



Qualys File Integrity Monitoring

Release Notes

Version 3.7.0

May 04, 2023

Here's what's new in features and improvements in Qualys File Integrity Monitoring 3.7.0!

What's New?

[New Search Tokens for Events Tab](#)

[New Error Code in Agent Health Status for FIM Prerequisite Check Failure](#)

[New Permission in Role-Based Access Control \(RBAC\)](#)

[View File Size in FIM Events](#)

[Display of Events Based on Descending Count of Events](#)

New Search Tokens for Events Tab

We have added three new tokens to FIM Event Details.

Token	Description	Examples
commandExecuted	Use text value ##### to get an executed command that results in an FIM event occurrence.	commandExecuted: 'chmod 655 /etc/shadow '
actor.auditUserName	Use a text value ##### to find the name of the user performing the actual task.	actor.auditUserName: john
actor.auditUserID	Use a text value ##### to find the id of the user performing the actual task. This ID is assigned to a user upon login and is inherited by every process, even when the user's identity changes (for example, switching user accounts from Joe to John.)	actor.auditUserID: '1001'

You can view the details on the event details page.

The screenshot shows the 'View Details: USERAUDITNAME.TXT' page. The main content area displays an event alert for 'File Content' with details for 'userAuditname.txt'. Key fields are highlighted with red boxes:

- actor.auditUserName:** root (ID)
- actor.auditUserID:** 000ac29d184d747f5d769e1549ed91e039d1783771c34b8373021636537a9f

The right sidebar provides asset information for 'localhost.localdomain' (AlmaLinux 9.0) and file details for 'userAuditname.txt' (File Path: /root/.x3_7/userAuditname.txt, Size: 17 B).

New Error Code in Agent Health Status for FIM Prerequisite Check Failure

A new error code in Agent Health Status is added to address the FIM prerequisite check failure. You can find the Linux assets with the FIM prerequisite failure query. This feature offers a checklist for prerequisites helping you to detect the possibilities that can lead to failure. We are introducing new token values for `agentservice.osStatus` in QQL Search.

For more details on the search token refer to the [Online help](#)

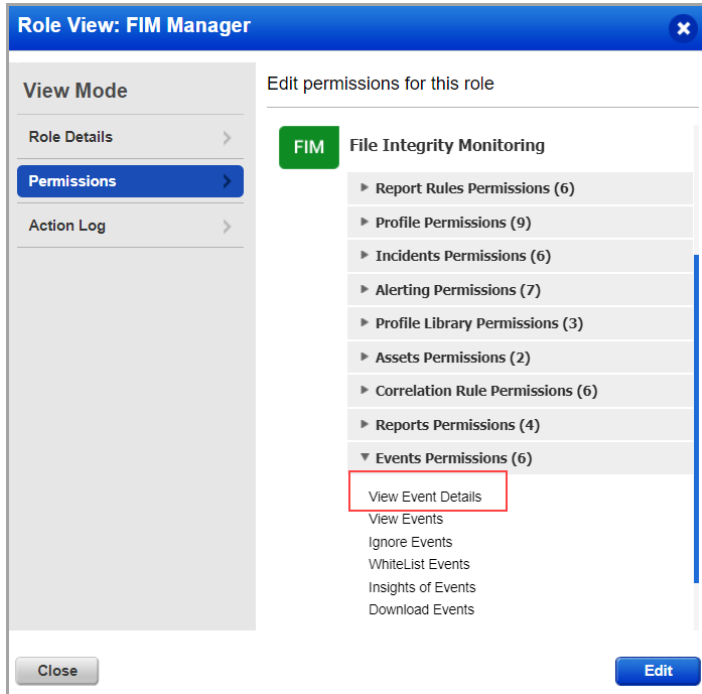
Token	Description	Examples
agentservice.osStatus	<p>Use the token to find Linux assets based on the operating system (OS) status.</p> <p>Select the token values from Q_AuditNotPresent, Q_AuditInImmutableState, Q_NeverTaskRuleExists, Q_SELinuxPackagesMissing.</p>	<ul style="list-style-type: none"> To see if FIM prerequisites checks are failed for Linux platform, you can use the following query: <pre>agentService.osStatus:`Q_AuditNotPresent` or agentService.osStatus:`Q_AuditInImmutableState` or agentService.osStatus:`Q_NeverTaskRuleExists` or agentService.osStatus:`Q_SELinuxPackagesMissing`</pre> Find Linux assets with the OS status where the audit service is not in the running state. <pre>agentservice.osStatus: Q_AuditNotPresent</pre>

New Permission in Role-Based Access Control (RBAC)

FIM Event might contain sensitive information. We can not expose this information to all users. To restrict access to these details to all users, we have enhanced the RBAC and provided additional permission **View Event Details**. By default, FIM Manager and FIM Analyst roles have this access. They can view event details. FIM Auditor and FIM Author roles are not granted this permission by default.

For more information on how to assign permission, refer to online help available in the [Administration utility](#)

Refer to the following screenshot, where we have shown permission for the Manager role.



View File Size in FIM Events

On **Event Details** page, you can view the file size of the FIM Event.

To view the event detail, go to **Events** tab > **Events Insights** and double-click the event.

Note:

- For Windows agents, you can view the file size of FIM events for Create, Content, and Attribute Action.
- For Linux agents, you can view the file size of FIM events for Create, Content, and Security Action.

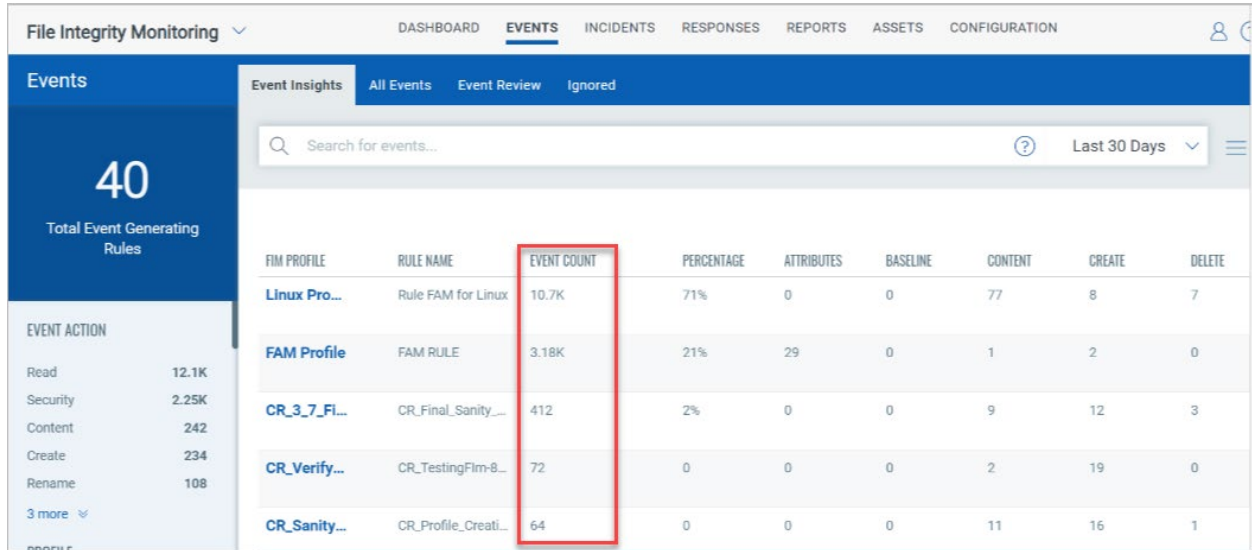
The screenshot displays the 'View Details: RG_CONFIG.CFG' page. The left pane shows the event alert for 'File Security' regarding 'rg_config.cfg'. The right pane provides details about the asset 'fim' and the file itself.

Event Alert: File Security	
	rg_config.cfg Changed On: a day ago Apr 24, 2023 at 5:33:21 PM Category: PCI By User: root File Path: /var/tmp/FIM_Content_Change_Monitoring/rg_config.cfg By Process: /usr/bin/vi Command Executed: Audit User Name: root (0)
	Triggers Monitoring Profile: ContentChange_Linux Section and Rules: RG_Linux

ABOUT ASSET	
	fim CentOS Linux 7.3.1611 Unknown Manufacturer / Model
Identification	
DNS Hostname:	fim
NetBIOS Name:	—
IPv4 Addresses:	10.115.74.104
IPv6 Addresses:	
Agent ID:	8ad4666a-51ae-41d1-853a-9095bca1cf0b
Host ID:	3347250
Activity	
Last User Login:	root
Last System Boot:	
Created On:	Apr 14, 2023 03:47 pm
Last Checked-In:	Apr 14, 2023 03:47 pm
ABOUT THE FILE	
File Name:	rg_config.cfg
File Path:	/var/tmp/FIM_Content_Change_Monitoring/rg_config.cfg
Size:	27 B

Display of Events Based on Descending Event Counts

With this release, the **Event Insights** tab displays the events based on descending count of events. This helps you see the rules creating the maximum number of events on the top, along with their corresponding FIM Profiles, thus giving you a fair idea of what to edit first in order to curb noise.



The screenshot shows the 'File Integrity Monitoring' dashboard with the 'EVENTS' tab selected. The 'Event Insights' sub-tab is active, displaying a table of event-generating rules. The 'EVENT COUNT' column is highlighted with a red box. The table lists rules such as 'Linux Pro...', 'FAM Profile', 'CR_3_7_FI...', 'CR_Verify...', and 'CR_Sanity...' with their respective event counts, percentages, and other attributes.

FIM PROFILE	RULE NAME	EVENT COUNT	PERCENTAGE	ATTRIBUTES	BASELINE	CONTENT	CREATE	DELETE
Linux Pro...	Rule FAM for Linux	10.7K	71%	0	0	77	8	7
FAM Profile	FAM RULE	3.18K	21%	29	0	1	2	0
CR_3_7_FI...	CR_Final_Sanity...	412	2%	0	0	9	12	3
CR_Verify...	CR_TestingFim-8...	72	0	0	0	2	19	0
CR_Sanity...	CR_Profile_Creati...	64	0	0	0	11	16	1