



Qualys File Integrity Monitoring (FIM)

Release Notes

Version 3.0

April 26, 2021

Here's what's new in File Integrity Monitoring 3.0!

[Addition of File Reputation Service](#)

[Addition of File Trust Status](#)

[Addition of Windows Registry Monitoring capability](#)

Addition of File Reputation Status

FIM now has a new feature that enables users to know reputation status of files. Based on the file content hash, file reputation status is derived.

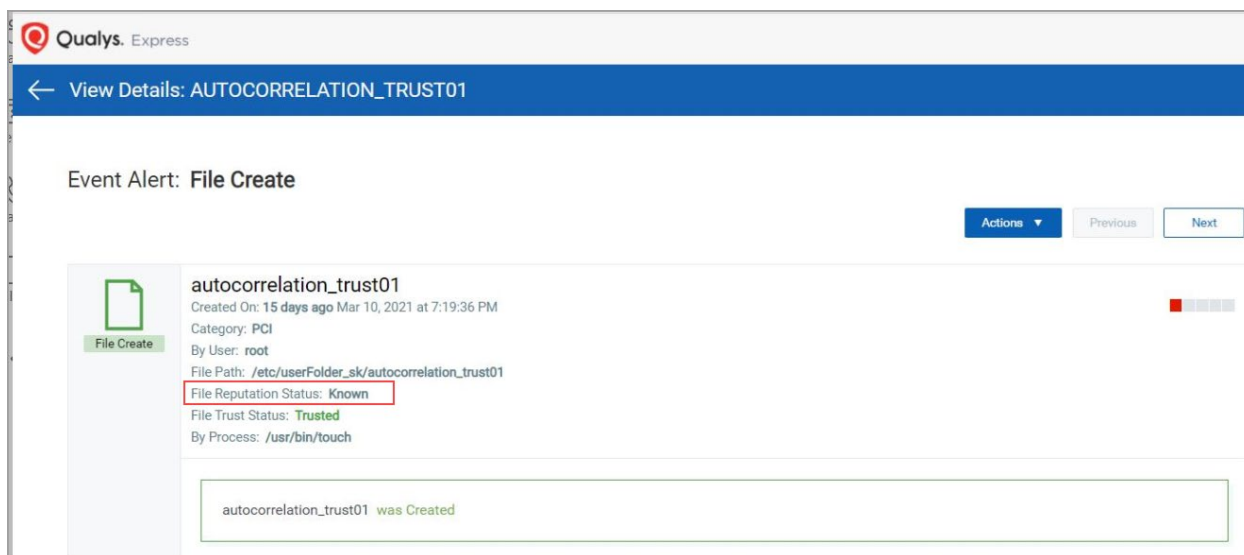
Reputation status of files can be seen in Events Details page for Events of type Create and Content. The source of Event Enrichment for File Reputation Status is Centralized Qualys Threat DB.

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.



The screenshot displays the 'View Details: AUTOCORRELATION_TRUST01' page in the Qualys Express interface. The main heading is 'Event Alert: File Create'. On the right, there are 'Actions', 'Previous', and 'Next' buttons. The event details are as follows:

- File Create** (indicated by a document icon)
- autocorrelation_trust01**
- Created On: 15 days ago Mar 10, 2021 at 7:19:36 PM
- Category: PCI
- By User: root
- File Path: /etc/userFolder_sk/autocorrelation_trust01
- File Reputation Status: Known** (highlighted with a red box)
- File Trust Status: **Trusted**
- By Process: /usr/bin/touch

A summary box at the bottom states: 'autocorrelation_trust01 was Created'.

Note: Reputation Status related event attributes are available in Event object in Events API output.

Automatic Incident Creation for Malicious Events

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

- Type: Automated
- Status: Open

The screenshot shows the Qualys Cloud Platform interface for File Integrity Monitoring. The 'INCIDENTS' tab is active. A search bar contains the query 'status: `OPEN`'. The dashboard displays 621 total incidents, with 621 assigned to the user and 621 pending. A table of incidents is shown, with one incident highlighted in red:

CREATED	NAME	TYPE	STATUS	ASSIGNEE	DISPOSITION	CHANGE TYPE	APPROVAL STATUS
Mar 3, 2021 4:27:24 PM	Defau...	DEFAULT	OPEN	quays_fa			
Mar 3, 2021 2:26:16 PM	Malici...	AUTOMATED	OPEN	SYSTEM	Malware	Compromise	Policy Violation

User has option to review the incident and take action accordingly.

The screenshot shows the Qualys Cloud Platform interface for File Integrity Monitoring. The 'INCIDENTS' tab is active. A search bar contains the query 'Search for incidents...'. The dashboard displays 977 total incidents, with 977 assigned to the user and 621 pending. A table of incidents is shown, with one incident highlighted in red:

CREATED	NAME	TYPE	STATUS	ASSIGNEE	DISPOSITION	CHANGE TYPE	APPROVAL STATUS
Mar 3, 2021 2:26:16 PM	Malici...	AUTOMATED	OPEN	SYSTEM	Malware	Compromise	Policy Violation

A 'Quick Actions' menu is open over the incident, showing options: 'View Details', 'Edit', 'Start Review', and 'Generate Report'.

Select correct approval type and rest of the 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 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

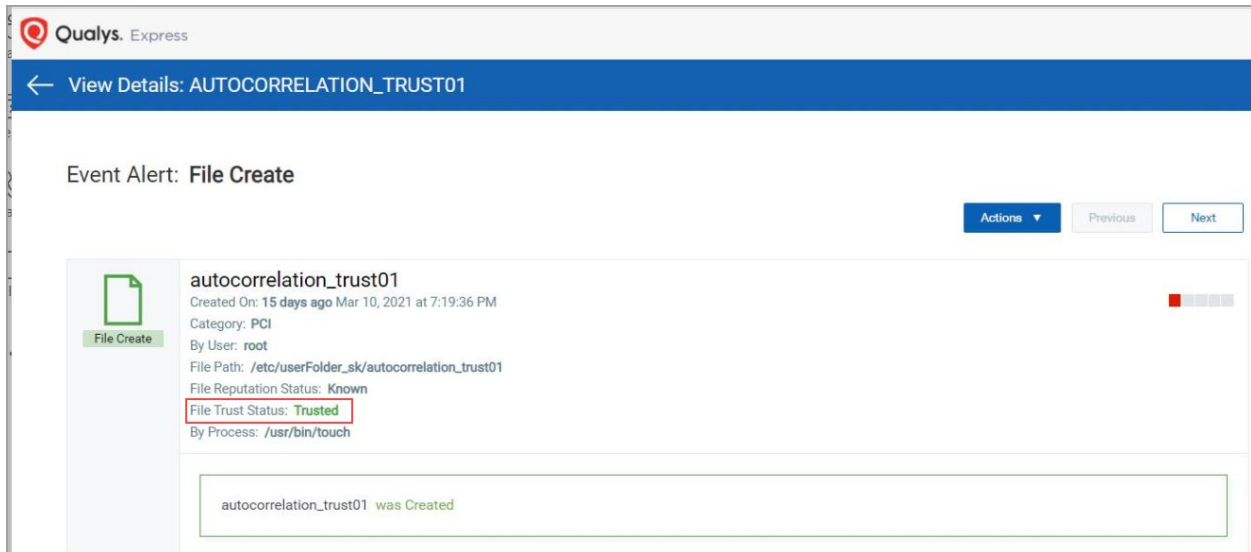
Addition of File Trust Status

FIM now has a new feature that 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
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.



The screenshot displays the 'View Details' page for an event alert titled 'File Create'. The event name is 'autocorrelation_trust01'. The details provided are: Created On: 15 days ago Mar 10, 2021 at 7:19:36 PM; Category: PCI; By User: root; File Path: /etc/userFolder_sk/autocorrelation_trust01; File Reputation Status: Known; File Trust Status: Trusted (highlighted with a red box); By Process: /usr/bin/touch. A summary box at the bottom states 'autocorrelation_trust01 was Created'. Navigation buttons for 'Actions', 'Previous', and 'Next' are visible in the top right.

Note: Trust Status related event attributes are available in Event object in Events API output.

Windows Registry Integrity Monitoring

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

The Windows registry stores crucial data about your Windows system and its configuration, along with all the information regarding the programs installed in it. Because of the criticality of the data it holds, the Windows registry serves as one of the most sought-after entry points for threat actors.

Once compromised, it can be manipulated to make modifications to programs and settings that might otherwise not be possible.

Tracking the changes occurring in the Windows registry, thus, becomes extremely important and is considered a security best practice.

Compromised integrity of the Windows Registry is a valuable indicator of the presence of malware or the system is compromised. A new System Library of Registry Rules has been added. User can add rules from this System Library to existing Windows profiles or while creating new Windows profile.

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.

Select Registry Key or Registry Value as Rule Type while defining the rule.

QUALYS GUARD EXPRESS SUITE

← Create New: Monitoring Profile Rule

Rule Name *
Example: System files rule

Description
2,500 characters limit
2500/2500 characters remaining

Section
Create Section

Monitoring Rule Parameters

Rule Type
Registry Key
Directory
File
Registry Key
Registry Value

Severity
Severity 3

ARE\Classes\Diagnostic.Resmon.Config

All

FIM provides following options to monitor registry:

- Install an asset > define rules > create a monitoring profile.
- Instead of manually creating the rules, you can select Import Registry Rules from the drop-down available in the Profiles tab.
- 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.

Note: The Registry related event attributes are available in Event object in Events API output.