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!

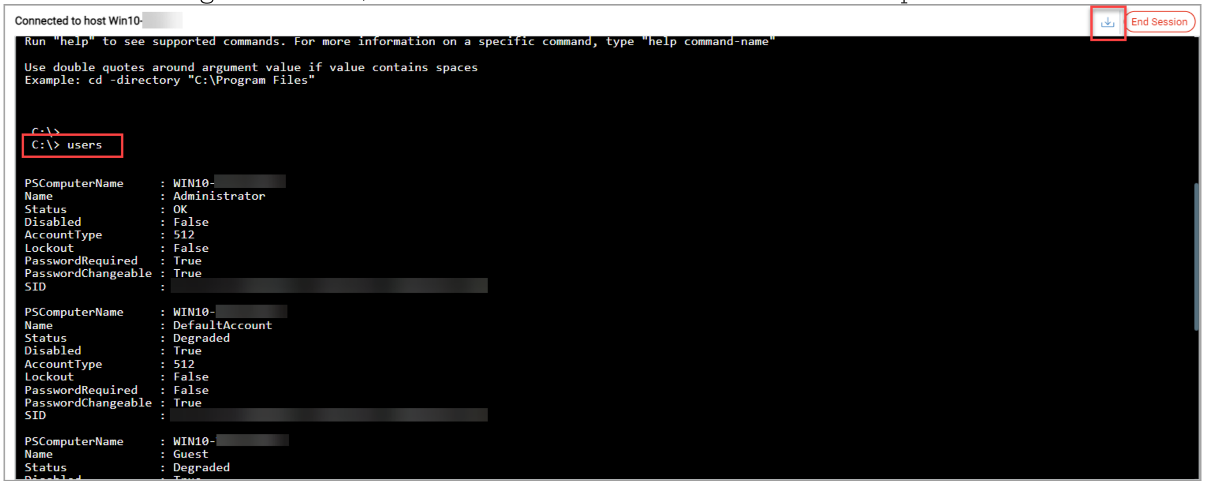
What’s New

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:



```
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:\>
 C:\> users


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

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

PSComputerName     : WIN10-[redacted]
Name               : Guest
Status             : Degraded
```

For detailed procedure on **Connect to Host**, see *EDR Online Help*.

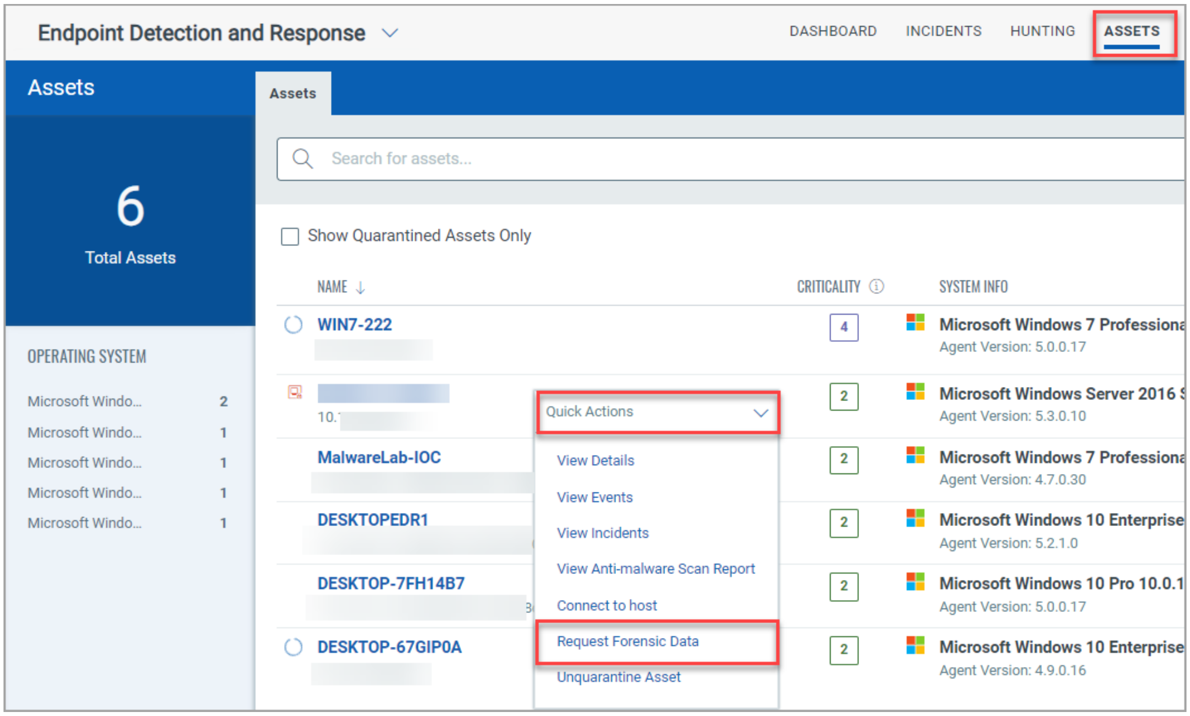
EDR for Linux

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.



□ Show Quarantined Assets Only

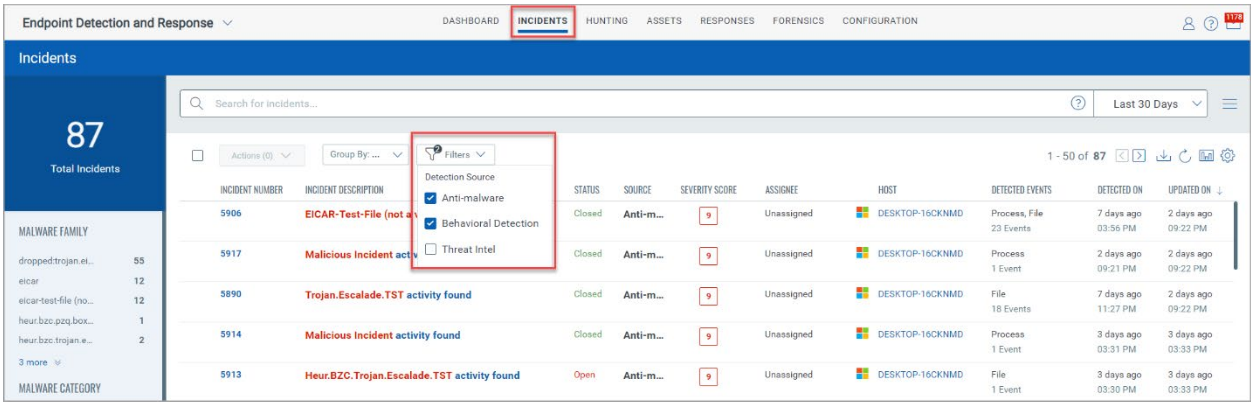
OPERATING SYSTEM	
Microsoft Windo...	2
Microsoft Windo...	1
Microsoft Windo...	1
Microsoft Windo...	1
Microsoft Windo...	1

NAME ↓	CRITICALITY ⓘ	SYSTEM INFO
WIN7-222 [redacted]	4	Microsoft Windows 7 Professiona Agent Version: 5.0.0.17
[redacted] 10.[redacted]	2	Microsoft Windows Server 2016 S Agent Version: 5.3.0.10
MalwareLab-IOC [redacted]	2	Microsoft Windows 7 Professiona Agent Version: 4.7.0.30
DESKTOPEDR1 [redacted]	2	Microsoft Windows 10 Enterprise Agent Version: 5.2.1.0
DESKTOP-7FH14B7 [redacted]	2	Microsoft Windows 10 Pro 10.0.1 Agent Version: 5.0.0.17
DESKTOP-67GIP0A [redacted]	2	Microsoft Windows 10 Enterprise Agent Version: 4.9.0.16

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:



Detection Source
☑ Anti-malware
☑ Behavioral Detection
□ Threat Intel

MALWARE FAMILY	
dropped:trojan.ei...	55
eicar	12
eicar-test-file (no...	12
heur.bzc.pzq.box...	1
heur.bzc.trojan.e...	2
3 more	

MALWARE CATEGORY

INCIDENT NUMBER	INCIDENT DESCRIPTION	STATUS	SOURCE	SEVERITY SCORE	ASSIGNEE	HOST	DETECTED EVENTS	DETECTED ON	UPDATED ON ↓
5906	EICAR-Test-File (not a	Closed	Anti-m...	9	Unassigned	DESKTOP-16CKNMD	Process, File 23 Events	7 days ago 03:56 PM	2 days ago 09:22 PM
5917	Malicious Incident act	Closed	Anti-m...	9	Unassigned	DESKTOP-16CKNMD	Process 1 Event	2 days ago 09:21 PM	2 days ago 09:22 PM
5890	Trojan.Escalade.TST activity found	Closed	Anti-m...	9	Unassigned	DESKTOP-16CKNMD	File 18 Events	7 days ago 11:27 PM	2 days ago 09:22 PM
5914	Malicious Incident activity found	Closed	Anti-m...	9	Unassigned	DESKTOP-16CKNMD	Process 1 Event	3 days ago 03:31 PM	3 days ago 03:33 PM
5913	Heur.BZC.Trojan.Escalade.TST activity found	Open	Anti-m...	9	Unassigned	DESKTOP-16CKNMD	File 1 Event	3 days ago 03:30 PM	3 days ago 03:33 PM

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 list of detected events 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.

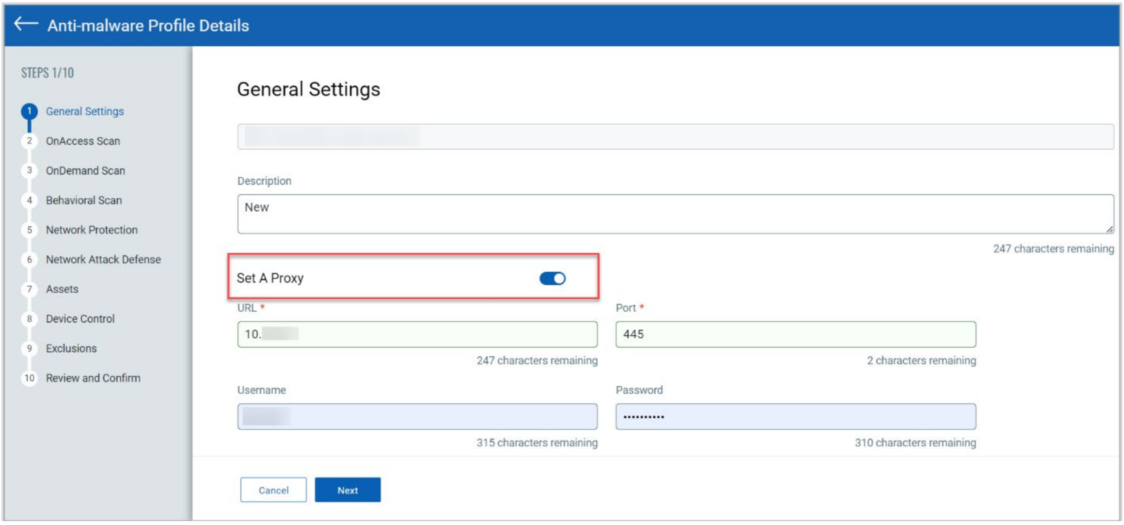
For more information on **Event Details**, see *EDR Online Help*.

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:



General Settings

[redacted]

Description: New

247 characters remaining

Set A Proxy: on

URL *: 10.[redacted]

247 characters remaining

Port *: 445

2 characters remaining

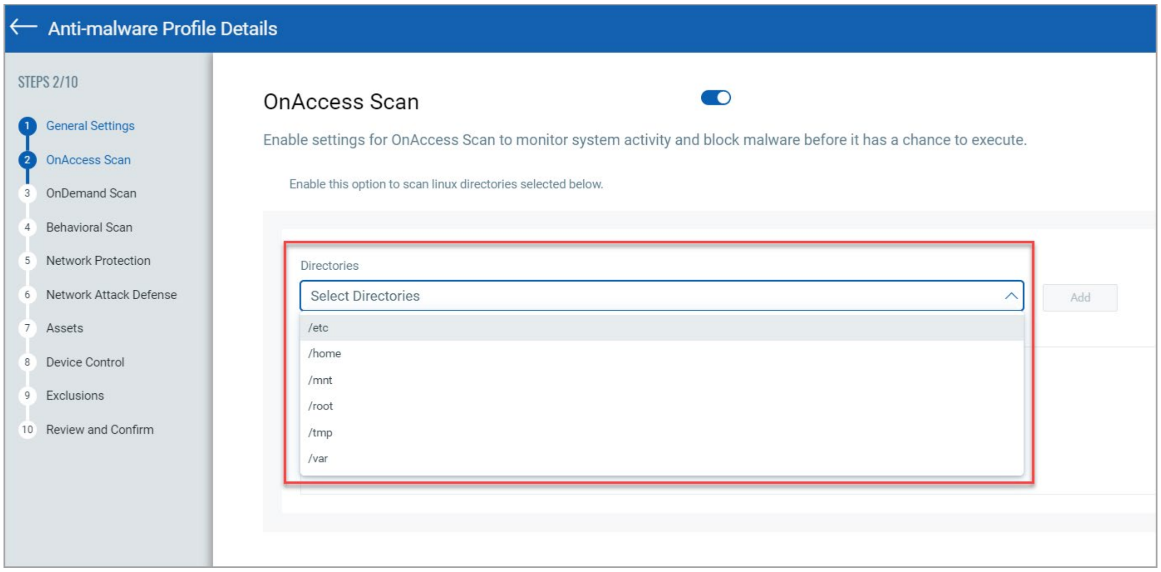
Username: [redacted]

315 characters remaining

Password: ....

310 characters remaining

- **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



OnAccess Scan

Enable settings for OnAccess Scan to monitor system activity and block malware before it has a chance to execute.

Enable this option to scan linux directories selected below.

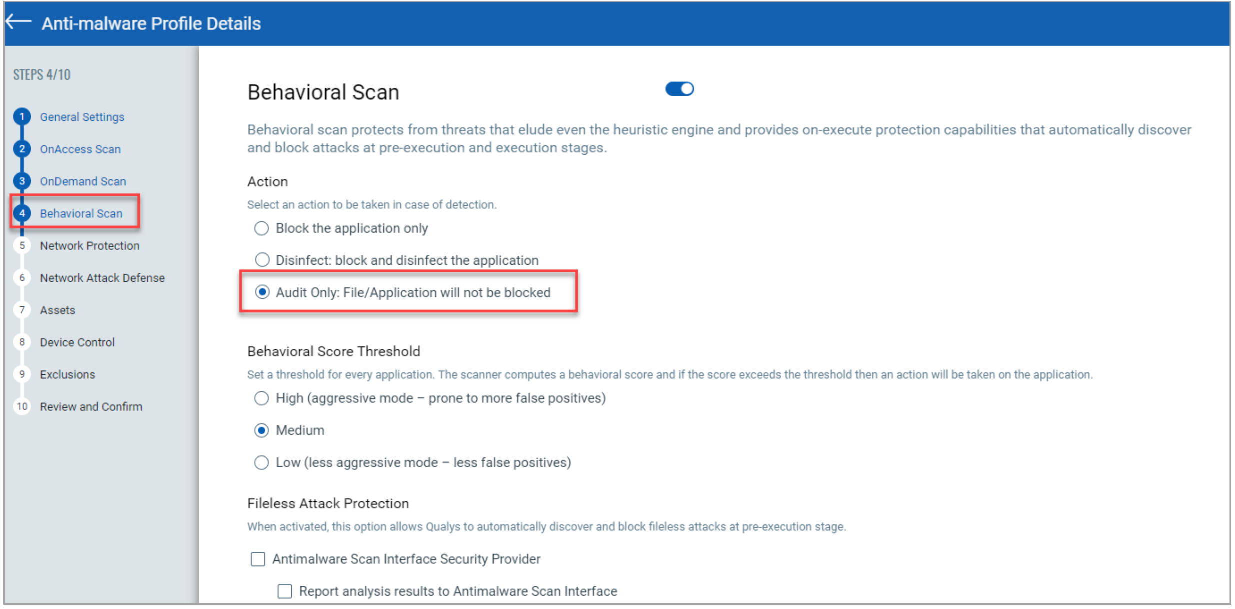
Directories

Select Directories

/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:



Behavioral Scan

Behavioral scan protects from threats that elude even the heuristic engine and provides on-execute protection capabilities that automatically discover and block attacks at pre-execution and execution stages.

Action

Select an action to be taken in case of detection.

○ Block the application only
○ Disinfect: block and disinfect the application
● Audit Only: File/Application will not be blocked

Behavioral Score Threshold

Set a threshold for every application. The scanner computes a behavioral score and if the score exceeds the threshold then an action will be taken on the application.

○ High (aggressive mode – prone to more false positives)
● Medium
○ Low (less aggressive mode – less false positives)

Fileless Attack Protection

When activated, this option allows Qualys to automatically discover and block fileless attacks at pre-execution stage.

□ Antimalware Scan Interface Security Provider
□ Report analysis results to Antimalware Scan Interface

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

- In the Assets tab, we have updated the antimalware.status token with a new status, Incompatible Agent.
- In the Assets tab, we have updated the token from assetavprofile.name token to antimalwareprofile.name.