File Integrity Monitoring

Getting Started Guide

Version 4.0

April 15, 2024

Qualys, Inc.
919 E Hillsdale Blvd|
4th Floor
Foster City, CA 94404
1 (650) 801 6100

Table of Contents

About This Guide

Thank you for your interest in Qualys File Integrity Monitoring (FIM).

Qualys FIM allows you to log and centrally track file change events across your global IT assets. All you have to do is install lightweight agents on your assets and set up FIM monitoring profiles. We'll help you get started quickly!

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com

Qualys Support

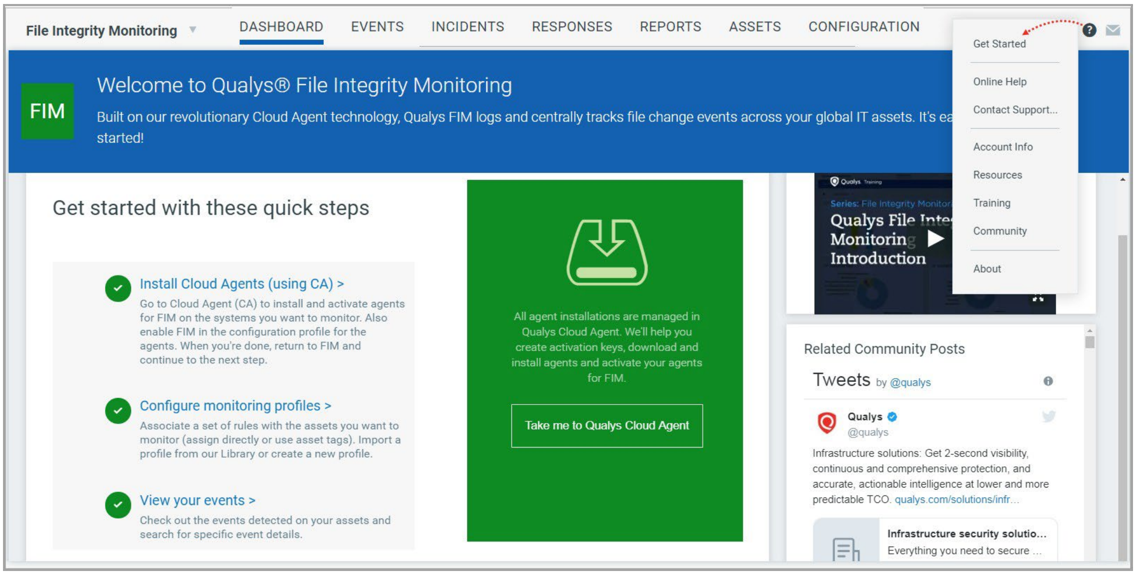
Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access support information at www.qualys.com/support/

Get Started with Qualys FIM

File Integrity Monitoring is a highly scalable, centralized solution that reduces the cost and complexity of detecting policy and compliance-related changes mandated by regulations such as the Payment Card Industry Data Security Standard.

Refer to our online tutorials

Just choose Get Started from the help menu and we'll walk you through the steps. Here you'll find links to helpful information.



Steps to start monitoring change events

Install lightweight agents in minutes on your IT assets. These can be installed on your on-premises systems, dynamic cloud environments and mobile endpoints. Agents are centrally managed by the cloud agent platform and are self-updating (no reboot needed).

Configure FIM monitoring profiles to tell us the files you want to monitor and the types of changes you want to know about. We provide several profiles in our Library to get you started but you can also create your own.

View your events in one central location. You'll see all events detected across all of your assets. Search all of your events in a matter of seconds.

We'll describe these steps in detail in the sections that follow.

Roles and Permissions

You can create users and then assign a role to it to grant access as per the role you define.

Depending on the roles and permissions assigned, the user can perform actions like creating, editing, or deleting rules and actions.

The Administration module is used to create FIM users and assign roles and permissions.

We have provided some pre-created user roles for FIM. Depending on the role, you get the associated set of permissions.

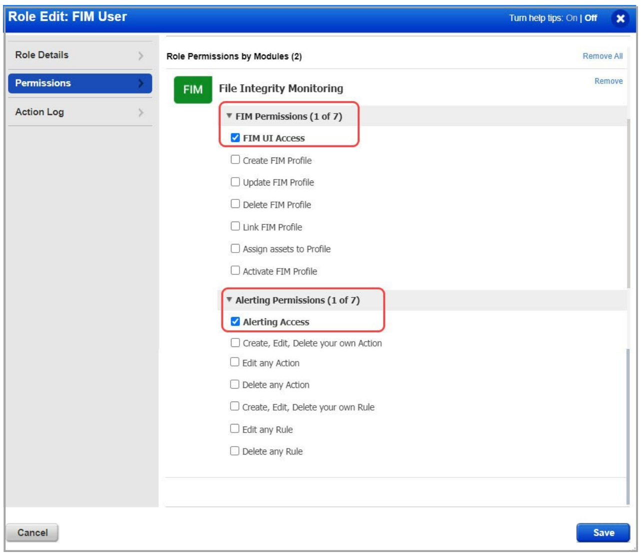
Note: Users created before FIM version 2.5 will continue to have the same permissions.

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.

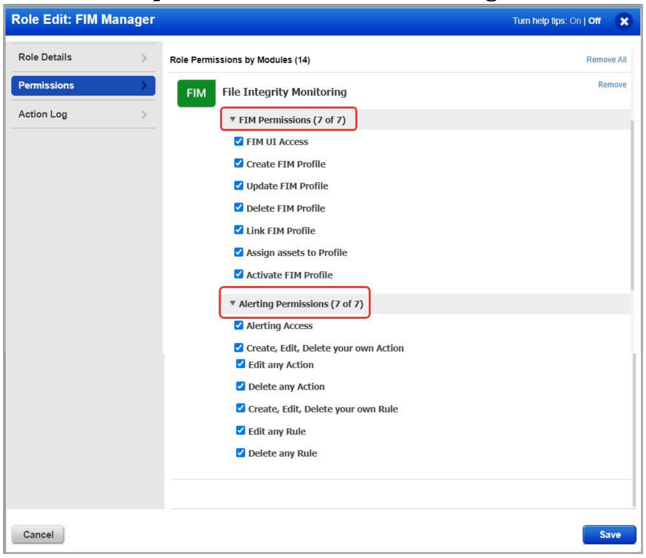
--FIM User: By default, the FIM user role has permission to FIM UI Access and Alert Access. So, the user with FIM user role can see the rules and actions but cannot create, edit, or delete them.

The default permissions for FIM User role:

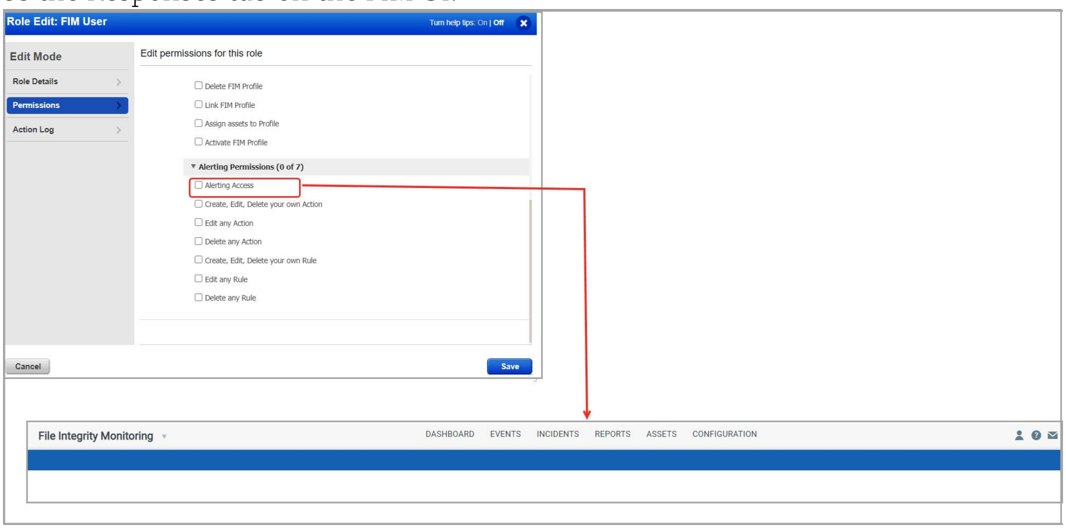


--FIM Manager: By default, this role has FIM Permissions and Alerting Permissions.

The default permissions for FIM Manager role:



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.



Setting up Asset Tags (optional)

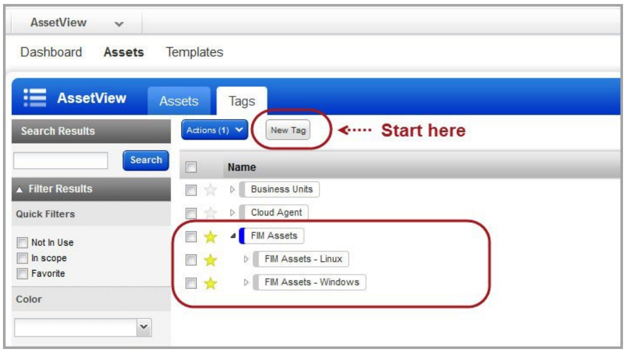
Setting up asset tags using AssetView helps you automate file integrity monitoring using FIM. You can avoid assigning configurations manually to each asset by adding asset tags to the required configurations - FIM monitoring profiles and CA configuration profiles.

We recommend you read these tips on configuring FIM monitoring profiles to help you with deciding how to assign tags to your assets.

How to create tags?

Select AssetView from the module picker.

Then go to Assets > Tags and click New Tag to add tags for your FIM assets. You can use a single tag or multiple tags to mirror your production configuration.



Not interested in tags? No problem. You can manually assign individual assets to your profiles.

Cloud Agent Installation

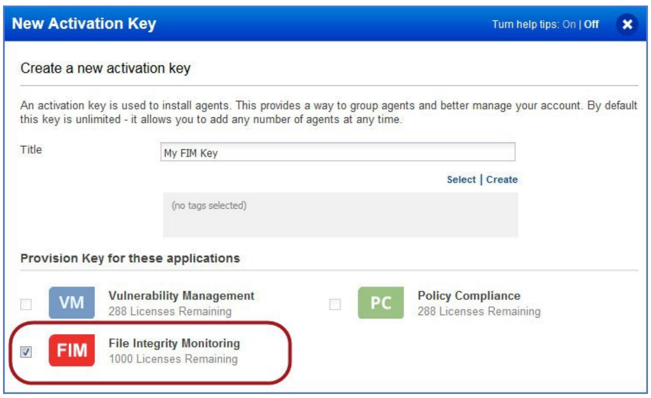
You'll need to install a cloud agent that's been activated for FIM on each asset you want to monitor for file integrity. You'll install and manage agents using Qualys Cloud Agent (CA).

Let's get started!

Select Cloud Agent (CA) from the module picker.

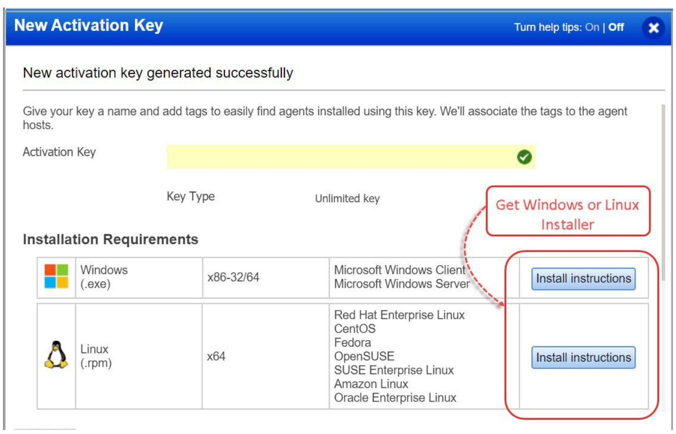
Creating an Activation Key

Create an activation key. Go to Activation Keys, click the New Key button. Give it a title, provision for the FIM application and click Generate.



As you can see you can provision the same key for any of the other applications in your account.

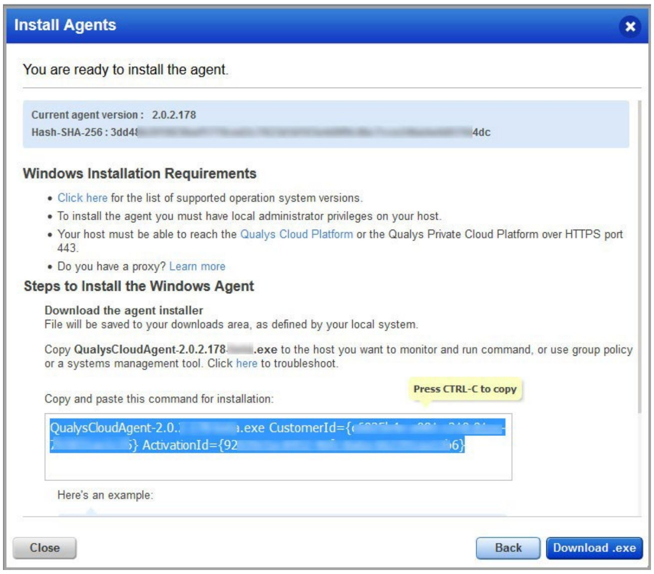
Pick either Windows or Linux to get install instructions and download the installer.



Want to do this step later?

No problem, just exit the wizard. When you're ready, return to your activation keys list, select the key you want to use, then Install Agent from the Quick Actions menu.

Review the installation requirements and click Download.

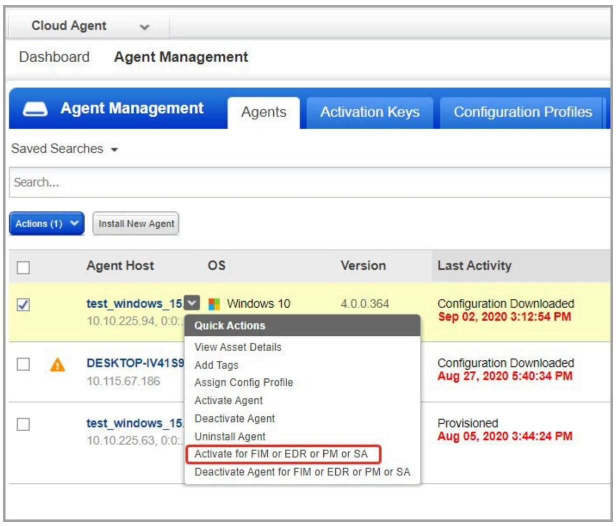


You'll run the installer on each host from an elevated command prompt or use a systems management tool or Windows group policy.

Your agents should start connecting to our cloud platform.

Activating Agents for FIM

Choose "Activate for FIM or EDR or PM or SA" for each FIM cloud agent on the Agents tab.



Enabling FIM in a Configuration Profile

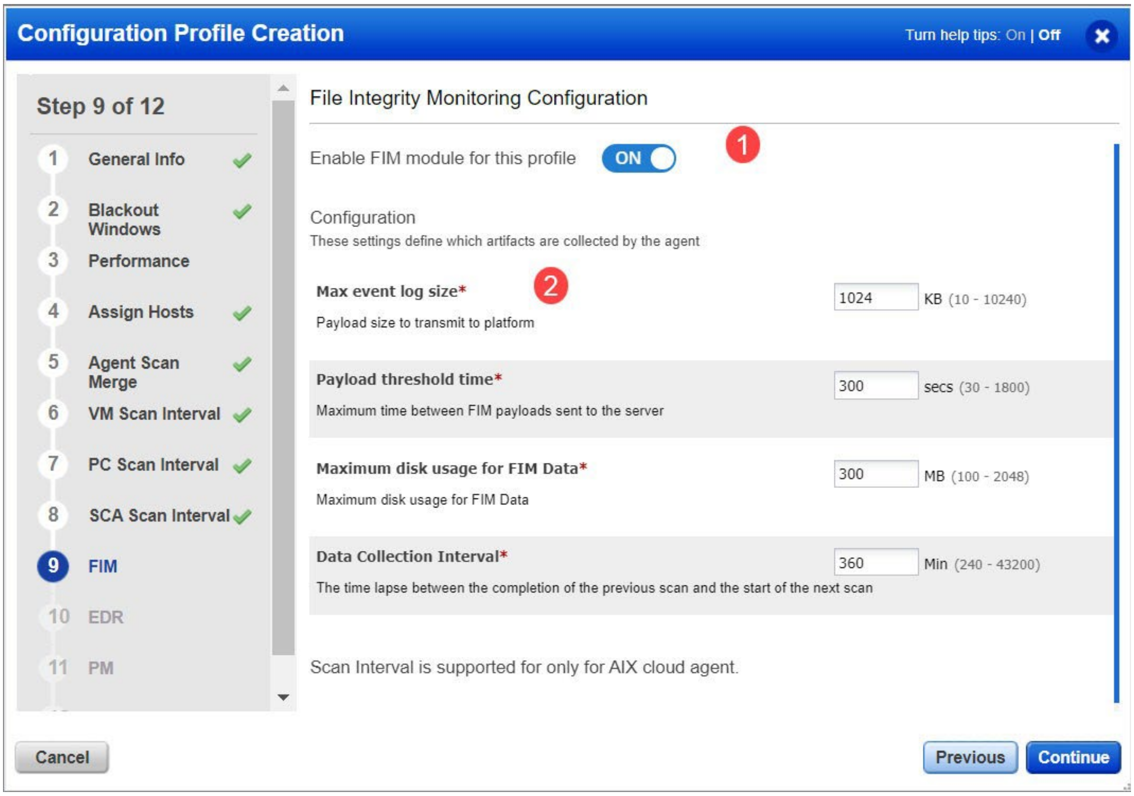
Go to the "Configuration Profiles" tab, create a new profile or edit an existing one. Walk through the profile creation wizard. When you get to the FIM tab:

1) Toggle "Enable FIM module for this profile" to On. This is required for FIM event data collection to occur.

2) Configure when events are transmitted to the Qualys Cloud Platform. Defaults are provided, so this step is optional. You can configure values for event log size, threshold time, disk usage.

(FIM settings are available only when FIM is enabled for your subscription).

Tip - We recommend you set up asset tags for your FIM assets using AssetView. This makes it easy to associate FIM assets with a CA configuration profile and a FIM monitoring profile - just apply the same FIM tags to these profiles.



Note: The Data Collection Interval configuration is applicable only when you configure a cloud agent for FIM on AIX.

Events are transmitted to the Qualys Cloud Platform when either of the following occurs:

- FIM event log reaches the maximum specified size
- Payload threshold time is hit
- Disk usage for total FIM data on the agent reaches the maximum specified size

What's next? Your assets will appear in Qualys FIM on the Assets list. Next we'll describe how to create FIM monitoring profiles for your assets.

FIM Monitoring Profiles

The FIM monitoring profile is where you'll tell us the files you want to monitor and the types of changes you want to know about. We provide several profiles in our Library to get you started but you can also create your own.

Best Practices for Creating Profiles

Configure as many profiles as needed for different situations, and apply multiple profiles to a single device. For example, you may want to configure profiles for these objectives:

- Monitor OS critical binary and configuration data
- Monitor application data
- Monitor rights and permissions database or log files
- Monitor application critical binaries

Define Windows and Linux profiles separately. We don't currently support defining OS version subsets to a profile. Be very granular in assignment of profiles to assets to prevent getting more events than intended. For example, let's say you have a Linux profile for CentOS and a Linux profile for Ubuntu and assign each a tag that contains both operating systems. Both profiles will be monitored for and if there are overlapping settings you could get more events than intended.

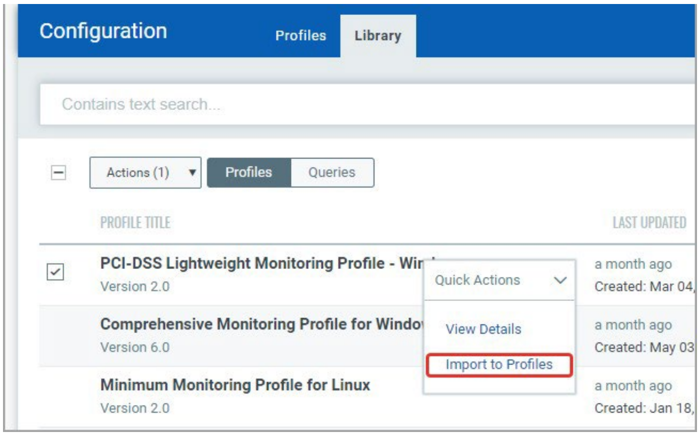
After creating a monitoring profile you must activate it to enable change detection. You can deactivate a profile at any time to suspend monitoring for that profile.

Creating a FIM Monitoring Profile

Choose File Integrity Monitoring (FIM) from the module picker.

We provide several profiles in our Library to help get you started. Our out of box OS based profiles include pre-defined monitoring rules.

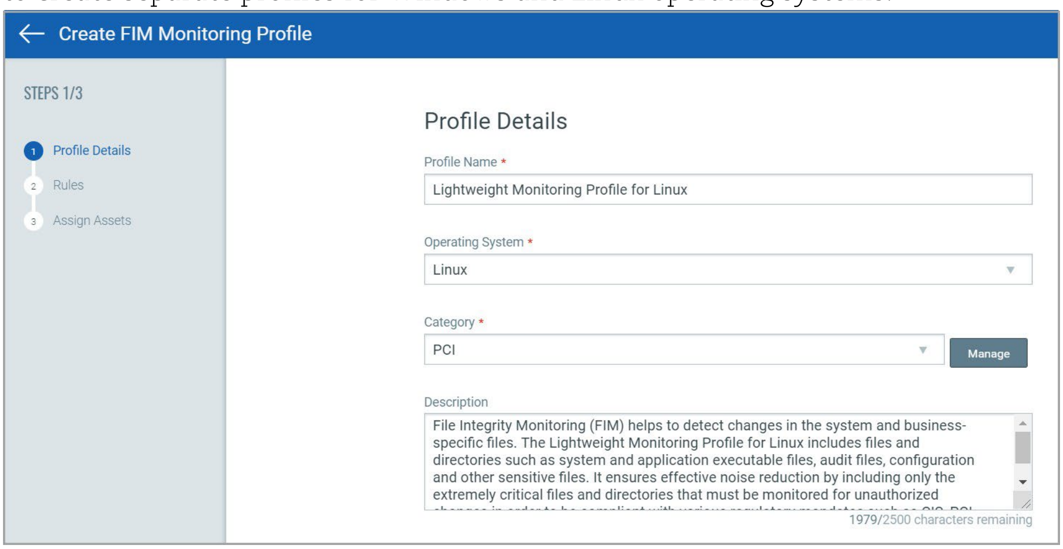
Go to Configuration > Library, select an OS specific profile and choose the Import to Profiles from the menu provided.



Choose whether to import the profile locked or without restrictions. Tip - If you pick No Restrictions, you can edit the profile once imported (on the Profiles tab)

You can also create your own profiles. Click Create New Profile on the Profiles tab.

Provide basic profile details (name, operating system, category). Keep in mind - you'll need to create separate profiles for Windows and Linux operating systems.



Note: FIM allows registry monitoring only for Windows assets. Hence, Select Operating

System as Windows when you wish to add the **Registry Key** and **Registry Value** rule types.

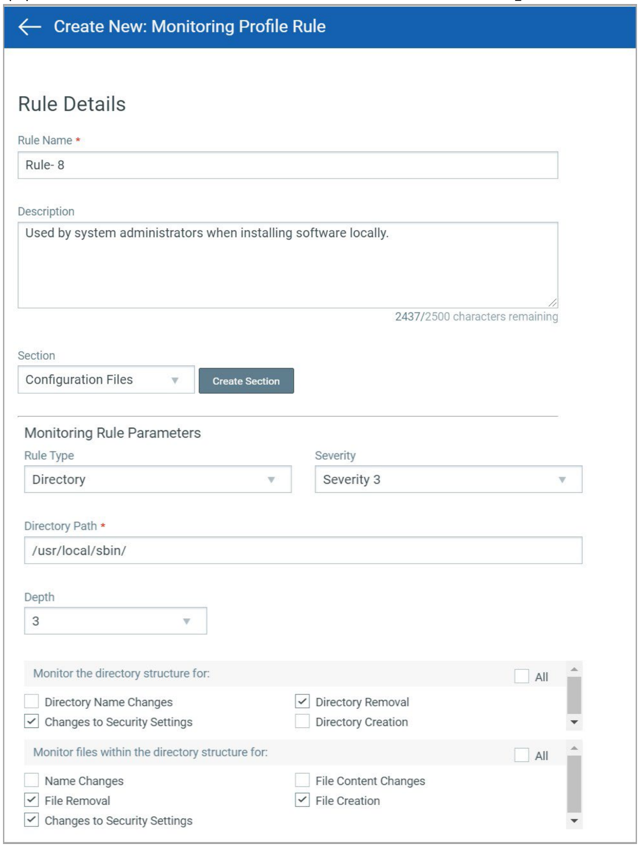
Add one or more rules to the profile to tell us what you want to watch for. Go to the Rules section, click Add New Rule and provide rule details.

When defining a rule:

(1) choose a rule type (File or Directory) and provide the full path to the file/directory.

(2) select the actions that should trigger events.

(3) click Save Rule to add the rule to the profile.

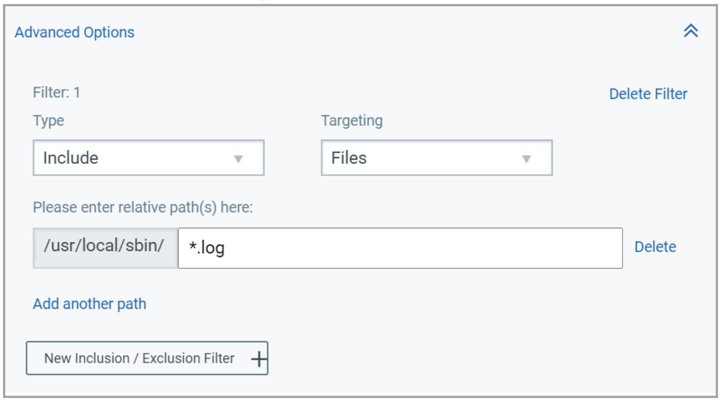


Note: Events get generated for FIM assets on AIX even if you do not select the **File Removal** and **Directory Removal** check boxes.

If you choose Rule Type as Registry Value, then in the Value Path field, add the registry value name to be monitored.

Depth: applicable to both directory or key.

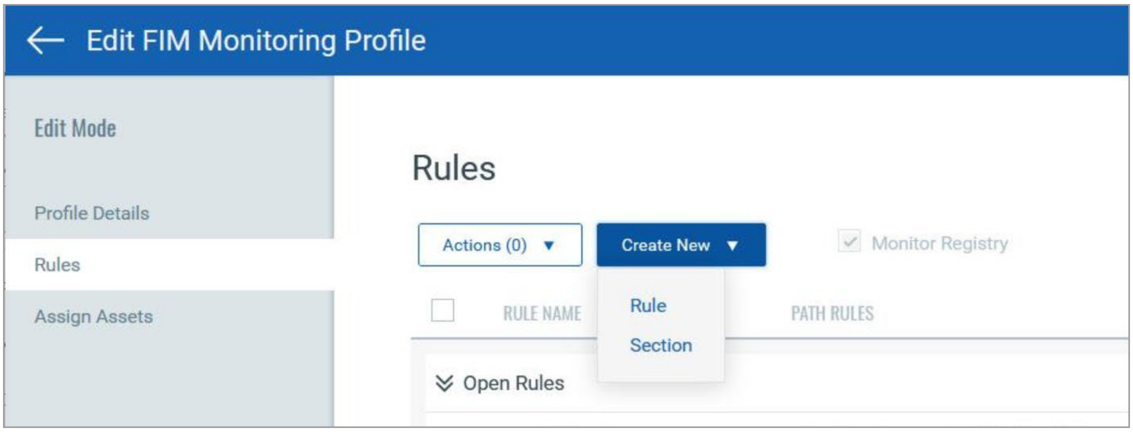
If you choose Directory/Registry Key as the Rule Type, you can click Advanced Options to include or exclude specific files/directories within that directory.



You can group the rules in sections. Create sections to group your monitoring rules. Go to the Rules tab and click New Section.

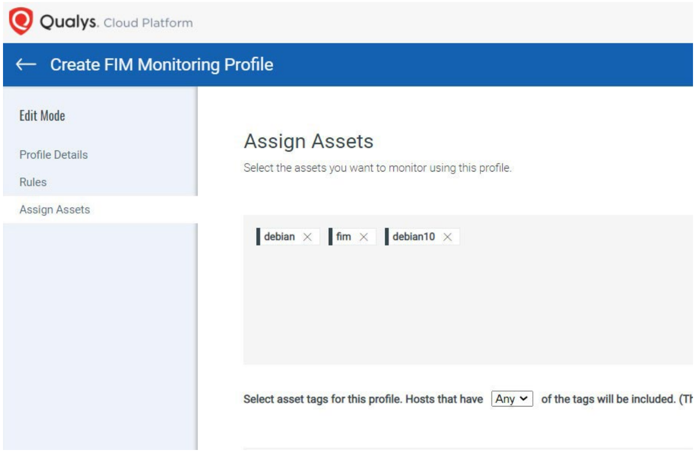
Note

It is mandatory for activated profiles to have at least one Rule or a Section with a rule in it. We show an error message if you try to 1) activate a profile that has no rule or section with a rule in it, 2) delete the only rule in the profile, and 3) remove the only section with rule.



Add assets to the profile. You can select individual assets in your account or assign asset tags in order to monitor all matching assets automatically.

We recommend you create asset tags and assign the assets tags to profiles if the number of assets to be monitored in the profile exceeds more than 50 assets.



To specify the assets to be included in the monitoring profile, use the **Any** or **All** option from the drop-down list.

The **Any** condition ensures that an asset is considered if it is included in any of the specified asset tags. Whereas the **All** condition considers an asset only if it is included in the scope of all the specified asset tags.

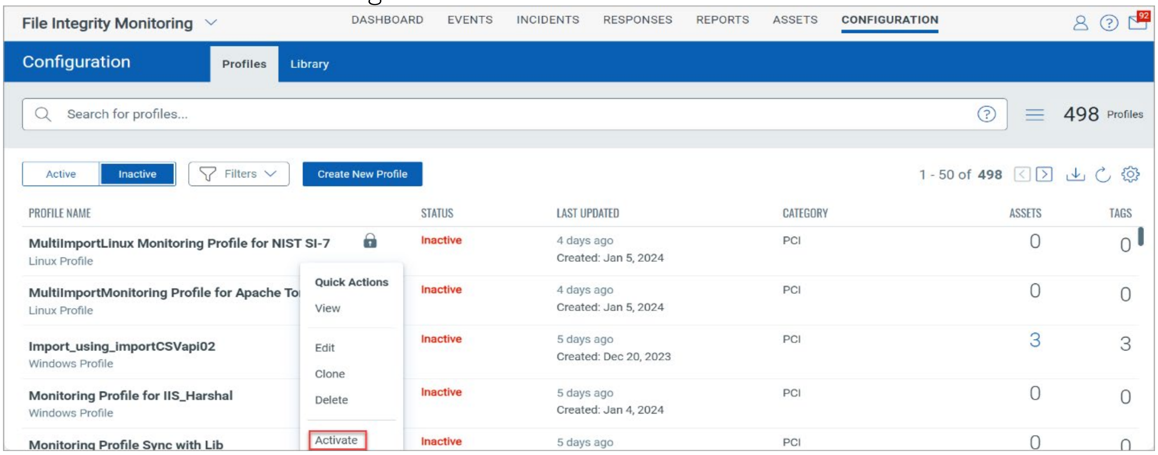
For example, you have two tags - 'HR_dept_Assets' and 'Finance_dept_Assets', and three assets in your scope - Asset1, Asset2, and Asset3. The 'HR_dept_Assets' tag is assigned to Asset1 and Asset2, and the 'Finance_dept_Assets' tag is assigned to Asset1 and Asset3.

You select the **Any** condition and then add the 'HR_dept_Assets' and the 'Finance_dept_Assets' tags for the profile you are creating. The profile rules will be applied to Asset1, Asset2, and Asset3, because an asset included in any of the specified tags will be included in the manifest.

You select the **All** condition and then add the 'HR_dept_Assets' and the 'Finance_dept_Assets' tags for the profile you are creating. The profile rules will be applied to Asset1 only, because only Asset1 is included in both the tags that you have specified.

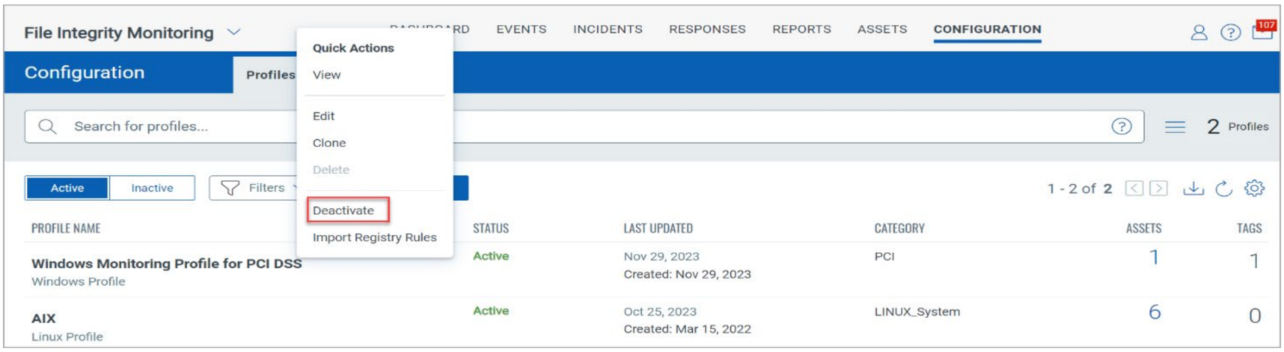
Activating a Profile

Activate your profile. New profiles are Inactive to start. Select the profile in the list and choose Activate to start using it.



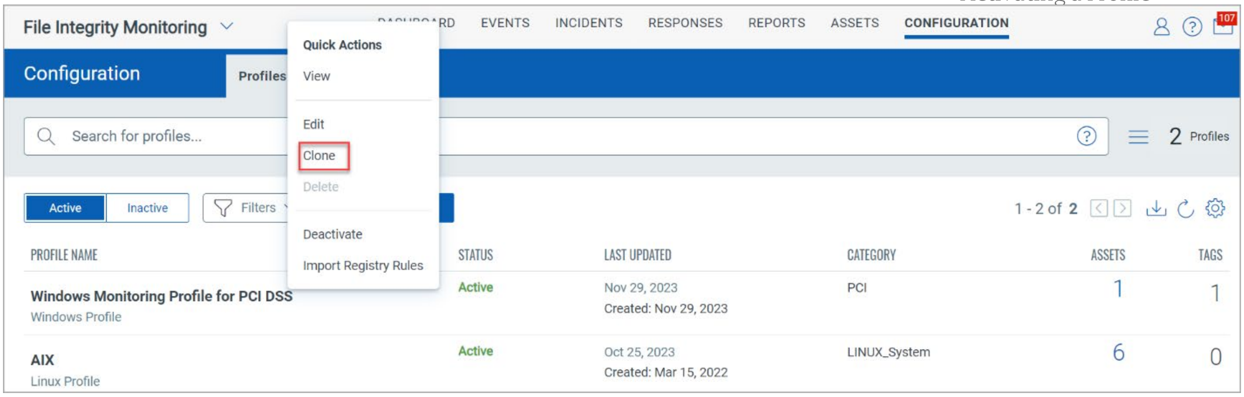
Deactivating a Profile

As mentioned earlier you must activate a profile to use it for monitoring. From the Profiles list, simply choose the action you want to take from the Quick Actions menu. Activate a profile to use it for monitoring; Deactivate a profile to suspend it from monitoring.



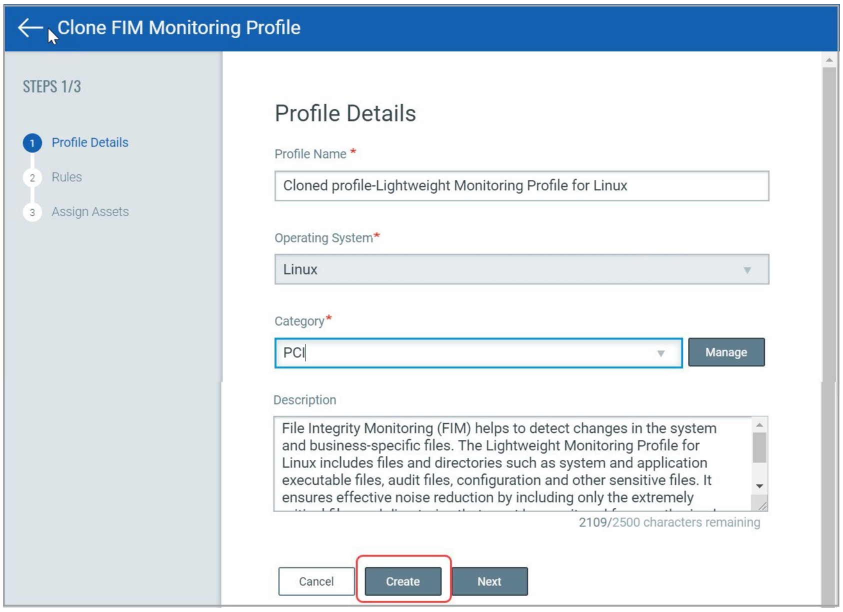
Cloning a Profile

You can copy a profile along with its rules. Select the required profile and from the Quick Actions menu click Clone.

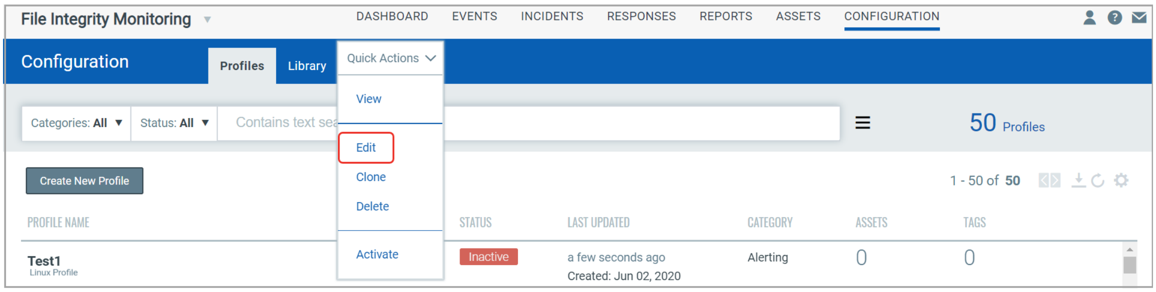


The Clone FIM Monitoring Profile page is displayed, and the Profile Name is prefixed with "Cloned profile". You can change the name, add Category and Description. Click Create to clone the profile along with its rules.

Note: You cannot change the Operating System of the cloned profile.



Select the cloned profile from the list and from the Quick Actions menu, click Edit.

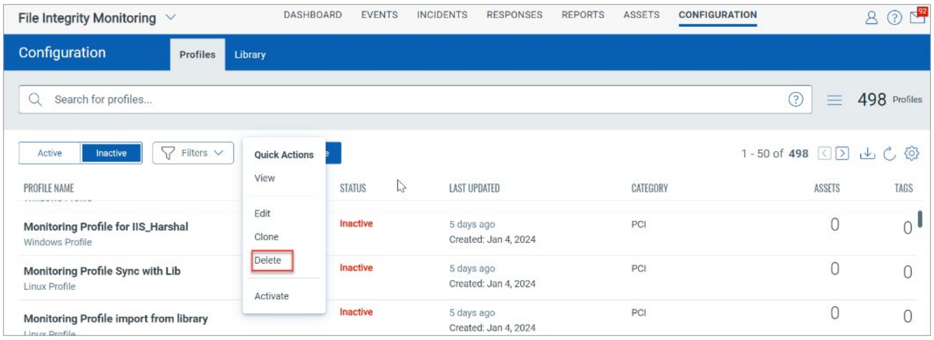


On the Rules page, edit the rules if required and click Next. On the Assign Assets page, add tags, assets, and click Save. To use the profile for monitoring, activate the profile.

Deleting a Profile

Select the profile from the list and click Delete from the Quick Actions menu. Then click Yes on the Delete Profile window.

Note: You can delete an active profile if they do not have tags or assets associated with it. However, to delete active profile that tags or assets associated with it, you must deactivate the profile first.


File Integrity Monitoring
DASHBOARD
EVENTS
INCIDENTS
RESPONSES
REPORTS
ASSETS
CONFIGURATION
Configuration
Profiles
Library
Search for profiles...
498 Profiles
Active
Inactive
Filters
Quick Actions
View
Edit
Clone
Delete
Activate
1 - 50 of 498
PROFILE NAME
STATUS
LAST UPDATED
CATEGORY
ASSETS
TAGS
Monitoring Profile for IIS_Harshal
Windows Profile
Inactive
5 days ago
Created: Jan 4, 2024
PCI
0
0
Monitoring Profile Sync with Lib
Linux Profile
Inactive
5 days ago
Created: Jan 4, 2024
PCI
0
0
Monitoring Profile import from library
Inactive
5 days ago
Created: Jan 4, 2024
PCI
0
0

Assigning a Profile to an Asset

Tip - If your profile has asset tags defined then there’s nothing you need to do. As long as the new asset has a tag that matches a tag in the profile it will use the profile automatically.

When you add a new asset, you can assign a monitoring profile to the asset by clicking on the Actions menu.

Windows Registry Integrity Monitoring

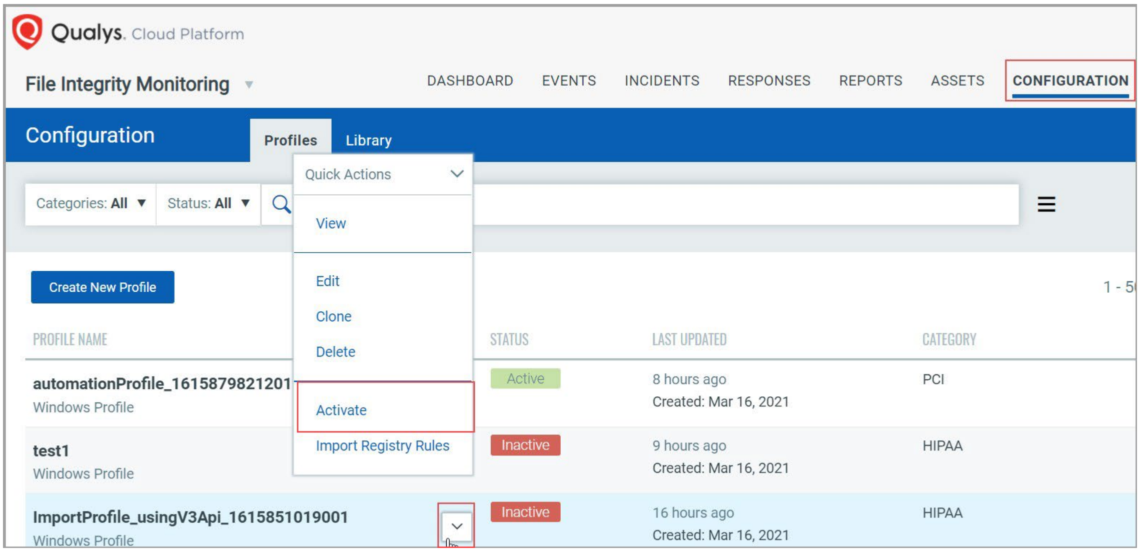
Windows registry provides rich information about the installed application and a store to persist the data.

Compromised integrity of the Windows Reg is a valuable indicator of the presence of malware or the system is compromised.

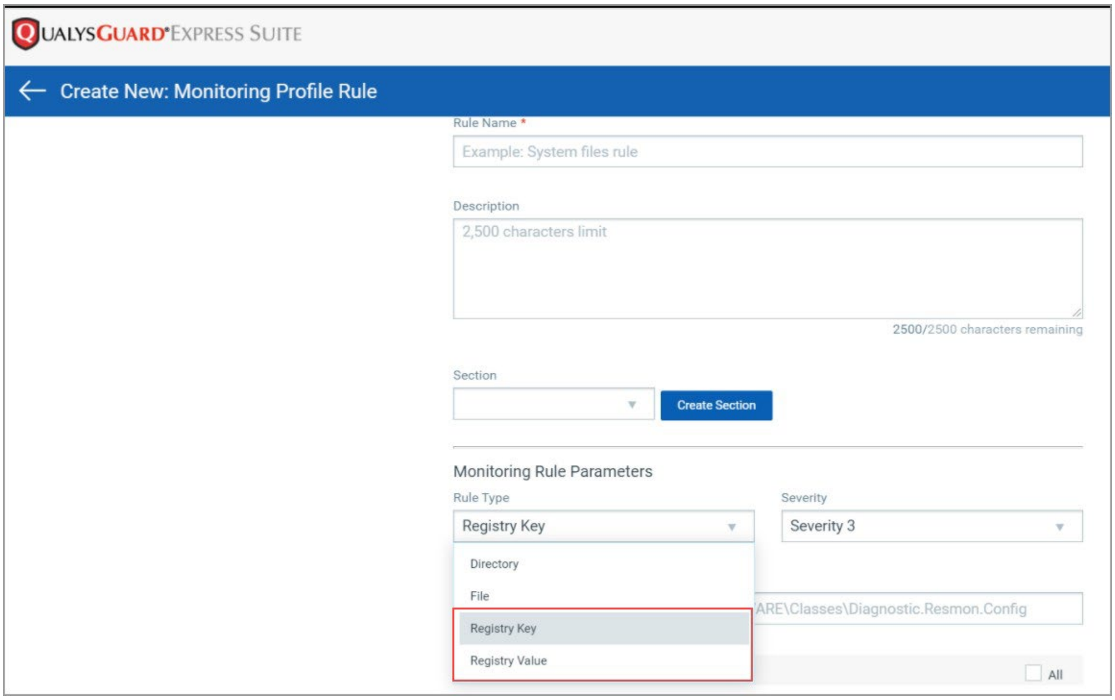
As Security Analysts, we need to have the capability to monitor the changes to the registry and determine if the integrity is compromised. Compliance standards such as PCI DSS, NERC CIP (CIP 010), FISMA, SOX, NIST (SI7), HIPAA, CIS controls, and GDPR mandates to have integrity monitoring solutions deployed on critical systems to be compliant.

Once an asset is installed from the cloud agent, activate the asset. You can view it under the Asset tab after activation.

From the Configurations tab, you can create a monitoring profile. For more information on creating a profile, refer to Creating a FIM Monitoring Profile.



While creating the rule, select Rule Type as Registry Key or Registry Value.



Selecting Registry Key as the Rule type:

Mention the Key path that you want to monitor. For example:
HKEY_LOCAL_MACHINE\SOFTWARE\<keyname>

Select the other attributes which you want to monitor and Save the rule.

Selecting Registry Value as the Rule type:

Mention the value you want to monitor. For example:
HKEY_LOCAL_MACHINE\SOFTWARE\<valuename>

Two attributes are available for the user to select: Value Removal (Deletion) and Value Write Changes (Content Change).

Also add data for Key Path and Value Path. Where in Key Path, enter the registry base path to be monitored and in Value Path, enter the value to be monitored.

For Registry Key Full Path -

HKEY_LOCAL_MACHINE and HKEY_USERS, only these two hives are supported for Registry monitoring.

For Registry Value Name -

Do not use these special characters / " < > | * ? in registry value name. Special characters allowed are [ ] {} ( )

Advanced Filters for Key -

Do not use these special characters / " < > | in key paths.

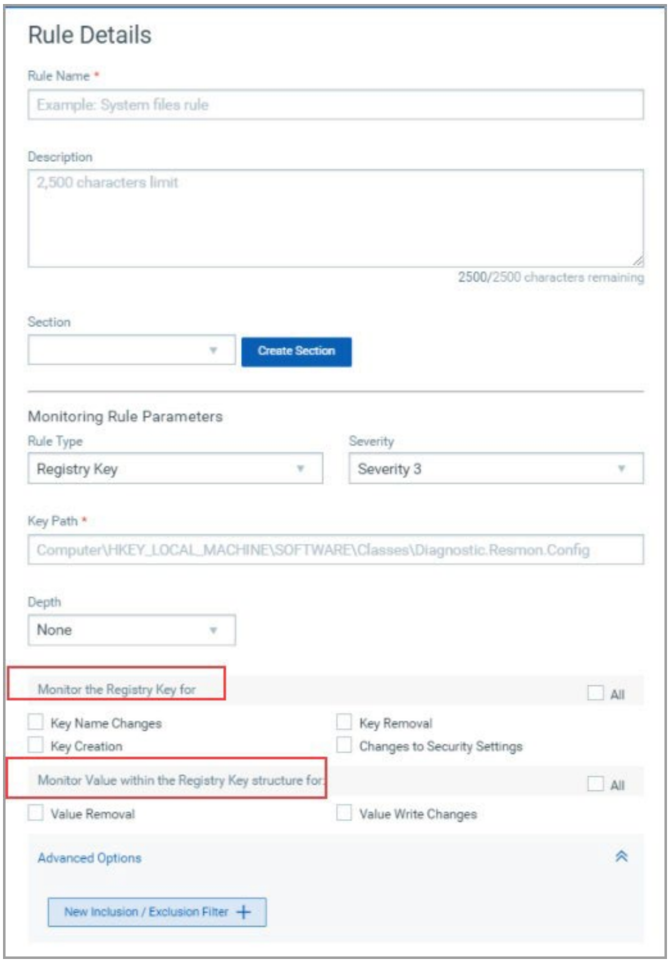
Although it can contain characters and numbers including spaces, slashes, commas(,) and [ ] {} ( )

Registry Keypath should not start or end with a slash (/).

Advanced Filters for Value -

Do not use these special characters / " < > | in file names. Special characters allowed are [ ] {} ( ) * ? ' (? is a single character wildcard, and * is a multi-character wildcard).

Can contain characters and numbers including spaces and commas(,).

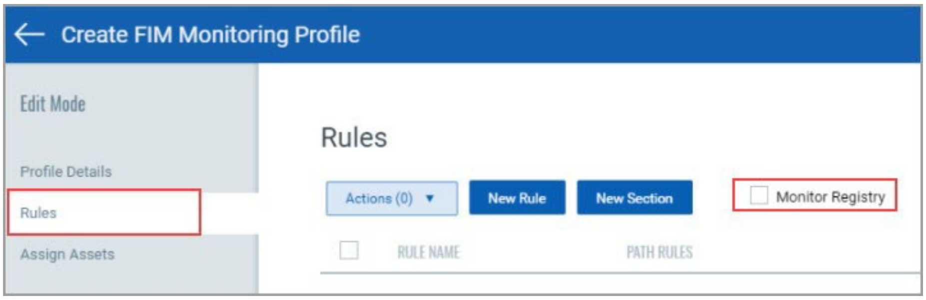


The newly created profile will appear as Inactive by default, Activate the profile.

Note: To activate a profile, user must have at least one rule defined.

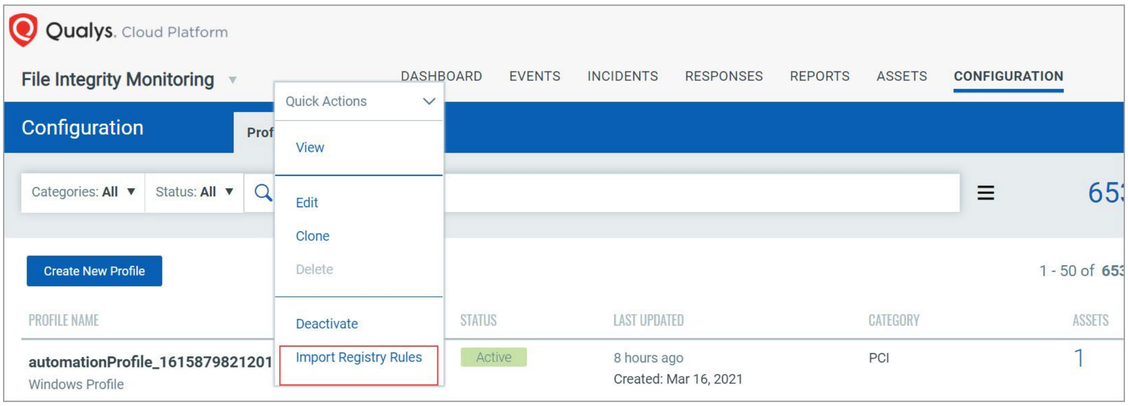
Instead of manually creating the rules, you can also import the rules from the library available.

- Select the option to **Monitor Registry** from the Rules tab and all the rules available in the library will be imported to your profile.



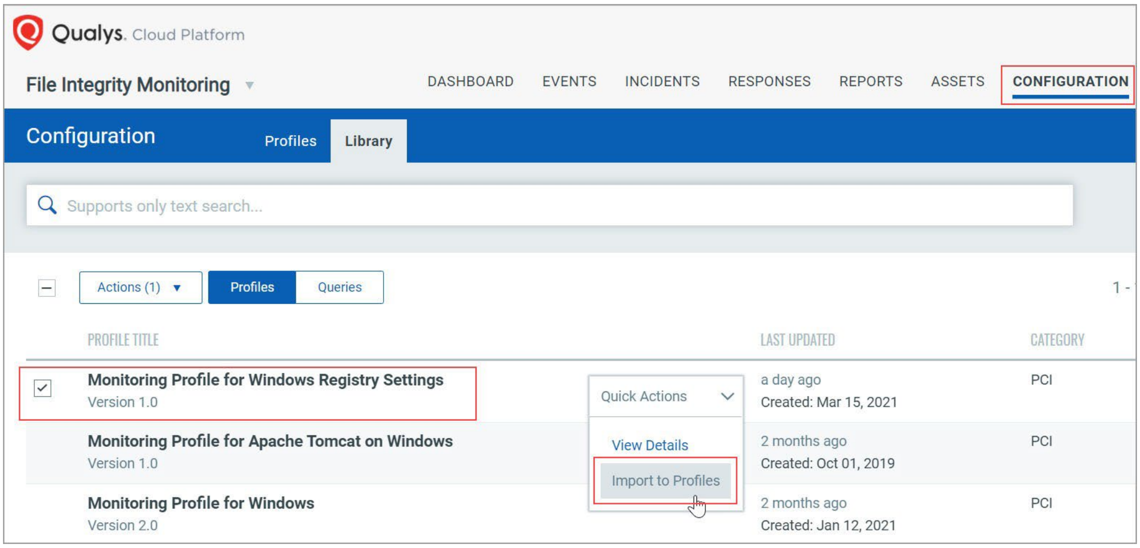
Don't forget to Save the profile after you select the option, as only after saving the profile your changes will be reflected.

- You can also select **Import Registry Rules** from the drop-down available in the Profiles tab.



For the profiles where the “Monitor Registry” check-box is already selected, the Import Registry Rules option will be disabled.

- You can also import the “Monitoring Profile for Windows Registry Settings” from the Library tab.



Once manifest is generated, it will start reporting the changes.

Any kind of activity that is marked to be monitored will be reported. You can view the events on the UI.

File Reputation Status

FIM enables users to know reputation status of files. Based on the file content hash, file reputation status is derived.

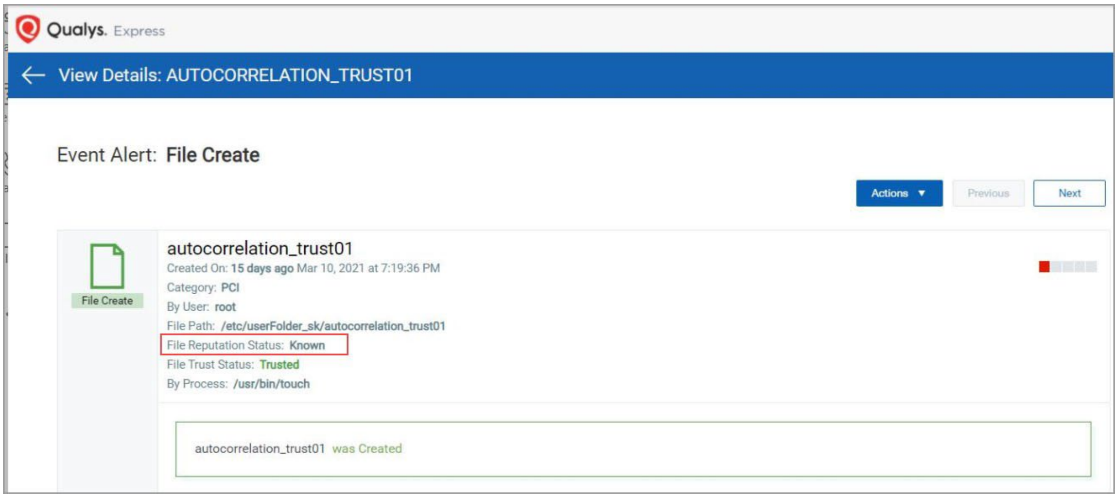
Reputation status of files can be seen in Events Details page for Events of type Create and Content. The source of Event Enrichment for File Reputation Status is Centralized Qualys Threat DB.

The file type can be any among: MALICIOUS/SUSPICIOUS/KNOWN/UNKNOWN/UNAVAILABLE.

Event Filtering is possible using the search tokens.

For Windows, it is applicable for PE files only and for Linux, it is applicable for all types of files.

Go to Events Details page to view the events in detail.

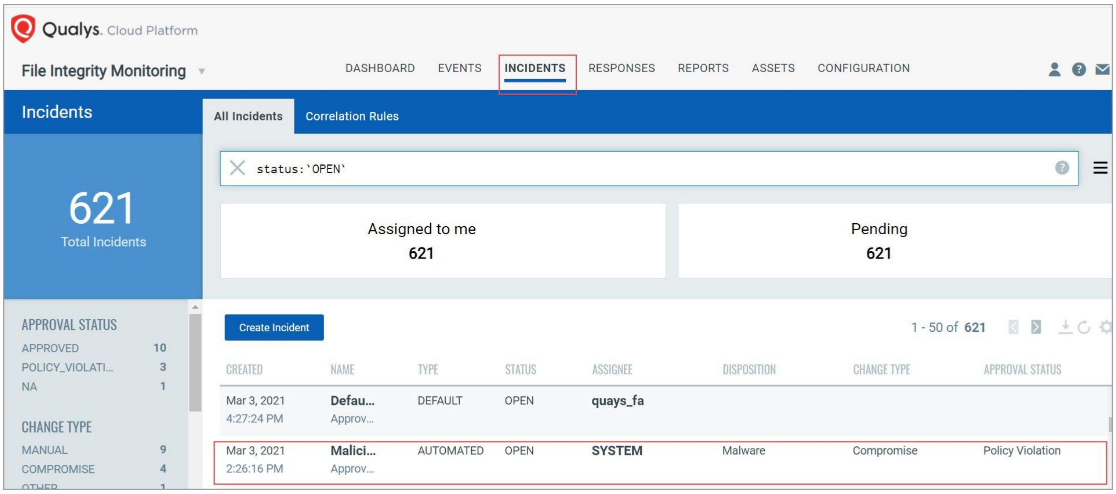


Automatic incident creation for malicious events

When FIM identifies the type of PE file reputation as Malicious in events details page, an incident is automatically created with below disposition details :

- Type: Automated

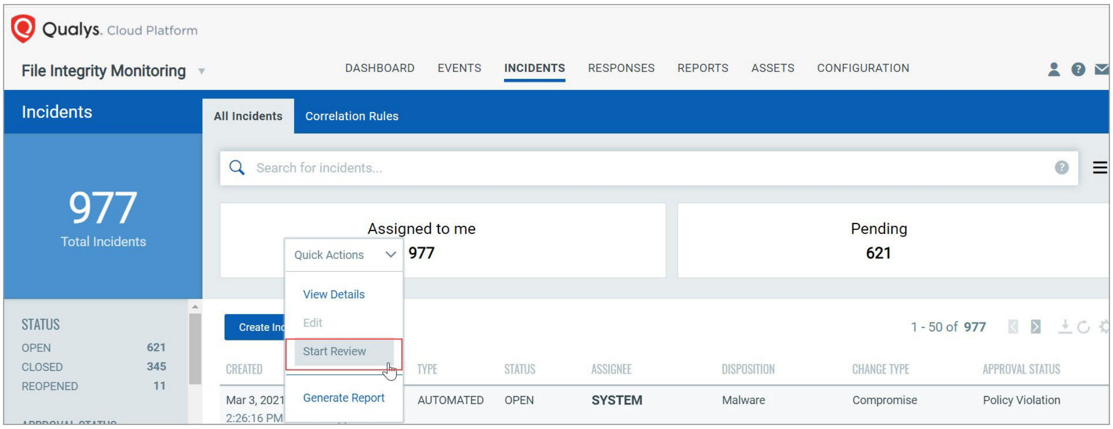
- Status: Open



This can be reviewed and appropriate action can be taken by the reviewer to close it.

Click on the drop-down arrow next to the Name of the incident to review it.

Select Start Review option to take required action the incident.



Incident review screen appears with severity and other important parameters that are required to take review actions.

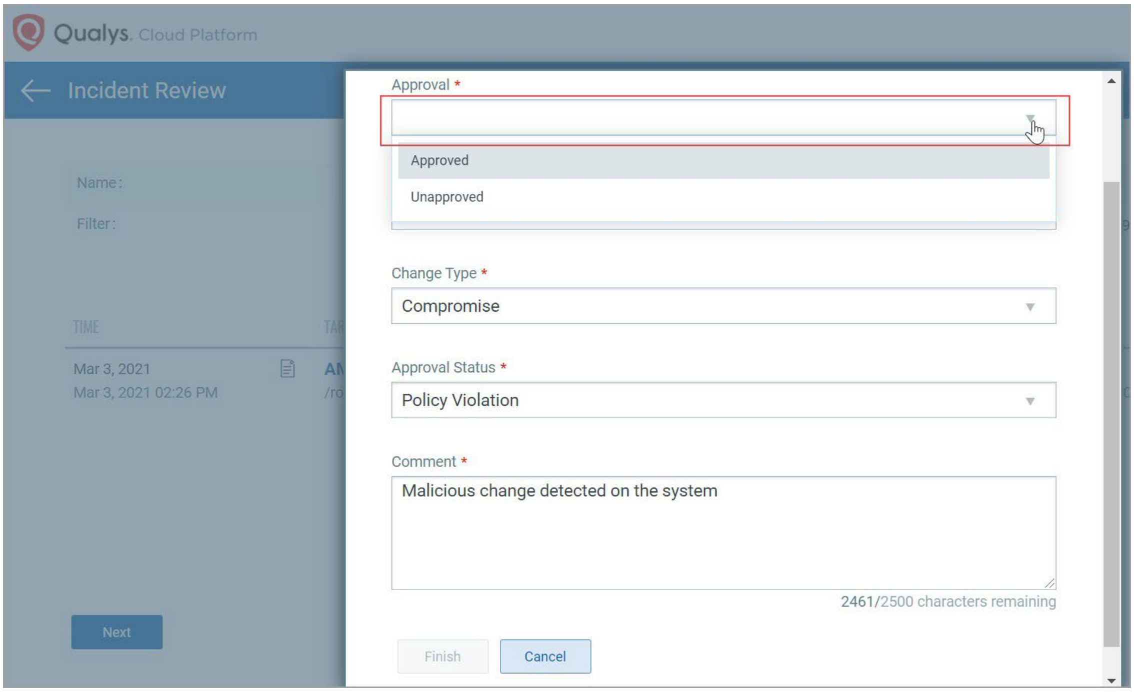
Click Next and select the appropriate approval status from the options available > click Finish to submit.

Other fields on the approval form will be auto populated with the following details:

- Disposition: Malware
- Change Type: Compromise

- Approval Status: Policy Violation

- Comment: Malicious change detected on the system



After you finish reviewing, the status appears as Closed on the Incident details page.

You can also perform other actions from the same drop-down, such as:

- View Details

- Generate Report

File Trust Status

FIM enables users to know whether a file was published by Trusted Source. Based on the file content hash, File Trust status is derived.

Trust status of files can be seen in Events Details page for Events of type Create and Content. The source of Event Enrichment for File Trust Status is Centralized Qualys Threat DB.

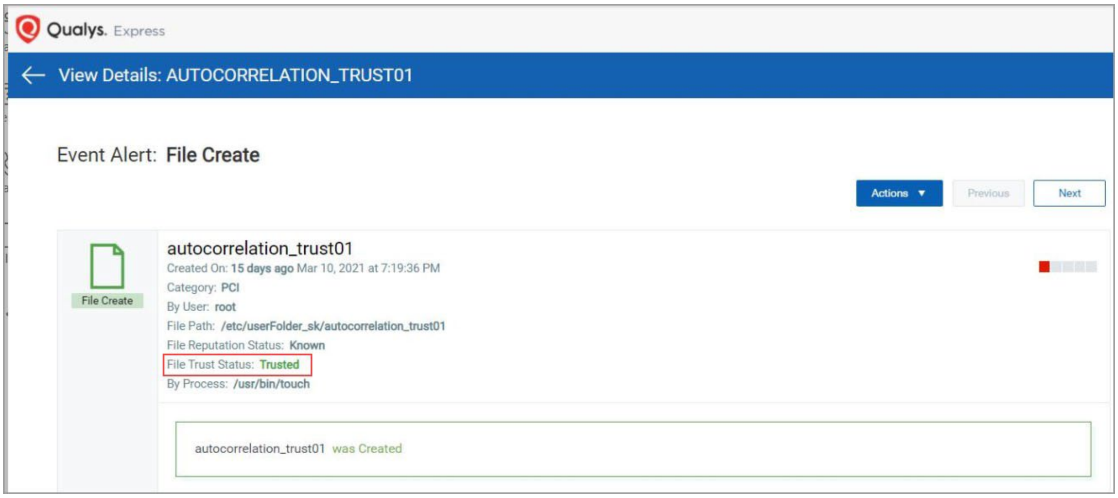
Possible values of trust status are: Trusted and Unavailable.

- TRUSTED: Indicates the file is published from a trusted source, for example Microsoft, Oracle etc.
- UNAVAILABLE: Status is not available in Centralized Qualys Threat DB.

Event Filtering is possible using the search tokens.

For Windows, it is applicable for PE files only and for Linux, it is applicable for all types of files.

Go to Events Details page to view the events in detail.



FIM Assets

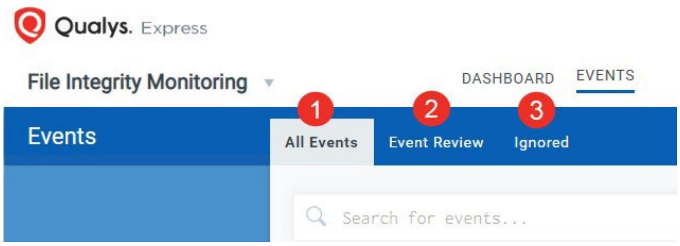
FIM provides one central location for viewing all of the events detected across all of your assets. The Events tab and the Assets tab contain search capabilities, group by options, and download options. In the Assets tab you can find all assets impacted by FIM events.

Use tabs in the Events section to quickly identify:

(1) All events detected across all of your assets, except ignored events.

(2) Events waiting to be reviewed. You can choose to ignore events or create incidents.

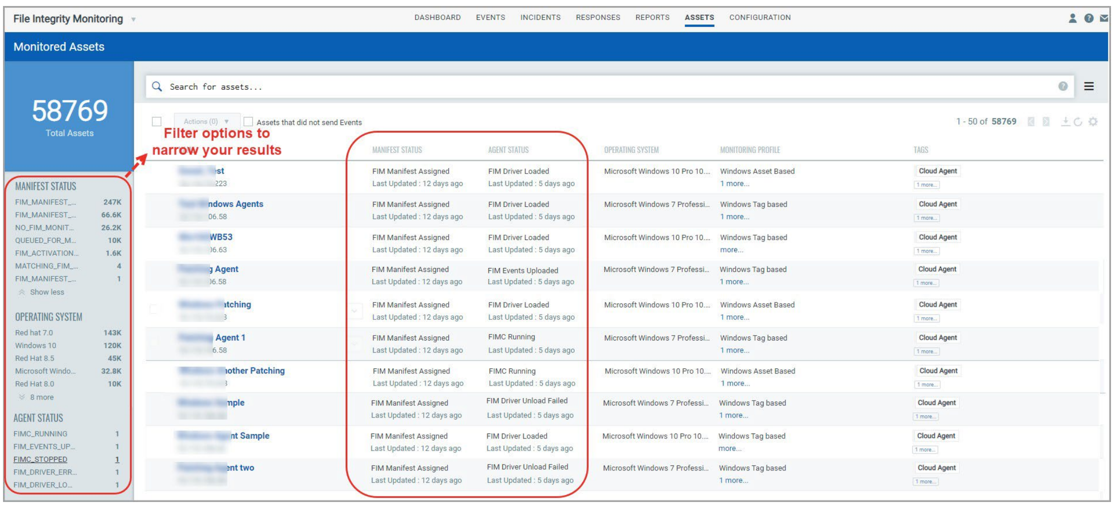
(3) Ignored events.



Note: To add a folder path for file.fullPath and actor.imagePath QQL, user should avoid using " \" at the end of the path as it results in invalid QQL while searching.

Viewing assets

You can find real-time assets based on the Operating System, Manifest Status, and Agent Status using the filters in the left-pane. The Manifest Status, and Agent Status columns also displays the time the status is updated.



Note: The QQL agentService.status: is not supported for FIM assets on AIX; hence, no data is fetched for AIX assets if you use this QQL and the **Agent Status** column does not display any data.

Manifest Status

As part of agent-status-core, 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:

- Manifest applied successfully
- Manifest application failed

Clicking **View Details** in **Quick Actions** for an asset shows complete information about the Asset impacted by FIM. Asset details can also be seen from the Events tab by clicking Asset Details for an event. This brings up details of the asset impacted by that FIM event.

Important: The following manifest statuses are not supported for AIX assets:

- FIM_MANIFEST_APPLICATION_FAILED

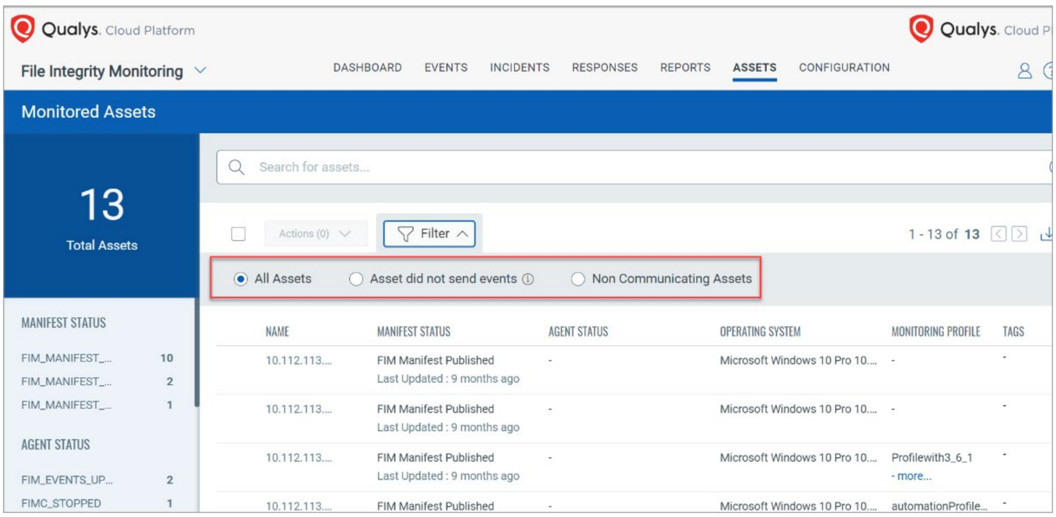
- FIM_MANIFEST_APPLIED_SUCCESS

- FIM_MANIFEST_ASSIGNED

- FIM_MANIFEST_ASSIGNMENT_FAILED

Filters

With **Filter**, you can filter out assets in three different categories. Following are the three filters.



Filter	Description
All Assets	All Assets shows the list of all assets
Assets that did not send Events	Select the **Assets that did not send Events** option and from the adjacent drop-down list, select the required duration. You can also filter the assets using tokens. For more information on tokens, see Asset Tokens.
Non-communicating Assets	The non-communicating assets enable you to view the list of assets that are non-responsive. These are the assets that have not communicated with the Qualys platform in seven days or more. These assets are highlighted with a tool-tip message and a warning icon. Note: We have an out-of-the-box dashboard widget for non-communicating assets. You can customize the widget for non-communicating assets based on your requirements. You can add the widgets to the dashboard to get a unified look of the non-communicating assets.

Scan Based Assets

Scan-based assets are the assets on which Qualys Agent cannot be installed, however, they can be monitored remotely with Qualys Scanner.

The scan-based assets page displays the asset details such as Name, Last Scanned Date, Technology, and Tags.

Scan-based assets are monitored via VM Scans. Hence Vulnerability Management is an integral part of this process of configuring scan based assets.

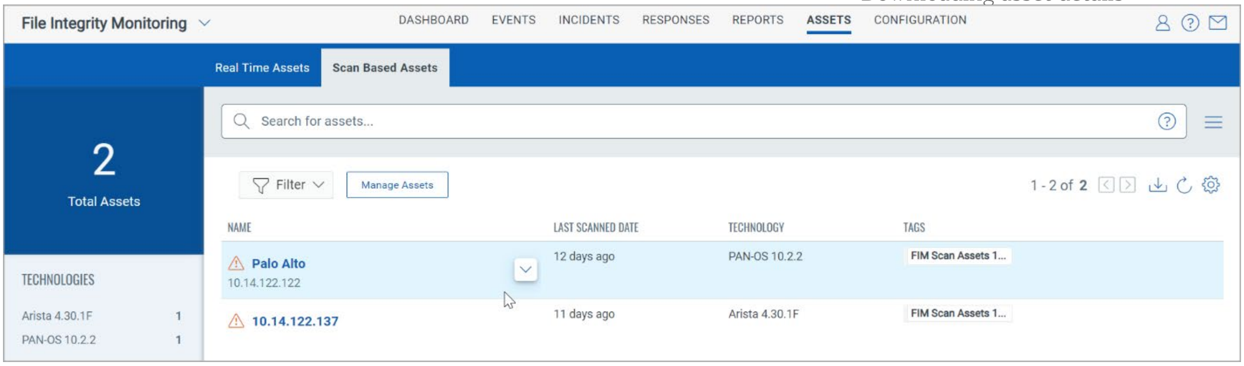
Pre-requisites:

- Enabled **Vulnerability Management** and **Global Asset View** along with the licensed or trial version of FIM. If you can see assets in Asset View but not in Global Asset View, kindly contact your TAM.
- Configure the Scan Schedule with the **Options Profile** and the Target Assets.
- The Minimum Vulnerability Signature required is VULNSIGS-2.5.991-2

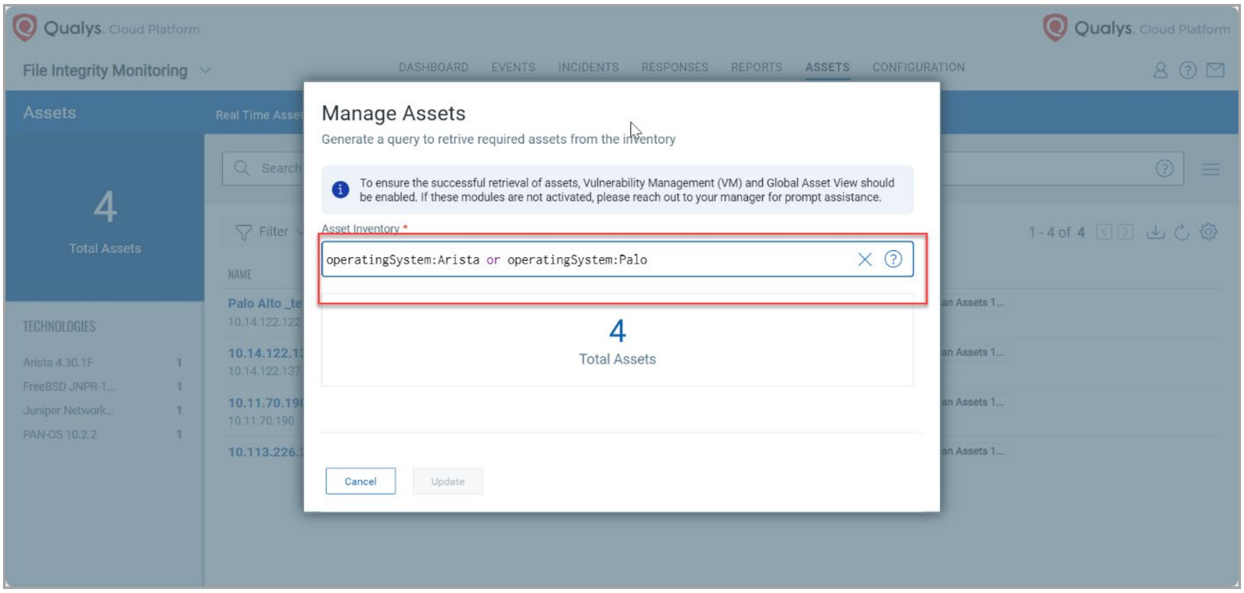
To monitor the scan-based assets for any network configuration change, you need to begin with the configuration of scan-based assets on FIM.

Configure the scan-based assets on FIM

1. Go to **Assets> Scan Based Assets**
2. Click **Manage Assets.**



3. Provide the QQL that will encompass the assets in your environment in the **Asset Inventory.** This QQL fetches the scan-based assets into the FIM Asset Inventory.

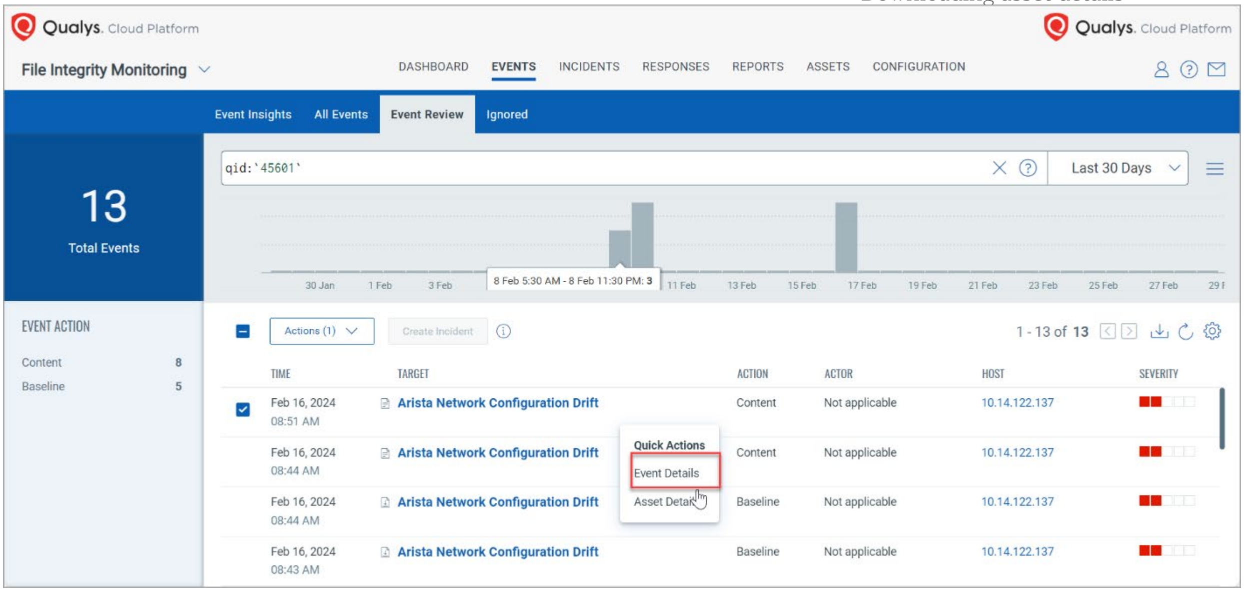


4. Click **Save. The assets will start coming in the FIM inventory.**

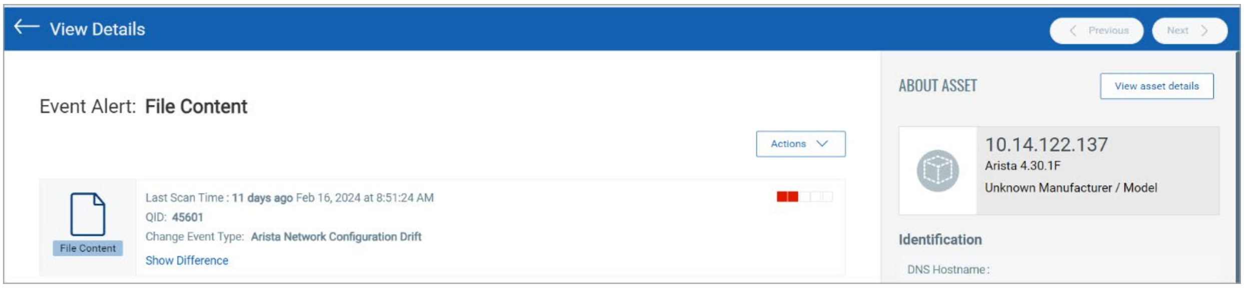
Once added you can see the scheduled scan results as events under **Events.**

To view the event details for the assets,

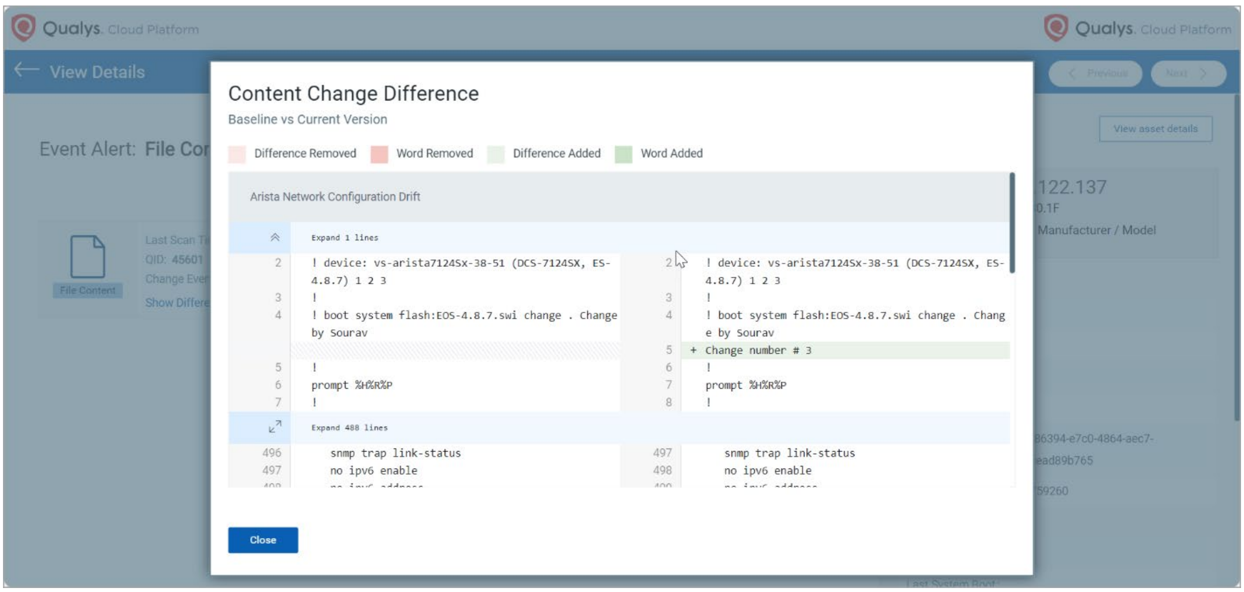
Go to **Events > All Events** and from the **Quick Actions** menu of the event, click **Event Details.**



Event Details page displays the details of the event.



To view the changes made in configuration devices click **Show Difference.**



Note: You can view the contents of baseline events.

You can make the event a baseline event.

Once you create the configuration of the scan-based assets then you must create the

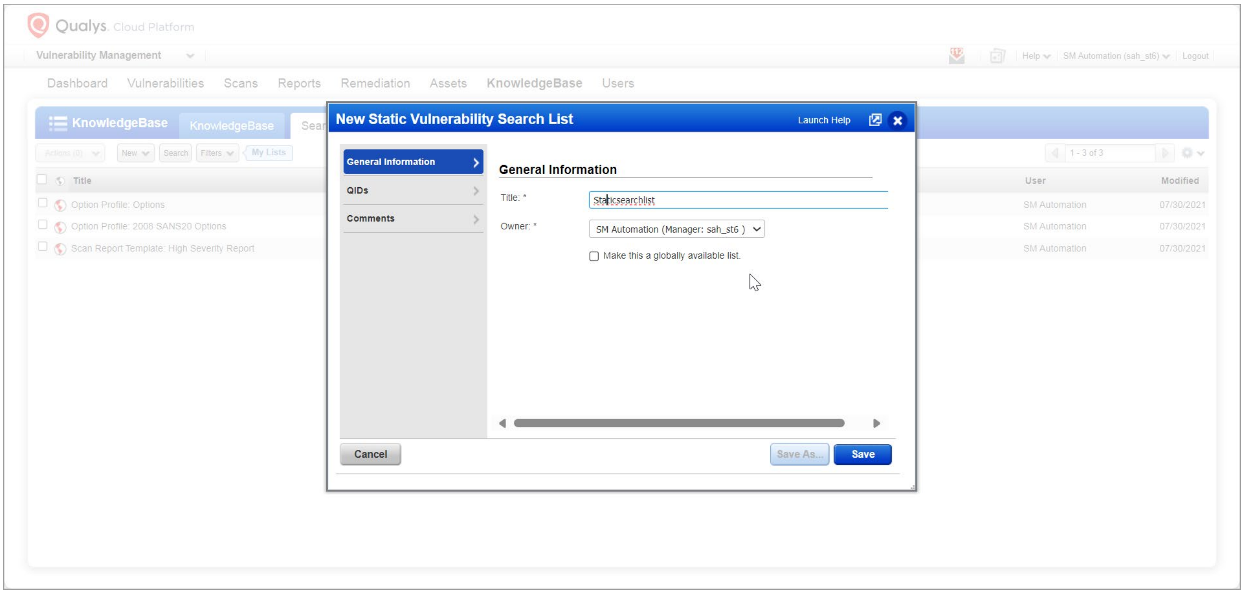
Search Lists, Option Profiles and configure the Scheduled Scan,

Next, go to the Vulnerability Module, create Search Lists, Option Profiles, and configure a scheduled scan.

Create Search Lists

1. Go to **VM/VMDR > KnowledgeBase> Search Lists> New> Static List.**

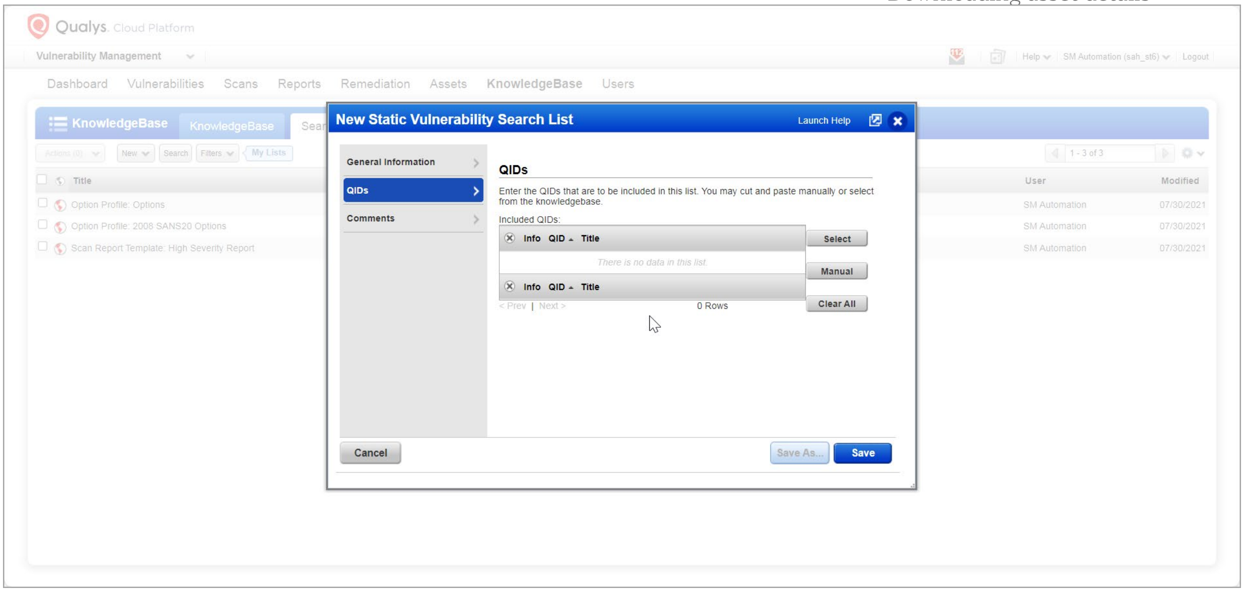
A tab pops up where you provide General Information like Title and Owner.



2. In QIDs, select the QIDs; Arista Device Configurations Detected (45601), Palo Alto Device Configurations Detected (45602), and Juniper Network Device Configurations Detected (45603).

We recommend you add QIDs for the assets with matching technology.

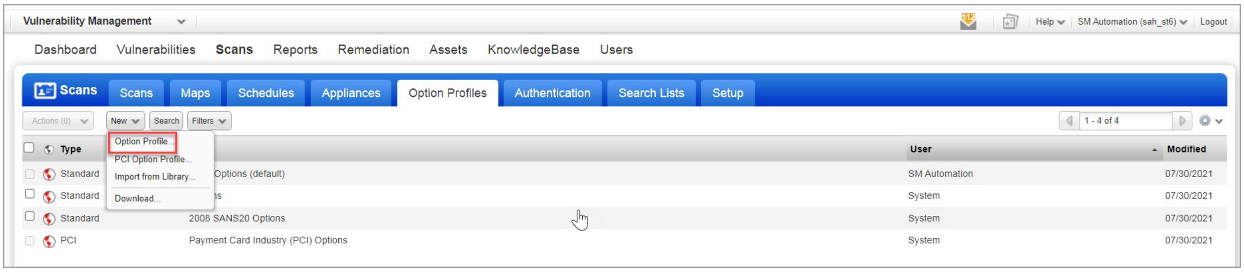
3. Click **Save.**



Your **Search List** is created.

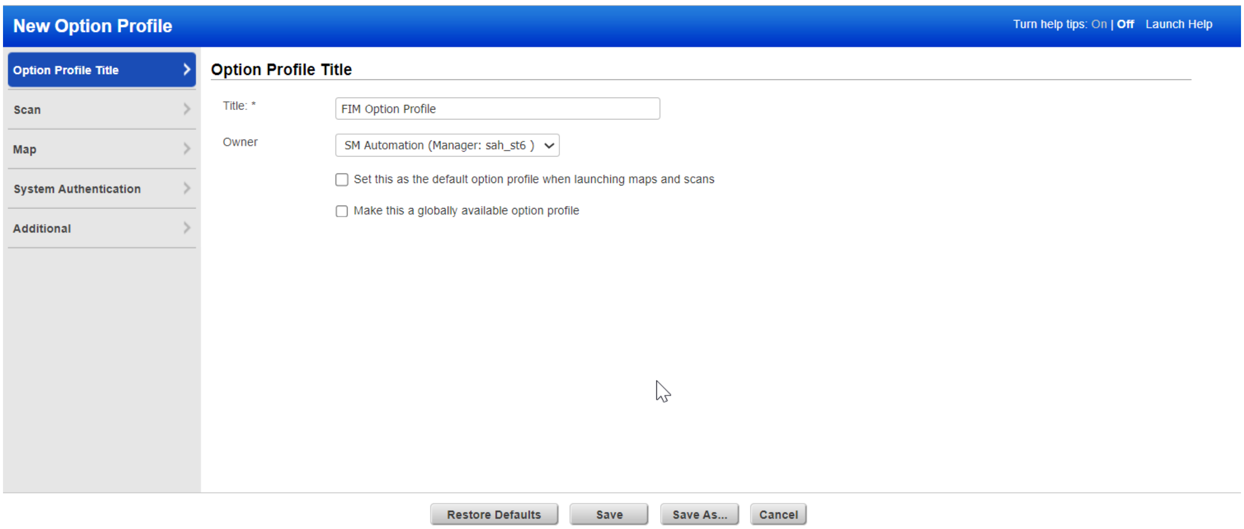
Create an Option Profile

1. Go to **VM/VMDR > Scans> Option Profiles> New> Option Profile**



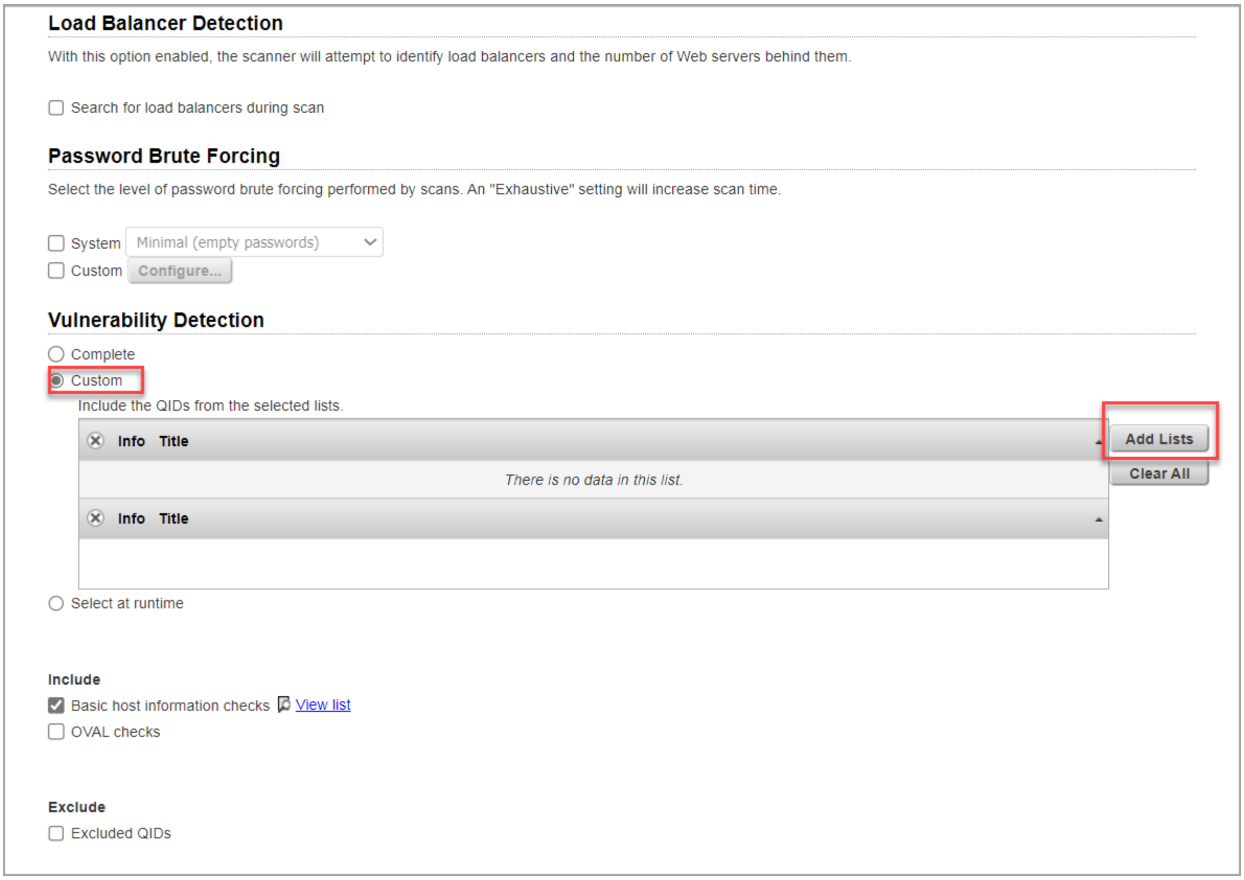
A New Option Profile tab pops up. Here provide the details like **Title and Owner.**

Click **Save.**



2. Go to **Scan.** Select **Custom** under **Vulnerability Detection** and **Add Lists.** You must add

the search list created by you.



3. Click **Ok** after adding the list.

4. Next, Under **Authentication** check **Unix/Cisco/Network SSH, Attempt least privilege for Unix and Palo Alto Network Firewalls.**

Note: It is important to check U**nix/Cisco/Network SSH and attempt the least privilege for Unix and Palo Alto Network Firewalls while creating Option Profile for scan-based assets**

5. Click **Save.**

Your **Option Profile** is created.

Configure a Schedule Scan

Let's Configure a Scheduled Scan,

1. Go to **VM/VMDR > Scan> Configure a Schedule Scan**

2. Next click **New Scan** and then from the quick actions menu click **Schedule Scan.**

New Schedule Vulnerability scan window pops up. Provide General Information
In the New Schedule Vulnerability Scan window, you provide the scan a title and select basic scan details like which option profile to use, and which scanner to use. Each option is described below.

Title : Give your scan a title to easily identify it later.

Task Owner: Provide the name of the Task owner.

Option Profile: Select an option profile for this scan job. The option profile has scan settings like which ports to scan, which QIDs to scan, and whether to use authentication. Pick the option profile you created from the list.

Processing Priority - If you have an important scan that you want to be processed before other scans, then you can prioritize it. Choose from nine priority levels with the highest priority being "1 - Emergency" and the lowest priority being "9 - Low". Scans with no priority will be processed after scans with priority. Get help choosing processing priority

Network - (Visible only when the Network Support feature is enabled for your subscription.) Select the network you want to scan. The Global Default Network is selected by default but you can choose a user-created network from the list.

Scanner Appliance - (Visible only when you have Scanner Appliances in your account.) If this option does not appear, then your scans will use external scanners automatically.

3. Click **Save.**

4. Next, select **Assets** that you want to monitor for configuration changes.

You can choose target hosts from **Assets** (IPs, asset groups, FQDNs) or **Tags**.

5. Choose Target Hosts from "Assets"

Select the **Assets** on which the scan needs to run**.**

6. Schedule the scans by defining the Start Time, Duration, Resume, and Occurs.

7. Click **Save.**

You configured a scheduled scan successfully.

Every time a scan runs you can see the entry under **Scans.**

Downloading asset details

You can download the asset details in CSV format. The following details are included in the report:

- Asset name

- Manifest status

- Agent status
- Operating System of the assets
- Profile
- Tags assigned to the assets

FIM Events and Incidents

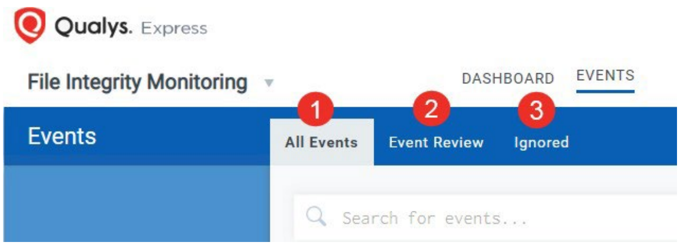
FIM provides one central location for viewing all of the events detected across all of your assets. The Events tab and the Assets tab contain search capabilities, group by options, and download options. In the Assets tab you can find all assets impacted by FIM events.

Use tabs in the Events section to quickly identify:

(1) All events detected across all of your assets, except ignored events.

(2) Events waiting to be reviewed. You can choose to ignore events or create incidents.

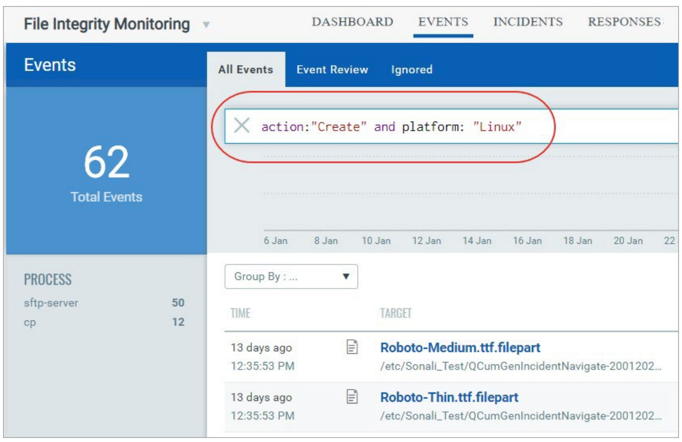
(3) Ignored events.



Note: To add a folder path for file.fullPath and actor.imagePath QQL, user should avoid using " \" at the end of the path as it results in invalid QQL while searching.

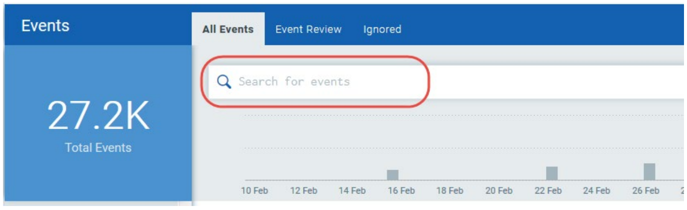
Viewing Events

You can find events based on event data, file information, monitoring profile, and more.

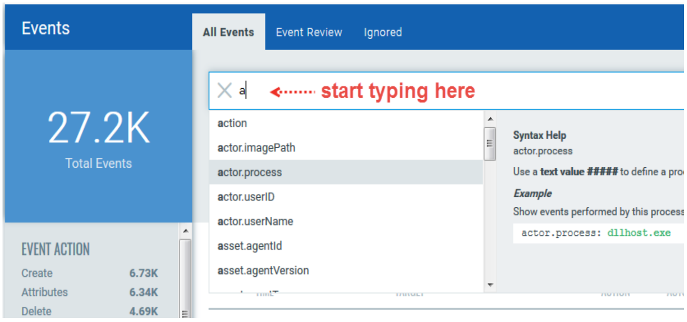


Searching for Events

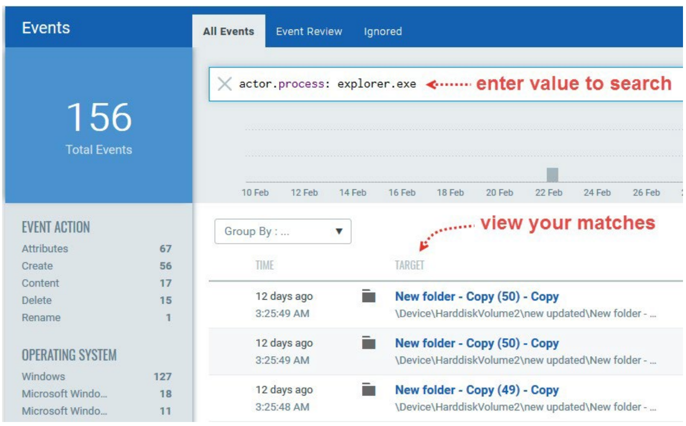
Our search capabilities give you the ability to quickly find events matching certain criteria. Here are the steps to search for events. Search for incidents and assets in a similar way.



You'll notice the Search field above the Events list. This is where you'll enter your search query.



Start typing and we'll show you the event properties you can search like actor process, asset hostname, profile name, etc. Select the one you're interested in.



Now enter the value you want to match, and click Search. That's it! Your matches will appear in your events list.

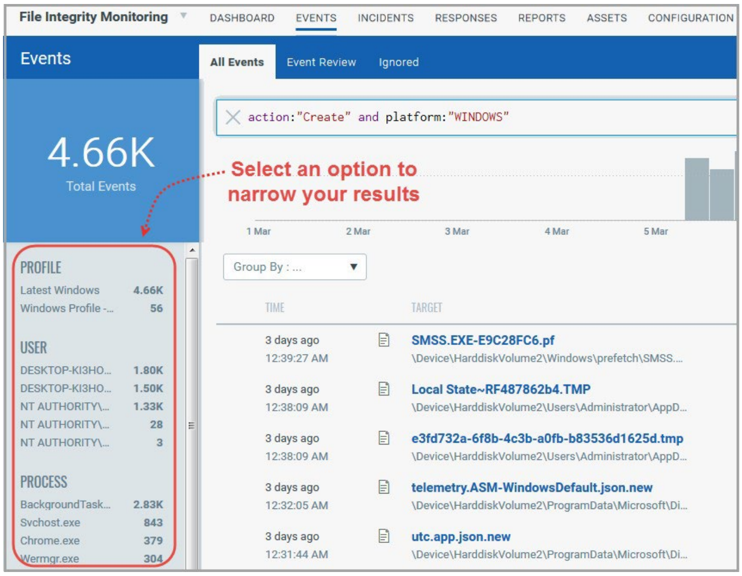
Tip - Go to the FIM online help for details on search language and sample queries.

Note

Date range for searching events should be less than or equal to 365 Days. That date range can be any year to any year, but difference between total number of days should be less than or equal to 365 days.

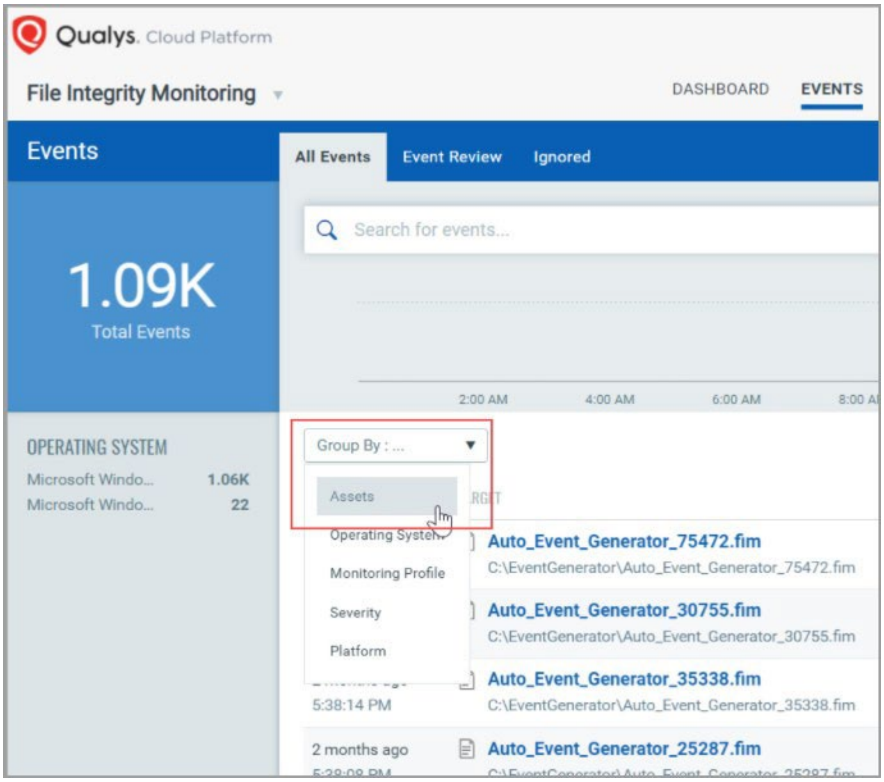
Narrowing your results

Once you have your search results you may want to organize them further into logical groupings. Choose a group by option on the left side. You'll see the number of events or assets per grouping. Click on any grouping to update the search query and view the matching events.

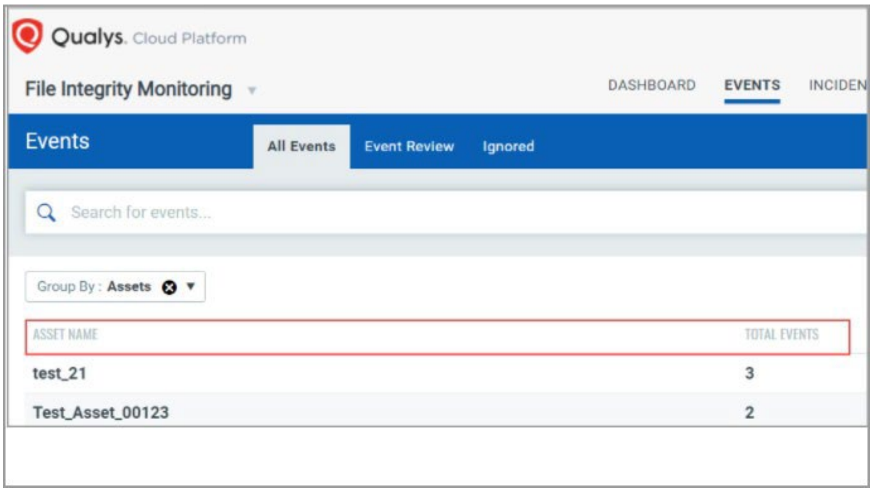


Grouping Assets

By using the Group By option, you can group similar assets under one list. Group by Assets option bring up maximum of 1000 assets without pagination option.



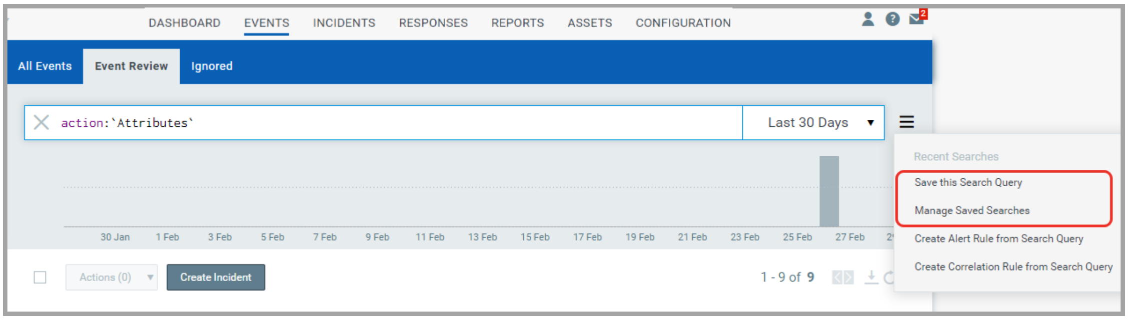
You can view event details with Asset Name and count of Total Events for that asset.



Saving and Managing Search Queries

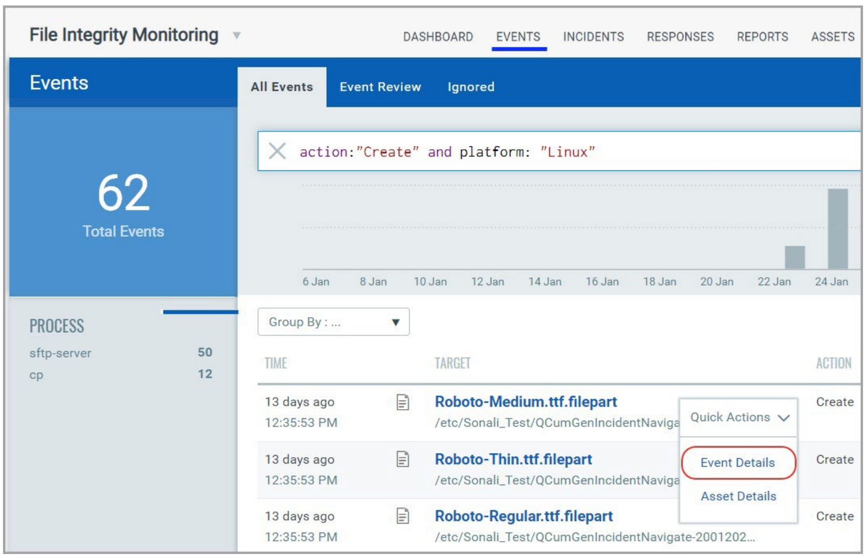
When you are searching for events in the All Events and Events Review tab, you can save these searches using the "Save this Search Query" option. Saved searches are available under "Manage Saved Searches" option.

Note: If you cannot see the saved search under the Manage Saved Searches option, press F5 or refresh the screen.



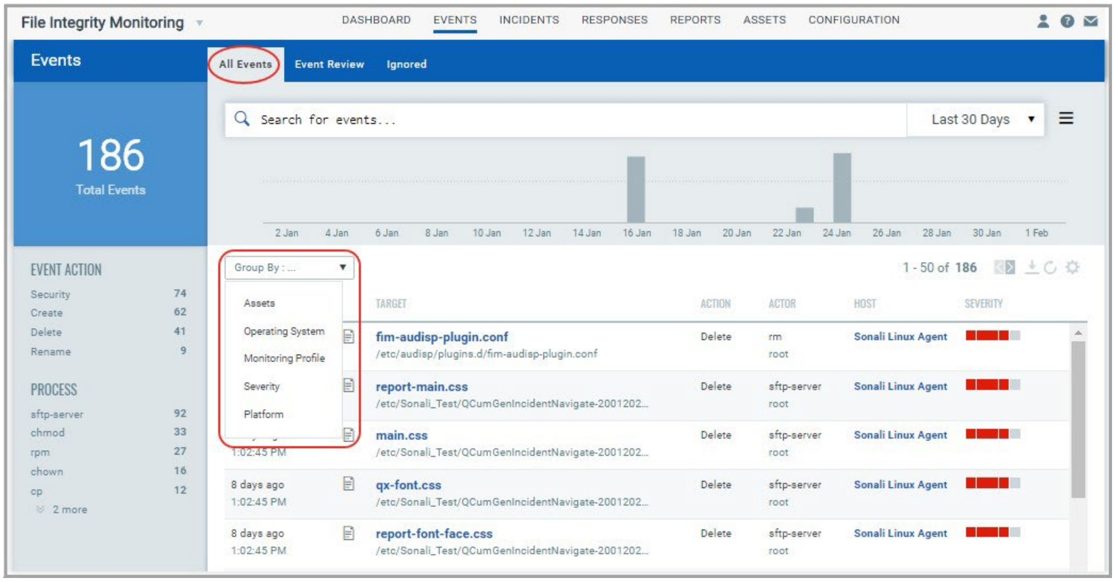
Viewing Event Details

Clicking Event Details in the Quick Actions for an event brings up the Event Details page. This page provides complete information about the FIM event



Note: The QQLs actor.process, actor.UserID, actor.UserName, actor.imagePath are not supported for FIM assets on AIX, hence no data is fetched for AIX assets if you use these QQLs and the **Actor** column does not display any data.

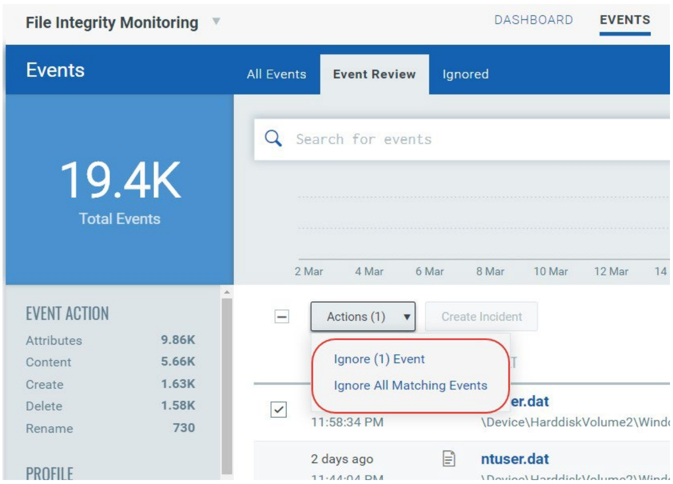
Grouping events by filters to get event count



You can view the total count of events by Assets, Operating System, Monitoring Profile, Severity and Platform in the All Events tab. To view the count of FIM events by any of the filters, go to Events > All Events tab, select a date range and select a filter from Group By drop-down.

Ignoring Events

Have an event you don't need to track? Ignore it to move it out of your list.Select specific events and choose Ignore Events from the Actions menu. Optionally, choose Ignore All Matching Events to ignore all events that are currently matching your query for the timeframe that you've selected. Ignored events are moved to the Ignored list. Note - You may get similar events in the future that will appear in your Events list and you'll want to ignore those too.



Did you ignore an event by mistake? No worries. Easily restore any ignored event from the Ignored list.

Correlation Rules for Incident Creation

We can help you automate the incident creation based on a QQL rule query 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 events that matched the rule query.

Through auto correlation rules, incidents will get created when there is an event created that matches the Incident criteria. The correlation rule wizard also provides you an option to create alerts for the incidents that are created for this rule.

You can access the correlation wizard from the following pages:

1) Go to Incidents > Correlation Rules tab.

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

Note: After you upgrade the Cloud Agent to 4.1 and above, the File Path is displayed as (c:\directory\sub-directory\file.ext). If all the agents in your subscription are not upgraded to 4.1 and above, edit the existing QQL queries to add the new File Path format along with the old one.

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.

Note: For events with 'reputationStatus' as 'MALICIOUS', an Automated Incident will be created with below configuration:

- Disposition = Malware

- Change Type = Compromise

- Approval Status = Policy Violation

- Start review option will be available immediately.

Creating a correlation rule using correlation rule wizard

Provide the correlation rule name and description. Enter a rule query. When the rule is triggered, the events matching the rule query are picked and added to the incidents. Optionally, use the Choose from my saved searches option to select a search query. We also provide a Query Library from which you can choose predefined queries.

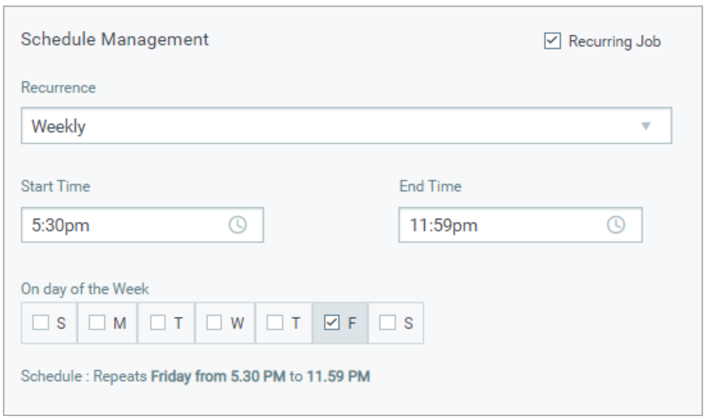
Scheduling a rule

Next, select the schedule to indicate when and how often you want to run the rule. By default, the rule will be run once. Schedule the rule by choosing a date, a start and end time. To set a recurring schedule, select Recurring Job check box. You have the option to schedule the rule to run daily between a specified time, every week or every month on chosen days 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 15 minutes from the current time for a job to get picked up. If you choose a Start Time less than 15 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.



Choosing the review options for the auto-created incidents

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.

Creating an alerting rule for incidents

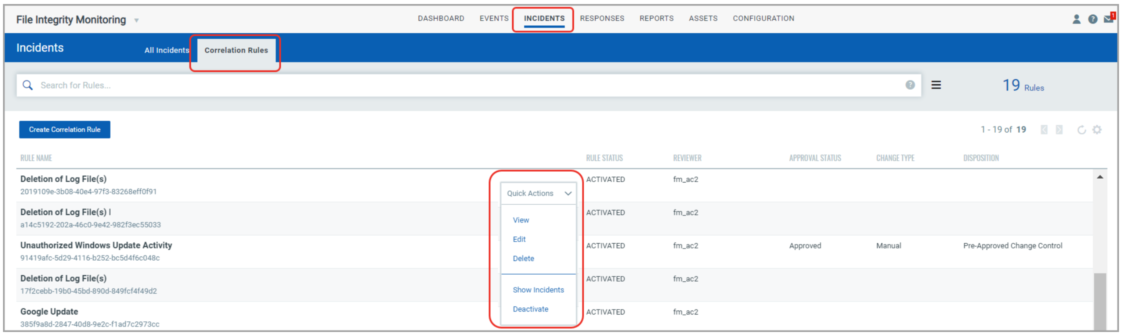
While saving a correlation rule, the Correlation rule wizard gives you an option to create alerts for the incidents created for a correlation rule.

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: The option to create an alerting rule is available only when you create a new correlation rule.

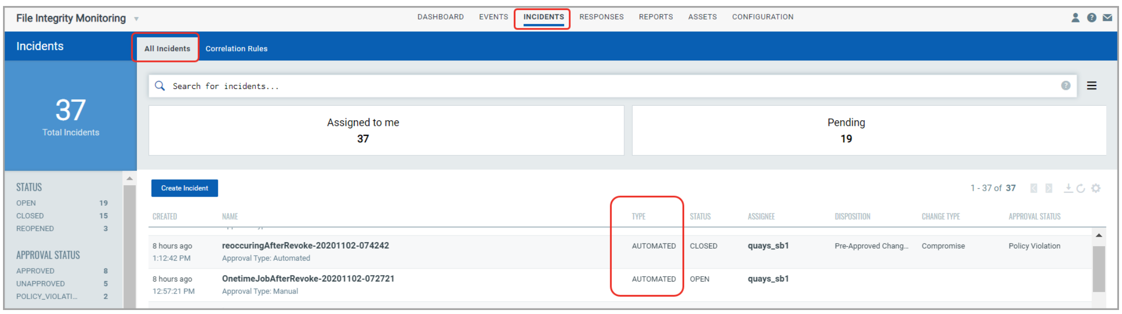
Managing Correlation Rules

The **Correlations Rules** tab lists all the correlation rules. The page shows details such as the name of the rule, rule id, 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.



Managing Incidents

All the incidents generated for a correlation rule are listed in the All Incidents tab with type as "Automated". Note that you can not delete incidents that are generated for a correlation rule. Activate/deactivate option will be available for correlation rule that has a recurring schedule.



Reviewing Incidents

An incident generated for a correlation rule is available for manual review after a grace period of 10 minutes from the scheduled end time of the rule. The “Start Review” option on the Quick Actions menu will be available for the incident after the grace period ends.

Creating and Tracking Incidents

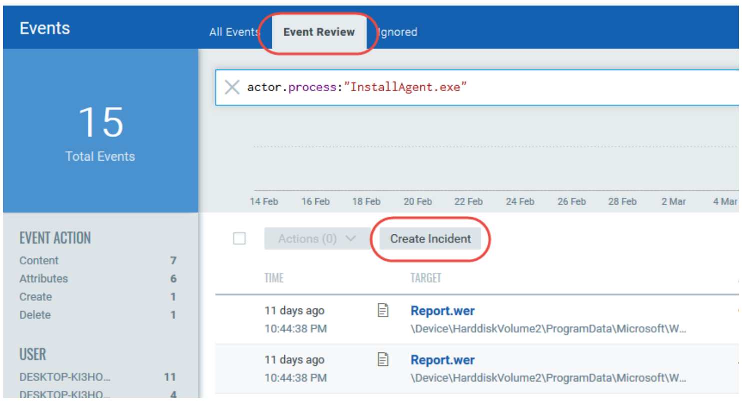
You’ll want to review the events detected on your assets and group related changes into incidents. Review your incidents to determine if they’re valid, mark them approved or unapproved and classify them by the type of change.

You also have an option to create incidents based on certain criteria defined in a correlation rule. See “Creating a correlation rule using correlation rule wizard.

Creating incidents from the Event tab

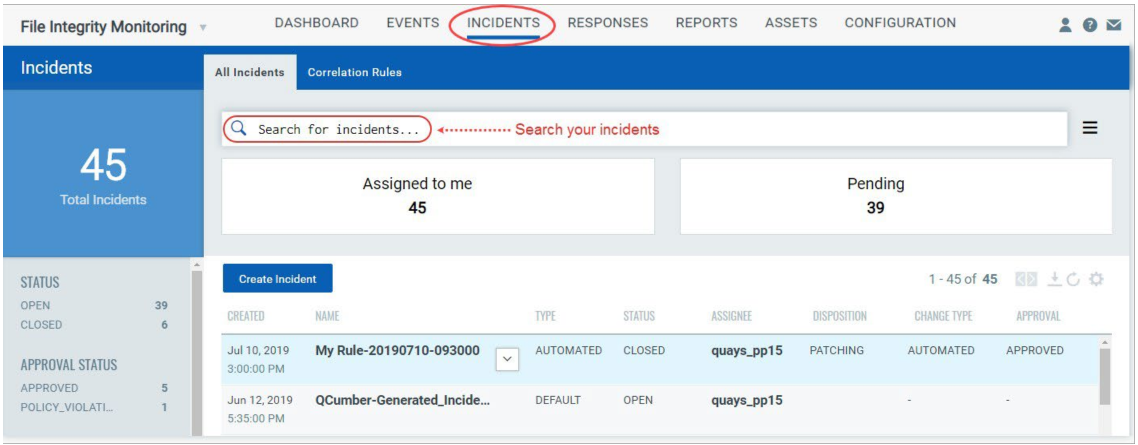
On the Event Review tab, run a query to find related events, click Create Incident and give your incident a name. Your new incident will be saved on the Incidents list where you can view and add details. All events matching your query will be included.

Note: The Create Incident option is enabled only after you enter a valid QQL query in the search bar.



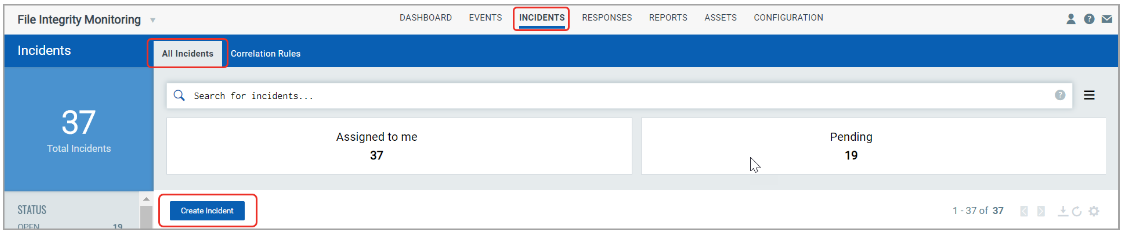
The Incidents list is where you’ll take actions on your incidents. View details for any incident to get a break-down of the events by severity, action and user. Edit any incident to rename it or change the events associated with it by modifying the query or timeframe.

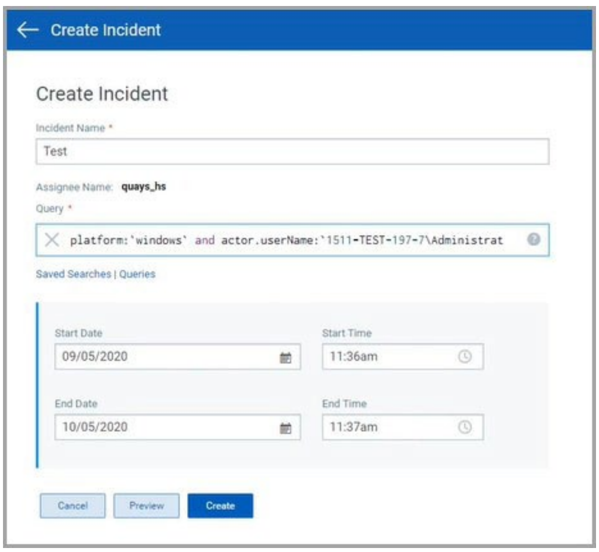
Note: After creating an incident manually, Events are marked to the incident after 24 hours.



Creating Incidents from the Incident tab

To create manual Incident, click Incidents > All Incidents > Create Incident.





Note: In Query field, to add a folder path for file.fullPath and actor.imagePath QQL, user should avoid using “ \” at the end of the path as it results in invalid QQL while searching.

On the Create Incident page, add the following details:

-- Incident Name: The name of the Incident.

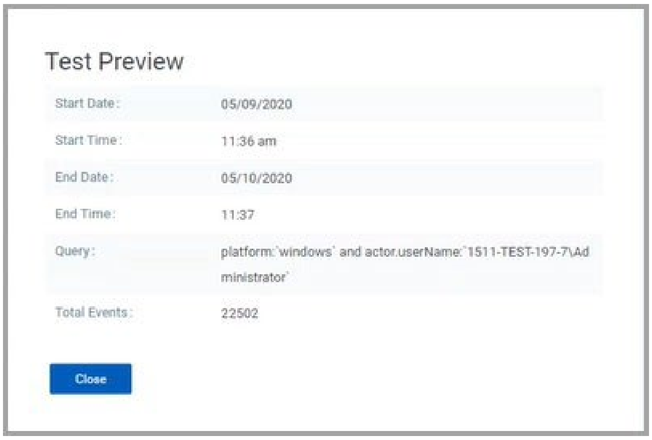
-- Query: Enter your QQL search query to find events. You can also select the required QQL query from the Saved Searches or Queries option.

-- Enter Start Date and Start Time and End Date and End Time: The duration for which you want to capture the events based on the QQL query.

Note: The End Date and Time should always be before or equal to the date and time you are creating the incident.

Click on the Preview option to see the total number of events that are generated based on your query. Click Close after you have reviewed the details.

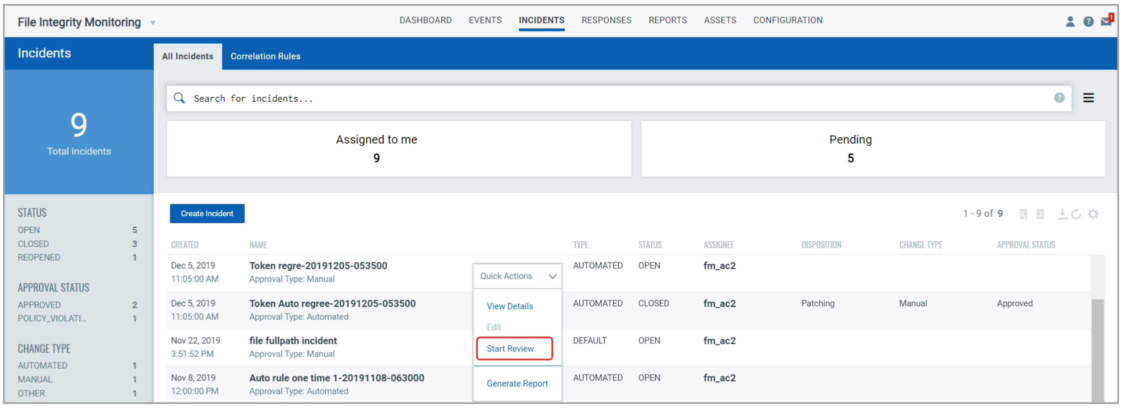
Note: You can create an incident only if there are events matching to your QQL query.



Click Create. The new incident is listed on the Incidents tab for a manual review.

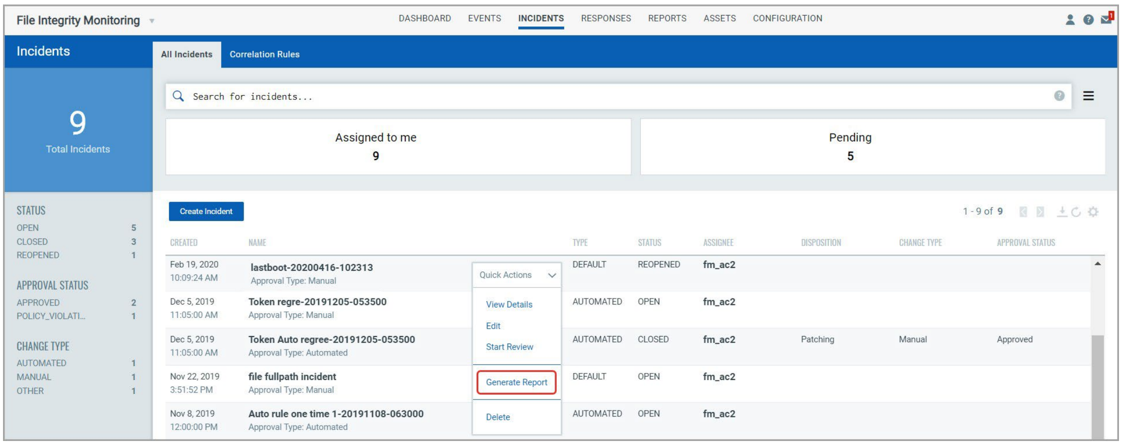
Reviewing incidents and taking action

Choose **Start Review** to review the events associated with an incident and then mark the incident Approved or Unapproved. You’ll also classify the events by disposition category (e.g. Pre-Approved by Change Control, Patching, Data Corruption, Human Error, etc.) and indicate the type of change (e.g. Manual, Automated, etc.)

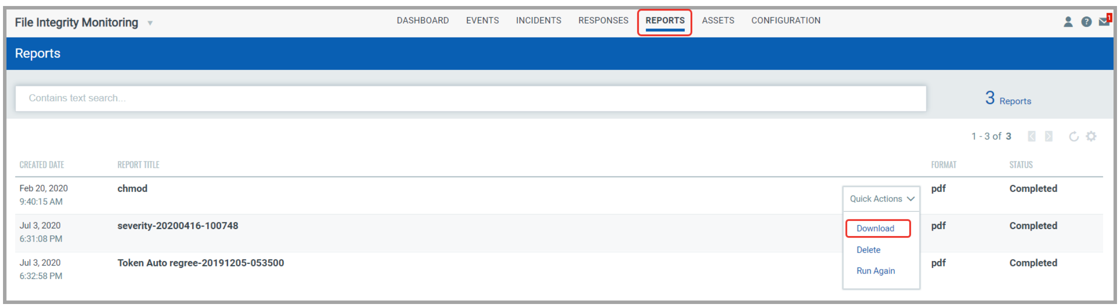


Generating Reports for Incidents

Select an incident and click “Generate Report” from the Quick Actions menu. Select PDF/HTML format and click Download.



The report is created for the incident and placed in the Reports tab. Go to the Reports tab and download the report. You can download report only if the status of the report is completed.



Report Status

When you submit a request for generating a report, FIM assigns the following status to the report which you can see in the Report tab during different stages of its processing:

- Accepted: The request for generating the report is accepted.

- Processing: The report generation is in progress.

- Completed: The report is generated and is available for download.

- Failed: Report generation process failed due to some reason.

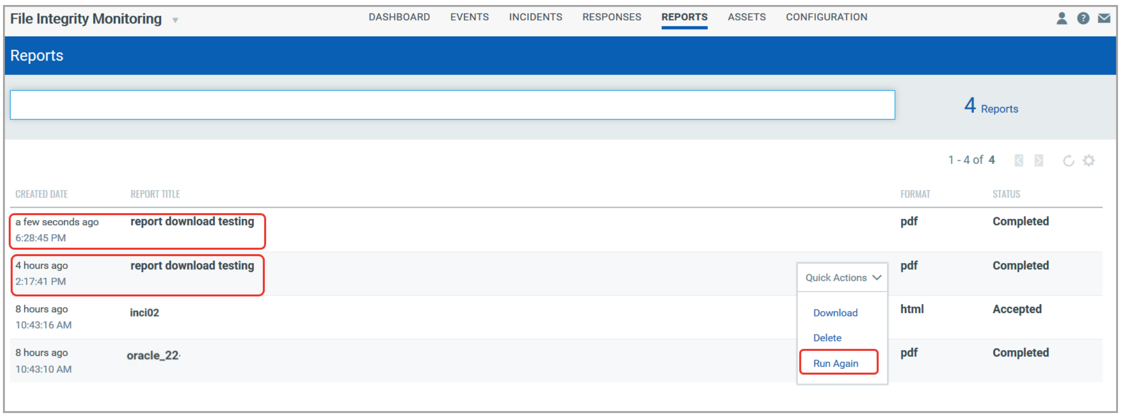
Note: If the report is in the “Failed” state or is stuck in a particular state (except Completed state) for a long time, you can run the report again using the "Run Again" options from the Quick Actions menu.

Re-running a Report

Click the Run Again option under the Quick Actions menu to generate a new report with the same name but updated data, date, and time.

The Run Again option is not available if the incident for which the report is generated is deleted.

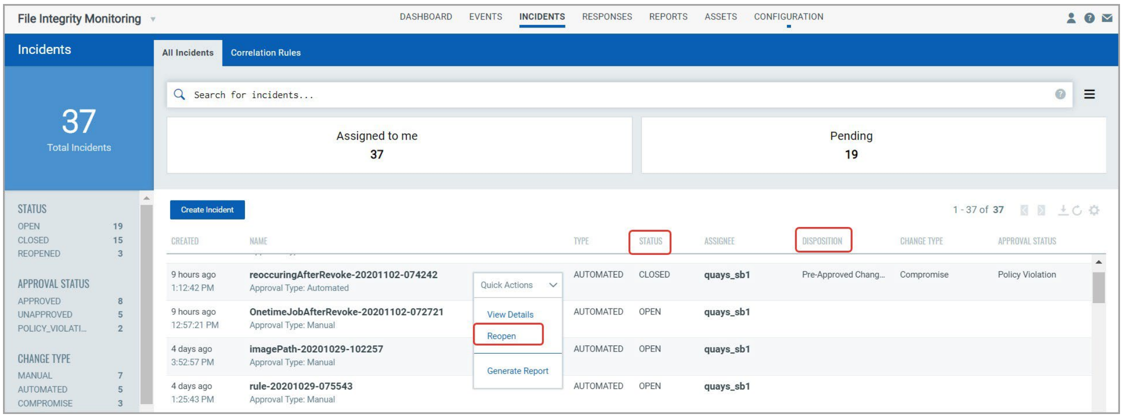
Note: You cannot rerun reports that have special characters in their name.



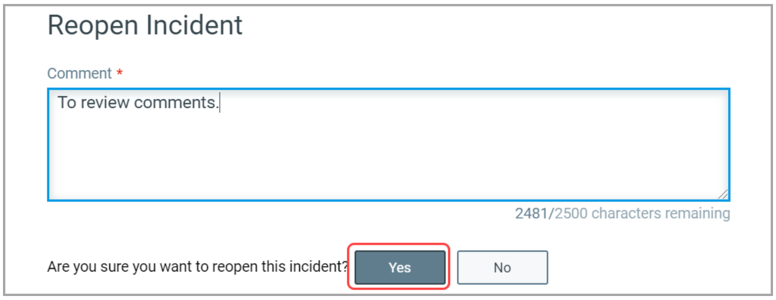
Reopening Closed Incidents

You 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.



Enter the comments and click Yes.



Rule-based alerts for events and incidents

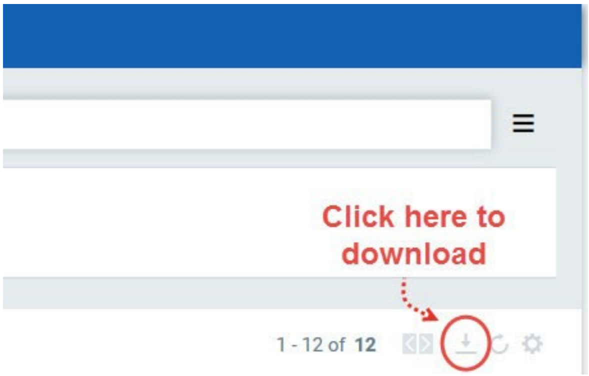
You can configure FIM to monitor critical events/incidents based on the conditions specified in a rule and send you alert messages by a specified messaging system if events/incidents matching the condition is found. The alert message will have the events/incidents details. For FIM to send alerts, you need to first configure a rule action to specify what action to be taken when events matching a condition is found. 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.

Downloading Results

By downloading search results to your local system you can easily manage file change events, incidents and assets outside of the Qualys platform and share them with other users. You can export results in multiple formats (CSV, XML, PDF, DOC, HTML, etc).

Just click the Download icon above any list, choose a format and click Download.



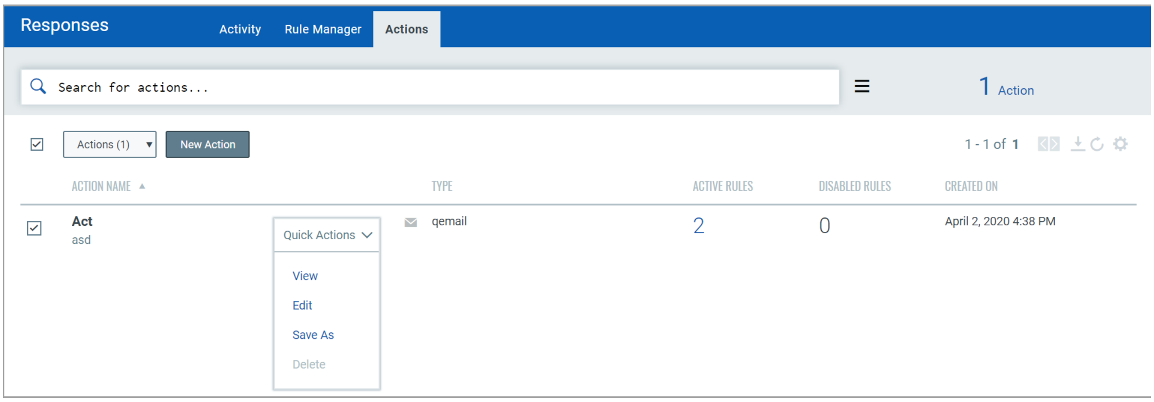
Responses

A Manager user or an equivalent role has the required permissions to carry out the user actions available under the Responses tab.

Note: If a user is assigned a role with no alerting access permission, the user cannot see the Responses tab.

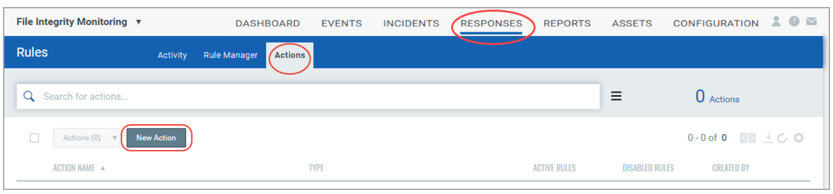
Managing Actions

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 view, 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.



Creating 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 Responses > Actions and then click 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.

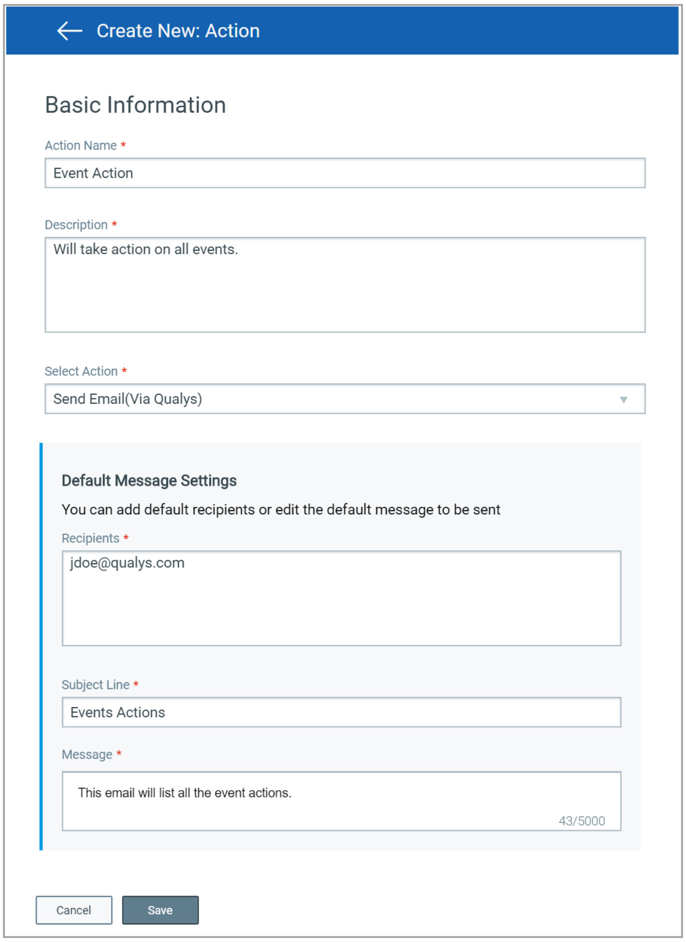
- Select an action from the Select Action drop-down and provide the settings for configuring the messaging system that FIM will use to send alerts.

- 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.

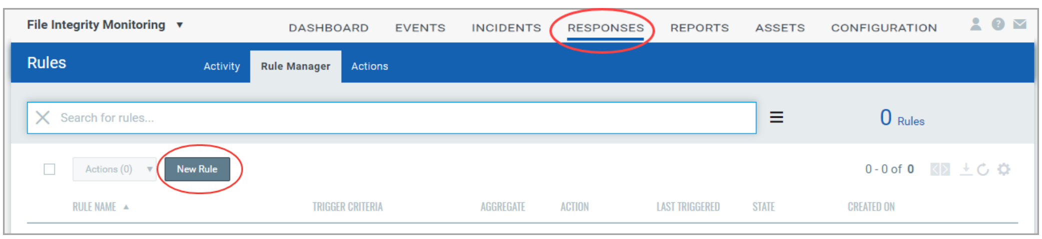
c) Select “Post to Slack” to post alert messages to your Slack account. Provide the Webhook URI that FIM will use to connect to your slack account to post alert messages.In Default Message Settings, specify the subject of the alert message and the customized alert message.



Creating a New Alert Rule

You can create a new rule from the following pages:

1) Go to Responses > 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 or Events > Event Review tab. Enter a search query in the search box and press Enter. Click menu button next to search box and select “Create Alert Rule from Search Query””. When you create an alert rule, the search query provided on the page is copied to the new rule.

4) Go to Incidents. Enter a search query in the search box and press Enter. Click menu button next to search box and select “Create Alert Rule from Search Query”. When you create an alert rule, the search query provided on the page is copied to the new rule.

Note: After you upgrade the Cloud Agent to 4.1 and above, the File Path is displayed as (c:\directory\sub-directory\file.ext). If all the agents in your subscription are not upgraded to 4.1 and above, edit the existing QQL queries to add the new File Path format along with the old one.

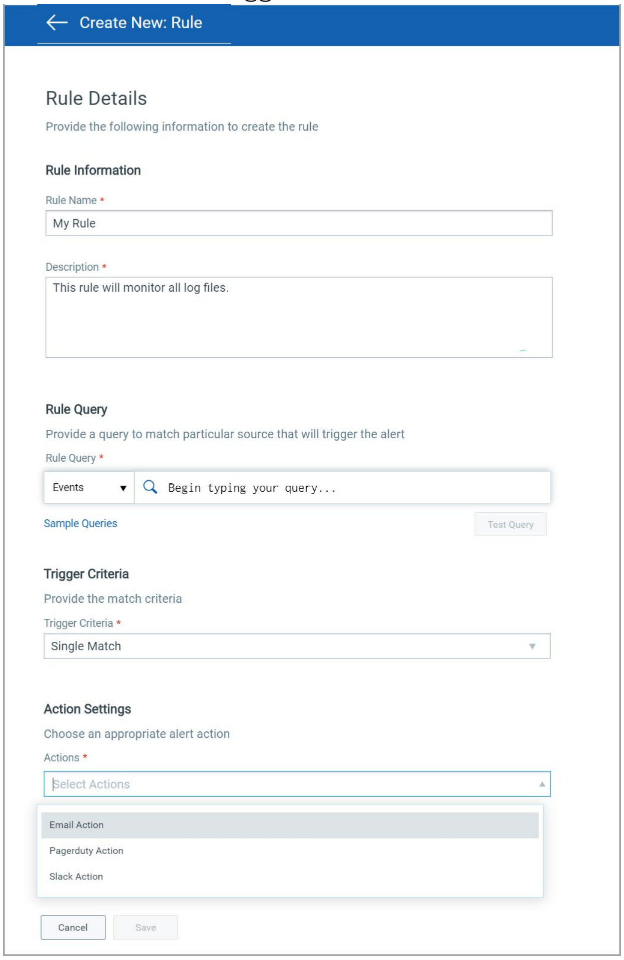
Provide required details in the respective sections to create a new rule:

- 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 three 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.

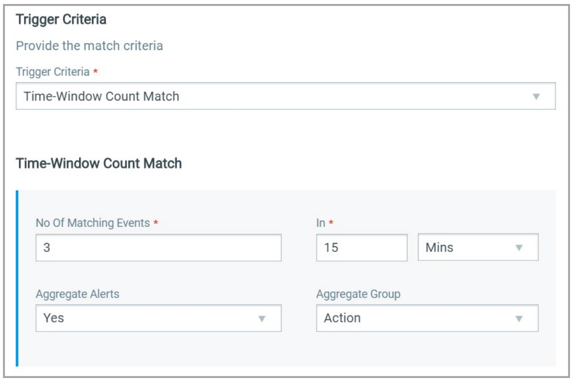
- In the Action Settings section, choose the actions that you want the system to perform when an alert is triggered.



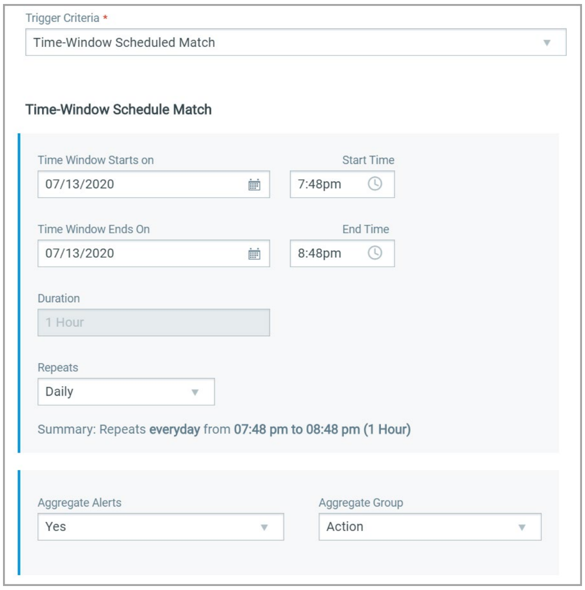
Selecting a trigger criteria

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

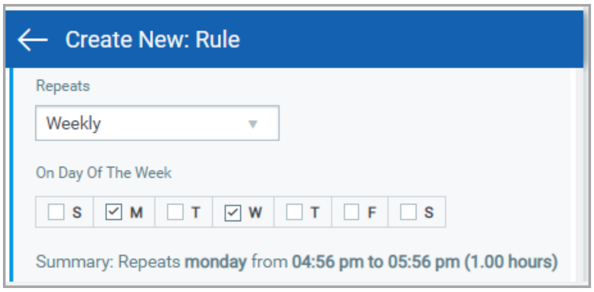
- Select “Time-Window Count Match" when you want to generate alerts based on the number of events/incidents returned by the search query in a fixed time interval. For example, an alert will be sent when three matching events are found within 15 minutes window.



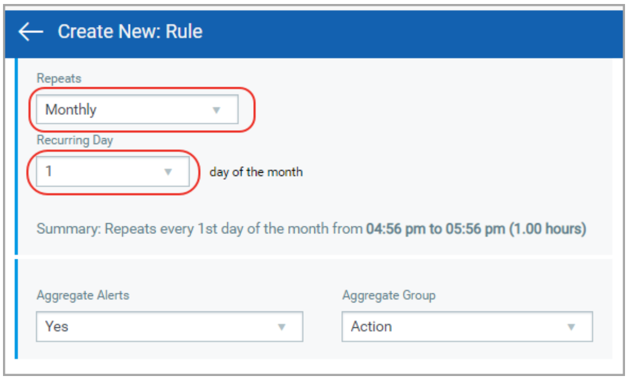
- Select **Time-Window Scheduled Match** when you want to generate alerts for matching events or incidents found during a scheduled time. The rule will be triggered only when an event/incident matching your search criteria is found during the time specified in the schedule. Choose a date and time range 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 rule will run. For example, send monthly alerts on the first day of every month.



For “Select Time-Window Count Match” and “Select 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.

Configuring action settings

Choose the action that you want the system to perform when an alert is triggered. You can choose one of the following actions: Send Email (Via Qualys),Post to Slack,and Send to Pager Duty.

Note that these actions must be configured before creating the Rule. For more information on actions, see Creating a new action.

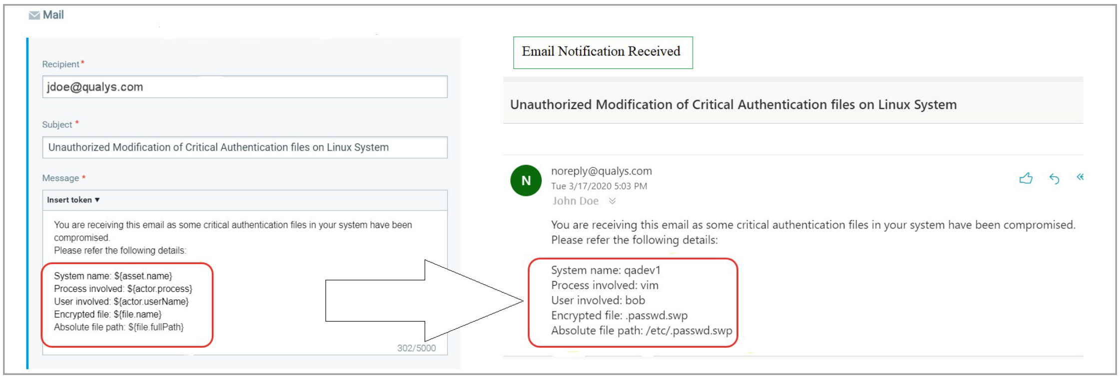
For example, you select the action Send Email (Via Qualys). Add the following information in the mail section to get all the relevant information in the email.

-**Recipient**: Specify the recipients' email ID who will receive the alert email.

-**Subject**: Subject of the alert message. E.g: "Unauthorized Modification of Critical Authentication files on Linux System".

- **Message**: You can customize the alert message. Click on the arrow next to Insert Token and add all the relevant tokens.

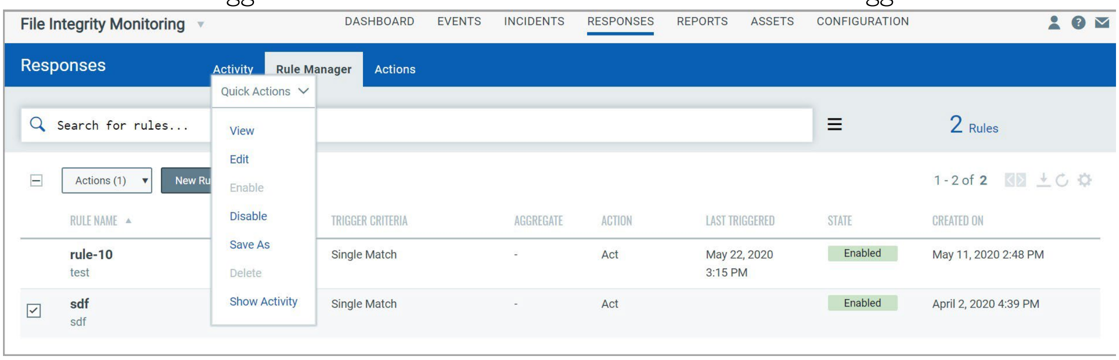
Ensure you add all the relevant information and tokens in the Message section to get all the crucial details of the alert in the notification.



Managing 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 Quick Actions menu to View, Edit, Enable, Disable, Save As, Delete, Show Activity for 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.

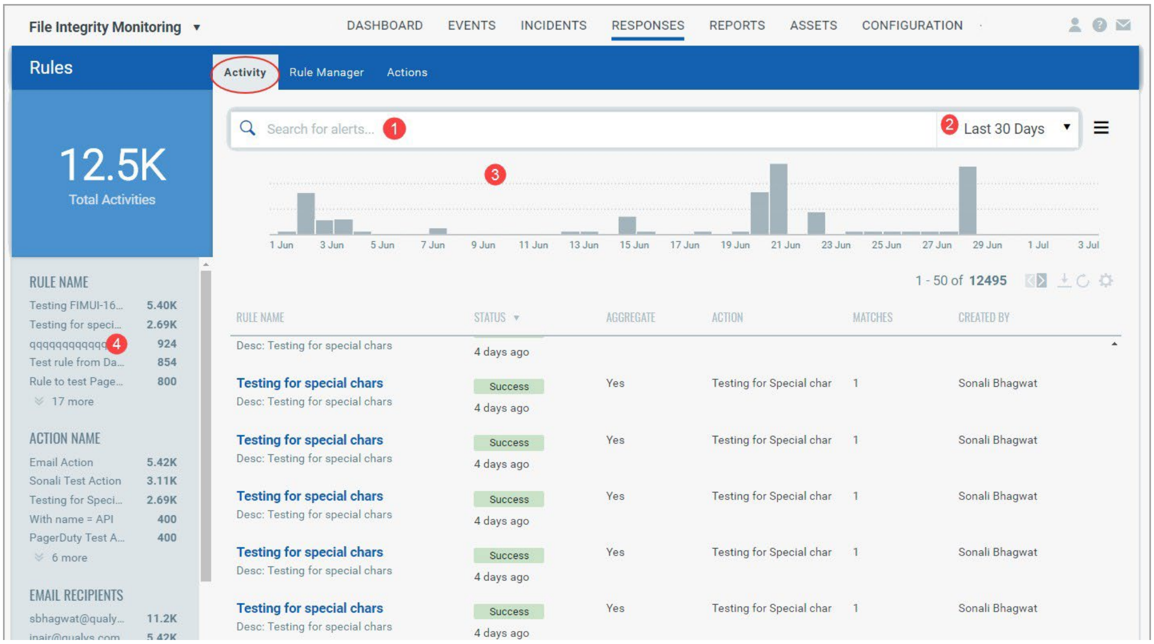
Note that Last Triggered value for a rule is shown after the rule is triggered.



Managing 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).



Dynamic Dashboards

You can create multiple dashboards and switch between them. Each dashboard has a collection of widgets showing event data of interest. And your dashboards/widgets are updated in real-time.

We have integrated Unified Dashboard (UD) with FIM. UD brings information from all Qualys applications into a single place for visualization. UD provides a powerful new dashboarding framework along with platform service that will be consumed and used by all other products to enhance the existing dashboard capabilities.

You can use the default FIM dashboard provided by Qualys or easily configure widgets to pull information from other modules/applications and add them to your dashboard. You can also add as many dashboards as you like to customize your application view.

For information on creating widgets, dashboards, templates, and more, refer to the Unified Dashboard Online Help.

Global Dashboards Permissions

Your access to Unified Dashboard depends on the global permissions granted to you from the Admin utility. Refer to the Online Help in the Admin utility for information on Global Dashboard Permissions.

Note: When you assign the Global Dashboard permissions to a role, the Global Dashboard permissions override the module-specific dashboard permissions. As a result, the module-specific dashboard permissions are ignored.

FIM dashboards

FIM defines some pre-defined dashboards for the users, to ease the access of defining the templates and adding the widgets.

The five default MITRE and Solar winds dashboards are introduced that have widgets with specific QQLs for certain types of events.

Note: Initially, if the user does not have any related events, the dashboard widgets may appear blank.

These dashboards are specific to FIM and include default template specific to the user and also the widgets that user might require.

Following are the specific dashboards defined in FIM:

- QFIM LINUX MITRE ATT&CK

- QFIM LINUX NIST SPECIAL PUBLICATION

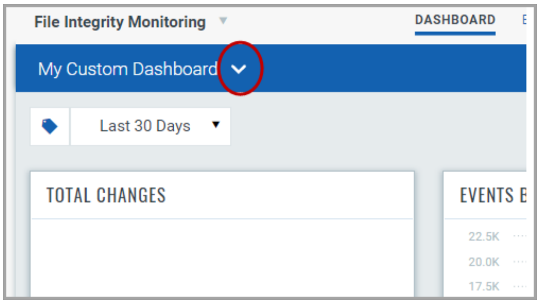
- QFIM WINDOWS MITRE ATT&CK

- QFIM WINDOWS NIST SPECIAL PUBLICATION
- SolarWinds Supply-Chain Attack

These dashboards are defined for both Linux and Windows users.

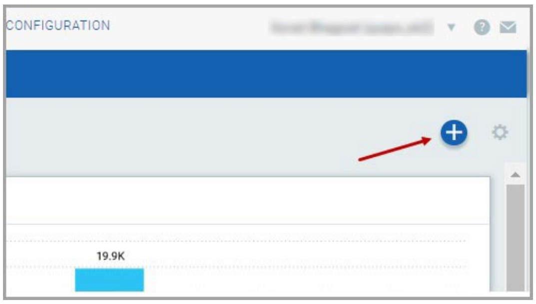
Switching dashboards

Click the down arrow next to the dashboard name and pick the one you want.



Adding widgets

1) Start by clicking the Add Widget icon on your dashboard.



2) Pick one of our widget templates - there are many to choose from - or create your own.

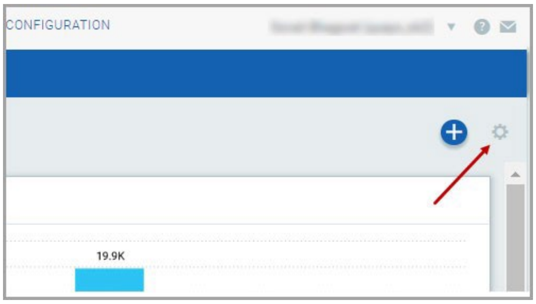
3) Each widget is unique. For some you'll select event data, a query and layout - count, table, bar graph, pie chart.

Tip - Wondering how we created the widgets on the default dashboard? Choose Edit from the widget menu to see the settings.

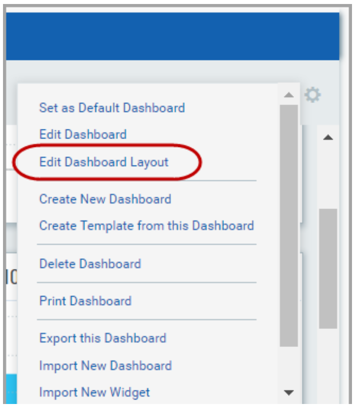
Resizing and layout

Resize any widget horizontally, drag & drop widgets to change the layout.

1) Click the Tools icon on your dashboard.



2) Select Edit Dashboard Layout.



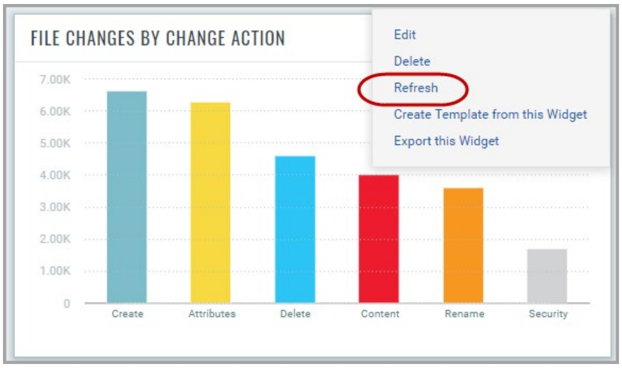
3) Adjust the width for any widget or drag the widget to a new location.

4) Click OK to save your changes.

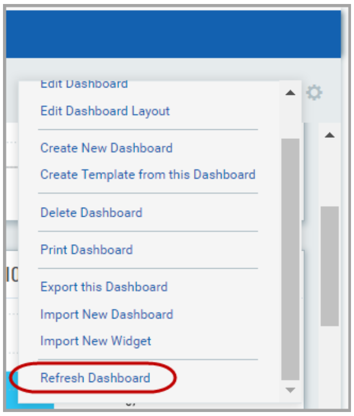
Refreshing your view

You might want to see the latest data for a particular widget.

Hover over the widget, click ☰ and from the widget menu choose Refresh.

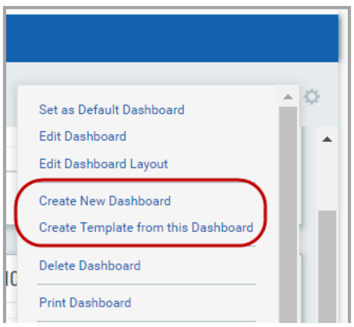


Choose the Refresh Dashboard option from the Tools menu to refresh all the widgets.



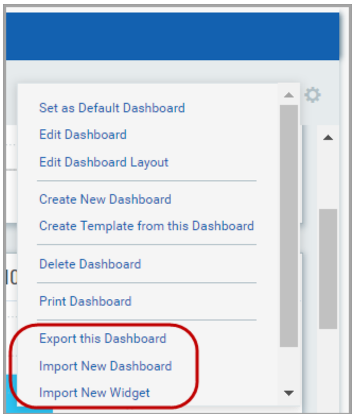
Creating dashboards and templates

From the Tools menu you can choose to create a new dashboard from scratch or create a template for your subscription from the current dashboard.



Importing and Exporting Dashboards

You can import and export dashboards with corresponding widgets, and import widgets.



Reports

Compliance reports offer detailed accounts of an organization's progress on particular compliance initiatives; and if taken collectively, can provide a broad summary of your organization's compliance efforts.

Creating reports on the events that occur as a result of any kind of action in your file system is important as the reports enable you to visualize the collected data. You can better analyze trends in events detected, generate graphical reports, and create executive reports that provide an in-depth insight into your network's file integrity.

FIM enables you to create on-demand reports or schedule your report generation at a future date and time. Specify your reporting criteria by leveraging QQL tokens and have access to the most accurate and up-to-date event and incident data in PDF, CSV, or HTML formats.

You can search for reports by the report title in the Reports sub-tab. You can also email reports to specified users by using the Notification option that's available while creating a report.

Note: The FIM reports are retained on the Qualys platform for seven days. It is recommended that you download your reports within seven days of generation for future reference and analysis.

Creating Reports

With FIM, you can create a variety of reports to gain insight into the events and incidents occurring in your file system. You can either leverage QQLs from Qualys Query Library or make use of the saved searches, or even enter your own custom queries, based on which change event data is filtered and included in the FIM reports.

After a report is generated, you can download the report in PDF, CSV, or HTML format.

Important: As per PCI DSS guidelines, event data is retained for 13 months on the Qualys platform. Hence, the on-demand reports can be generated for data collected in the past one year. Once generated, reports are purged from the Qualys platform after seven days from the day of generation.