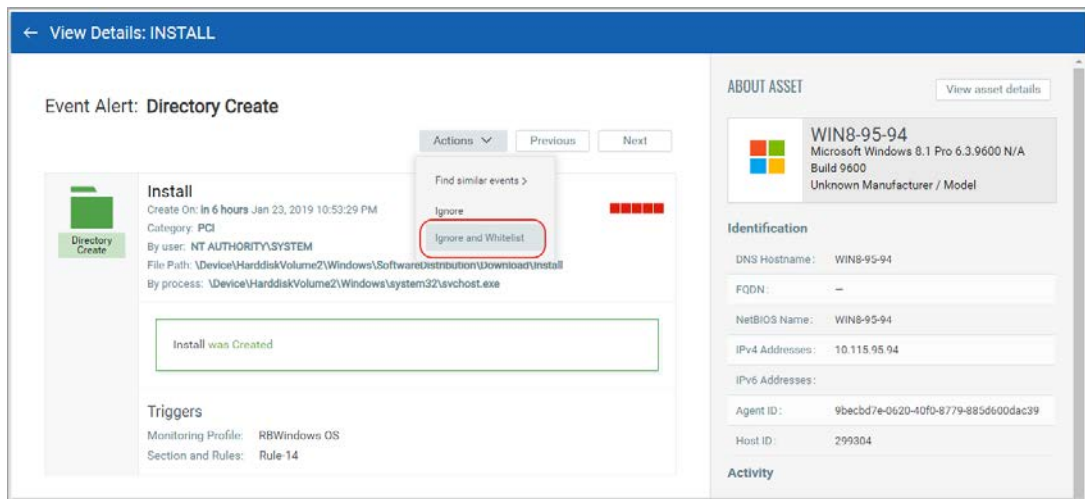


Now Permissions, Inheritance, Ownership and Audit details are visible only in the Security change event and Attribute in the Attribute change event. For the events generated for the content change, we only display the file name for which content has changed.



Ignore Events and Apply Exclusion Filters for the Triggering Rules

You can now ignore an event and at the same time modify the rule or rules that triggered the event. Identify the event and then drill down the event to go to the Event details page. From the Actions menu, choose "Ignore and Whitelist". Note that this option is unavailable for events that were generated from locked monitoring profile and for rules created for rule type as File.



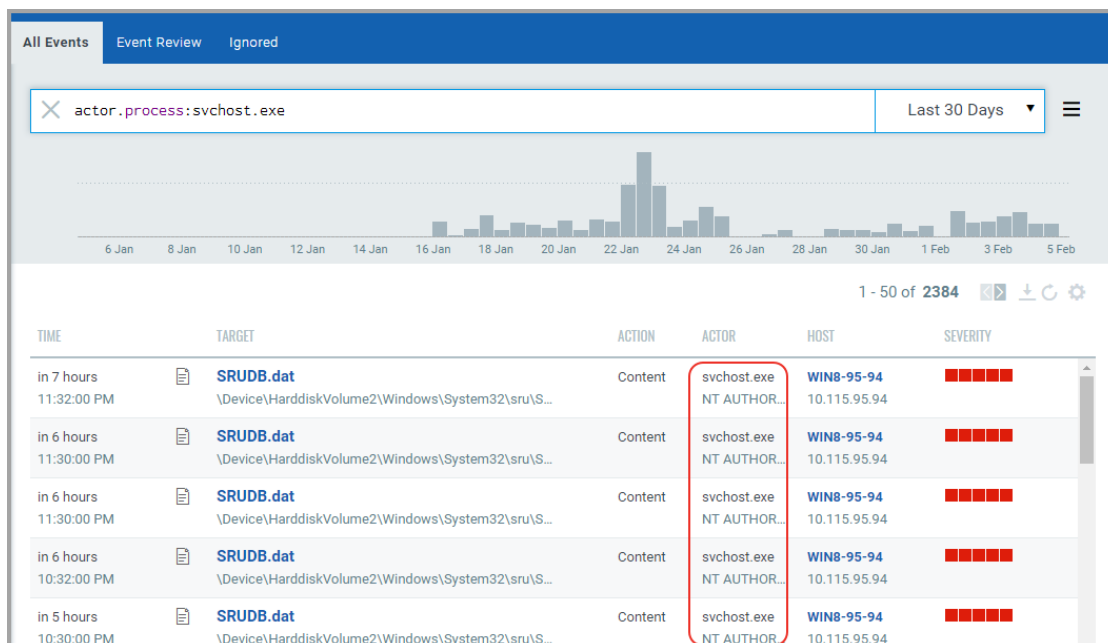
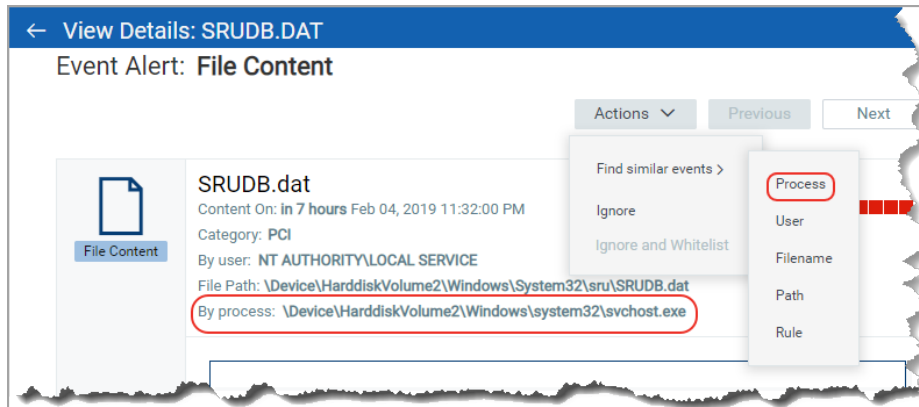
You'll see a list of profiles/rules associated with the event and a new exclude filter for the target directory or file. Feel free to make changes to the exclude filter before saving it.

Once you hit Save, we'll add the exclude filter to the selected profile rules. The event will be moved to the Ignored list and new events will not be generated for the excluded directory/file.

Find Similar Events

You can now search for events that are generated by the same process, user or for the same filename, file path or rule. Drill Down an event and on the Event details page, click the Actions menu on the top. Select Find similar events and then choose a filter to view events that matches the value of the filter for the selected event.

For example, choose the Process filter to view all the events that are generated by the same process as the current event.



Closed Incidents can now be Reopened

You now have an option to reopen a closed incident to modify the incident's review information. When you reopen an incident, all the review information in the incident such as disposition, change type, approval and other information is set to blank. You can then review the reopened incident, provide review comments and mark it Closed.

To reopen an incident, click Reopen from the Quick Actions menu.

The screenshot shows the Qualys Express interface with the 'INCIDENTS' tab selected. A search bar at the top shows 'status:CLOSED'. Below the search bar, there are two summary boxes: 'Assigned to me' with a count of 2, and 'Pending' with a count of 0. A table of incidents is displayed below, with columns: CREATED, NAME, STATUS, ASSIGNEE, DISPOSITION, CHANGE TYPE, and APPROVAL. The first incident is dated Oct 15, 2018, with status 'CLOSED', assigned to 'quays_sb2', and disposition 'CHANGE_CONT...'. The second incident is dated Sep 24, 2018, with status 'CLOSED', assigned to 'quays_sb2', and disposition 'PATCHING'. A 'Quick Actions' menu is open for the first incident, showing options: 'View Details', 'Reopen' (highlighted with a red circle), and 'Generate Report'.

Enter the comments and click Yes.

The screenshot shows the Qualys Express interface with the 'INCIDENTS' tab selected. A 'Reopen Incident' dialog box is open in the foreground. The dialog box has a title 'Reopen Incident' and a 'Comment' field with the text 'To review comments'. Below the comment field, there is a question 'Are you sure you want to reopen this incident?' with 'Yes' and 'No' buttons. The background shows the 'Incidents' page with a sidebar on the left displaying statistics: 42 Total Incidents, STATUS (OPEN: 24, REOPENED: 16, CLOSED: 2), APPROVAL STATUS (POLICY_VIOLATL: 1, UNAPPROVED: 1, NA: 1), CHANGE TYPE (AUTOMATED: 1, MANUAL: 1, OTHER: 1), and DISPOSITION (CHANGE_CONTR: 2, PRE_APPROVED: 1). The main table shows incidents with columns: profile.category, REOPENED, quays_sb2, and CHANGE_CONT...

View Reports for Incidents

You can now generate reports for incidents. Downloaded Report has three sections: Report Settings, Report Statistics and Report Event Details. Report Settings shows incident details. Report Statistics shows graphical data for counts of changes by action, user, and type and counts of events by severity levels and assets. Report Event Details shows the list of events in the incident.

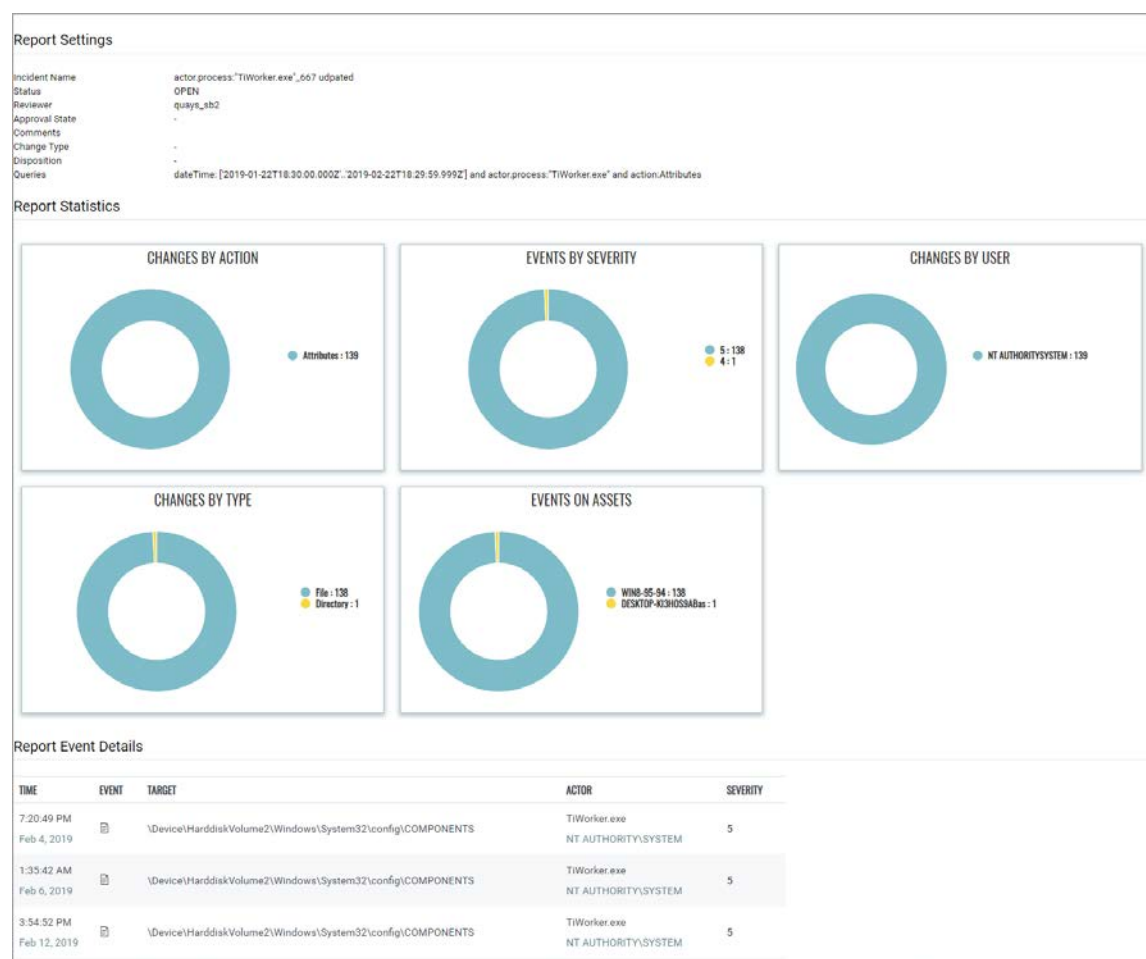
Select an incident and click Generate Report from the Quick Actions menu. Select PDF/HTML format and click Download on the Download formats screen.

The screenshot shows the 'Incidents' page in the File Integrity Monitoring interface. The top navigation bar includes 'DASHBOARD', 'EVENTS', 'INCIDENTS' (selected), 'ASSETS', 'CONFIGURATION', and 'REPORTS'. The left sidebar shows 'Incidents' with a count of 36 Total Incidents. The main area displays a table of incidents with columns: CREATED, NAME, STATUS, ASSIGNED, DISPOSITION, CHANGE TYPE, and APPROVAL. A 'Quick Actions' menu is open for the first incident, showing options: View Details, Edit, Start Review, Generate Report (highlighted with a red circle), and Delete. The incident details shown are: 3 days ago, 5:03:51 PM, QCumber-Generated Incident, REOPENED, quays_sb2.

The report is created for the incident and placed in the Reports tab. Go to the Reports tab and download the report.

The screenshot shows the 'Reports' page in the File Integrity Monitoring interface. The top navigation bar includes 'DASHBOARD', 'EVENTS', 'INCIDENTS', 'ASSETS', 'CONFIGURATION', and 'REPORTS' (selected). The left sidebar shows 'Reports' with a count of 29 Reports. The main area displays a table of reports with columns: CREATED DATE, REPORT TITLE, FORMAT, and STATUS. A 'Quick Actions' menu is open for the second report, showing options: Download (highlighted with a red circle), Delete, and Run Again. The report details shown are: 7 days ago, 4:02:53 PM, QCumber-Generated_Incident_12202018_095517, html, Completed.


Here is a sample Incident Report in the HTML format.




Enhancements to Assets View

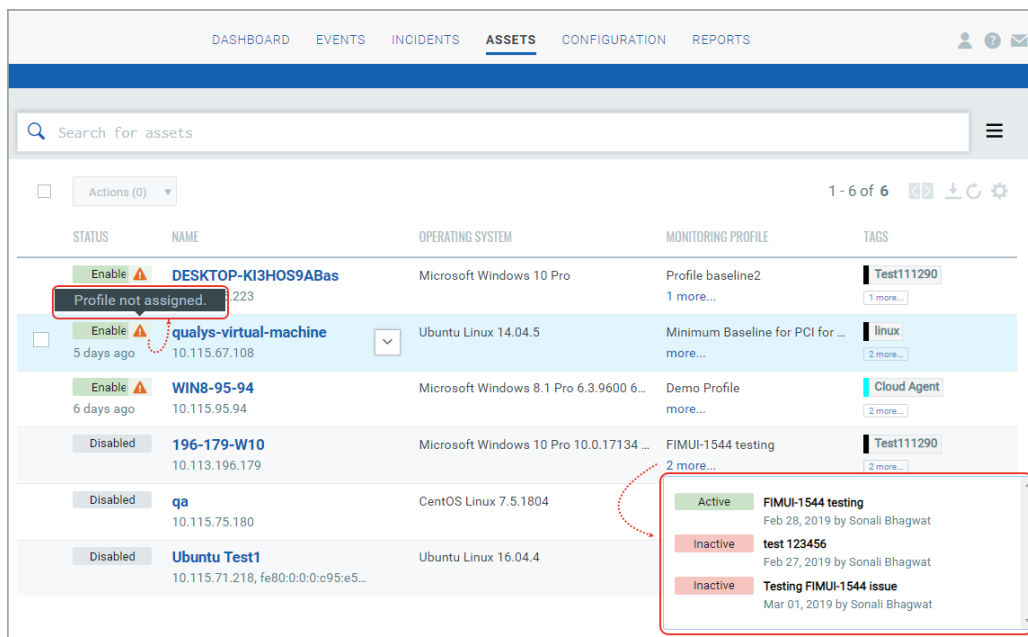
Now you can view the actual status of the installed agent and the monitoring profiles and their status for each asset. We have added Status and Monitoring Profile columns to show this information. The Status column shows Enable when agent is active and Disable when agent is inactive/disabled for the asset.

DASHBOARD EVENTS INCIDENTS ASSETS CONFIGURATION REPORTS					
<div> <div> <div></div> <div>Search for assets</div> </div> <div> <div> <div></div> <div>Actions (0)</div> </div> <div>1 - 6 of 6</div> <div> </div> </div> </div>					
STATUS	NAME	OPERATING SYSTEM	MONITORING PROFILE	TAGS	
<div>Enable</div> <div>5 days ago</div>	<div>qualys-virtual-machine</div> <div>10.115.67.108</div>	Ubuntu Linux 14.04.5	<div>Minimum Baseline for PCI for ...</div> <div>more...</div>	<div>linux</div> <div>2 more...</div>	
<div>Enable</div> <div>6 days ago</div>	<div>DESKTOP-KI3HOS9ABas</div> <div>10.115.75.223</div>	Microsoft Windows 10 Pro	<div>Profile baseline2</div> <div>1 more...</div>	<div>Test111290</div> <div>1 more...</div>	
<div>Enable</div> <div>6 days ago</div>	<div>WIN8-95-94</div> <div>10.115.95.94</div>	Microsoft Windows 8.1 Pro 6.3.9600 6...	<div>Demo Profile</div> <div>more...</div>	<div>Cloud Agent</div> <div>2 more...</div>	
<div>Disabled</div>	<div>196-179-W10</div> <div>10.113.196.179</div>	Microsoft Windows 10 Pro 10.0.17134 ...	<div>FIMUI-1544 testing</div> <div>2 more...</div>	<div>Test111290</div> <div>2 more...</div>	




For assets with agent status enabled, the Status column displays an  icon when any of the following events occurred for the asset:

- No FIM monitoring profile is assigned to the asset.
- Agent uninstallation is complete for the asset.
- Manifest generation is in progress for the asset.
- The agent is not found for the asset.
- FIM manifest is decommissioned on the agent.
- Received an agent uninstallation request for the asset.
- FIM manifest is published on the agent.
- Error in generating FIM manifest for the asset.
- Received request for activating/deactivating FIM for the asset.
- Matching FIM profile is found for the asset, and the FIM profile is waiting for manifest generation.

Move your mouse over the  icon to view the status. Monitoring Profile column shows a “more” link. Click the link to view the names of all the monitoring profiles assigned to the asset and profiles status as active/inactive.



The screenshot displays the Qualys Assets interface. The top navigation bar includes links for DASHBOARD, EVENTS, INCIDENTS, ASSETS (selected), CONFIGURATION, and REPORTS. A search bar is present with the text "Search for assets". Below the navigation bar, there is a table of assets. The table has columns for STATUS, NAME, OPERATING SYSTEM, MONITORING PROFILE, and TAGS. The first asset, "DESKTOP-KI3HOS9ABas", has a status of "Enable" with a warning icon and a tooltip that says "Profile not assigned.". The second asset, "qualys-virtual-machine", has a status of "Enable" with a warning icon and a tooltip that shows a list of monitoring profiles: "FIMUI-1544 testing" (Active), "test 123456" (Inactive), and "Testing FIMUI-1544 issue" (Inactive). The third asset, "WIN8-95-94", has a status of "Enable" with a warning icon. The fourth asset, "196-179-W10", has a status of "Disabled". The fifth asset, "qa", has a status of "Disabled". The sixth asset, "Ubuntu Test1", has a status of "Disabled".

STATUS	NAME	OPERATING SYSTEM	MONITORING PROFILE	TAGS
Enable 	DESKTOP-KI3HOS9ABas 223	Microsoft Windows 10 Pro	Profile baseline2 1 more...	Test111290 1 more...
Enable 	qualys-virtual-machine 10.115.67.108	Ubuntu Linux 14.04.5	Minimum Baseline for PCI for ... more...	linux 2 more...
Enable 	WIN8-95-94 10.115.95.94	Microsoft Windows 8.1 Pro 6.3.9600 6...	Demo Profile more...	Cloud Agent 2 more...
Disabled	196-179-W10 10.113.196.179	Microsoft Windows 10 Pro 10.0.17134 ...	FIMUI-1544 testing 2 more...	Test111290 2 more...
Disabled	qa 10.115.75.180	CentOS Linux 7.5.1804		
Disabled	Ubuntu Test1 10.115.71.218, fe80:0:0:c95:e5...	Ubuntu Linux 16.04.4		

We have removed the “Group by” menu provided to group the assets by monitoring profile from the Asset View page. You can see this information on the Profiles List page in the Configuration tab. The Profiles List page has Assets column that shows the total count of assets assigned to the monitoring profiles.

Issues Addressed

- We have updated the "asset.tag" token to "asset.tags".
- We have updated the help syntax on UI for the asset.tags token to inform that token accepts asset tag ID instead of the tag name when used for searching an asset.
- We have fixed an issue where clicking on any of the widgets: "Events by Severity", "Changes by Action" and "Changes by user" on the Incident Summary page were not navigating the user to the events related to that widget. Now when you click on the widgets, the application shows events for the filter.
- We have fixed an issue where incorrect notification was shown when importing a pre-defined profile from Library that has already been imported by the user. Now the user is notified that profile is already imported.
- We have fixed an issue where a category for a profile could be created with a blank name. Now category name cannot be blank.
- We have updated the notification shown when you ignore an event from the Event Review tab to inform that listing the ignored events in Ignored tabs may take some time.
- We have fixed an issue where on the Event Details page, long path names were not getting wrapped. Now the path names are shown on multiple lines.
- We have fixed an issue where junk characters were shown in DNS names on the Event Details Page. Now DNS names do not show junk characters.
- We have improved our notifications to show user-friendly messages for success or failure of user operations.
- We have fixed the widget layout issue to show the Asset Details page properly in the Internet Explorer browser.
- We have fixed an issue where the "Set as Default Dashboard" was enabled for the dashboard that was already marked as the default dashboard. Now, this option is not available for the default dashboard.
- We have fixed an issue where when assigning and saving "localhost"<i>.localdomain" asset to a monitoring profile from the Assign Assets page was showing junk characters in the asset name. This issue is now fixed.
- We have fixed an issue where incidents were created with a blank name. Now, the incident name cannot be blank.
- We have fixed an issue where dashboards were created with a blank name. Now, the dashboard name cannot be blank.
- We have updated the description for Install Cloud Agents (using CA) on the Get Started page.
- We have fixed an issue where pre-defined profiles in Library when opened in the View mode show incorrect values for Date Created and Last Updated. Now Date Created and Last Updated show correct values.
- We have fixed an issue where Categories and Status filter settings on the Configuration > Profiles page were not getting applied when the user returns to this page from other pages. Now the filters will be reset when the user navigates to another page.
- We have fixed an issue where during monitoring profile create or edit, assets and tags were not getting assigned to the locked profiles from the Assign Assets tab on saving. Now assigned assets and tags are getting saved for locked monitoring profiles.

- We have fixed an issue where when assigning assets to a Linux profile, the user is unable to search for Red Hat, Ubuntu, CentOS, Oracle Enterprise Linux, Amazon Linux, SuSE Linux assets on the Asset selector page. This issue is now fixed.
- During monitoring profile create or update, the profile description now accepts only 2500 characters.
- We have fixed an issue where existing rules for monitoring profiles were not displayed in the Rules tab. Now the existing rules are shown for profiles.
- During creating or updating a monitoring profile, you can not specify special characters in the category name when creating a new profile category using the Manage button shown on the Profile Details page.
- Now you can edit the profile names imported from our library to contain a maximum of 128 characters.
- The Event Details page now shows "Created on" and "Last Checked-in" under the Activity section in the ABOUT ASSET pane.
- During creating or updating rule profile, now the attribute: "Monitor the file for" or "Monitor the directory structure for" in the Monitoring Rule Parameters section: does not show the file/directory path that you have entered in "File Path".
- We have fixed an issue where the monitoring profile page was showing wrong asset counts for monitoring profiles. This issue is now fixed.