



# Qualys Endpoint Detection and Response v2.x

## Release Notes

Version 2.3

February 28, 2023 (Updated on May 17, 2023)

Here's what's new in Endpoint Detection and Response 2.3!

### What's New

[Added New Field in OnAccess Scan Page of Anti-Malware Profile](#)

[Added Exclusion Type in Exclusions Page of Anti-Malware Profile](#)

[Added Create Exception Option in Quick Actions Menu of Hunting Tab](#)

[Enhanced Incident Workflow](#)

[Introduced Auto-Remediation of an Event](#)

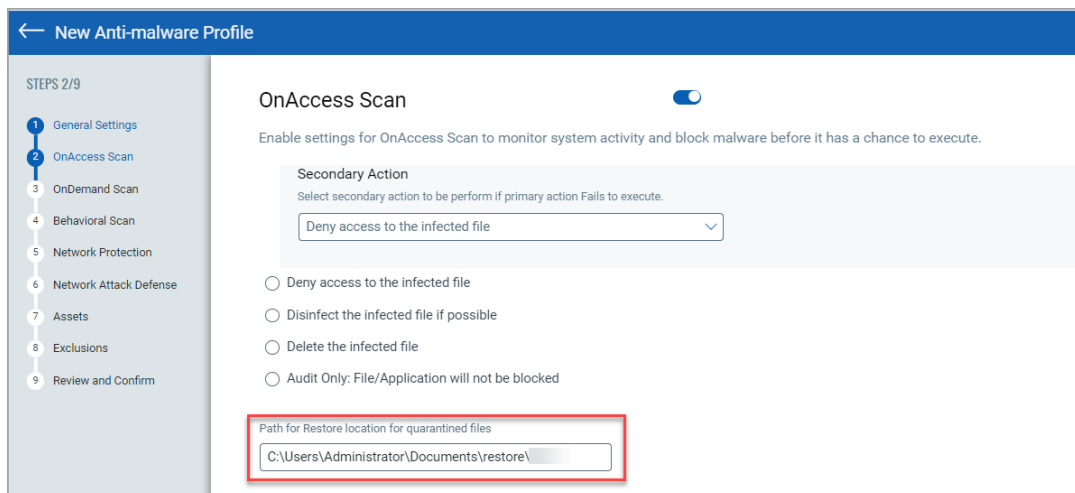
[Introduced New Tokens](#)

Endpoint Detection and Response 2.3 brings you some improvements and updates!

## Added New Field in OnAccess Scan Page of Anti-Malware Profile

With this release, we have added a new field, **Path for Restore location for quarantined files**. This is an optional field and can be accessed from the **Configuration** tab. In this field, you can provide the path where you want the quarantined files to be restored. Perform the following steps to restore the quarantine file:

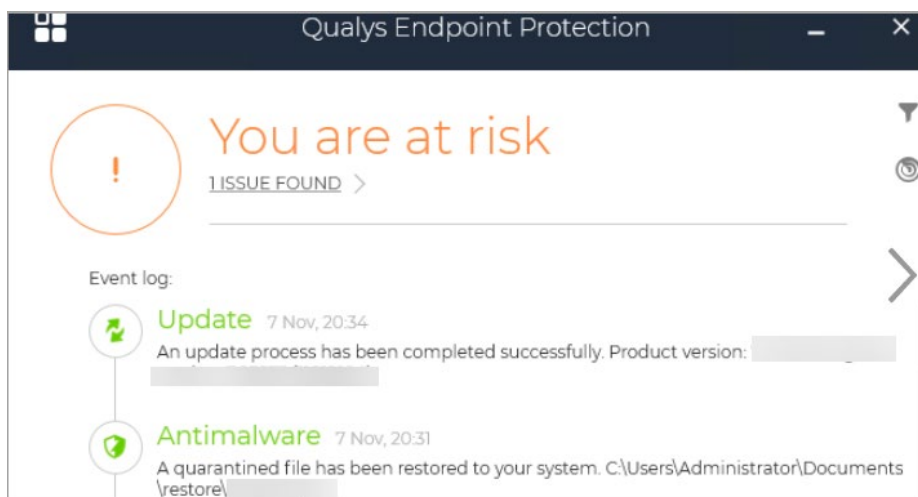
1. From the **Configuration** tab, click **Anti-Malware Profile**.
2. Click **New Anti-malware Profile**.
3. In the **OnAccess Scan** page, provide the **Path for Restore location for quarantined files**.



4. Provide the information for other pages per your organization's requirement.
5. Click **Create Anti-malware Profile**. For more information about creating an anti-malware profile, see [EDR Online Help](#).

**Note:** The custom restore location path is used when the file's original location cannot be restored. Hence, it is recommended to set the custom restore location path available in the system. The custom restore path should be excluded from File Exclusions. For more information about File Exclusion, see [EDR Online Help](#).

The following screenshot is an example of the notification:



## Added Exclusion Type in Exclusions Page of Anti-Malware Profile

With this release, we have defined the type of exclusions you can include while creating a new Anti-malware profile or for an existing profile. The inputs for **File Exclusions**, **Behavioral Scan Exclusions**, **Traffic Scan Exclusions**, and **Anti-Phishing Exclusions** are listed in the **Configuration** tab under the **Anti-Malware Profile** tab. Toggle the exclusion type to exclude the type from the scan. For more information about Exclusion Support, see [EDR Online Help](#).

The following screenshot is an example of File Exclusions:

← New Anti-malware Profile

STEPS 8/9

- 1 General Settings
- 2 OnAccess Scan
- 3 OnDemand Scan
- 4 Behavioral Scan
- 5 Network Protection
- 6 Network Attack Defense
- 7 Assets
- 8 Exclusions**
- 9 Review and Confirm

### Exclusions

**File Exclusions** ☒

Exclude the following from OnAccess and OnDemand Scans.

Type Extension Add

260 characters remaining

Delete All 0 - 1 of 1

<input type="checkbox"/>	FILE NAME / FOLDER / EXTENSION / PROCESS / SHA256 / THREAT NAME / COMMAND LINE TO BE EXCLUDED	TYPE	ACTIONS
<input type="checkbox"/>	chrome.exe	Extension	<a href="#">Edit</a> <a href="#">Delete</a>

**Behavioral Scan Exclusions** ☐

Exclude following from Behavioral Scan Exclusions.

Cancel Previous Next

## Added Create Exception Option in Quick Actions Menu of Hunting Tab

We have introduced the **Create Exception** option that allows you to suppress a past or a future event that you consider non-malicious. This option is available in the **Quick Actions** menu and can be performed for an event in **Historic View** or **Current View**. While creating an exception, you need to choose the **Reason** among the following Reason option categories:

- **False Positive**: It reduces the indicator score associated with the event that is 8 or greater than 8.
- **Risk Accepted**: It reduces the indicator score associated with the event that is between 1 to 7.
- **Hide**: If you do not want to change the False Positive or Risk Accepted score, you can choose this option to hide the event. Events from the **Current View** tab are moved to the **Exempted Events** tab.

← Create: Exceptions

STEPS 1/3

- 1 Basic Information
- 2 Event
- 3 Review and Confirm

### Basic Details

Provide basic details for the exception creation.

Exception Title \*

exception for process

79 characters remaining

Reason \*

☒ False Positive ☐ Risk Accepted ☐ Hide

**Note:** False positive will reduce the "indicator score" associated with the event.

Explanation \*

creating exception for Google Chrom for asset test123

197 characters remaining

Information Security Policy

Please provide additional explanation for tracking purpose

250 characters remaining

Information Security Procedure

Please provide additional explanation for tracking purpose

250 characters remaining

[Cancel](#) [Next](#)

For details on steps to Create Exception, see [EDR Online Help](#).

## Enhanced Incident Workflow

We have enhanced incident workflow by introducing **Change Status** and **Assign Incident** as the two new options. You can perform bulk **Change Status** and **Assign Incident** actions using the **Actions** drop-down menu. The bulk actions cannot be performed if the Assignee is different.

- **Change Status:** The status of an event can be – Open, In Progress, Closed, and Re-open. By default, the status of an event is **Open**.
- **Assign Incident:** An incident can be assigned to the user using the Assign Incident option. By default, the assignee is displayed as **Unassigned**.

The screenshot displays the 'Incidents' tab in the Endpoint Detection and Response (EDR) interface. The top navigation bar includes 'DASHBOARD', 'INCIDENTS' (selected), 'HUNTING', and 'ASSETS'. The left sidebar shows '814 Total Incidents' and a 'MALWARE FAMILY' list. The main content area features a search bar, a 'SCORE' bar, and a 'DETECTED INCIDENTS' count of 119. A red box highlights the 'Actions (50)' dropdown menu, which contains 'Change Status' and 'Assign Incident' options. The table below the dropdown has columns for 'STATUS', 'RISK SCORE', 'ASSIGNEE', and 'HO'.

MALWARE FAMILY	Count
adfind	1
ai:ransom.45829....	1
ai:swort.45829.0...	2
application.nirsof...	1

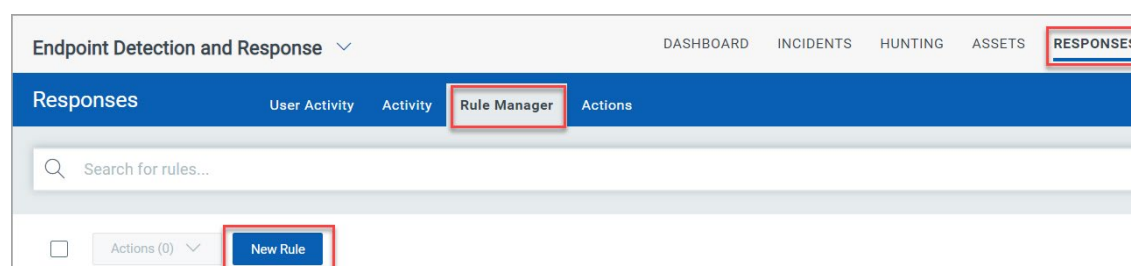
After the status is changed or an incident is assigned, the updated changes are listed in the **Incidents** tab. For more information on how to change the status and assign incidents, see [EDR Online Help](#).

## Introduced Auto-Remediation of an Event

With this release, we have introduced a feature that auto-remediates an event. The following table lists the supported QQL tokens for auto-remediation:

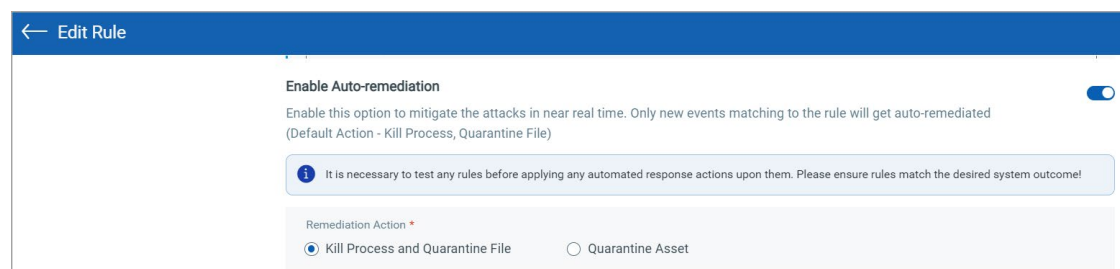
Process Events	File Events	Process and File Events
process.name	file.name	malware.family
process.pid	file.hash.sha256	malware.category
process.image.fullpath	file.hash.md5	indicator.severitiescore
process.image.path	file.fullpath	type
process.processfile.sha256	file.properties.certificate.hash	asset.agentId
process.processfile.md5	file.path	platform

You can auto-remediate an event by setting a rule from the **Responses** tab.

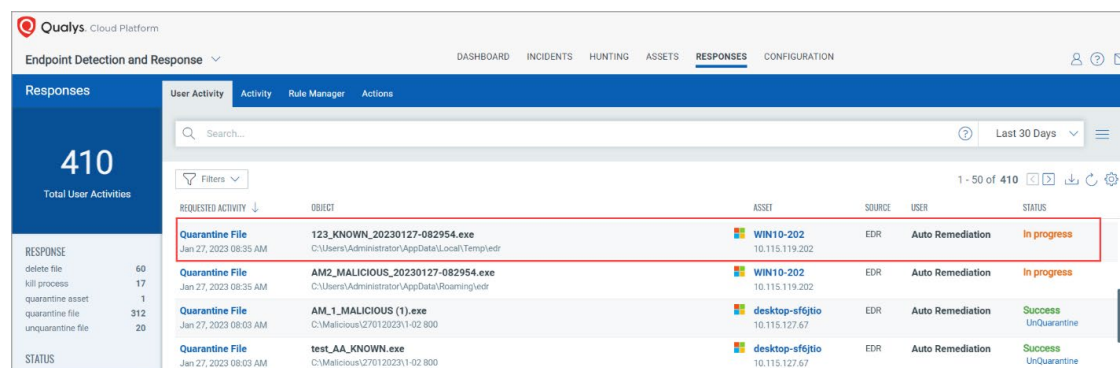


Auto-remediation can be done for the following:

- Kill Process and Quarantine file
- Quarantine Asset



After the changes are saved the quarantined action is automatically triggered. The following screenshot is an example:



To perform the Auto-remediation step-by-step, see [EDR Online Help](#).

## Introduced New Tokens

- **assets.tags.name:** This token uses the string value to list the assets with the tag name.
- **incident.status:** This token uses the string value to list the incident status.
- **incident.assignee:** This token uses the string value to list the assignees.

For more information about these tokens, see [EDR Online Help](#).