Qualys File Integrity Monitoring v2.x

Release Notes

Version 2.5

December 3, 2020

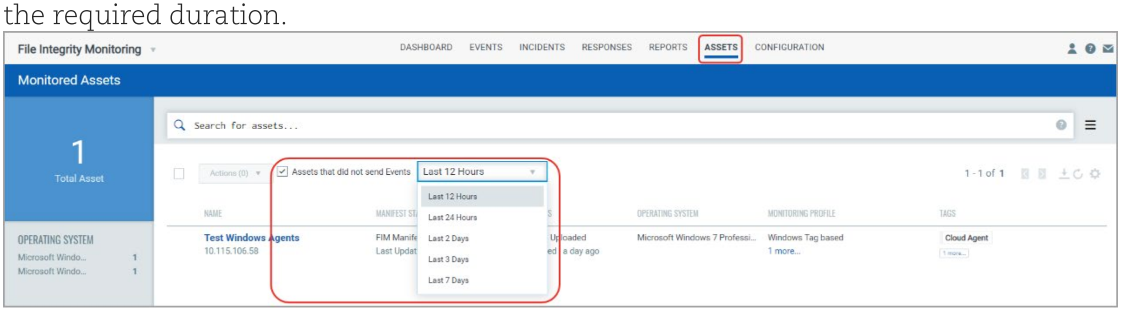
FIM 2.5 brings you more improvements and updates! Learn more

Agent Health Tracking

With this release, we give you the option to filter assets based on the current agent status. After an asset is provisioned in FIM, you can use the UI filters or QQL queries to know if an asset is performing as expected.

We have revamped the Assets tab to include additional filters:

1. You can now filter assets that have not sent events. On the **Assets** tab, select the **Assets that did not send Events** option and from the adjacent drop-down list, select the required duration.



1 Total Asset

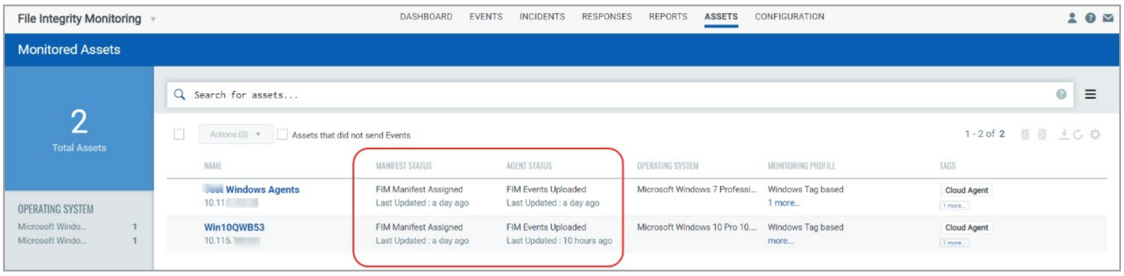
OPERATING SYSTEM
Microsoft Windo... 1
Microsoft Windo... 1

☑ Assets that did not send Events — Last 12 Hours

- Last 12 Hours
- Last 24 Hours
- Last 2 Days
- Last 3 Days
- Last 7 Days

NAME	MANIFEST STA	S	OPERATING SYSTEM	MONITORING PROFILE	TAGS
Test Windows Agents 10.115.106.58	FIM Manife Last Updat	Uploaded ed : a day ago	Microsoft Windows 7 Professi...	Windows Tag based 1 more...	Cloud Agent 1 more...

2. We have added two new columns Manifest Status and Agent Status. These columns also list the time of the status update.



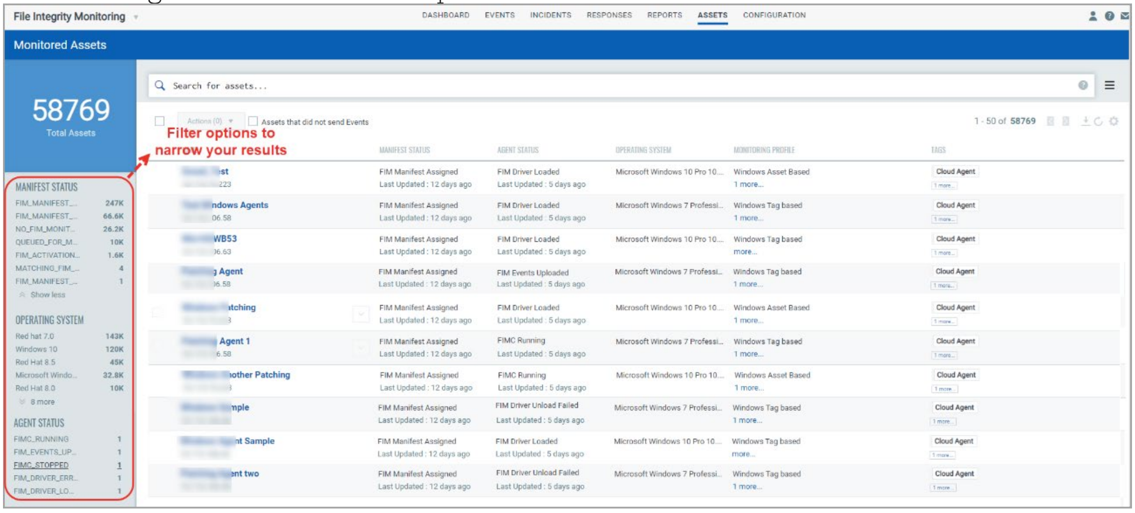
2 Total Assets

OPERATING SYSTEM
Microsoft Windo... 1
Microsoft Windo... 1

□ Assets that did not send Events

NAME	MANIFEST STATUS	AGENT STATUS	OPERATING SYSTEM	MONITORING PROFILE	TAGS
[redacted] Windows Agents 10.11[redacted]	FIM Manifest Assigned Last Updated : a day ago	FIM Events Uploaded Last Updated : a day ago	Microsoft Windows 7 Professi...	Windows Tag based 1 more...	Cloud Agent 1 more...
Win10QWB53 10.115.[redacted]	FIM Manifest Assigned Last Updated : a day ago	FIM Events Uploaded Last Updated : 10 hours ago	Microsoft Windows 10 Pro 10...	Windows Tag based more...	Cloud Agent 1 more...

3. You can find assets based on the Operating System, Manifest Status, and Agent Status using the filters in the left-pane.



58769 Total Assets

MANIFEST STATUS	
FIM_MANIFEST_...	247K
FIM_MANIFEST_...	66.6K
NO_FIM_MONIT...	26.2K
QUEUED_FOR_M...	10K
FIM_ACTIVATION...	1.6K
MATCHING_FIM_...	4
FIM_MANIFEST_...	1
Show less	

OPERATING SYSTEM	
Red hat 7.0	143K
Windows 10	120K
Red Hat 8.5	45K
Microsoft Windo...	32.8K
Red Hat 8.0	10K
8 more	

AGENT STATUS	
FIMC_RUNNING	1
FIM_EVENTS_UP...	1
FIMC_STOPPED	1
FIM_DRIVER_ERR...	1
FIM_DRIVER_LO...	1

□ Assets that did not send Events

NAME	MANIFEST STATUS	AGENT STATUS	OPERATING SYSTEM	MONITORING PROFILE	TAGS
[redacted]st [redacted]223	FIM Manifest Assigned Last Updated : 12 days ago	FIM Driver Loaded Last Updated : 5 days ago	Microsoft Windows 10 Pro 10...	Windows Asset Based 1 more...	Cloud Agent 1 more...
[redacted]ndows Agents [redacted]06.58	FIM Manifest Assigned Last Updated : 12 days ago	FIM Driver Loaded Last Updated : 5 days ago	Microsoft Windows 7 Professi...	Windows Tag based 1 more...	Cloud Agent 1 more...
[redacted]WB53 [redacted]06.63	FIM Manifest Assigned Last Updated : 12 days ago	FIM Driver Loaded Last Updated : 5 days ago	Microsoft Windows 10 Pro 10...	Windows Tag based more...	Cloud Agent 1 more...
[redacted]g Agent [redacted]06.58	FIM Manifest Assigned Last Updated : 12 days ago	FIM Events Uploaded Last Updated : 5 days ago	Microsoft Windows 7 Professi...	Windows Tag based 1 more...	Cloud Agent 1 more...
[redacted]tching [redacted]3	FIM Manifest Assigned Last Updated : 12 days ago	FIM Driver Loaded Last Updated : 5 days ago	Microsoft Windows 10 Pro 10...	Windows Asset Based 1 more...	Cloud Agent 1 more...
[redacted] Agent 1 [redacted]6.58	FIM Manifest Assigned Last Updated : 12 days ago	FIMC Running Last Updated : 5 days ago	Microsoft Windows 7 Professi...	Windows Tag based 1 more...	Cloud Agent 1 more...
[redacted]nother Patching [redacted]3	FIM Manifest Assigned Last Updated : 12 days ago	FIMC Running Last Updated : 5 days ago	Microsoft Windows 10 Pro 10...	Windows Asset Based 1 more...	Cloud Agent 1 more...
[redacted]mple [redacted]	FIM Manifest Assigned Last Updated : 12 days ago	FIM Driver Unload Failed Last Updated : 5 days ago	Microsoft Windows 7 Professi...	Windows Tag based 1 more...	Cloud Agent 1 more...
[redacted]nt Sample [redacted]	FIM Manifest Assigned Last Updated : 12 days ago	FIM Driver Loaded Last Updated : 5 days ago	Microsoft Windows 10 Pro 10...	Windows Tag based more...	Cloud Agent 1 more...
[redacted]ent two [redacted]	FIM Manifest Assigned Last Updated : 12 days ago	FIM Driver Unload Failed Last Updated : 5 days ago	Microsoft Windows 7 Professi...	Windows Tag based 1 more...	Cloud Agent 1 more...

Along with the UI filters, you can also filter the assets using the QQL queries. Here are a few use-cases and the corresponding QQL queries that you can use to know the asset status.

1. Asset Activation

   To list the asset that are provisioned during a time range:

```
activationDate: ['2020-11-08' .. '2020-11-10']
```

2. Manifest Generation

   After the assets are activated, here are few possible scenarios for manifest generation:

   a. To list the assets that have received the FIM activation request and waiting for manifest generation process:

```
manifest.status : `FIM_ACTIVATION_REQUEST_RECEIVED`
```

   b. To list the assets that do not have FIM monitoring profile assigned and hence will not get any manifest:

```
manifest.status : `NO_FIM_MONITORING_PROFILE_FOUND`
```

   c. To list the assets for which the manifest generation request is either queued or in progress:

```
manifest.status : `QUEUED_FOR_MANIFEST_GENERATION`
```

   d. To list the assets for which manifest has been published successfully to Cloud Agent:

```
manifest.status : `FIM_MANIFEST_PUBLISHED`
```

   e. To list that assets for which manifest has been assigned and acknowledged successfully by Cloud Agent:

```
manifest.status : `FIM_MANIFEST_ASSIGNED`
```

   f. To list assets for which manifest has been decommissioned:

```
manifest.status : `FIM_MANIFEST_DECOMMISSIONED`
```

3. Agent Error

   To list the assets which has some error on the Agent.

```
agentService.status : ['FIM_DRIVER_LOADED_FAILURE',
'FIM_EVENTS_UPLOADED_FAILURE', 'FIMC_STOPPED',
'FIM_DRIVER_UNLOADED_FAILURE']
```

For a complete list of tokens on the Assets tab, see Tokens on Assets Tab.

New Token on Events Tab

With this release, we have added the following new token on Events tab.

- profile.rule.name: This token will help you find the events based on the rule name.

New Fill Path Format

With an upgrade to Cloud Agent version 4.1, the File Path will be displayed in the following format:

```
c:\directory\sub-directory\file.ext
```

We recommend you upgrade all the agents in your environment to 4.1 and above and then edit the existing QQL queries to include the new file path.

If you cannot upgrade all the agents to 4.1 and above, you must edit the existing QQL queries and add the new file path format along with the old one.

Also, events that are registered before the agent is upgraded to 4.1, will continue to display the file path in the old format.

Alerting Permissions

With this release, we introduce new set of Alerting permissions for FIM User and FIM Manager. Depending on the roles and permissions assigned, the user can perform actions like creating, editing, or deleting rules and actions.

Using the Administration module, the Manager user for the subscription can assign these roles and permissions for all the other users.

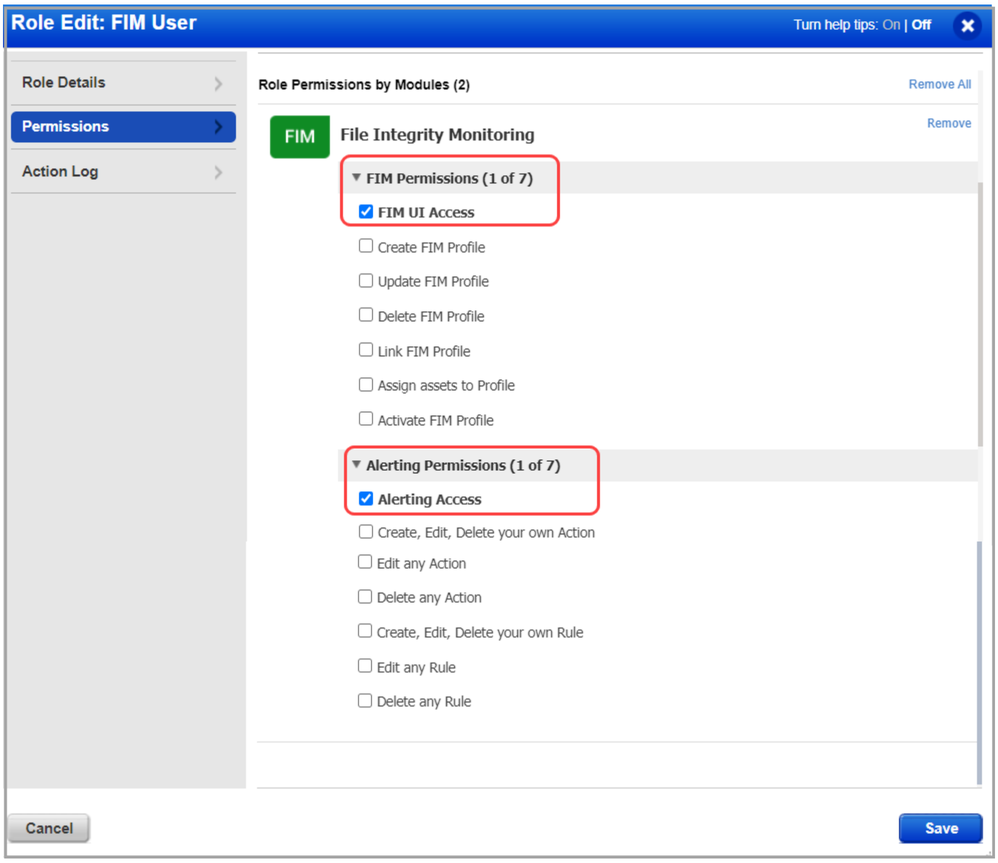
Note: FIM users created before version 2.5 will continue to have the same permissions.

Manager- A user with the Manager role is considered a super-user and has all the available permissions. They have full privileges and access to all modules in the subscription. Only users with Manager role can create other users and assign roles.

Note: The Manager user can customize permissions for the FIM User and FIM Manager.

- FIM User**:** By default, the FIM User role has permission to FIM UI and Alert Access. So, the user with FIM User role can see the rules and actions but cannot create, edit, or delete them.

  The default permissions for FIM User role:



Role Permissions by Modules (2)

File Integrity Monitoring

▾ FIM Permissions (1 of 7)

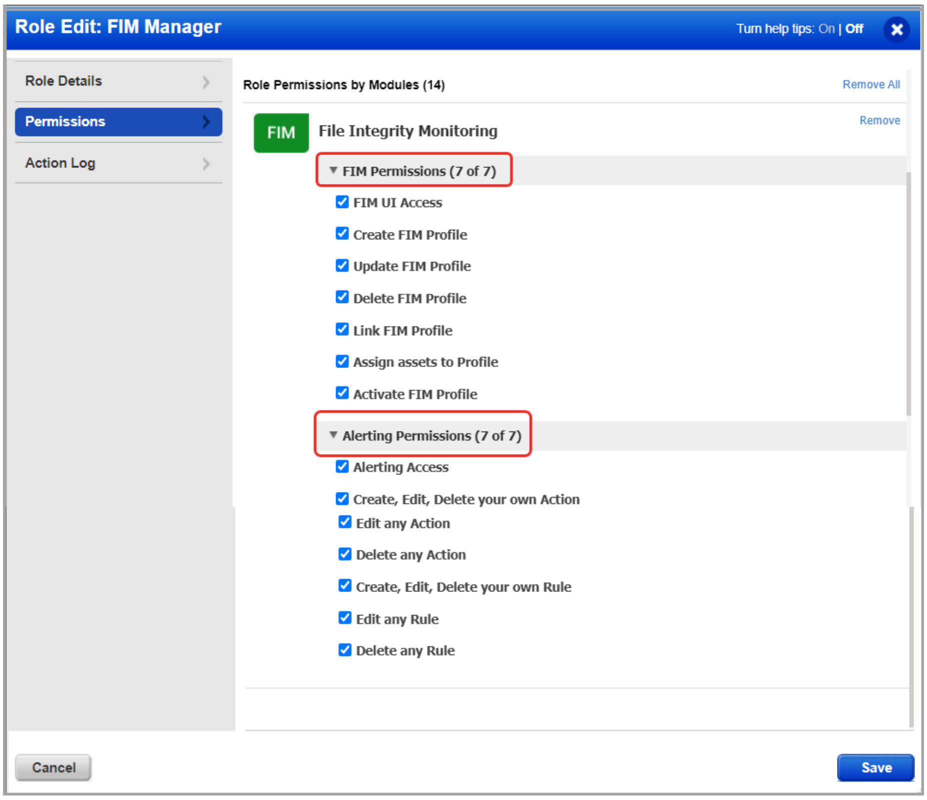
- ☑ FIM UI Access
- ☐ Create FIM Profile
- ☐ Update FIM Profile
- ☐ Delete FIM Profile
- ☐ Link FIM Profile
- ☐ Assign assets to Profile
- ☐ Activate FIM Profile

▾ Alerting Permissions (1 of 7)

- ☑ Alerting Access
- ☐ Create, Edit, Delete your own Action
- ☐ Edit any Action
- ☐ Delete any Action
- ☐ Create, Edit, Delete your own Rule
- ☐ Edit any Rule
- ☐ Delete any Rule

- FIM Manager: By default, this role has FIM Permissions and Alerting Permissions.

  The default permissions for FIM Manager role:



Role Permissions by Modules (14)

File Integrity Monitoring

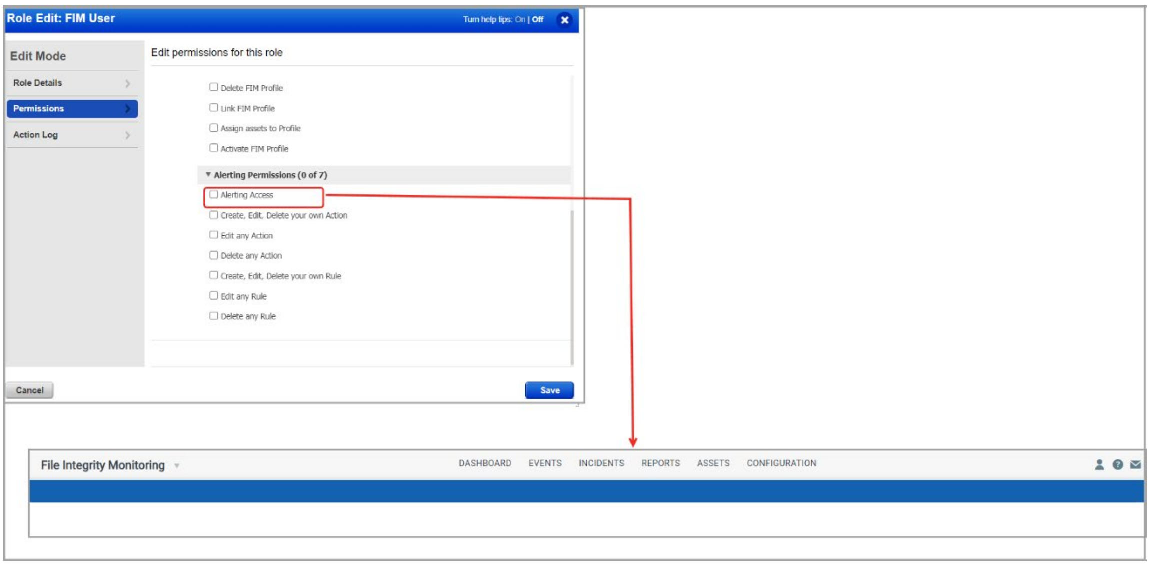
▼ FIM Permissions (7 of 7)

- ☑ FIM UI Access
- ☑ Create FIM Profile
- ☑ Update FIM Profile
- ☑ Delete FIM Profile
- ☑ Link FIM Profile
- ☑ Assign assets to Profile
- ☑ Activate FIM Profile

▼ Alerting Permissions (7 of 7)

- ☑ Alerting Access
- ☑ Create, Edit, Delete your own Action
- ☑ Edit any Action
- ☑ Delete any Action
- ☑ Create, Edit, Delete your own Rule
- ☑ Edit any Rule
- ☑ Delete any Rule

Note: If the user is assigned a role with no Alerting Access permission, the user will not see the Responses tab on the FIM UI.



Edit permissions for this role

- □ Delete FIM Profile
- □ Link FIM Profile
- □ Assign assets to Profile
- □ Activate FIM Profile

▼ Alerting Permissions (0 of 7)

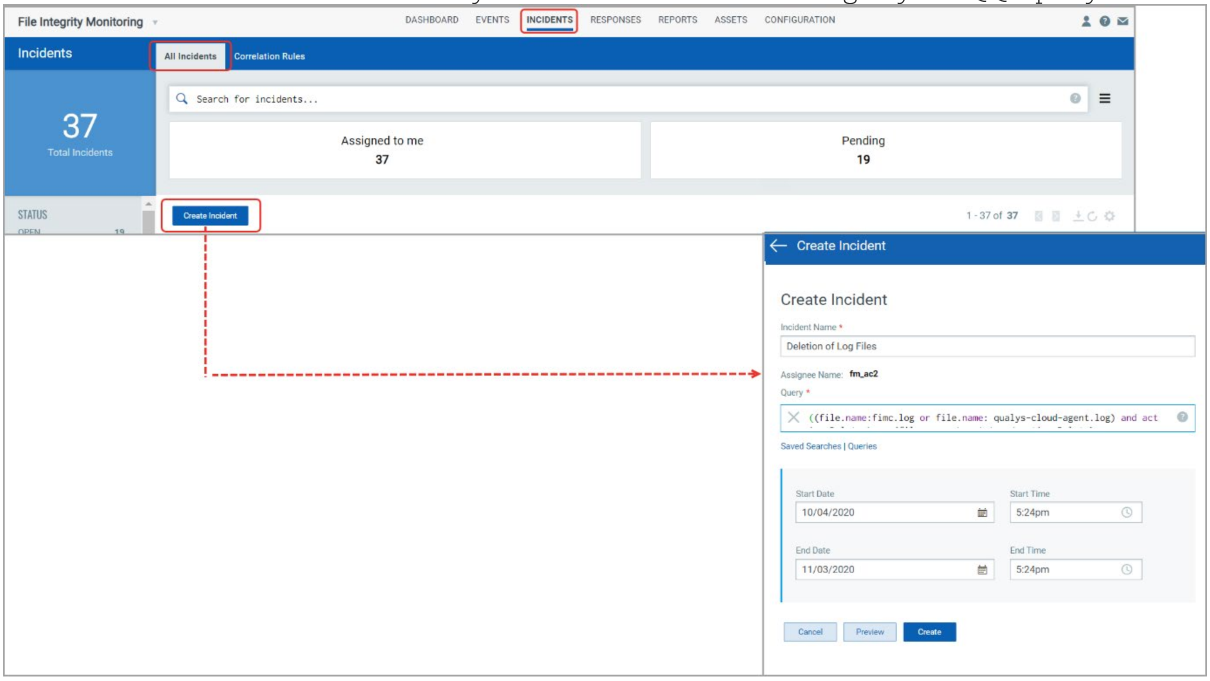
- □ Alerting Access
- □ Create, Edit, Delete your own Action
- □ Edit any Action
- □ Delete any Action
- □ Create, Edit, Delete your own Rule
- □ Edit any Rule
- □ Delete any Rule

Create Incidents

With this release, we give you the option to create manual incident from the Incidents tab.

To create an incident, click **Incidents** > **All Incidents** > **Create Incident**. On the **Create Incident** page, enter the required details and click **Create**.

Note: You can create an incident only if there are events matching to your QQL query.



Create Incident

Incident Name * Deletion of Log Files

Assignee Name: fm_ac2

Query *

```
((file.name:fimc.log or file.name: qualys-cloud-agent.log) and act
```

Start Date 10/04/2020

Start Time 5:24pm

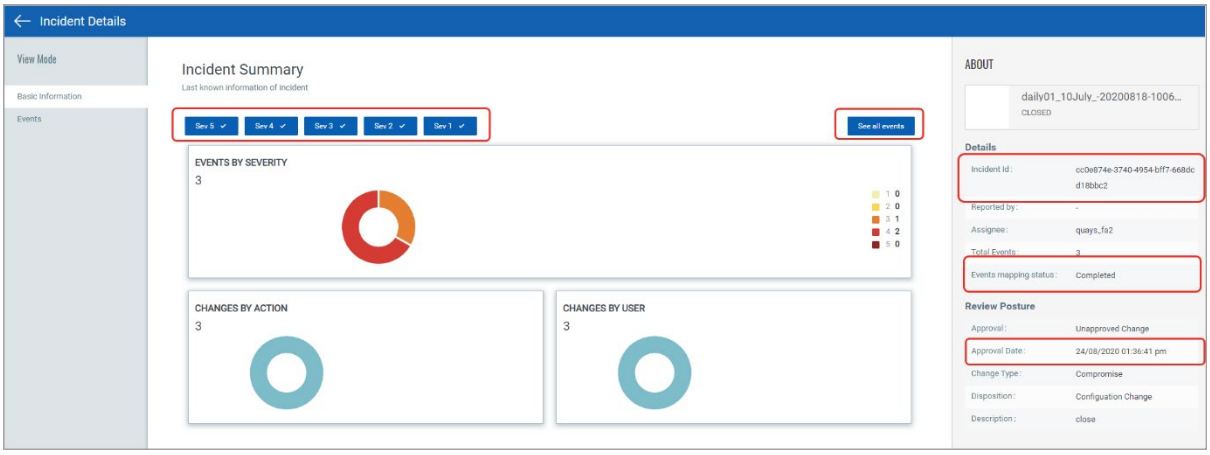
End Date 11/03/2020

End Time 5:24pm

Revamped Incident Details Page

For better customer experience, we have made the following enhancements to the Incident Details page:

- Added the following new fields:
  - Incident Id: This field displays the Incident UUID.
  - Event mapping status: This field displays the status of automatic incident creation of the event.
  - Approval Date: Displays the date and time when an automatic incident was approved.
- All the severity options (Sev 5 **-** Sev 1) will now be selected by default.
- Renamed the “View All” field to “See all events”.



daily01_10July_-20200818-1006...
CLOSED

Details

Incident Id : cc0e874e-3740-4954-bff7-668dcd18bbc2
Reported by : -
Assignee : quays_fa2
Total Events : 3
Events mapping status : Completed

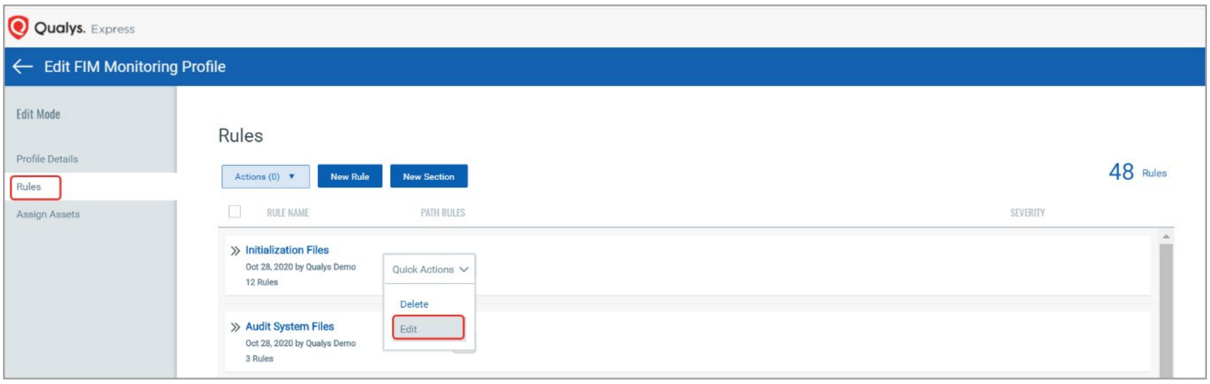
Review Posture

Approval : Unapproved Change
Approval Date : 24/08/2020 01:36:41 pm
Change Type : Compromise
Disposition : Configuation Change
Description : close

Edit a Section

We now give you the option to edit a section that is created for a profile. Using the edit option, you can edit the references (up to 10 references) and section details.

To edit a section, go to **Configuration** > **Profiles**. Select the required profile and click **Quick Actions** > **Edit** > **Rules.** Select the required section and click **Quick Action > Edit.**

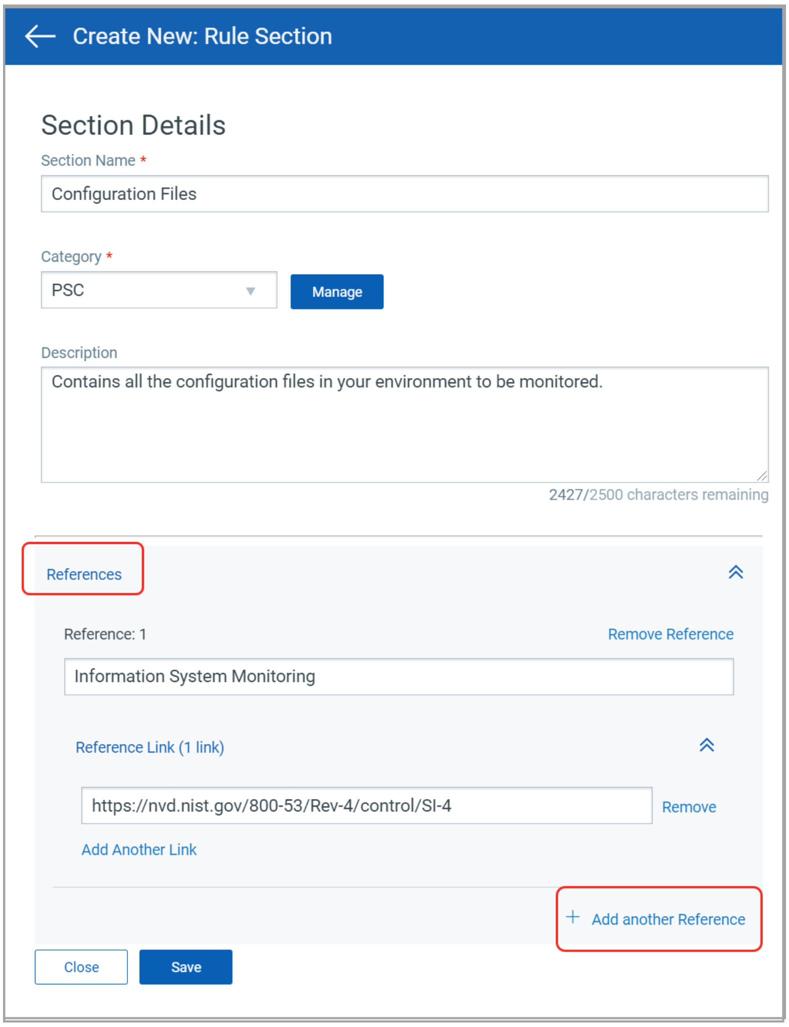


Initialization Files
Oct 28, 2020 by Qualys Demo
12 Rules

Audit System Files
Oct 28, 2020 by Qualys Demo
3 Rules

Add and Edit Section References

With this release, we give you an option to add and edit up to 10 References under each section. References are added to map the section with the relevant compliance standards that it adheres.



Section Details

Section Name *: Configuration Files

Category *: PSC

Description: Contains all the configuration files in your environment to be monitored.

2427/2500 characters remaining

Reference: 1

Information System Monitoring

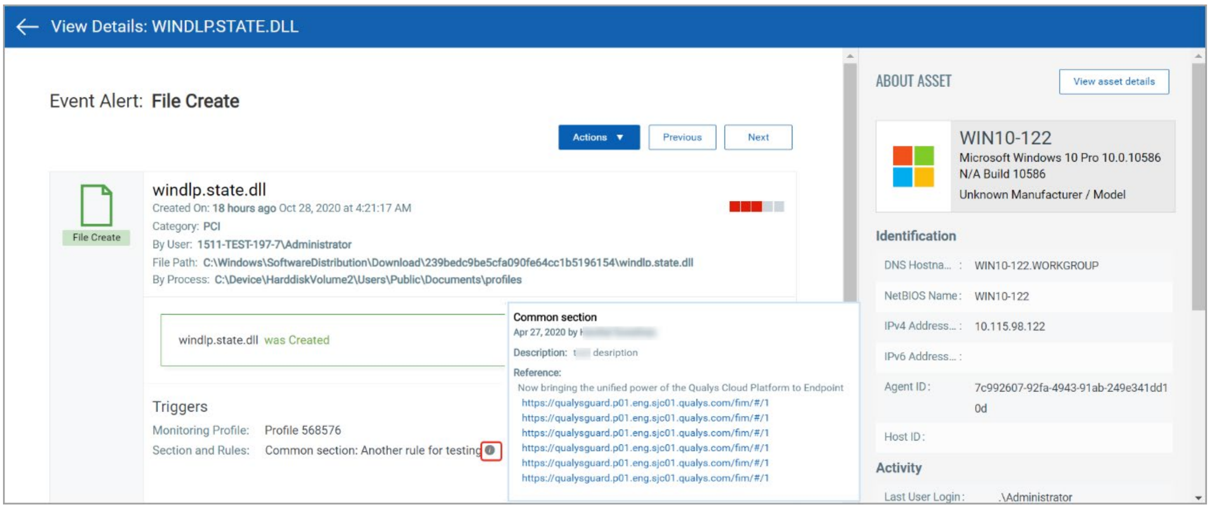
Reference Link (1 link)

https://nvd.nist.gov/800-53/Rev-4/control/SI-4

Section Details on Event Details Page

For better customer experience, we have made the following enhancements to the Event Details page:

- To adhere to the compliance standards, we now display the section details on the Event Details page. This information will help you know:
  - The Rule and Profile for which the event is generated.
  - The Section and Section Details mapped to the rule.



Event Alert: **File Create**

windlp.state.dll

Created On: 18 hours ago Oct 28, 2020 at 4:21:17 AM

Category: PCI

By User: 1511-TEST-197-7\Administrator

File Path: C:\Windows\SoftwareDistribution\Download\239bedc9be5cfa090fe64cc1b5196154\windlp.state.dll

By Process: C:\Device\HarddiskVolume2\Users\Public\Documents\profiles

windlp.state.dll was Created

Triggers

Monitoring Profile: Profile 568576

Section and Rules: Common section: Another rule for testing

Common section

Apr 27, 2020 by H[redacted]

Description: t[redacted] desription

Reference:

Now bringing the unified power of the Qualys Cloud Platform to Endpoint

https://qualysguard.p01.eng.sjc01.qualys.com/fim/#/1
https://qualysguard.p01.eng.sjc01.qualys.com/fim/#/1
https://qualysguard.p01.eng.sjc01.qualys.com/fim/#/1
https://qualysguard.p01.eng.sjc01.qualys.com/fim/#/1
https://qualysguard.p01.eng.sjc01.qualys.com/fim/#/1
https://qualysguard.p01.eng.sjc01.qualys.com/fim/#/1

ABOUT ASSET

WIN10-122

Microsoft Windows 10 Pro 10.0.10586 N/A Build 10586

Unknown Manufacturer / Model

Identification

DNS Hostna... : WIN10-122.WORKGROUP

NetBIOS Name : WIN10-122

IPv4 Address... : 10.115.98.122

IPv6 Address... :

Agent ID : 7c992607-92fa-4943-91ab-249e341dd10d

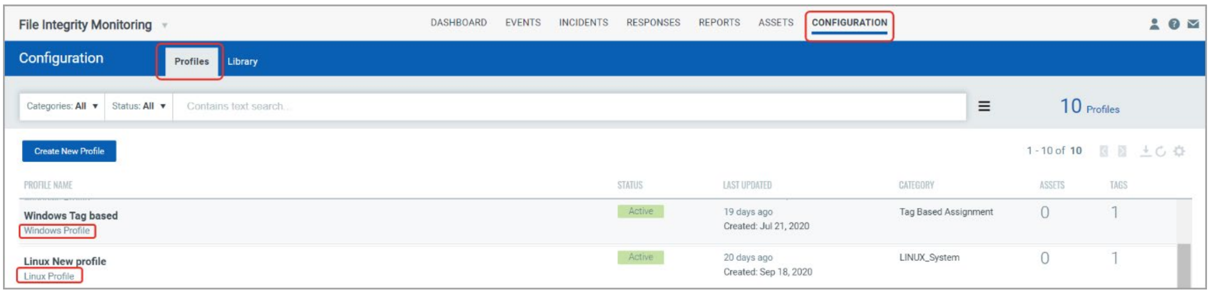
Host ID :

Activity

Last User Login : .\Administrator

Profile Type Displayed on Profiles Tab

To help you identify the operating system of the profile upfront, we now display the operating system under each profile name.



PROFILE NAME	STATUS	LAST UPDATED	CATEGORY	ASSETS	TAGS
Windows Tag based Windows Profile	Active	19 days ago Created: Jul 21, 2020	Tag Based Assignment	0	1
Linux New profile Linux Profile	Active	20 days ago Created: Sep 18, 2020	LINUX_System	0	1

Tokens on Assets Tab

With this release, you will see the following sub-set of tokens on the Assets tab. These tokens will help you filter assets based on different criteria:

- activated: This token will help you find assets based on the activation status.
- activationDate: This token will help you find assets based on the activation date.
- agentService.httpStatus: This token will help you find Linux assets based on the http status.
- agentService.osStatus: This token will help you find Linux assets based on the operating system (OS) status.
- agentService.status: This token will help you find assets based on the agent service status. (Accepted values: FIM_DRIVER_LOADED, FIM_DRIVER_LOADED_FAILURE, FIM_DRIVER_UNLOADED, FIM_DRIVER_UNLOADED_FAILURE, FIM_EVENTS_UPLOADED, FIM_EVENTS_UPLOADED_FAILURE, FIMC_RUNNING, FIMC_STOPPED).
- agentService.statusCode: This token will help you find assets based on the agent service code (Accepted values: 2001, 2002, 2003, 2004, 2007, 2008, 2009, 2010).
- agentService.updatedDate: This token will help you find assets based on the agent updated.
- agentUuid: This token will help you find assets based on agent UUID.
- agentVersion: This token will help you find assets based on agent version you're interested in.
- assetId: This token will help you find assets based on by agent ID.
- assetType: This token will help you find assets based on asset type.
- created: This token will help you find assets based on the date created.
- netbiosName: This token will help you find assets based on the netbios name.
- ec2.region: This token will help you find assets based on the EC2 region.
- ec2.instanceId: This token will help you find assets based on the EC2 instance ID.
- ec2.hostname: This token will help you find assets based on the EC2 hostname.
- ec2.availabilityZone: This token will help you find assets based on the EC2 availability zone of assets.
- interfaces.macAddress: This token will help you find assets based on the MAC address.
- interfaces.address: This token will help you find assets based on the IP address.
- interfaces.hostname: This token will help you find assets based on the hostname.
- interfaces.interfaceName: This token will help you find assets based on the interface name.
- lastLoggedOnUser: This token will help you find assets based on the last logged in user.

- lastCheckedIn: This token will help you find assets based on the last check-in.
- operatingSystem: This token will help you find assets based on the operating system.
- manifest.status: This token will help you find assets based on manifest status. (Accepted values: FIM ACTIVATION REQUEST RECEIVED, NO FIM MONITORING PROFILE FOUND, QUEUED FOR MANIFEST GENERATION, FIM MANIFEST PUBLISHED, FIM MANIFEST DOWNLOADED, FIM MANIFEST DECOMMISSIONED).
- manifest.id: This token will help you find assets based on manifest ID.
- manifest.updatedDate: This token will help you find assets based on manifest updated date.
- name: This token will help you find assets based on name.
- system.boot: This token will help you find assets based on the last boot date.
- tags.name: This token will help you find assets based on the tag name.

Issues addressed in this release

- We have fixed an issue for QQL query in Correlation Rules creation where ‘and’ and ‘or’ operands keywords within a profile name caused the misinterpretation of the query.
- We have fixed the issue where IPv4 Address and IPv6 Address for an asset were not displayed on the Event Details page.
- We have fixed the discrepancy issue in DNS Hostname on the Events Details page.
- The dateTime on the Incident Review page will be displayed in the browser time zone.
- The FIM MANIFEST DOWNLOADED option for manifest.status token is now renamed to FIM MANIFEST ASSIGNED on Assets tab.
- We have now added the Add new review option to the View Details page of the reopened incident.
- You can now create incidents from the events that are generated from QQL search of a partial file path and image path.
- The Advanced Option on the Edit Rule page now displays the excluded and included files and directories.