Qualys File Integrity Monitoring (FIM)

Release Notes

Version 3.1

July 30, 2021

What’s new in 3.1!

Manifest Status

Grouping Events by Assets in All Events tab

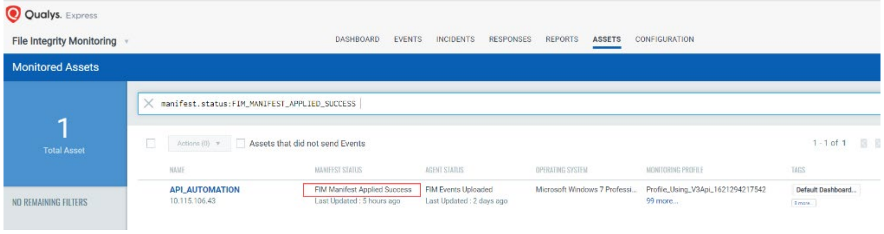
Wildcard character support for QQL in Events tab

Bugs and Improvements

Manifest Status

Introducing a new value for Manifest Status, under Assets tab. User will get to know if agent has downloaded the manifest. Only after the Agent further applies the downloaded manifest, it comes into effect. After downloading the manifest, two additional manifest statuses are displayed for Windows Agent:

- Manifest applied successfully
- Manifest applicationfailed

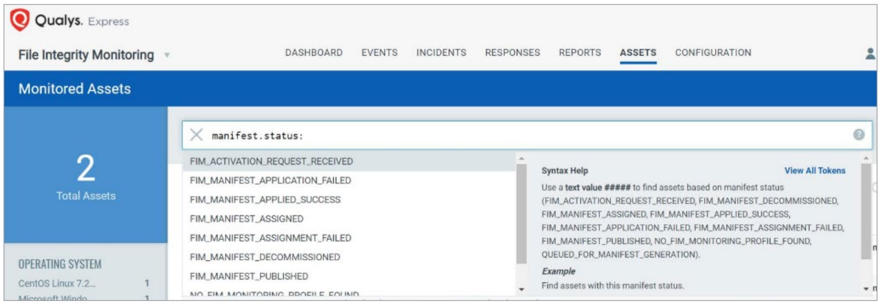


```
manifest.status:FIM_MANIFEST_APPLIED_SUCCESS
```

□ Assets that did not send Events

NAME	MANIFEST STATUS	AGENT STATUS	OPERATING SYSTEM	MONITORING PROFILE	TAGS
API_AUTOMATION 10.115.106.43	FIM Manifest Applied Success Last Updated : 5 hours ago	FIM Events Uploaded Last Updated : 2 days ago	Microsoft Windows 7 Professi...	Profile_Using_V3Api_1621294217542 99 more...	Default Dashboard...

QQL token added as manifest.status on Assets tab.



```
manifest.status:
```

FIM_ACTIVATION_REQUEST_RECEIVED
FIM_MANIFEST_APPLICATION_FAILED
FIM_MANIFEST_APPLIED_SUCCESS
FIM_MANIFEST_ASSIGNED
FIM_MANIFEST_ASSIGNMENT_FAILED
FIM_MANIFEST_DECOMMISSIONED
FIM_MANIFEST_PUBLISHED
NO_FIM_MONITORING_PROFILE_FOUND

Syntax Help View All Tokens

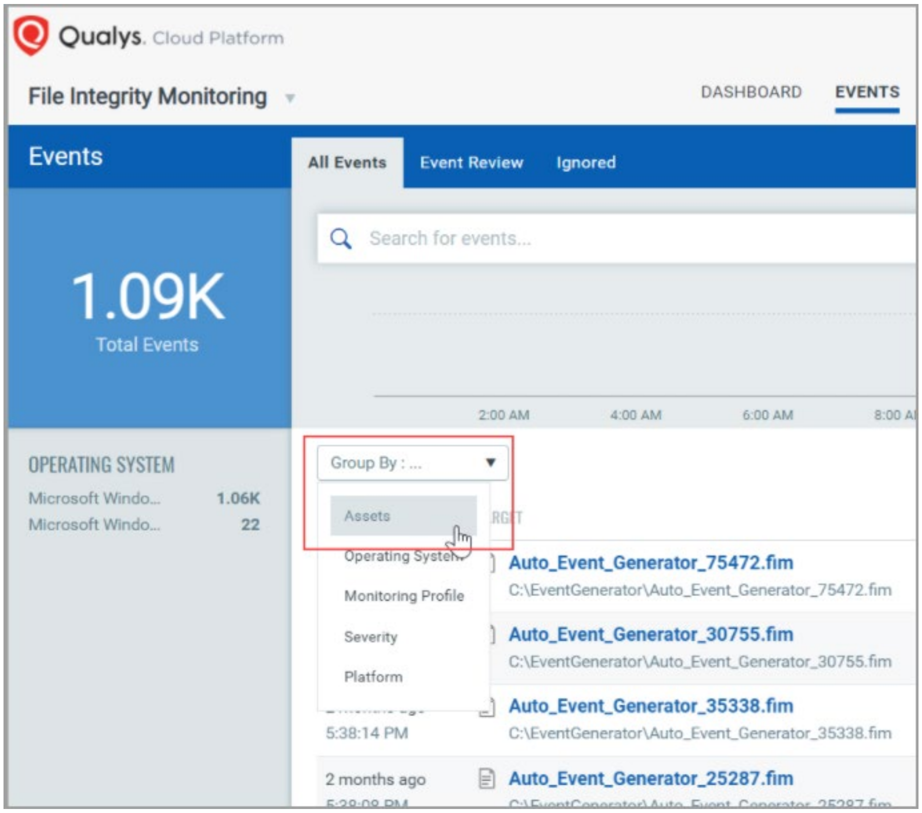
Use a **text value #####** to find assets based on manifest status (FIM_ACTIVATION_REQUEST_RECEIVED, FIM_MANIFEST_DECOMMISSIONED, FIM_MANIFEST_ASSIGNED, FIM_MANIFEST_APPLIED_SUCCESS, FIM_MANIFEST_APPLICATION_FAILED, FIM_MANIFEST_ASSIGNMENT_FAILED, FIM_MANIFEST_PUBLISHED, NO_FIM_MONITORING_PROFILE_FOUND, QUEUED_FOR_MANIFEST_GENERATION).

Example

Find assets with this manifest status.

Grouping Events by Assets in All Events tab

Grouping Events by Assets in the All Events tab, brings up maximum of 1000 grouped assets. Pagination is now removed.



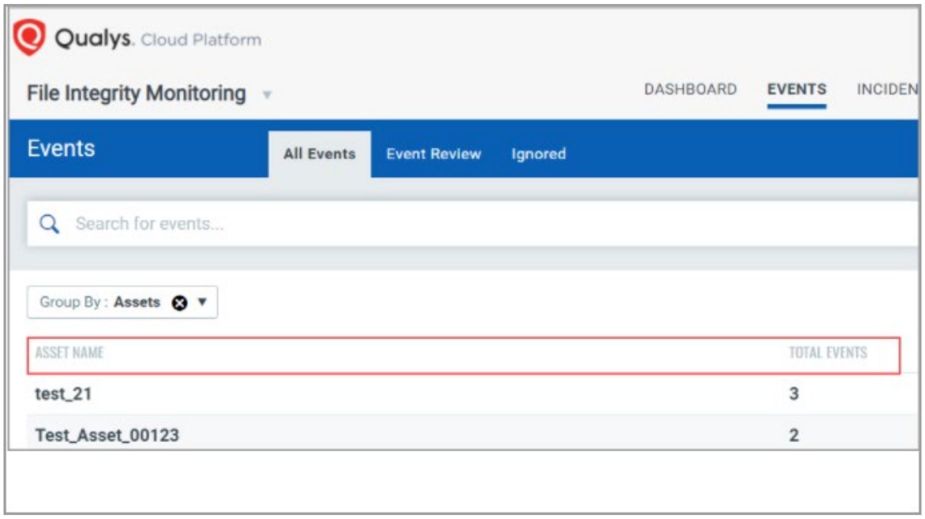
Auto_Event_Generator_75472.fim
C:\EventGenerator\Auto_Event_Generator_75472.fim

Auto_Event_Generator_30755.fim
C:\EventGenerator\Auto_Event_Generator_30755.fim

5:38:14 PM
Auto_Event_Generator_35338.fim
C:\EventGenerator\Auto_Event_Generator_35338.fim

2 months ago
Auto_Event_Generator_25287.fim

You can view Event details with **Asset Name** and count of **Total Events** for that asset.



Group By : Assets

ASSET NAME	TOTAL EVENTS
test_21	3
Test_Asset_00123	2

Wildcard character support for QQL in Events tab

Wildcard character search is now supported for Events tab.

Two types of searches supported for the users:

- Suffix matching

  Suffix matching is supported for searching events for the fields: asset.name, asset.netbiosName, asset.operatingSystem, actor.userID, actor.process, profile.name, profile.rule.name, registryKey.name, file.name. You can match event fields by specifying ending part in a string and the starting of the field will be represented with *.

  Example: This query can fetch all results for log file deletions.

  action:Delete and file.name:*.log

  Example: Similarly this query will fetch all events for configuration file modifications in Linux.

  action:Content and file.name:*.conf

  Suffix based searches are applicable only for Events tab in FIM.

- Prefix matching

  Prefix matching is supported for searching events using text fields that are same as the fields for suffix matching. You can match event fields by specifying starting part in a string and the ending of the field will be represented with *.

  Example: This query matches events with an asset name starting with "xp", example - xpsp2-jp-26-111.

  asset.name:xp*

  Example: This query matches events with file name starting with "Expl" example - Explorer.exe.

  file.name:Expl*

  Example: This query matches events with assets having operating system starting with "Lin", example - Linux 2.4-2.6.

  asset.operatingSystem:Lin*

  Note: Wildcards can only be used for prefix and suffix matching (as described above). Substring wildcards are not supported, that is, you cannot search for a string in the middle of another string.

  Prefix based searches are applicable only for Events tab in FIM.

  Note: Matches are case insensitive for both prefix and suffix.

Bugs and Improvements

- FIM UI showing one tag multiple times is fixed now.
- For Event Details, **File size** is also added.
- Grouping Events by Assets only Lists 50 Assets issue is resolved. It is now possible to see max 1000 assets when grouped by Event (in All Events Tab) removing pagination for Assets page and displaying 1000 Assets in the list.