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
  Setting up asset tags (optional) ..................................................................................... 6

Download and Configure Cloud Agent for EDR.............................................................. 7
  Download Cloud Agent for EDR .................................................................................... 7
  Configure Agents for EDR ............................................................................................ 8
  Activate your agents for EDR ....................................................................................... 11
  Enable EDR in a configuration profile ........................................................................ 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 .......................................................................................................... 19
  Remediation action for file events .............................................................................. 20
  Remediation action for Process, Mutex, Network events ....................................... 22
  User Activity ............................................................................................................... 24
  Event Details ................................................................................................................. 27

Customizable Dynamic Dashboards ................................................................................ 29

Alerts, Rules, and Actions ............................................................................................... 31
  Roles and Permissions ............................................................................................... 31
  Configure Rule Based Alerts for Events ................................................................. 33
  Create a New Action .................................................................................................. 33
  Create a New Rule ..................................................................................................... 34
  Manage Actions ......................................................................................................... 37
  Manage Rules .......................................................................................................... 38
  Manage Alerts .......................................................................................................... 39
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 app, contact your Technical Account Manager (TAM) or Qualys Support.

We’ll help you get started quickly!

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 a 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.

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

Copy and run the Installation Command on the Host.

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.

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

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.

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:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max event log size</td>
<td>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.</td>
</tr>
<tr>
<td>Payload threshold time</td>
<td>EDR events are transmitted to the Qualys Cloud platform when the EDR payload threshold time is hit, i.e., 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.</td>
</tr>
<tr>
<td>Maximum disk usage for EDR Data</td>
<td>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.</td>
</tr>
</tbody>
</table>
**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 asset 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.

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

Hunting events

That's it! Your matches will appear in the list your 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.

Hunting events

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

Investigate incidents by Active Threats By Host, Active Threats by Malware name and Malware family name.

Look into assets monitored by EDR

Get up to date views on a selected asset’s details, its events and incidents.
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).

Just click the Download icon above the incidents list, choose a format and click Download.
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, Process, Network, and Mutex events from the Hunting and the Event Details page.

The remediation options are available under the Remediation Action column and Events Detail page only for:
- Events in Active View.
- Events that score between 1 to 10.

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 Event Details page.

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.
Remediation action for Process, Mutex, Network events

For process, mutex, and network events, we provide Kill Process remediation action. When you perform the Kill Process action for mutex or network 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.

2) The Kill Process screen is displayed. Under Related Events column, you can see the related file, network, and mutex events. 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.
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.

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.

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

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

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.

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

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

From the Event Details page, you can perform the remediation actions (Quarantine File/ Delete File/ Kill Process) on File, Mutex, Network, and Process events. For more information on remediation action, see Remediation action for file events and Remediation action for Process, Mutex, Network 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.
View Process Tree for Events

Click Event Details > Process Tree tab, to view the process tree for File, Process, Mutex, Registry, and Network events. The process tree displays all the related events of the selected event.

An event of the “Process” type will show its parent and child processes along with the mutex and network connection of the process. For the event of Network type, you see network connection of a process and for the event of Mutex type, mutex connection of a process.

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.

To help you identify event types of nodes in a hierarchy view, similar events are grouped under an event type (example: Mutex or Network) and respective event icons are added against the node.

Process tree view displays a zoom bar and reset option..
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.
Customizable Dynamic Dashboards
Alerts, Rules, and Actions

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 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.

![Role Management Screenshot]![User Activity Tab Screenshot]
-----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 for 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 Stack and Send to PagerDuty 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.
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 Rule from Search Query” from the menu.

Provide required details in the respective sections to create a new action:
- 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.
**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.

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.
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.

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.

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 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.
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.

![Manage Rules](image-url)
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).