Qualys File Integrity Monitoring

Release Notes

Version 3.8
October 11, 2023 (Updated on 20 December 2023)

What's New?

Templates for Dashboard Widgets: Non-Compliant Assets and Non-Communicating Assets

FIM Incident Reporting: Download Reports in CSV Format

Visibility of Non-Communicating Assets

Service Level Agreement for Incident Review Process

Reviewer-Based RBAC in FIM Incident Workflow

Report Generation for Non-Communicating Assets

New QQL Tokens

New Feature: File Access Monitoring

Qualys Cloud Platform 3.8 brings you many more improvements and updates! Learn more

Templates for Dashboard Widgets: Non-Compliant Assets and Non-Communicating Assets

With this FIM release, we added the widgets on the dashboard for **Non-Compliant Assets** and **Non-Communicating Assets.** This widget offers a unified view of the data related to Non-Communicating Assets and Non-Compliant Assets through a visual representation. You can customize the widgets to suit your needs.

The following image displays the dashboard with **Non-Communicating and Non-Compliant assets.**

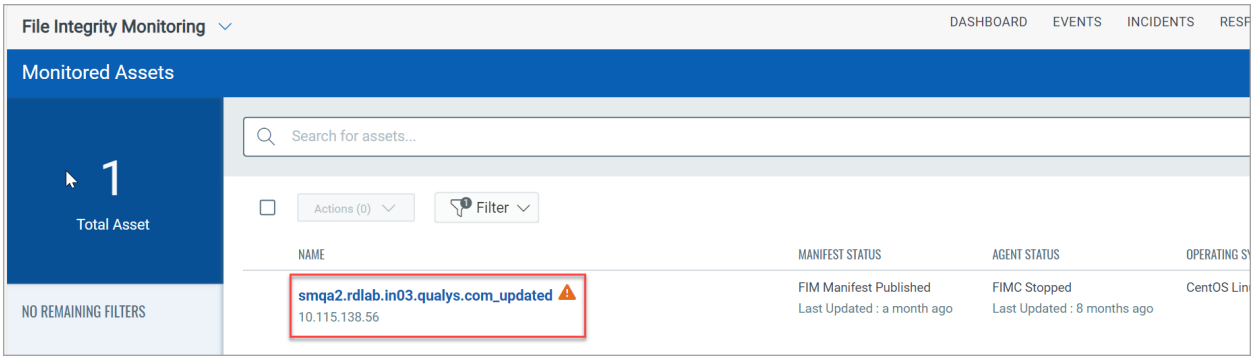
FIM Incident Reporting: Download Reports in CSV Format

With this release, we have added a new **CSV** format to download the FIM incident reports. We have introduced CSV format as it can store more records. Earlier, you could download the incident reports in PDF and HTML format only. Now you can download the incident reports in PDF, HTML, and **CSV** format.

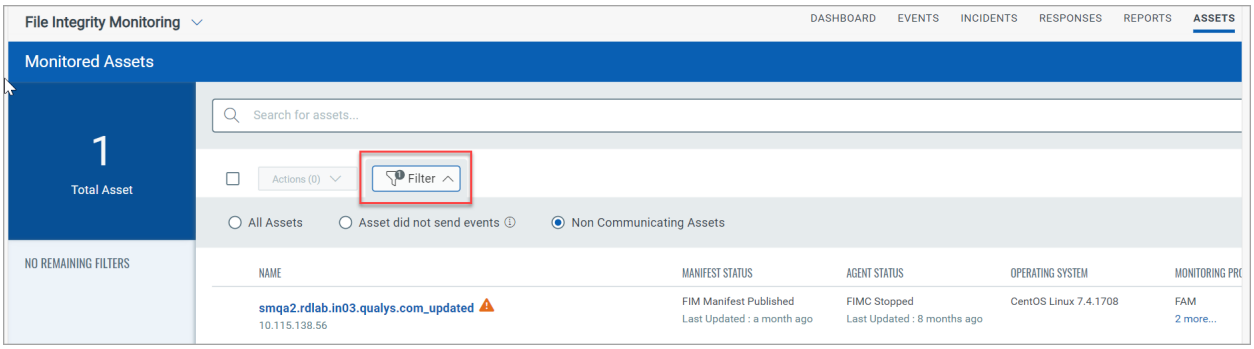
Visibility of Non-Communicating Assets

With this release, you can now view a comprehensive list of assets that are not communicating. **Non-communicating assets** are the assets that have not communicated with the Qualys Cloud Platform in the last seven days. These assets are highlighted with a warning icon. If assets do not communicate then it implies FIM failure, therefore, it is essential to identify and have visibility of such assets.

The following image displays a **Non-Communicating Asset.**



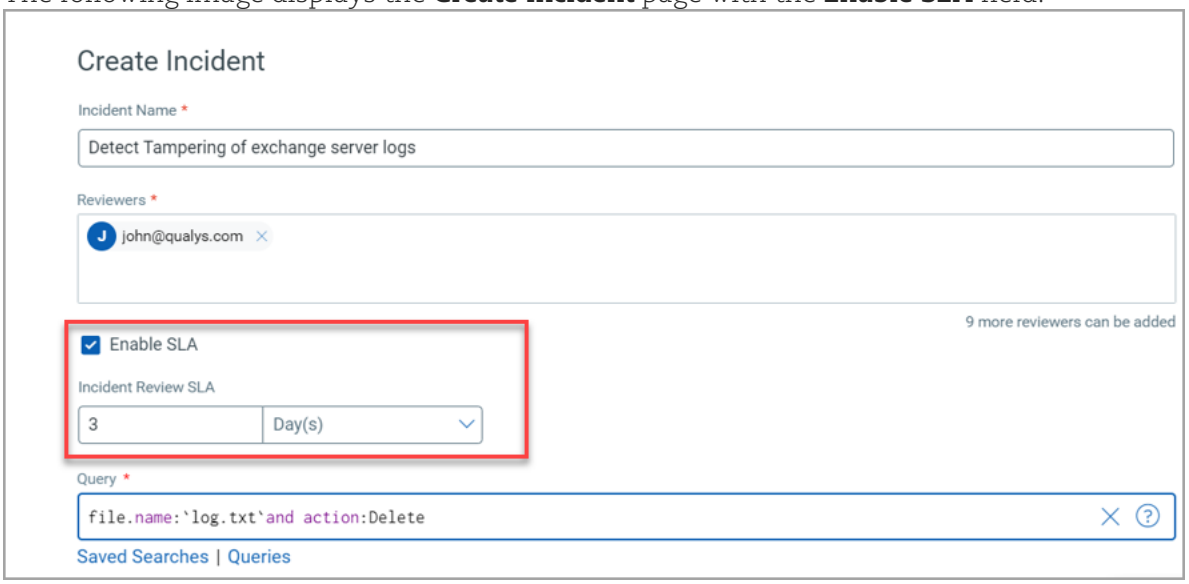
You have the option to filter the assets that are not communicating through **Filter**. This feature helps you manage your assets efficiently.
The following image displays the filter option in Assets tab.



Service-Level Agreement for Incident Review Process

With this release, you can enable the **SLA** for reviewers. SLA is a Service-Level Agreement that keeps you informed of the incidents that require your review.

To enable SLA navigate to,
Incidents> Create Incident> Enable SLA
The following image displays the **Create Incident** page with the **Enable SLA** field.



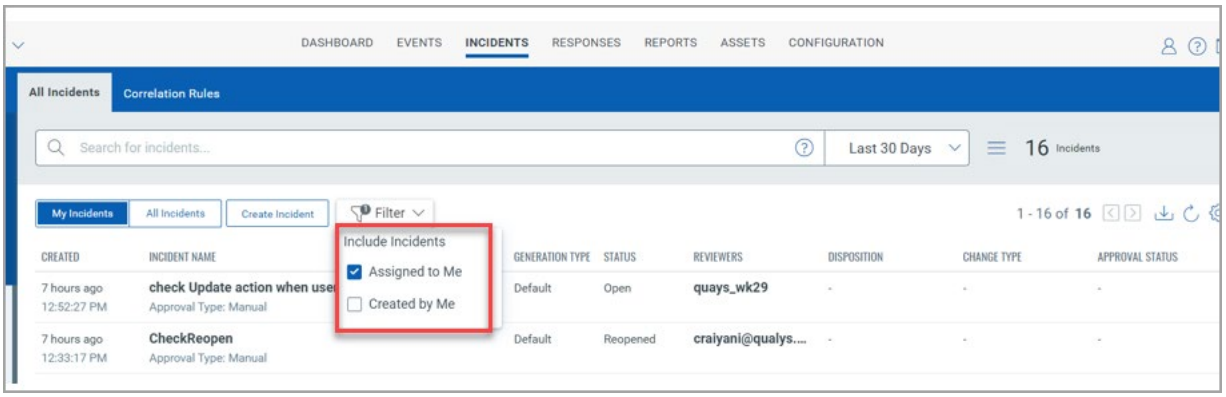
Enable SLA to receive email notification when the reviewer does not review the incident within the defined SLA. You can specify the SLA duration in days, weeks, or months. The minimum time to define an SLA is one day and the maximum is six months.

It is mandatory to provide the email ID of the reviewer so that the reviewers can receive email notifications regarding SLA breaches.

Reviewer-Based RBAC in FIM Incident Workflow

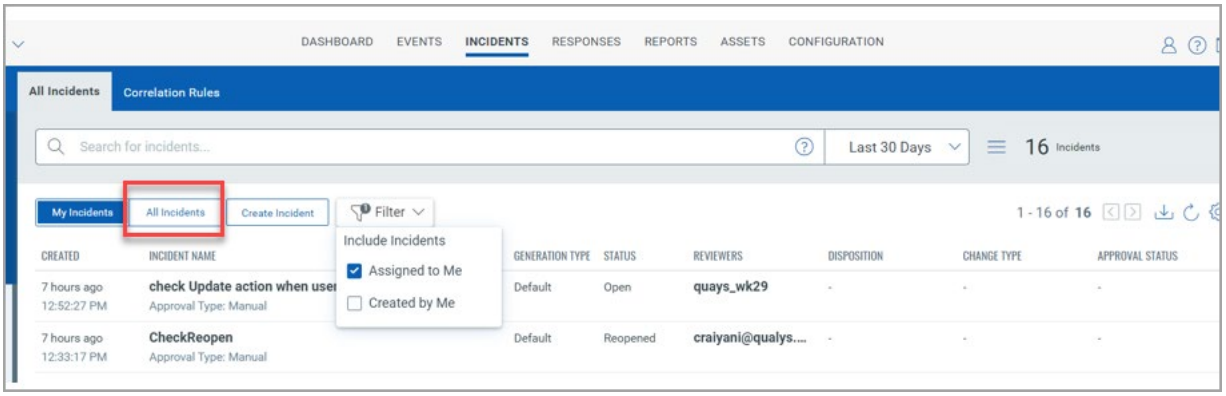
It is now possible to view the incidents based on the reviewers. You can view incidents assigned to you or created by you. This allows you to filter out the incidents for which you are the reviewer.

The following image displays Incidents tab with filter to find incidents for which you are the reviewer.



You can also view all incidents using the **All Incidents** option.

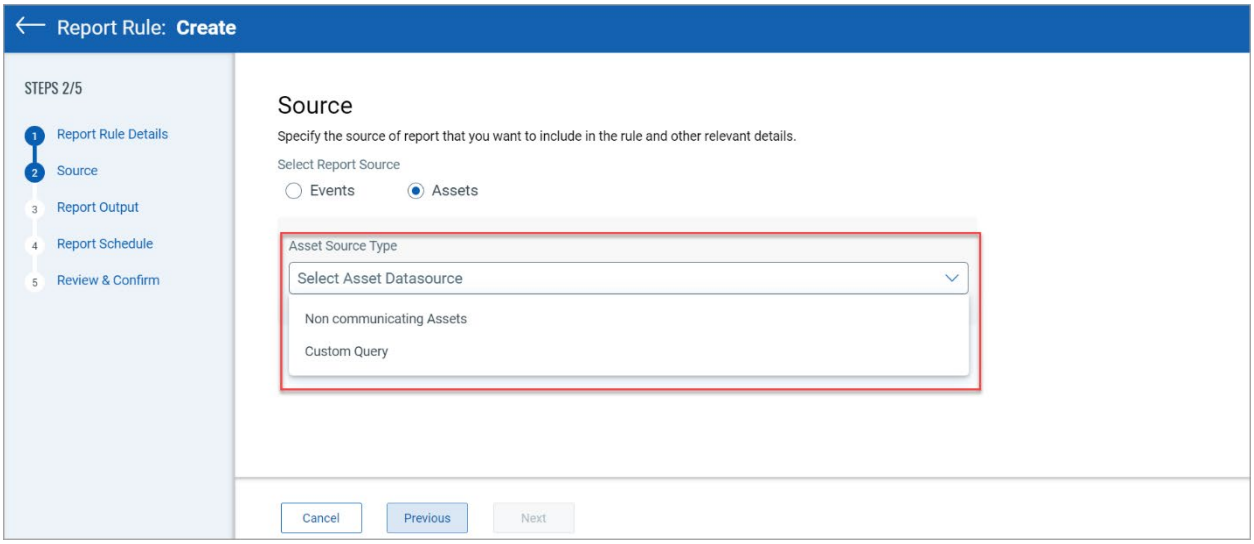
The following image displays **Incidents** page with **All Incidents.**



Report Generation for Non-Communicating Assets

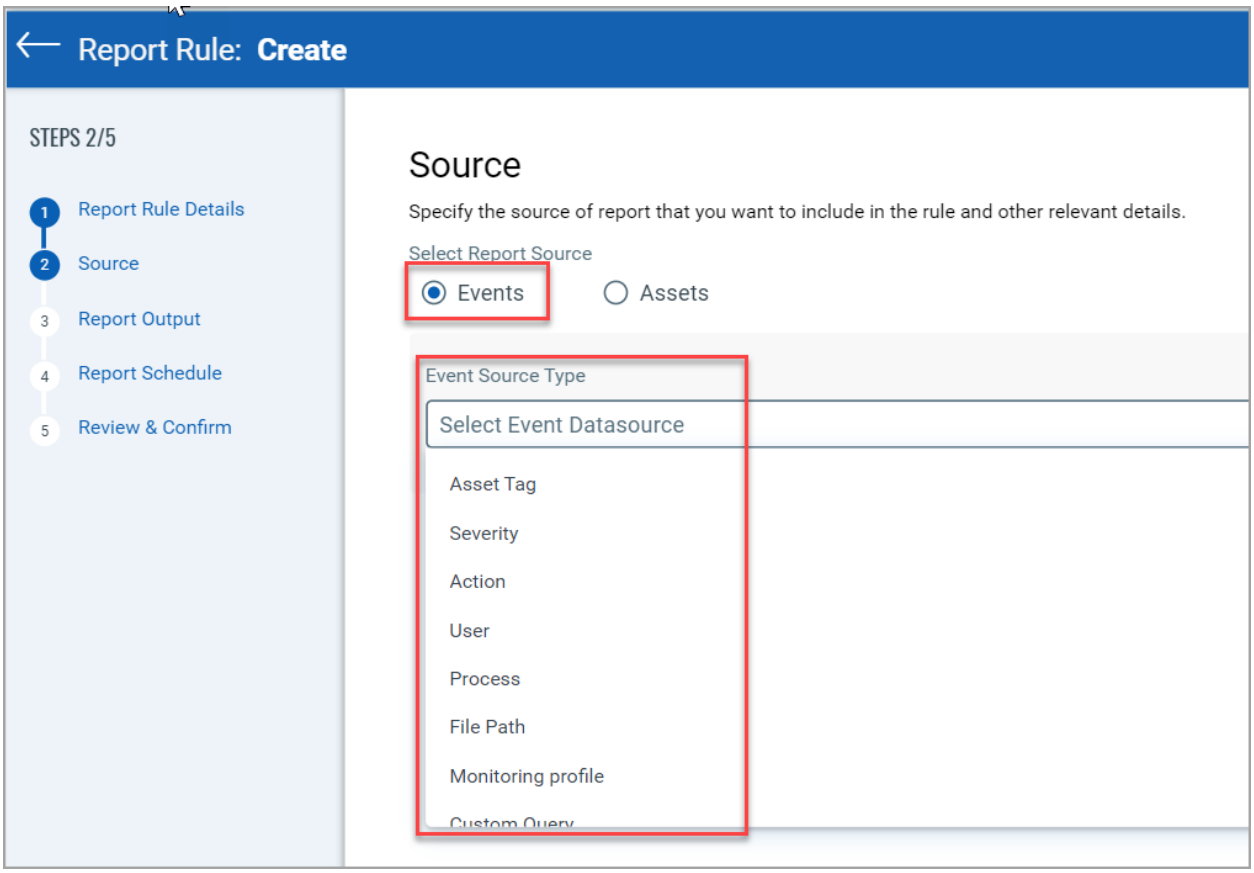
You can now create a report for non-Communicating assets directly by selecting **Assets Source Type** and **Non-Communicating Assets** from the list.

We have added **Custom Query** option to create rules for **Non-Compliant Assets** and for another user-defined asset query.
The following image displays the **Source** page in report rule creation.



We have removed the default section of **Asset Tag** for the **Events** data source. It lets you start with your event search query.

The following image displays the Report Source in the Source.



New QQL Tokens

With this release, we added new tokens to search/find FIM Incidents.

Token	Description	Example
reviewers	reviewers token is used to filter the incidents based on reviewers.	reviewers: jdoe@qualys.com
markupStatus	markupStatus is used to view the state of event marking for the incident. When the markupStatus is completed, it means all the events under the incident are marked and added to that incident.	markupStatus: COMPLETED
slaDurationKey	slaDurationKey token is used to filter incidents based on timeframe like DAYS, WEEKS, OR MONTHS.	slaDuationKey: DAYS
slaDurationValue	slaDurationValue token is used to filter incidents based on the SLA defined for a number of days, weeks, or months.	slaDurationValue:1

Token	Description	Example
slaRequired	slaRequired token is used to filter incidents based on whether the SLA is defined for the incident.	slaRequired: true

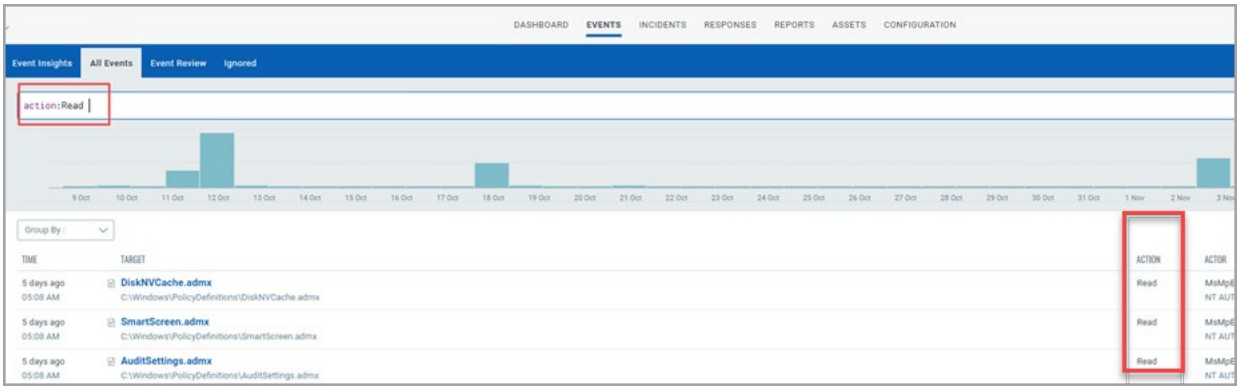
New Feature: File Access Monitoring

File Access Monitoring allows you to exclusively track files that are read. With this release, FIM generates the **Read** event for the files that are accessed. This helps you to track the details of the files that are accessed for reading.

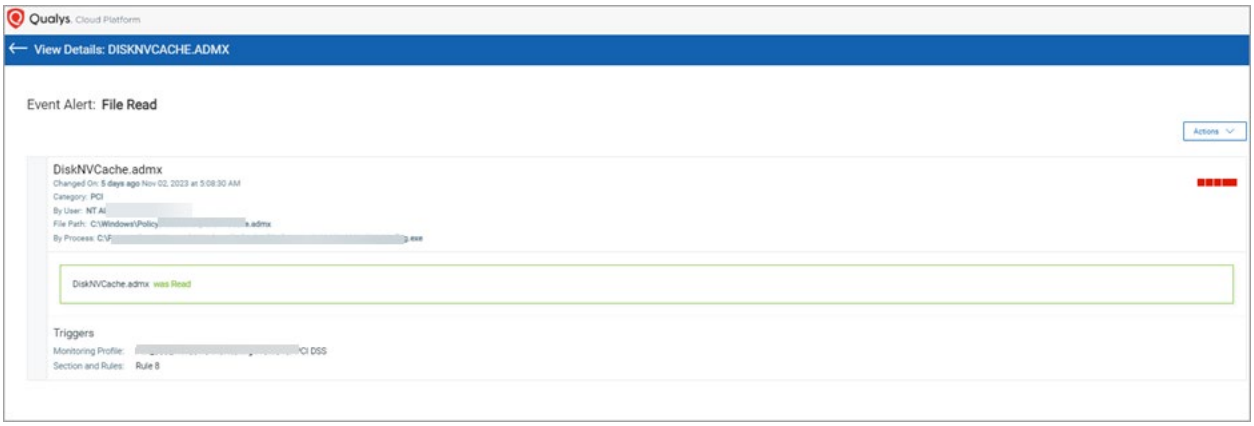
Pre-requisites

- Cloud Agent for Windows 5.3.0.0
- Cloud Agent for Linux 6.1.0.28

The following image displays the **All Events** tab with the **Read** events.

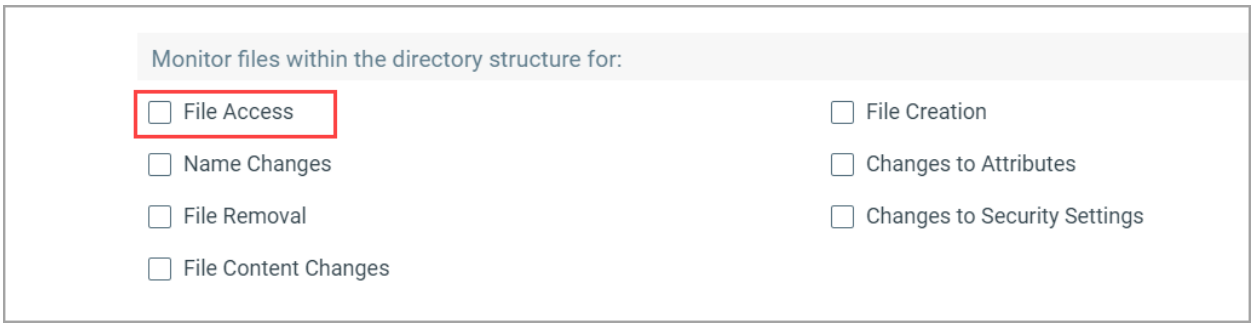


To view the event details, select an event, and click on **Event Details** from the **Quick Actions.** The following image presents an example of read event details.



To get the Read events:

- Navigate to FIM **Configuration Profile** > **Rules** page.
- In the **Rules Details** > **Monitor the files within the directory structure for** section, select **File Access.**



Important:

- Read events are not generated for the files opened in the Notepad application.
- Read event is generated only once even if the same file is accessed multiple times by a Windows agent.
- If a file is read in Linux with less command with the kernel versions earlier than 5.14.0-70.49.1.el9_0.x86_64 for the agent machine then the agent sends two Read events every time.
- **Command Executed** field is not available for Read events on the Linux platforms with kernel version earlier than 3.10.0-229.el7.x86_64 for the agent machine.
- In Read event, the **Audit User Name** field will have unknown as a value for the directory path like '/usr/local/qualys' , '/etc/passwd'.

Enhancement

- With this release, we have enhanced the format of path-related QQL tokens. You can skip the backward slash (\) at the end of the path while using the path-related QQL tokens such as the file.fullPath, actor.imagePath, and registryKey.path.
  For example,
  file.fullPath:'F:\INTERNAL\Incoming'

Fixed Issues

- An issue with editing rules in the monitoring profiles has been fixed. Earlier, you could not exclude unwanted monitoring actions such as File Creation and File Removal from the rule, even if you cleared them. However, with this release, you can clear them successfully.
- We have fixed an issue where the status of the manifest was displaying as 'FIM Manifest Application Failed'. Also, there was a manifest parsing failure at the agent level for certain inclusion filters in a profile rule. This was causing problems in creating events, but the issue has been resolved now.