



Qualys Endpoint Detection and Response v2.x

Release Notes

Version 2.6

September 11, 2023

Here's what's new in Qualys Endpoint Detection and Response 2.6!

What's New

[Connect to Host](#)

[EDR for Linux](#)

[Request Forensic Data](#)

[Enhanced Filters in Incidents tab](#)

[Enhanced Sections in the Incident Details Page](#)

[Enhanced Sections in the Event Details Page](#)

[Enhanced Anti-malware Profile Details Page](#)

[New Tokens](#)

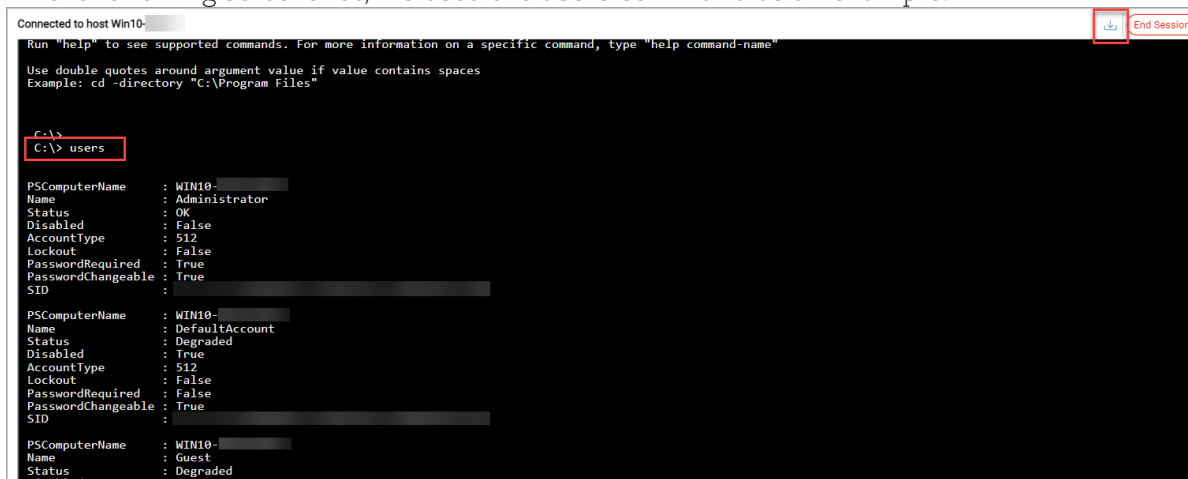
[Updated Tokens](#)

Qualys Endpoint Detection and Response 2.6 brings you some improvements and updates!

Connect to Host

The **Connect to host** option in the **Quick Actions** menu of the **Assets** tab allows you to execute the Windows shell command on the selected endpoint for investigation purposes. Windows Agent version 5.2.1 and above and GAV Agent version 5.3.0 and above are the prerequisites to implement this feature. Once the connection is established to the host, You can type and execute the command in the remote shell. The remote shell lists the supported commands.

In the following screenshot, we used the **users** command as an example:



The screenshot shows a terminal window titled "Connected to host Win10-...". The terminal displays instructions for using the shell, followed by the command `C:\> users` being entered. The output lists system user information for three accounts: Administrator, DefaultAccount, and Guest.

```
Run "help" to see supported commands. For more information on a specific command, type "help command-name"
Use double quotes around argument value if value contains spaces
Example: cd -directory "c:\Program Files"

C:\> users

PSComputerName : WIN10-...
Name           : Administrator
Status        : OK
Disabled      : False
AccountType   : 512
Lockout       : False
PasswordRequired : True
PasswordChangeable : True
SID           : ...

PSComputerName : WIN10-...
Name           : DefaultAccount
Status        : Degraded
Disabled      : True
AccountType   : 512
Lockout       : False
PasswordRequired : False
PasswordChangeable : True
SID           : ...

PSComputerName : WIN10-...
Name           : Guest
Status        : Degraded
```

For detailed procedure on **Connect to Host**, see [EDR Online Help](#).

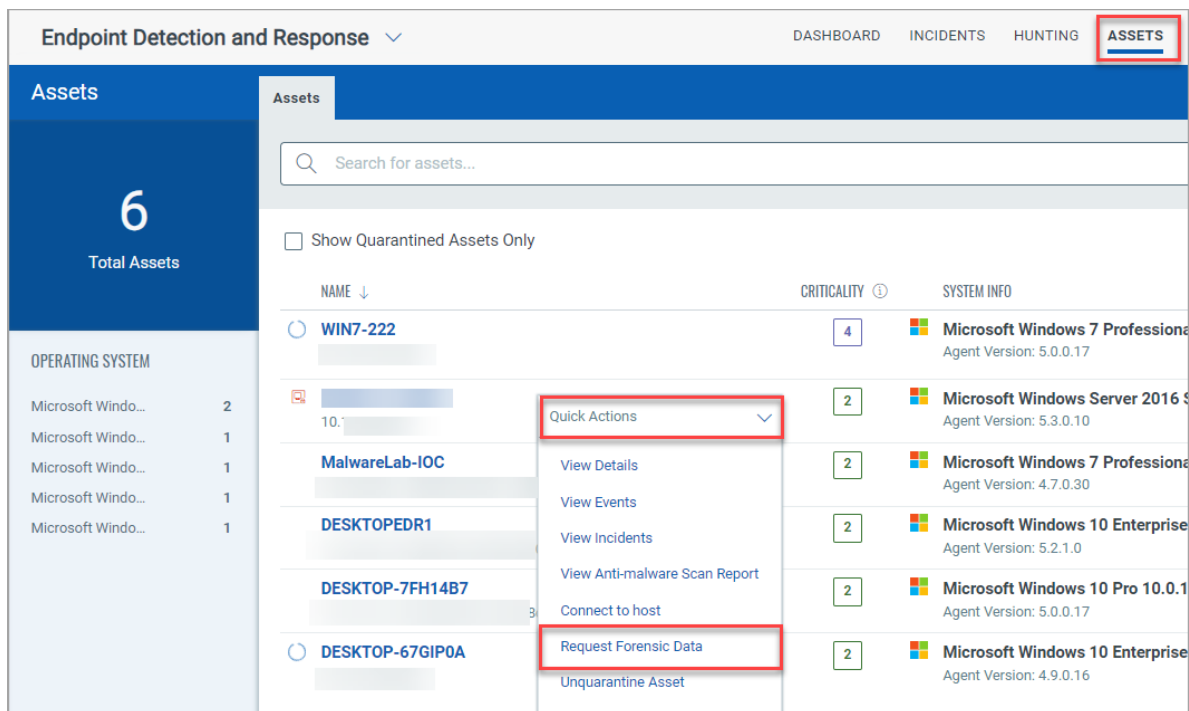
EDR for Linux

From this release, we have introduced EDR for Linux agents. With EDR support for Linux, you can now actively monitor and secure your network on Linux hosts. We recommend you perform all the onboarding activities with the support of your TAM.

For more information about EDR Onboarding for Linux, see [EDR Online Help](#).

Request Forensic Data

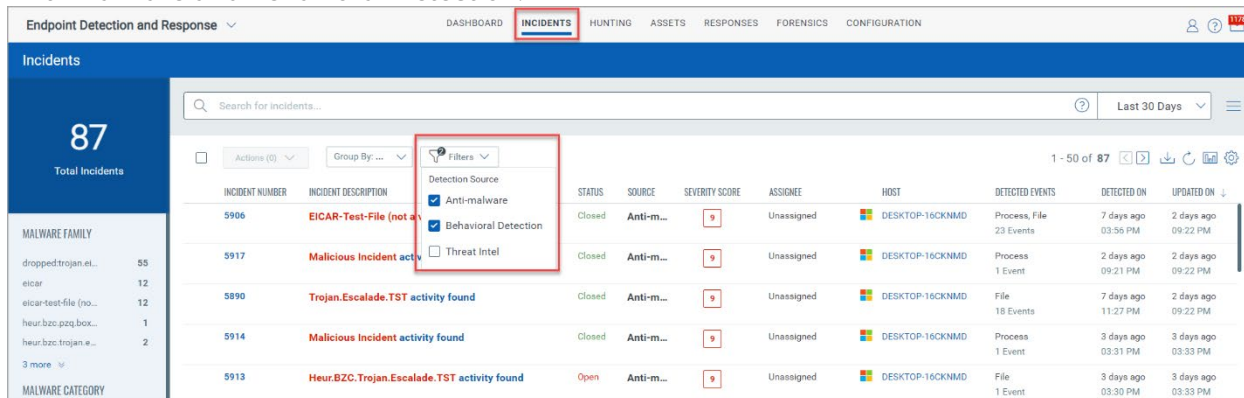
From this release, you can perform a forensic analysis of an incident and perform the necessary response action. You can access the feature from the Quick Actions menu of the Assets tab. Windows Agent version 5.2.1 and above and GAV Agent version 5.3.0 and above are the prerequisites to implement this feature. Request Forensic Data collects Event Log, Persistence, User Accounts, Network, and Process Files of the Windows Agent Version.



For detailed procedure on **Request Forensics Data**, see [EDR Online Help](#).

Enhanced Filters in Incidents tab

You can now use **Anti-malware**, **Behavioral Detection**, and **Threat Intel** filters from the **Incidents** tab. The following screenshot is an example that lists the incidents that have source as Anti-malware and Behavioral Detection:



For more information on the **Incidents** tab, see [EDR Online Help](#).

Enhanced Sections in the Incident Details Page

We have made a few enhancements to the Incident Details page to ease the search results and monitor the changes. The following sections are enhanced:

- **Timeline**:- You can filter the detected events list using the **Assessment** and **Detection Source** filters. The Assessment filter is based on the severity score, and the Detection Source is based on the threat source.
- **Activity Log**:- You can view logs of all the actions performed on the Incident page.

For more information on **Incident Details**, see [EDR Online Help](#).

Enhanced Sections in the Event Details Page

We have made enhancements to the Related Events and Process Tree section of the Event Details page. The enhancements include:

- **Related Events**:-The search for related events can be enhanced using the **Assessment, Detection Source, and Surrounding Events** filters.
 - **Assessment**: based on the severity score.
 - **Detection Source**: based on the threat source.
 - **Surrounding Events**: events occurred within (+)/(-) 1 minute or (+)/(-)3 minute timeframe.
- **Process Tree**:-If a parent node is available for a root node, you can now view the parent node in the Process Tree.

For more information on **Event Details**, see [EDR Online Help](#).

Enhanced Anti-malware Profile Details Page

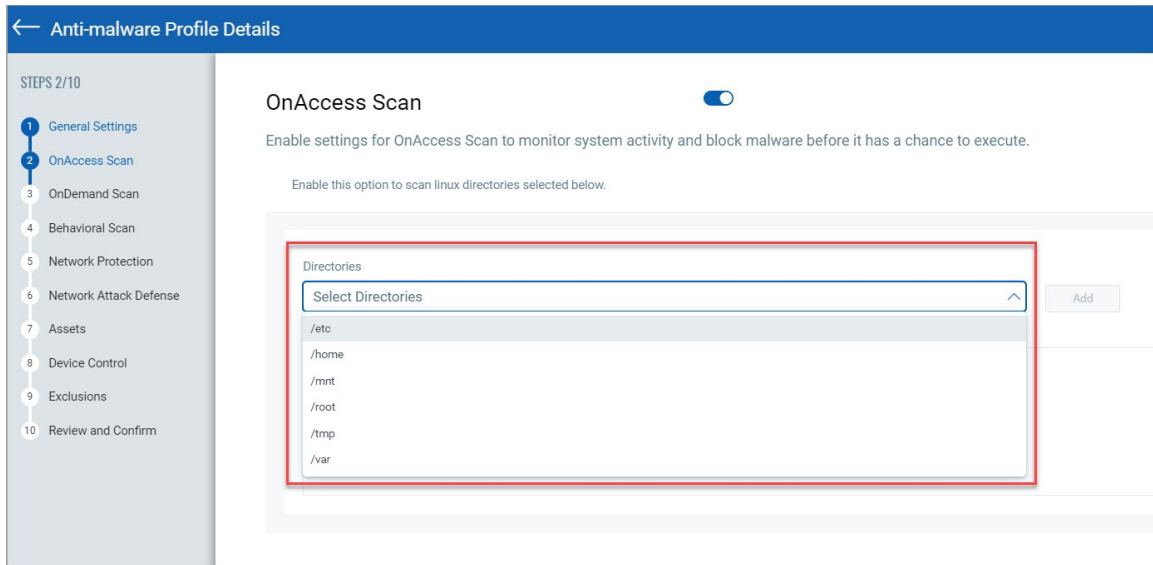
The **Anti-malware Profile Details** page now includes added options in the **General Settings, OnAccess Scan,** and **Behavioral Scan** sections.

- **Set a Proxy Toggle in General Settings**- To ensure data protection and enhance security, you can set a proxy while configuring the Anti-Malware profile. The **Set a Proxy** toggle can be enabled from the General Settings of the Anti-malware Profile.

The following screenshot is an example of the **Set a Proxy** option enabled in the **Anti-malware Profile** settings:

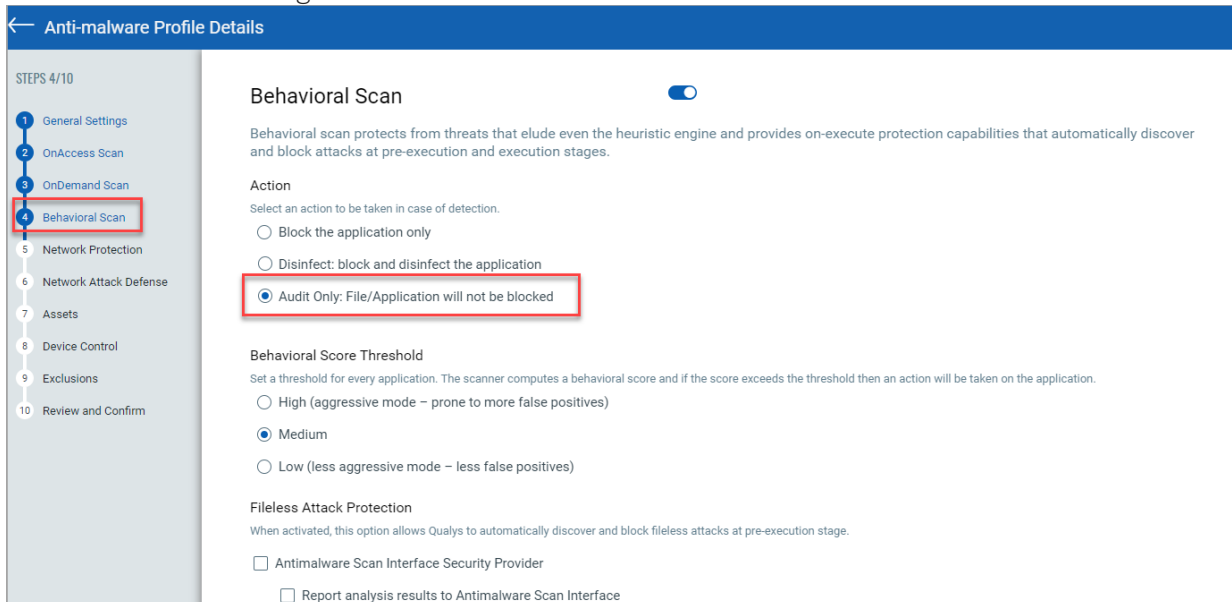
The screenshot shows the 'Anti-malware Profile Details' page with the 'General Settings' section active. A sidebar on the left lists steps 1 through 10, with 'General Settings' selected. The main content area includes a 'Description' field with the value 'New' (247 characters remaining). Below this is a 'Set A Proxy' toggle switch, which is currently turned on. Underneath the toggle are four input fields: 'URL *' with the value '10.' (247 characters remaining), 'Port *' with the value '445' (2 characters remaining), 'Username' (315 characters remaining), and 'Password' (310 characters remaining). At the bottom of the form are 'Cancel' and 'Next' buttons.

- **OnAccess Scan**- Linux directories can now be scanned from the **OnAccess Scan** step. The Linux directories that can be scanned are as follows:
 - /etc
 - /home
 - /mnt
 - /root
 - /tmp
 - /var



- **Audit Only: File/Application will not be blocked in Behavioral Scan**- The **Audit Only** option monitors the applications and processes running on your system and does not block or kill the application. The process information is in the **Hunting** tab.

The following screenshot is an example of the **Audit Only** option selected in the **Anti-malware Profile** settings:



For more information about [OnDemand](#) and [OnAccess Scan](#), see EDR Online Help.

New Tokens

The following tokens are newly added in **Forensics** and **Incidents** tab:

	Token Name	Description
Forensics	asset.agentid	Filter forensic requests by the asset agent id.
	asset.hostname	Filter forensic requests by the asset hostname.
	request.requesttime	Filter forensic requests by the requested time.
	request.expirytime	Filter forensic requests by the expiry time.
	request.status	Filter forensic requests by the request status.
	request.userid	Filter forensic requests by the requested user id.
	request.username	Filter forensic requests by the username.
Incidents	incident.mitre.attack.technique.name	View the technique name that represents its respective technique id.
	incident.mitre.attack.technique.id	View the technique id that represents how a tactical goal can be achieved.

For more information about the tokens, see *EDR Online Help*.

Updated Tokens

- We have updated the `assetavprofile.name` token to `antimalwareprofile.name`. For more information about the Asset tokens, see *EDR Online Help*.