



Endpoint Detection and Response

Getting Started Guide

September 11, 2023

Copyright 2017-2023 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

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



Table of Contents

About this Guide.....	4
About Qualys	4
Qualys Support	4
Get Started.....	5
Steps to start investigating EDR incidents and events	5
Download and Configure Cloud Agent for EDR	6
Download Cloud Agent for EDR	6
Configure Agents for EDR	7
Activate your agents for EDR	10
Enable EDR in a configuration profile	11
Setting up asset tags (optional)	12
EDR Investigation.....	14
How to Search	14
Hunting events	15
Investigate incidents	16
Look into assets monitored by EDR	16
Narrow your results	17
Download your results	17
Remediation Action	18
Remediation Action for File Events	19
Remediation Action for Process Events	21
User Activity	23
Event Details	26
Customizable Dynamic Dashboards	28
Alerts, Rules, and Actions.....	29
Roles and Permissions	29
Configure Rule Based Alerts for Events	31
Create a New Action	31
Create a New Rule	32
Manage Actions	35
Manage Rules	36
Manage Alerts	37
Malware Protection	38

About this Guide

Thank you for your interest in Qualys Endpoint Detection and Response (EDR).

Qualys EDR expands the capabilities of the Qualys Cloud Platform to deliver threat hunting and remediation response. EDR detects suspicious activity, confirms the presence of known and unknown malware, and provides remediation response for your assets.

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

Endpoint Detection and Response (EDR) is an evolved superset of the IOC app. EDR expands the capabilities of the Qualys Cloud Platform to deliver threat hunting and remediation response. EDR detects suspicious activity, confirms the presence of known and unknown malware, and provides remediation response for your assets.

EDR unifies different context vectors like asset discovery, rich normalized software inventory, end-of-life visibility, vulnerabilities and exploits, misconfiguration, in-depth endpoint telemetry, and network reachability with a powerful backend to correlate it all for accurate assessment, detection and response all, in a single, cloud-based app.

For more information on the Endpoint Detection and Response application, contact your Technical Account Manager (TAM) or Qualys Support.

You can also refer the following onboarding sections in EDR Online Help:

- [EDR Onboarding for Windows](#)
- [EDR Onboarding for Linux](#)

Steps to start investigating EDR incidents and events



Discover and Monitor

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

Enable EDR in the CA Configuration Profile and tell us which EDR artifacts you want to transmit to the Qualys Cloud Platform.

For more information, see [Download and Configure Cloud Agent for EDR](#).

Detect and Investigate

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

For more information, see [EDR Investigation](#).

Respond and Prevent

Remediate the suspicious and malicious events from a central location. A remediation action option will be displayed against the malicious or suspicious event.

For more information, see [Remediation Action](#).

Download and Configure Cloud Agent for EDR

You'll need to install a Cloud Agent that's been activated for EDR on each asset you want to monitor for suspicious activity.

If you are new customer, you must first download and install the default EDR key. For more information, see [Download Cloud Agent for EDR](#).

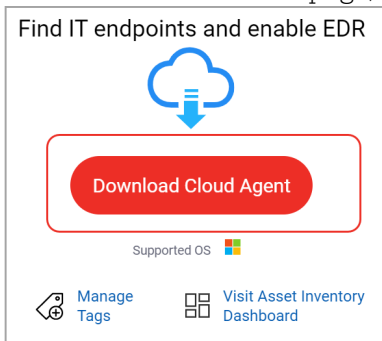
If you are an existing customer, you can either:

- Select the existing activation key and upgrade the associated agents for EDR. For more information, see [Upgrade Existing Agents](#).
- Install new Cloud Agent and activate the agent for EDR. For more information see, [Install Cloud Agent](#).

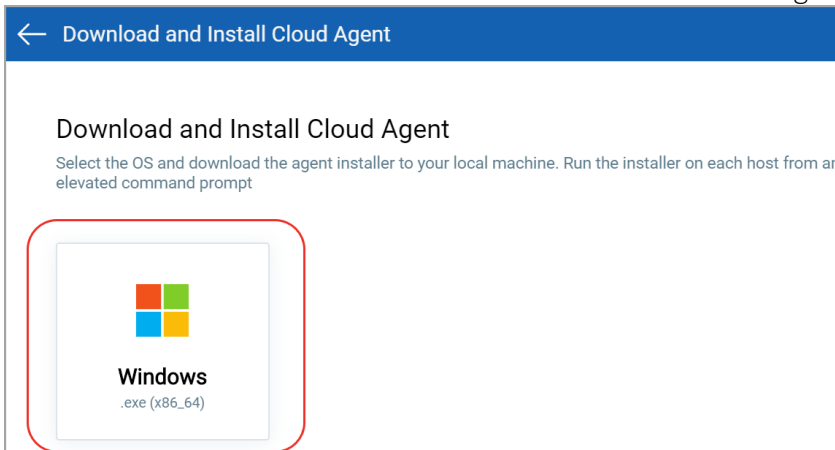
Note: You must upgrade to Cloud Agent version 4.1 and above to utilize all the EDR functionality.

Download Cloud Agent for EDR

From the EDR welcome page, click Download Cloud Agent.



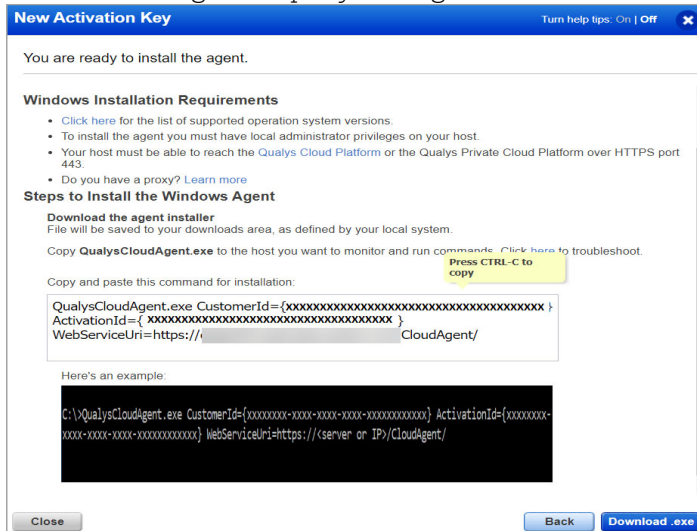
Click on Windows.exe from the Download and Install Cloud Agent page.



From the Installation Instructions page, download the agent installer and copy it to the host machine.

```
> QualysCloudAgent.exe CustomerId={xxxxxxxx-xxxx-xxxx-  
xxxxxxxxxxxxxxxx} ActivationId={xxxxxxxx-xxxx-xxxx-xxxx-  
xxxxxxxxxxxxxxxx}  
  
WebServiceUri=<platform_url>/CloudAgent/
```

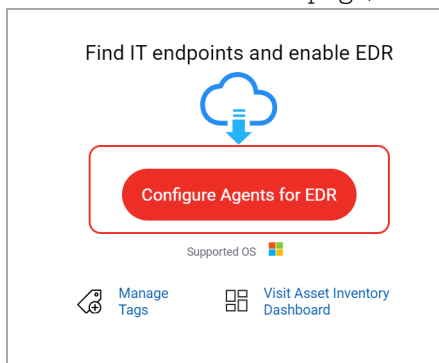
Run the command from an elevated command prompt, or use a system management tool to install the agent as per your organization's standard process to install a software.



After you have successfully downloaded and installed the default installation key. You can install more activation keys. For more information, see [Install Cloud Agent](#).

Configure Agents for EDR

From the EDR welcome page, click Configure Agents for EDR.

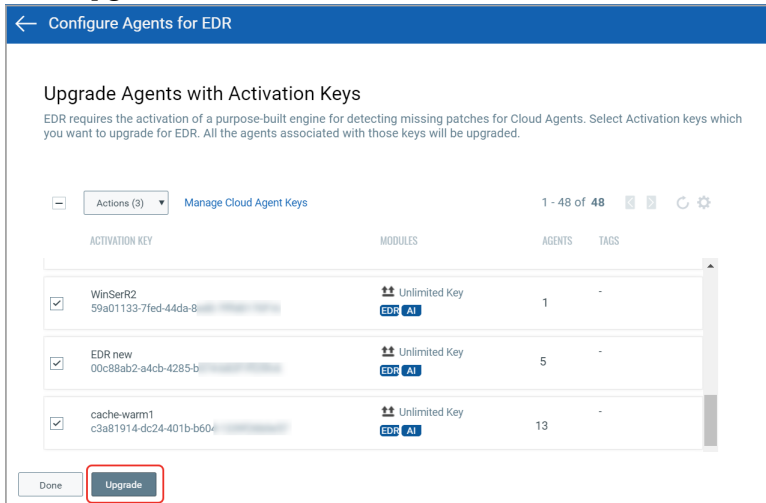


On the Configure Agents for EDR window, you can:

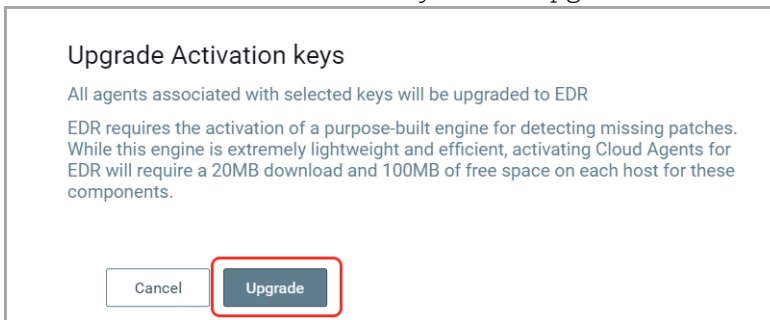
- Select the existing activation key and upgrade the associated agents for EDR.
- Install new Cloud Agent and activate the agent for EDR.

Upgrade Existing Agents

From the Configure Agents for EDR window, select one or multiple Activation Key and click Upgrade.

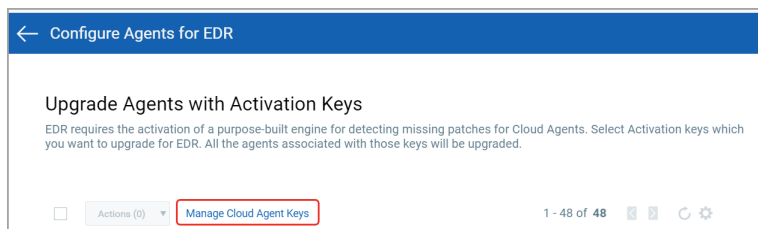


On the confirmation window, click Upgrade to initiate the process. All the agents associated with the activation key will be upgraded and enabled for EDR.



Install Cloud Agent

From the Configure Agents for EDR window, click Manage Cloud Agent Keys. You will be re-directed to the Cloud Agent app.



Click Agent Management > Activation Keys > New Key. Give it a title and provision for the EDR application and click Generate.

New Activation Key Turn help tips: On | Off

Create a new activation key

An activation key is used to install agents. This provides a way to group agents and better manage your account. By default this key is unlimited - it allows you to add any number of agents at any time.

Title: Select | Create

(no tags selected)

Provision Key for these applications

<input type="checkbox"/> AI Asset Inventory Activations managed by AI.	<input type="checkbox"/> PM Patch Management 10000 Activations Remain
<input type="checkbox"/> VM Vulnerability Management 9995 Activations Remaining	<input type="checkbox"/> PC Policy Compliance 1000 Activations Remaining
<input checked="" type="checkbox"/> EDR Endpoint Detection and Response 9992 Activations Remaining	<input type="checkbox"/> FIM File Integrity Monitoring 98 Activations Remaining
<input type="checkbox"/> SCA Secure Config Assessment 10000 Activations Remaining	

Close Unlimited Key **Generate**

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

New Activation Key Turn help tips: On | Off

New activation key generated successfully

Give your key a name and add tags to easily find agents installed using this key. We'll associate the tags to the agent hosts.

Activation Key: ✓

Key Type: Unlimited key

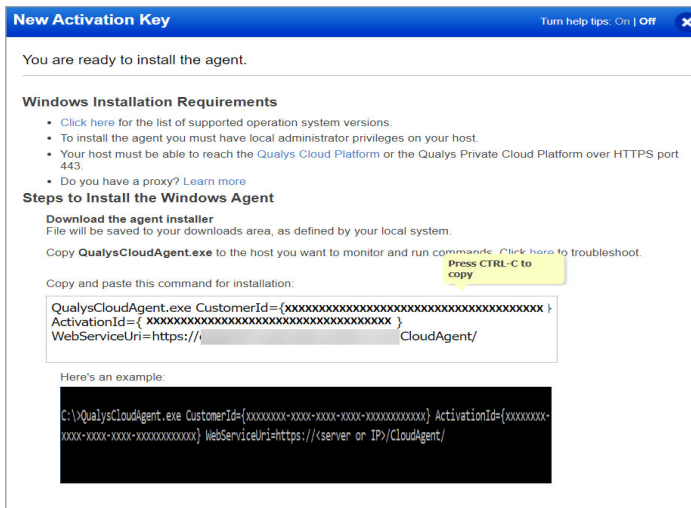
Installation Requirements

Windows (.exe)	x86-32/64	Microsoft Windows Client Microsoft Windows Server	Install instructions
Linux (.rpm)	x64	Red Hat Enterprise Linux CentOS Fedora OpenSUSE SUSE Enterprise Linux Amazon Linux Oracle Enterprise Linux	Install instructions
Linux (.rpm)	ARM64	Red Hat Enterprise Linux CentOS Amazon Linux	Install instructions
Linux (.deb)	x64	Debian Ubuntu	Install instructions

Close

Click on Install Instructions against the Windows (.exe) option.

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.

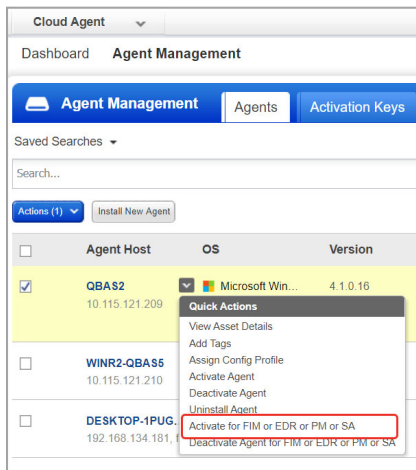


Review the installation requirements and click Download.exe.

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.

Activate your agents for EDR



On the Agents tab choose your agent and "Activate for FIM or EDR or PM or SA" from the Quick Actions menu. (Bulk activation is supported using the Actions menu).

Enable EDR 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 EDR tab:

(1) Toggle Enable EDR module for this profile to ON. This is required for EDR data collection to occur.

(2) Configure what EDR artifacts are transmitted to the Qualys Cloud Platform. Defaults are provided as shown, so this step is optional. You can configure values for max event log size, payload threshold time, and maximum disk usage for EDR data. Toggle a configuration setting to ON before you using it. You must set at least one configuration setting to ON if you have enabled EDR for this profile.

Configure settings constitute the time lapse after which the following types of EDR events are transmitted to the Qualys Cloud Platform:

Max event log size

EDR events are transmitted to the Qualys Cloud platform when the EDR event log file reaches the maximum specified size. You can specify a file size between 10 KB and 10240 KB. Default is 1024 KB. This value can be lower if the Payload threshold time is lower.

Payload threshold time

EDR events are transmitted to the Qualys Cloud platform when the EDR payload threshold time is hit, ie., the specified seconds elapse after the previous payload was sent to the Qualys cloud Platform. You can specify a threshold between 30 seconds and 1800 seconds. Default is 60 seconds. This value is lower the better to prevent data loss on busy systems.

Maximum disk usage for EDR Data

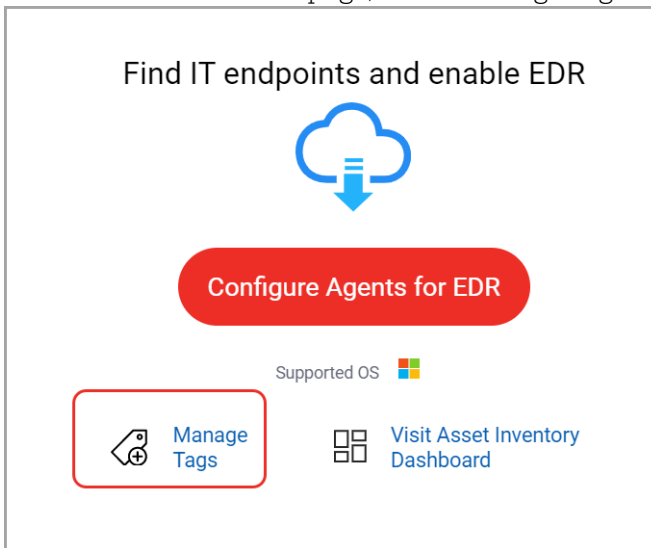
This is the maximum size on disk available to a Cloud Agent for caching EDR events to be sent to the Qualys Cloud Platform for processing. If the maximum size is reached, the oldest events are deleted in order to create space for newly generated events. You can specify a disk usage size between 100 MB and 2048 MB. Default is 1024 MB.

Setting up asset tags (optional)

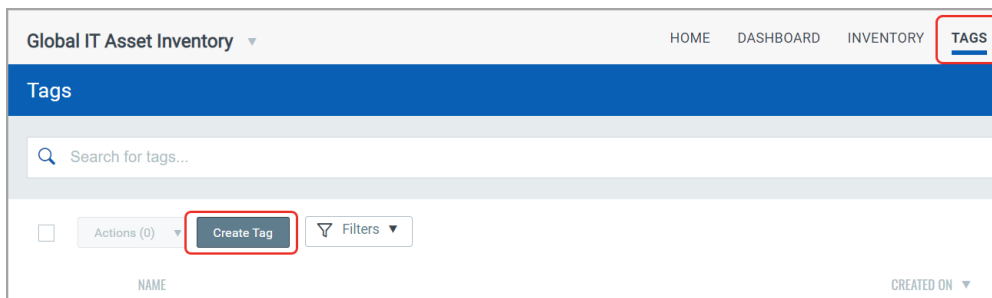
Setting up asset tags using Global IT Asset Inventory helps you to associate EDR assets with a CA configuration profile enabled for EDR. You can avoid assigning configurations manually to each asset by adding asset tags to the required CA configuration profiles.

How to create tags

From the EDR Welcome page, select Manage Tags.



Click Create Tags to add tags for your EDR 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.

Additional Reference

For information on Cloud Agent Platform Matrix, see [Cloud Agent Platform Availability Matrix](#).

What's next?

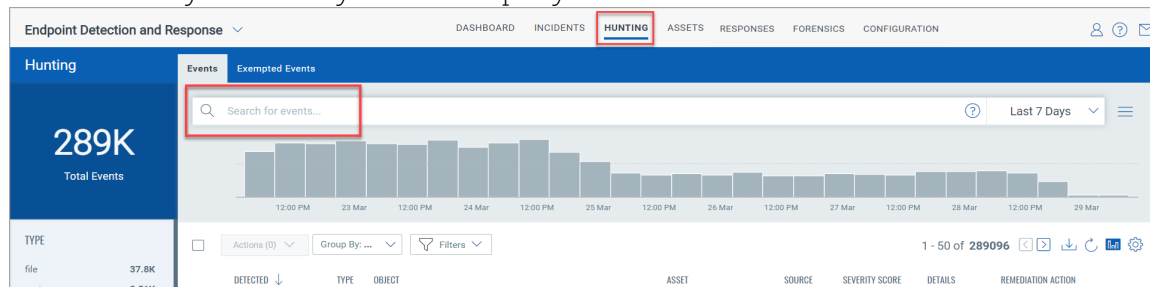
EDR starts collecting data and analyzing your systems right away! Return to the EDR app where you can check out the incidents detected by EDR and system events and details captured by the cloud agent.

EDR Investigation

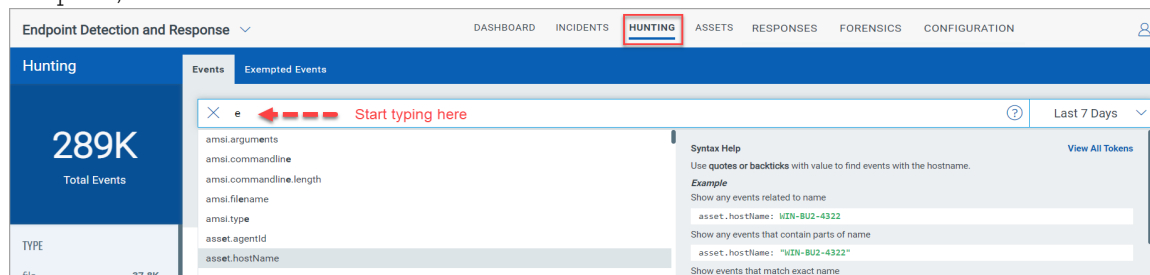
How to Search

Our searching and filtering capabilities give you the ability to quickly find all about your incidents, events and assets all in one place using Qualys Advanced Search. You can search for incidents and assets in the respective tabs in the similar way.

You'll notice the Search box while viewing dynamic lists of events, incidents, and assets. This is where you'll enter your search query.

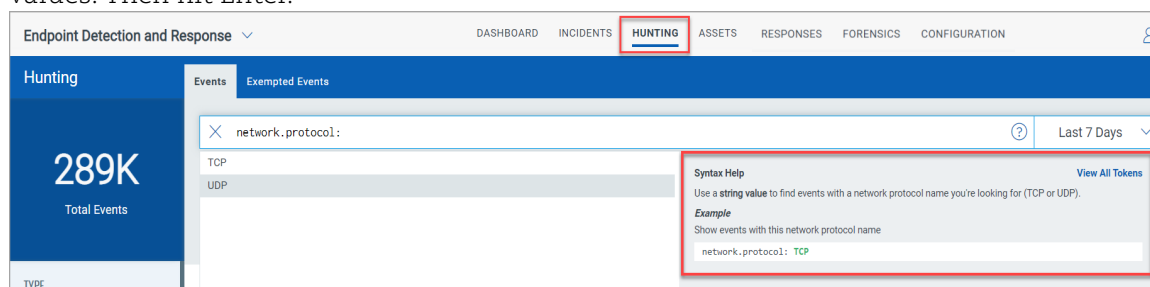


Start typing and we'll show you the properties (fields) you can search like `asset.localIPv4`, `file.path`, etc. and scroll down to see all the fields.



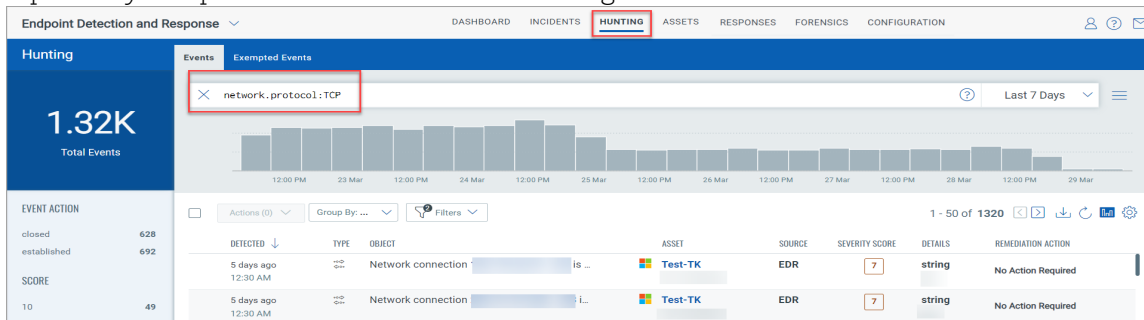
Select the one you're interested in. Check out the Syntax help for the selected field to the right to help with creating your query.

Enter the value you want to match. For this field you select from a list of predefined values. Then hit Enter.



That's it! Your matches will appear in the list you're viewing. Filters on the left help you drill down to objects of interest.

Tip - Use your queries to create dashboard widgets on the Dashboards tab.



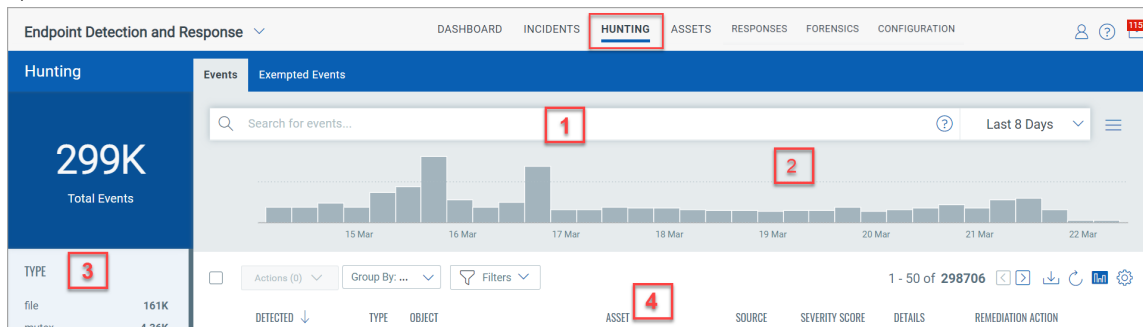
Tip - Go to the EDR online help for details on search language and sample queries.

Hunting events

The Hunting tab, has the following two sub tabs:

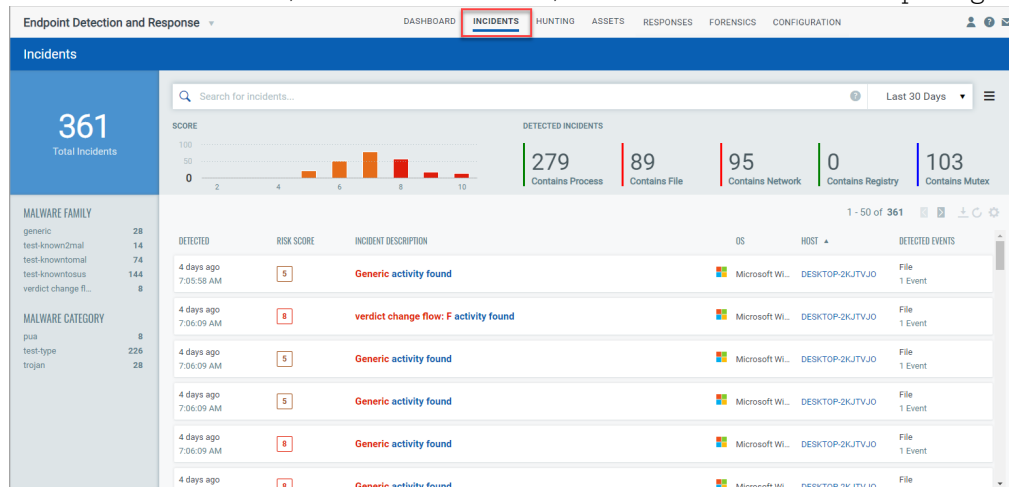
- **Events:** It lists all the events registered and executed on the assets.
- **Exempted Events:** It lists all the events for which exceptions are created.

- 1) Search for events by event properties
- 2) jump to events that occurred in certain time-frame
- 3) group events by type
- 4) view event details and asset details.



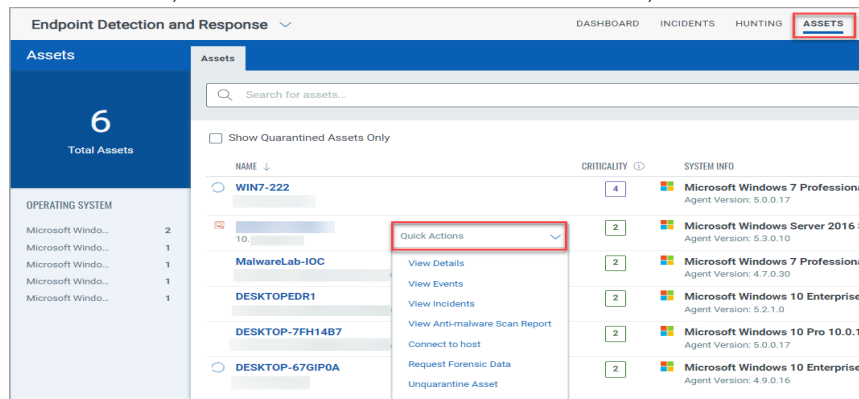
Investigate incidents

Investigate incidents for active threats by Malware name and malware family name. Here all the incidents detected on an asset are listed here. Know the OS and host on which the incident was detected, the events detected, and other information at quick glance..



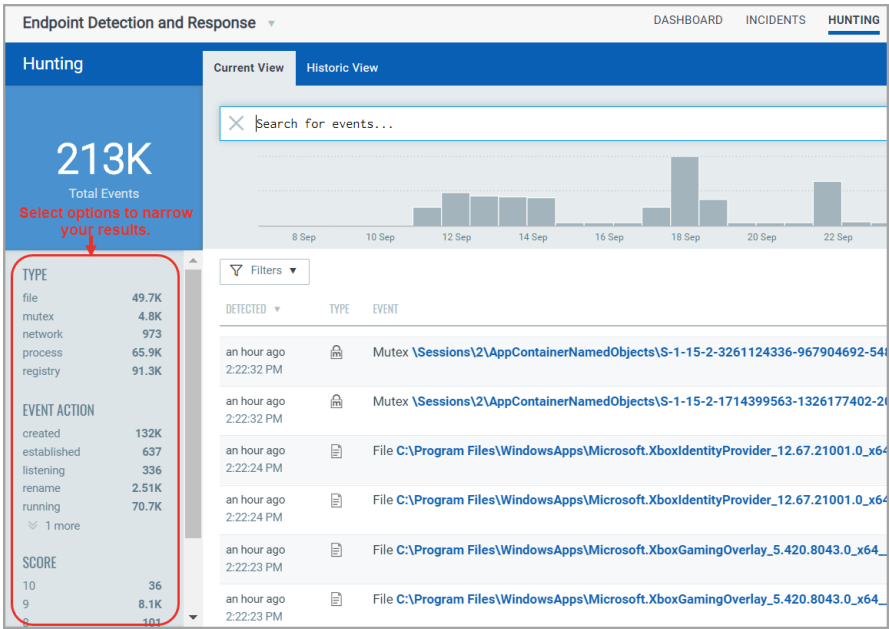
Look into assets monitored by EDR

Get up to date views on a selected asset's details, its events and incidents. Using the Quick action menu, view the Asset Details. Event Details, and Incident details..



Narrow 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 incidents or events.



Download your results

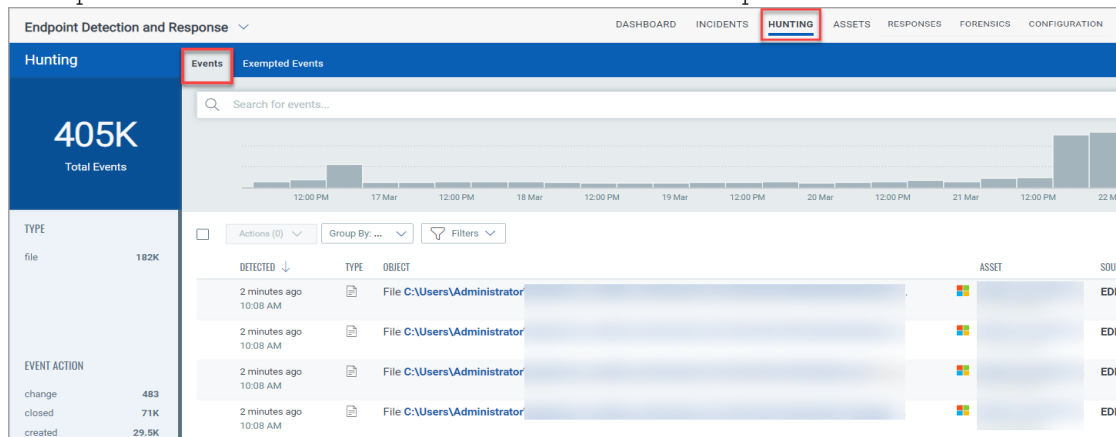
By downloading search results to your local system you can easily manage incidents or events outside of the Qualys platform and share them with other users. You can export results in multiple formats (CSV, XML, PDF, DOC, PPT, HTML-ZIP, HTML-Web Archive).

Remediation Action

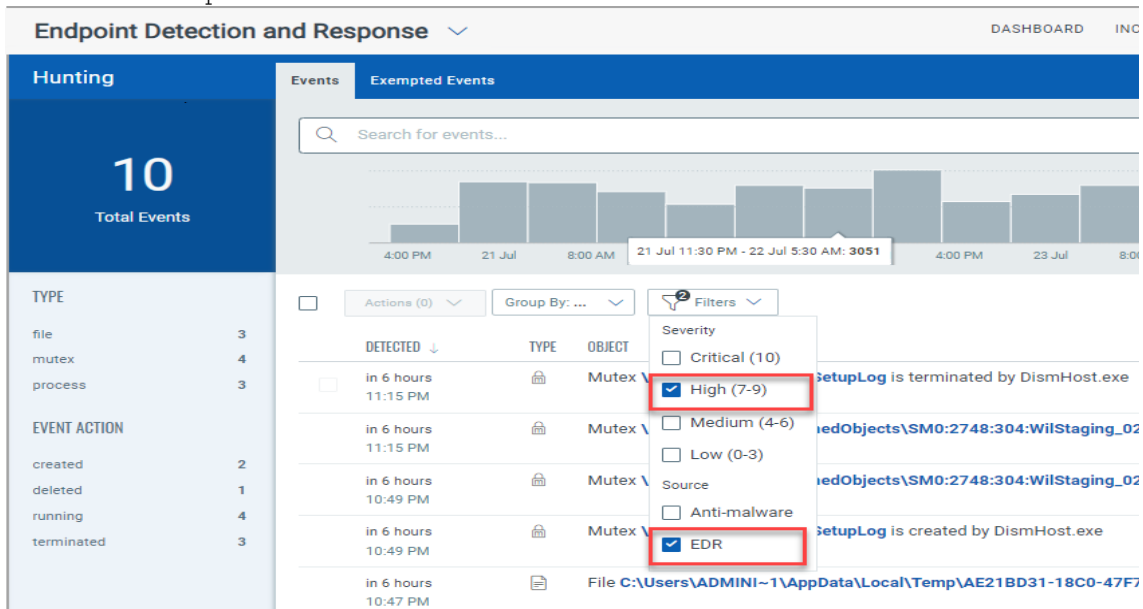
You can remediate malicious events detected on the assets using the Quarantine File, Delete File, and Kill Process options. Remediation actions can be performed for File and Process events from the **Events** page of the **Hunting** tab.

The remediation options are available under the **Remediation Action** column and **Events** page only for:

- Events: It lists all the events for which the exceptions are created.
- Exempted Events: It lists all the events for which the exceptions are created.



Use the **Filters** option to view the malicious events from the list.



Remediation Action for File Events

You can remediate malicious file events, using the following options:

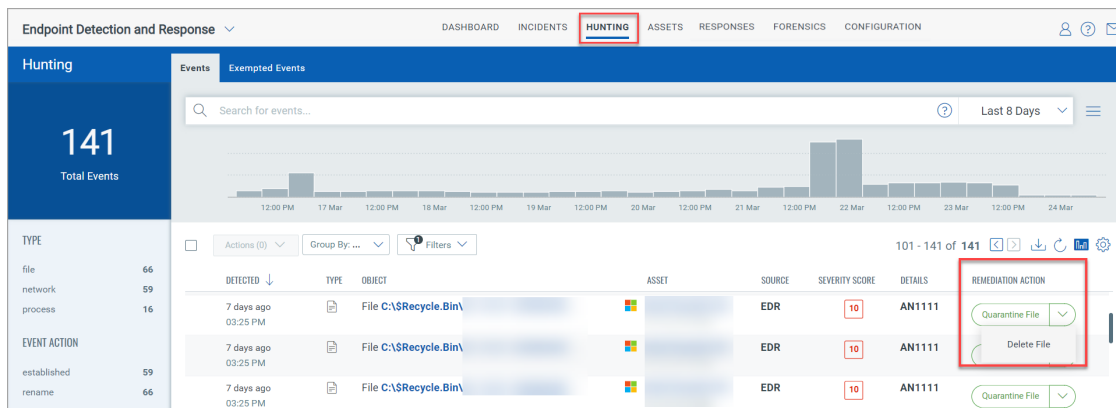
- **Quarantine File:** Using this option, the file is encrypted and then moved to the Quarantine folder (C:\ProgramData\Qualys\QualysAgent\Quarantine\) on your asset. The Quarantine folder is automatically created once you upgrade to agent 4.0 and above. You can undo this action and restore the file to its original position using the UnQuarantine option from the **User Activity** tab. For more information, see [UnQuarantine File](#).

- **Delete File:** Using this option, the file is permanently deleted from your asset. You cannot undo this action.

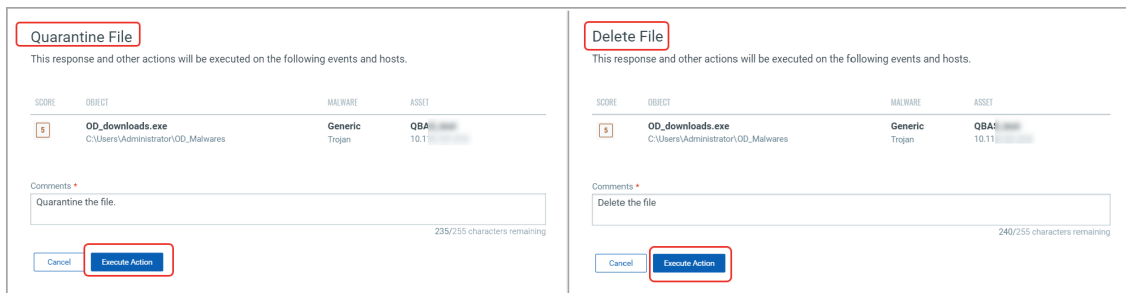
To perform remediation action on file events:

1) Select the required file event and from the **Remediation Action** column, click **Quarantine File** or **Delete File** from the drop-down list.

Note: You can also perform the remediation action from the Events page from the **Quick Actions** menu.



2) Based on your selection (Quarantine File/Delete File), one of the following window is displayed. Enter the required comment and click **Execute Action**.



3) A pop-up message indicating the status of submission request is displayed on the screen. You can click **View Request Status** from the pop-up message, to view the status (In Progress, Success, Failed) of the remediation request on the **User Activity** tab.

Alternatively, you can also view the status for the remediation request from the **Remediation Action** column on the **Hunting** tab.

Endpoint Detection and Response

DASHBOARD INCIDENTS **HUNTING** ASSETS RESPONSES FORENSICS CONFIGURATION

Hunting

145
Total Events

Events Exempted Events

Search for events... Last 8 Days

12:00 PM 17 Mar 12:00 PM 18 Mar 12:00 PM 19 Mar 12:00 PM 20 Mar 12:00 PM 21 Mar 12:00 PM 22 Mar 12:00 PM 23 Mar 12:00 PM 24 Mar

TYPE

file 66
network 63
process 16

Actions (0) Group By: ... Filters

101 - 145 of 145

DETECTED	TYPE	OBJECT	ASSET	SOURCE	SEVERITY SCORE	DETAILS	REMEDIATION ACTION
7 days ago 02:36 PM	File	C:\Windows\System32\drivers\bddcl.s...		EDR	10	AN1111	Delete File: In Progress

Endpoint Detection and Response

DASHBOARD INCIDENTS HUNTING ASSETS **RESPONSES** FORENSICS CONFIGURATION

Responses

145
Total User Activities

User Activity Activity Rule Manager Actions

response.userId: Last 30 Days

Filters

1 - 50 of 145

REQUESTED ACTIVITY	OBJECT	ASSET	SOURCE	USER	STATUS
Quarantine File Mar 23, 2023 11:01 AM	file-sample_100kB.docx		EDR		In Progress
Delete File Mar 23, 2023 11:00 AM	bddcl.sys C:\Windows\System32\drivers		EDR		In Progress

Remediation Action for Process Events

For process events, we provide Kill Process remediation action. When you perform the Kill Process action for events, it kills the corresponding parent process.

1) Select the required event from the **Hunting** tab and from the **Remediation Action** column, select **Kill Process**.

Note: You can also perform the remediation action from the **Event Details** page from the **Quick Actions** menu.

The screenshot shows the EDR interface with the 'Hunting' tab selected. On the left, a sidebar shows '145 Total Events' and a breakdown by type: file (66), network (63), and process (16). The main area displays a timeline of events from 12:00 PM on 17 Mar to 12:00 PM on 24 Mar. Below the timeline, there are filters for 'Actions (0)', 'Group By: ...', and 'Filters'. A table of events is shown with columns: DETECTED, TYPE, OBJECT, ASSET, SOURCE, SEVERITY SCORE, DETAILS, and REMEDIATION ACTION. One event is highlighted with a red border, showing '7 days ago 10:01 AM', 'Process C...', 'PID:6416', 'ASSET', 'EDR', and a 'SEVERITY SCORE' of 10. The 'REMEDIATION ACTION' column for this event shows a 'Kill Process' button.

2) The **Kill Process** window is displayed. Use the arrow button next to the Score column to view the list of related events.

Note: We display up to 50 related events.

If the event has related files, you can choose to **Quarantine file**, **Delete files** or perform no action by selecting **None**.

3) Enter the comment and click **Execute Action**.

The 'Kill Process' window displays a table of related events with columns: SCORE, OBJECT, MALWARE, PID, ASSET, and RELATED EVENTS. The first row shows a score of 10, object 'DB Browser for SQLite...', malware 'sus-mal test-type', PID '10452', and asset 'QL...'. Below the table, there is a section for 'Other Available Actions For Related File Events' with radio buttons for 'None', 'Quarantine File', and 'Delete File'. A 'Comments' field contains the text 'Kill Process and quarantine file.' and a character count '222/255 characters remaining'. At the bottom, there are 'Cancel' and 'Execute Action' buttons, with the 'Execute Action' button highlighted by a red box.

4) A pop-up message indicating the status of submission request is displayed on the screen. You can click **View Request Status** from the pop-up message, to view the status (In Progress, Success, Failed) of the remediation request on the **User Activity** tab.

Endpoint Detection and Response

DASHBOARDINCIDENTSHUNTINGASSETSRESPONSESFORENSICSCONFIGURATION

Responses

145
Total User Activities

response.userId: Last 30 Days

Filters

101 - 145 of 145

REQUESTED ACTIVITY	OBJECT	ASSET	SOURCE	USER	STATUS
Kill Process			EDR		Success

Alternatively, you can also view the status for the remediation request from the **Remediation Action** column on the **Hunting** tab.

User Activity

The User Activity page lists all the remediation activities performed on the events, with the following details:

- The requested remediation action along with the date and time.
- The object (file/process) and the asset on which the action is performed.
- The user who performed the remediation action.
- The current status of the remediation action.

The screenshot shows the 'Responses' tab in the Microsoft Defender for Endpoint console. The 'User Activity' sub-tab is selected. A search filter 'response.userId:' is applied. The table displays a list of remediation actions with columns for Requested Activity, Object, Asset, Source, User, and Status.

REQUESTED ACTIVITY	OBJECT	ASSET	SOURCE	USER	STATUS
Kill Process Mar 20, 2023 10:57 AM	msedge.exe C:\Program Files\Microsoft Edge\Application\msedge.exe		EDR		Success
Delete File Mar 20, 2023 10:17 AM	procexp_remediation_test1.exe C:\test\VC\ProcessExplorer\ProcessExplorer		EDR		Success
Kill Process Mar 20, 2023 10:17 AM	procexp_remediation_test1.exe C:\test\VC\ProcessExplorer\ProcessExplorer\procexp_remediation_test1.exe		EDR		Success
UnQuarantine File Mar 20, 2023 09:10 AM	123_SUSPICIOUS.exe C:\Users\Administrator\Desktop\123\Suspicious.exe		EDR		Success

For additional information about the remediation action, click on the remediation action from the **Requested Activity** column.

Quarantine File

This remediation action is successfully executed. Refer to the following details.

file-sample_100kB.docx

Action Status: Success

8 Score

File Details

Object	file-sample_100kB.docx	Asset	Win10-IOC20
Malware Family	test-knownfomal	IP Address	10.115.109.87
Request Time	May 12, 2021 04:38 AM	Path	C:\Users\Administrator\Documents\file-sample_100kB.docx
Execution Time	May 12, 2021 04:38 AM		Test\Pe NonPE Files\Pe NonPE Files\Office Files
User		Comment	1234

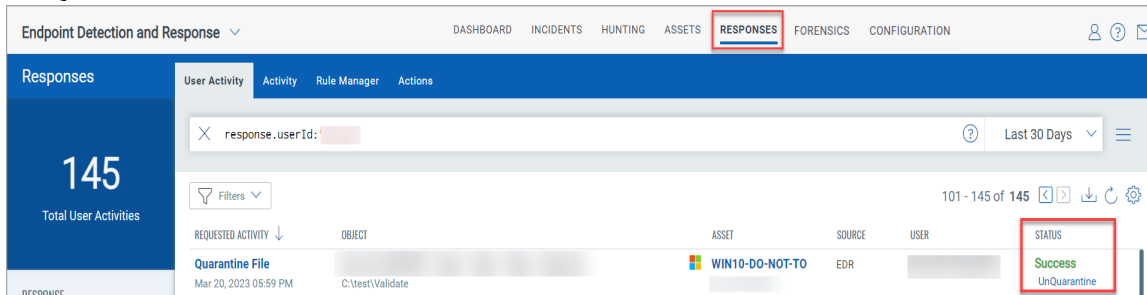
Ok

UnQuarantine File

This option allows you to restore the quarantine file back to its original position.

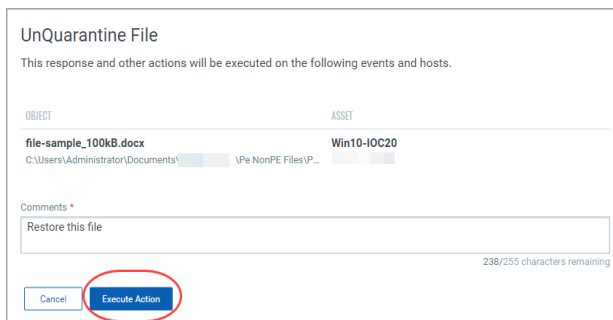
1) Click **Responses > User Activity**.

2) From the list, select a quarantine file event and from the **Status** column, click **UnQuarantine**.



The screenshot shows the 'Endpoint Detection and Response' dashboard. The 'Responses' section is active, displaying a list of user activities. A sidebar on the left shows '145 Total User Activities'. The main table has columns for 'REQUESTED ACTIVITY', 'OBJECT', 'ASSET', 'SOURCE', 'USER', and 'STATUS'. One row is highlighted, showing a 'Quarantine File' event for 'file-sample_100KB.docx' on 'Win10-IOC20'. The 'STATUS' column for this row shows 'Success' and 'UnQuarantine'.

3) The **UnQuarantine File** window is displayed. Enter the required comment and click **Execute Action**.



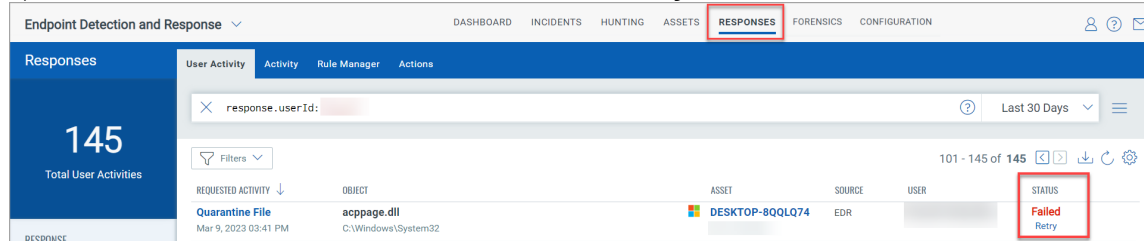
The 'UnQuarantine File' window is shown. It displays the object 'file-sample_100KB.docx' and the asset 'Win10-IOC20'. Below this, there is a 'Comments' section with a text box containing 'Restore this file'. At the bottom, there are two buttons: 'Cancel' and 'Execute Action'. The 'Execute Action' button is circled in red.

4) You can track the progress of the action from the **User Activity** tab.

Retry Option

This option allows you to retry the remediation action on failed events.

1) Select the Failed remediation event and click **Retry** from the **Status** column.



Endpoint Detection and Response

DASHBOARD INCIDENTS HUNTING ASSETS **RESPONSES** FORENSICS CONFIGURATION

Responses

145
Total User Activities

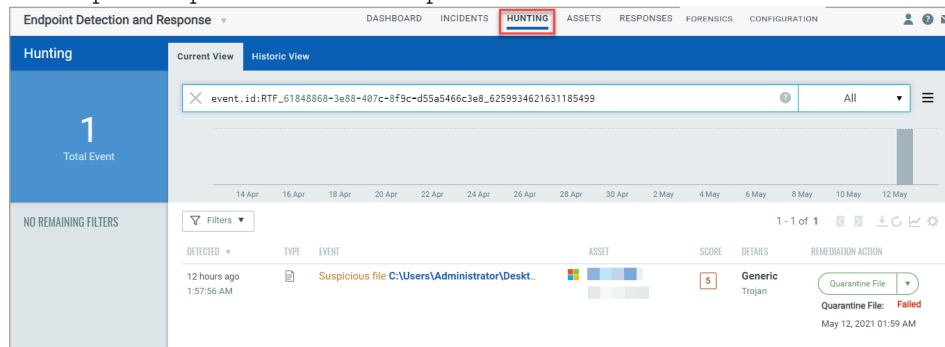
response.userId: [Search Bar] Last 30 Days

Filters

101 - 145 of 145

REQUESTED ACTIVITY	OBJECT	ASSET	SOURCE	USER	STATUS
Quarantine File Mar 9, 2023 03:41 PM	acppage.dll C:\Windows\System32	DESKTOP-8QQLQ74	EDR		Failed Retry

2) You will be redirected to the **Hunting** tab. From the **Remediation Action** column, select the required option from the drop-down list.



Endpoint Detection and Response

DASHBOARD INCIDENTS **HUNTING** ASSETS RESPONSES FORENSICS CONFIGURATION

Hunting

1
Total Event

event.id: RTF_61848868-3e88-407c-8f9c-d55a5466c3e8_6259934621631185499 All

14 Apr 16 Apr 18 Apr 20 Apr 22 Apr 24 Apr 26 Apr 28 Apr 30 Apr 2 May 4 May 6 May 8 May 10 May 12 May

1 - 1 of 1

DETECTED	TYPE	EVENT	ASSET	SCORE	DETAILS	REMEDIATION ACTION
12 hours ago 1:57:56 AM		Suspicious file C:\Users\Administrator\Desktop\...		5	Generic Trojan	Quarantine File Quarantine File: Failed May 12, 2021 01:59 AM

Event Details

The Event Details page lists all the information about the events. To view the Event Details page, click **Quick Actions > Event Details**.

The screenshot shows the EDR interface with the 'Hunting' tab selected. A table of events is displayed, with a red box highlighting the 'Quick Actions' dropdown menu for a specific event. The dropdown menu includes options: 'Event Details', 'Asset Details', 'Events', 'View Surrounding Events', and 'Create Exception'.

From the Event Details page, you can perform the remediation actions (Quarantine File/ Delete File/ Kill Process) on File and Process events. For more information on remediation action, see [Remediation Action for File Events](#) and [Remediation Action for Process Events](#).

MITRE ATT&CK Tactics and Techniques

MITRE ATT&CK defines the tactics, techniques, and procedures that are leveraged by adversaries and malware. EDR helps detect malicious behavior on the endpoint by evaluating the events in context with MITRE ATT&CK.

Events registered on the agents are analyzed, and appropriate ATT&CK tactics and techniques are applied on the Event Details page.

The screenshot shows the 'Event Details: chrome.exe' page. A red box highlights the 'MITRE ATT&CK Technique/s' section, which lists 'T1154: Abuse Elevation Control Mechanism'. The 'MITRE ATT&CK Tactics/s' section lists 'T1043: Reconnaissance'. The 'Process' section shows the process name 'chrome.exe' and its full path.

Non-Portable Executable Files

All the detected non-Portable Executable (non-PE) files are listed in the **Events** page of the **Hunting** tab. Navigate to a non-pe file and in the event details section you can view the details of the file as well as Parent Process and Process Tree details. For example if it is a .pptx file, you will view the following details in your event details Summary:

The screenshot shows the 'Event Details: Introduction to cloud.pptx' page. The left sidebar has 'VIEW MODE' with options: Summary, Parent Process, and Process Tree. The main area is titled 'Summary' and shows file details for 'Introduction to cloud.pptx' (Path: C:\Users\Administrator\...). A red box highlights the 'File' section, which includes: File Action (WRITE), File Type (-), File Extension (pptx), Macro Enabled (No), File Name (Introduction to cloud.pptx), File Size (971.11 KB), Created On (Apr 12, 2021 11:34 PM), Modified On (Apr 13, 2021 12:04 AM), Accessed On (Apr 13, 2021 12:14 AM), Author, Last Modified By, Creating Application (Microsoft Office PowerPoint), Title (Introduction to cloud), Pages (7), Version (-), Path (C:\Users\Administrator\...), Full Path (C:\Users\Administrator\...\Introduction to cloud.pptx), MD5 (9ce94e23857fa74245e74dbf317601e0), and SHA256 (d1750735d827668572653d31c0761acfc5a3c43ac4404deafb054e3e23370c5). The right sidebar shows 'Asset Details' for WIN10-98-91 (OS: Windows) and 'Activity' logs.

View Process Tree for Events

Click **Event Details** > **Process Tree** tab, to view the process tree for File or Process events. The process tree displays all the related events of the selected event and its parent and child processes. In the process tree view, the selected event node is highlighted with the blue color. You can traverse between the nodes by clicking a node in the hierarchy. You can click on the (+) and (-) to expand and collapse the tree nodes and display the related events.

You can click on the event node to view the details of the selected node in the right pane.

The screenshot shows the 'Event Details: bddci.sys' page. The left sidebar has 'VIEW MODE' with options: Summary, Event History, Certificate, Parent Process, Response, and Process Tree. The main area is titled 'Process Tree' and shows a tree diagram with 'Installer.exe' highlighted in a red box. Other nodes include 'gemma.sys', 'atc.sys', 'bdelam.sys', and 'bddci.sys'. The right sidebar shows 'FILE DETAILS' for 'bddci.sys' and 'Threat details' including Threat Name (T1036_1), Anti-malware (-), Behavioral (T1036_1), ATT&CK Tec... (T1036 - Masquerading), ATT&CK Tact... (TA0005 - Defense Evasion), Family (-), and Category (-). The Severity Score is 10.

Customizable Dynamic Dashboards

Dashboards help you visualize your assets, see your threat exposure, leverage saved searches, and remediate priority of malicious/suspicious events quickly.

We have integrated Unified Dashboard (UD) with EDR. 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 EDR 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 vulnerability posture view.

For more information on Unified Dashboards, refer [Online Help](#).

Alerts, Rules, and Actions

Roles and Permissions

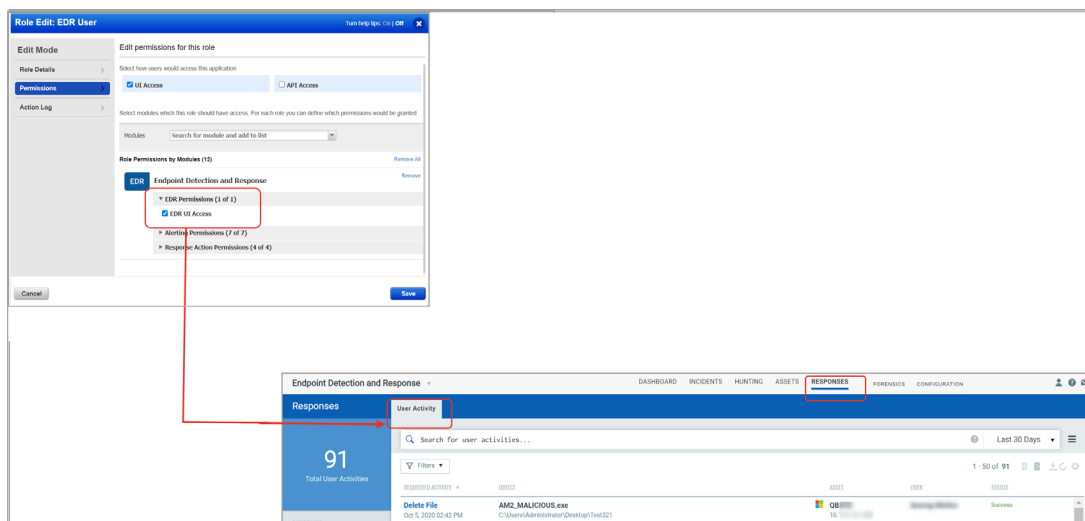
You can create users and then assign a role to them to grant access as per the role you define. Depending on the roles and permissions assigned, the user can perform actions like creating, editing, or deleting rules and actions.

The Administration module is used to create EDR users and assign roles and permissions. We have provided some pre-created user roles for EDR. Depending on the role, you get the associated set of permissions.

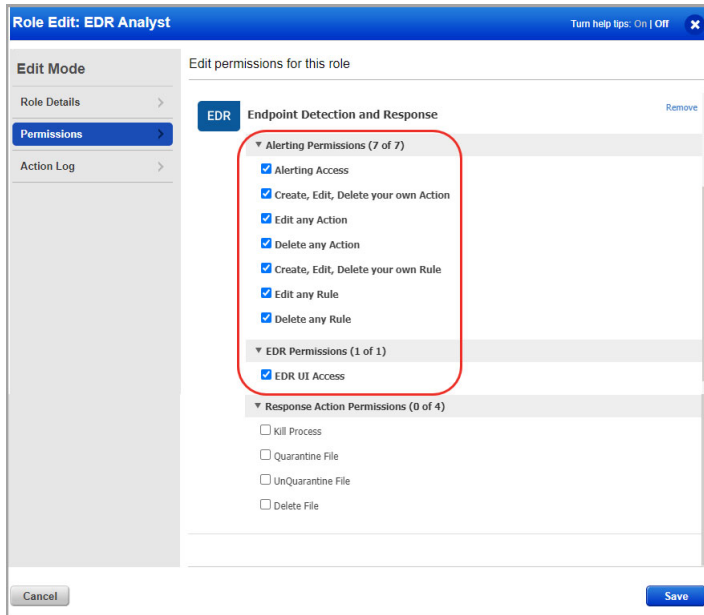
Note: Users created before EDR version 1.1.0 will continue to have the same permissions.

--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 the Manager role can create other users and assign roles.

--EDR User: By default, the EDR role have EDR UI Access permissions only. So, the user can only see the User Activity tab under Responses..



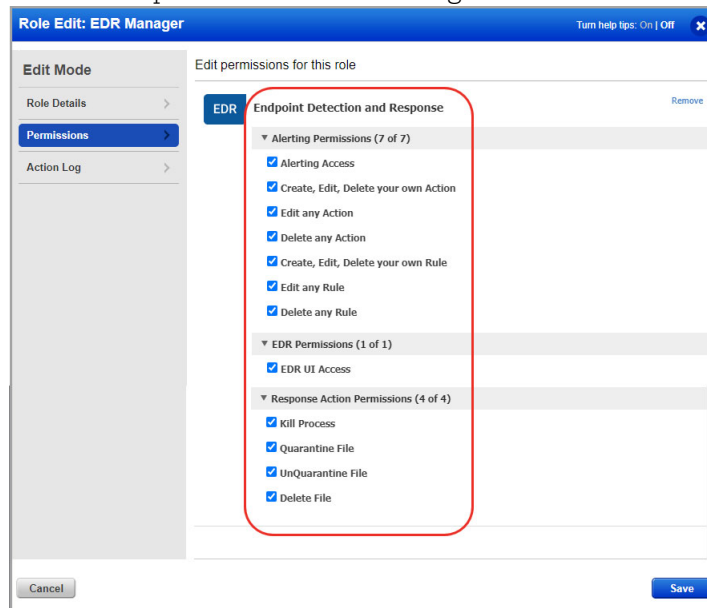
--EDR Analyst: By default, the EDR Analyst role has EDR UI Access permissions and Alerting Permissions.



--EDR Incident Responder and EDR Manager: By default, these roles have EDR UI Access permissions, Alerting Permissions, and Response Action Permissions.

Note: The Manager user can customize the permissions for all the EDR roles.

The default permissions EDR Manager role:

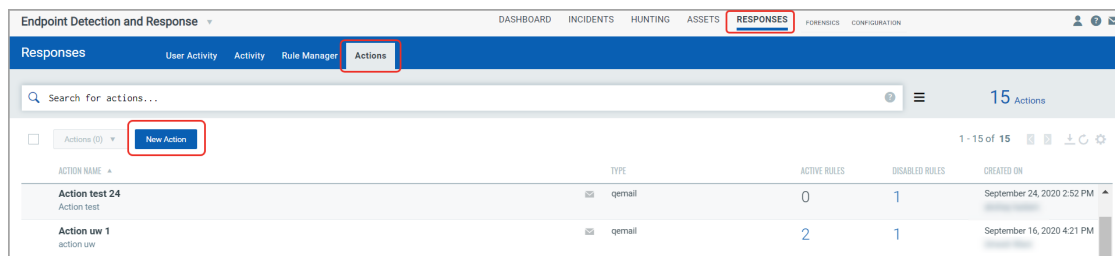


Configure Rule Based Alerts for Events

You can configure EDR to monitor events that satisfy the conditions specified in a rule and send you alerts if events matching the condition is detected. For EDR to send alerts, you need to first configure a rule action to specify what action to be taken when events matching a condition is detected. EDR will use the rule action settings to send you the alerts. Finally, create a rule to specify the conditions for triggering the rule and select rule actions for sending the alert when a rule is triggered.

Create a New Action

To create an action, go to Responses > Actions > 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 EDR will use to send alerts.
- We support these three actions: Send Email (Via Qualys), Post to Slack, or Send to Pager Duty for alerts.
- Select Send Email (Via Qualys) to receive email alerts and specify the recipients' email ID who will receive the alerts, subject of the alert message and the customized alert message.
- Select "Send to PagerDuty" to send alerts to your PagerDuty account. Provide the service key that EDR will require to connect to your PagerDuty account. In Default Message Settings, specify the subject and the customized alert message.
- Select Post to Slack to send messages to your Slack channel. Provide the webhook URL to post messages from Qualys into Slack. Also, provide the channel and alert message that should be posted by default.

←

Create New: Action

Basic Information

Action Name *

Log events action

Description *

This action will record all events on log files.

Select Action *

Send Email(Via Qualys)

Default Message Settings

You can add default recipients or edit the default message to be sent

Recipients *

jdoe@qualys.com

Subject Line *

Events on log files

Message *


This message is sent for all log events|

40/5000

Cancel

Save

Create a New Rule

To create a rule, go to Responses > Rule Manager > New Rule. You can also create rules from the customized queries that are used for widgets on your dashboard. Select the Widget menu and choose “Create Rule from this Widget”. This option is also available on the Hunting page. Go to the Hunting tab, select an event filter in the left pane or type a search query in the search bar. Click actions menu  on the right of the search bar and select “Create Alert Rule From Search Query” from the menu.

Endpoint Detection and Response

DASHBOARD

INCIDENTS

HUNTING

ASSETS

RESPONSES

FORENSICS

CONFIGURATION

Responses

User Activity

Activity

Rule Manager

Actions

Search for rules...

14 Rules

Actions (0)

New Rule

RULE NAME	TRIGGER CRITERIA	AGGREGATE	ACTION	LAST TRIGGERED	STATE	CREATED ON
Rule 25	Single Match	-	Action uw 1	September 25, 2020 12:23 PM	Disabled	September 25, 2020 12:23 PM
Rule uw 1	Single Match	-	Action uw 1	September 29, 2020 10:15 PM	Enabled	September 16, 2020 4:24 PM
Rule uw 2	Single Match	-	Action uw 2	September 23, 2020 6:05 PM	Disabled	September 16, 2020 4:25 PM
Rule uw 2_copy	Single Match	-	Action uw 2	September 29, 2020 10:15 PM	Enabled	September 25, 2020 6:18 PM

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, specify a query for the rule. The system uses this query to search for events. Use the Test Query button to test your query. Click Sample Queries link to select from predefined queries.
- You can 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.
- In the Action Settings section choose the actions that you want the system to perform when an alert is triggered.

← Create New: Rule

Rule Details

Provide the following information to create the rule

Rule Information

Rule Name *

Rule for score indicator

Description *

This rule will list all score between 8 to 10.

Rule Query

Provide a query to match particular source that will trigger the alert

Rule Query *

✕ indicator.score:[8,9,10]

Sample Queries

Test Query

Trigger Criteria

Provide the match criteria

Trigger Criteria *

Single Match ▼

Action Settings

Choose an appropriate alert action

Actions *

pager-1 ✕ ▼

pager-1

Description *

Pager alert from POD1

Message *

Insert token ▼

["key":"value"]

15/5000

Cancel

Save

33

Trigger Criteria

- Select Single Match if you want the system to generate an alert each time the system detects an event matching your search query.
- Select Time-Window Count Match when you want to generate alerts based on the number of events 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 mins window.

The screenshot shows the 'Trigger Criteria' configuration interface. At the top, it says 'Provide the match criteria' and 'Trigger Criteria *'. A dropdown menu is set to 'Time-Window Count Match'. Below this, the section 'Time-Window Count Match' is active. It contains two input fields: 'No Of Matching Events *' with the value '3' and 'In *' with the value '15' and a unit dropdown set to 'Mins'. At the bottom, there are two more dropdowns: 'Aggregate Alerts' set to 'Yes' and 'Aggregate Group' set to 'Action'.

- Select Time-Window Scheduled Match when you want to generate alerts for matching events that occurred during a scheduled time. The rule will be triggered only when an event 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 pm and 5 pm.

The screenshot shows the 'Trigger Criteria' configuration interface for a scheduled match. It says 'Provide the match criteria' and 'Trigger Criteria *'. A dropdown menu is set to 'Time-Window Scheduled Match'. Below this, the section 'Time-Window Schedule Match' is active. It contains several fields: 'Time Window Starts on' with a date picker set to '07/20/2020', 'Start Time' with a time picker set to '2:26pm', 'Time Window Ends On' with a date picker set to '07/20/2020', 'End Time' with a time picker set to '3:26pm', 'Duration' with a slider set to '1 Hour', and 'Repeats' with a dropdown set to 'Daily'. A summary line reads 'Summary: Repeats everyday from 02:26 pm to 03:26 pm (1 Hour)'. At the bottom, there are two more dropdowns: 'Aggregate Alerts' set to 'Yes' and 'Aggregate Group' set to 'Action'.

For the Weekly option, select the days of the week on which schedule will run. For example, send weekly alerts with all matches generated between 4.56 pm and 5.56 pm on every Monday and Wednesday.

The screenshot shows the 'Create New: Rule' form with the 'Repeats' dropdown set to 'Weekly'. Under 'On Day Of The Week', the checkboxes for Monday (M) and Wednesday (W) are selected. The summary at the bottom states: 'Summary: Repeats monday from 04:56 pm to 05:56 pm (1.00 hours)'.

For the Monthly option, specify the day of the month on which the schedule will run. For example, send monthly alerts on the first day of every month.

The screenshot shows the 'Create New: Rule' form with the 'Repeats' dropdown set to 'Monthly'. The 'Recurring Day' is set to '1' day of the month. The summary at the bottom states: 'Summary: Repeats every 1st day of the month from 04:56 pm to 05:56 pm (1.00 hours)'. At the bottom, 'Aggregate Alerts' is set to 'Yes' and 'Aggregate Group' is set to 'Action'.

For “Time-Window Count Match” and “Time-Window Scheduled Match”, you have the option to aggregate the alerts by aggregate groups such as based on action, asset hostname and so on.

Manage 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 edit, delete and rename an action. Use the search bar to search for actions using the search tokens.

The screenshot shows the 'Manage Actions' interface. The 'Responses' tab is selected, and the 'Actions' sub-tab is active. A search bar at the top says 'Search for actions...'. Below it, a table lists actions. A 'Quick Actions' menu is open over the first row, showing options: View, Edit, Save As, and Delete.

ACTION NAME	TYPE	ACTIVE RULES	DISABLED RULES	CREATED ON
<input checked="" type="checkbox"/> Action uw 1 action uw	gmail	2	1	September 16, 2020 4:21 PM
<input type="checkbox"/> Action uw 2 action uw	gmail	1	1	September 16, 2020 4:22 PM
<input type="checkbox"/> AlertSanityRequestedByAlertTeam jvkid	gmail	1	0	October 6, 2020 2:02 PM
<input type="checkbox"/> Delete OD Test	slack	0	0	September 30, 2020 7:03 PM

Manage 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 Actions menu or Quick Actions menu to edit, enable, disable, delete and rename a rule. Use the search bar to search for rules using the search tokens.

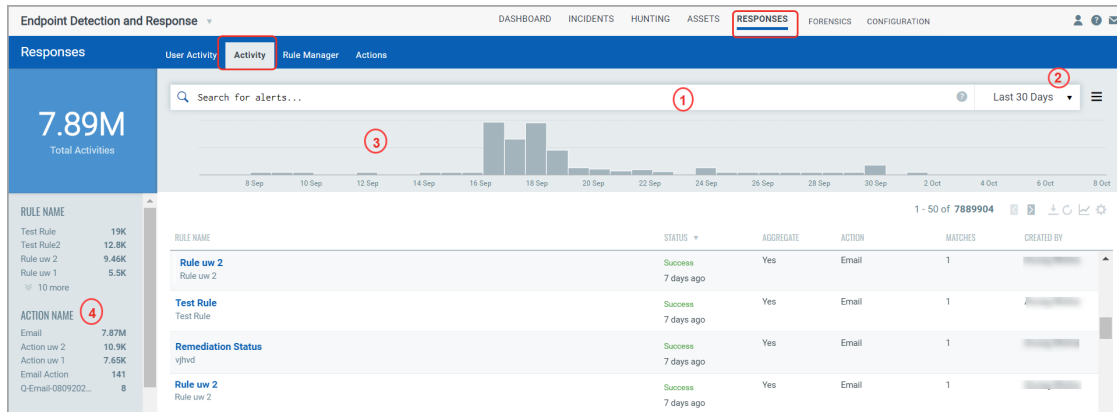
The screenshot displays the 'Endpoint Detection and Response' interface. The top navigation bar includes 'DASHBOARD', 'INCIDENTS', 'HUNTING', 'ASSETS', 'RESPONSES' (highlighted), 'FORENSICS', and 'CONFIGURATION'. The 'RESPONSES' section has a sub-navigation bar with 'User Activity', 'Activity', 'Rule Manager' (selected), and 'Actions'. Below this is a search bar 'Search for rules...' and a 'New Rule' button. The main table lists rules with columns: RULE NAME, TRIGGER CRITERIA, AGGREGATE, ACTION, LAST TRIGGERED, STATE, and CREATED ON. A 'Quick Actions' menu is open for the first rule, showing options: View, Edit, Enable, Disable, Save As, Delete, and Show Activity.

RULE NAME	TRIGGER CRITERIA	AGGREGATE	ACTION	LAST TRIGGERED	STATE	CREATED ON
Remediation Status vftvd	Single Match	-	Email Action	September 25, 2020 5:36 PM	Enabled	September 7, 2020 8:20 PM Anurag Mishra
Rule 25 Rule uw 25	Single Match	-	Action uw 1	September 25, 2020 12:23 PM	Disabled	September 25, 2020 12:23 PM akashay kadam
Rule uw 1 Rule uw 1	Single Match	-	Action uw 1	September 29, 2020 10:15 PM	Enabled	September 16, 2020 4:24 PM Umesh Wani
Rule uw 2 Rule uw 2	Single Match	-	Action uw 2	September 23, 2020 6:05 PM	Disabled	September 16, 2020 4:25 PM Umesh Wani
Rule uw 2_copy Rule uw 2	Single Match	-	Action uw 2	September 29, 2020 10:15 PM	Enabled	September 25, 2020 6:18 PM akashay kadam
Rule_23 Rule_23	Single Match	-	Action uw 1	September 29, 2020 10:15 PM	Enabled	September 23, 2020 10:47 AM Anurag Mishra

Manage Alerts

Activity tab lists all the alerts. Here you will see for each alert, rule name, success or failure in sending the alert message, aggregate enabled (Yes) or 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).



Malware Protection

Qualys Multi-Vector EDR now includes integrated antimalware detection capabilities, providing additional real-time protection against the latest threats. The new release expedites the inevitable convergence of Malware Protection Products with Endpoint Detection & Response (EDR) to deliver comprehensive protection against known and unknown threats.

Easily enabled on any endpoint where the Qualys Cloud Agent is installed, the new release of Qualys Multi-Vector EDR can be fully managed remotely on any endpoint with internet connectivity. No need for a VPN or any other network change. Once deployed, the new anti-malware component protects you against all kinds of malware (such as viruses, spyware and trojans, ransomware), network attacks, and phishing. Details of actions taken and information about program operation are available in the Qualys cloud-based console.

Key Capabilities

- On-access protection: prevents new malware threats from entering the system by scanning local and network files when they are accessed (opened, moved, copied or executed), boot sectors, and potentially unwanted applications (PUA).
- On-demand scanning: scans the file system and memory for malware and other threats and takes remediation actions
- Advanced Protections: Continuously monitors applications running on the endpoint for malware-like actions and automatically disinfects the detected file. In addition, Qualys Malware Protection can expose advanced attacks and suspicious activities in the pre-execution stage. This layer of security contains machine learning models and stealth attack detection technology
- Behavioral-based protection: operating on a zero-trust assumption, Qualys Malware Protection can monitor active applications and processes for any signs of malicious behavior. It relies on actual behavior characteristics instead of signatures or binary or code fingerprints. This allows Qualys Malware Protection to consistently detect new ransomware variants, other zero-day threats, and file-less attacks
- Network and Traffic Protection: prevents malware from being downloaded to the endpoint by scanning incoming emails and web traffic in real-time. In addition, protect against attack techniques used to gain access to specific endpoints, such as brute-force attacks, network exploits, and password stealers.
- Phishing Protection: Automatically block known phishing web pages to prevent users from inadvertently disclosing private or confidential information to online fraudsters.

Malware detection events can be viewed and analyzed from the Qualys Cloud Console, allowing customers to enrich malicious events with contextual events collected by Qualys EDR.

Get Started with Malware Protection

We'll help you quickly get started with the Malware Protection setup. You will need to install the Qualys Cloud Agent in your environment and have an active Endpoint Detection and Response (EDR) subscription.

Step	Details
Setup Cloud Agent	Install a Cloud Agent that's been activated for EDR on each asset you want to monitor for suspicious activity. See
Enable Malware Protection on Cloud Agent	To start collecting information on your endpoints, you need to install the Malware Protection on your asset. For that, first, you must enable the Malware Protection for the Cloud Agent profile.
Configuring the AV Profile	As the virus definitions are downloaded on the endpoint, the default antivirus configurations are also downloaded on this endpoint asset.
Use the Endpoint Detection and Response UI	In your Qualys EDR module, navigate to the Hunting tab > Events tab to view the detections done by the Malware Protection. Use the filter to view only Malware Protection events in your list.
Monitor Assets	You can monitor the detections and the actions performed on those detections on your endpoint asset using the Malware Protection and the EDR UI. You can view all the files that were terminated or quarantined as per the profile you configured. You can also undo actions performed on those detections.

For more information, see the [EDR Online help](#).