



Qualys Endpoint Detection and Response v2.x

Release Notes

Version 2.1

July 25, 2022

Here's what's new in Endpoint Detection and Response 2.1!

[New Asset and Malware Summary Widget](#)

[Quarantine an Asset](#)

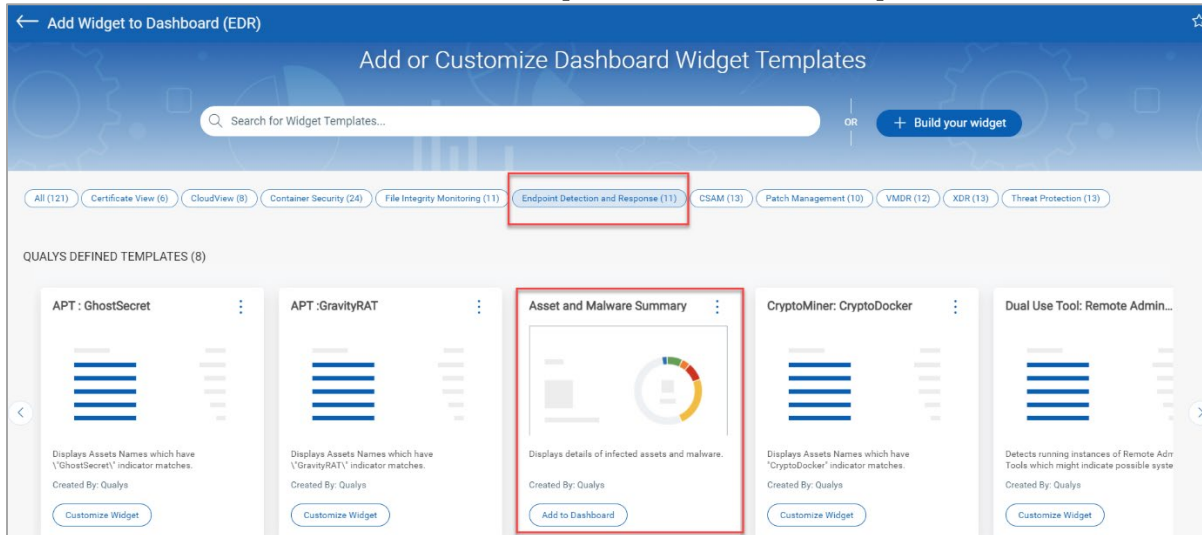
[Search Bar in the Incidents Timeline](#)

Endpoint Detection and Response 2.1 brings you some improvements and updates!

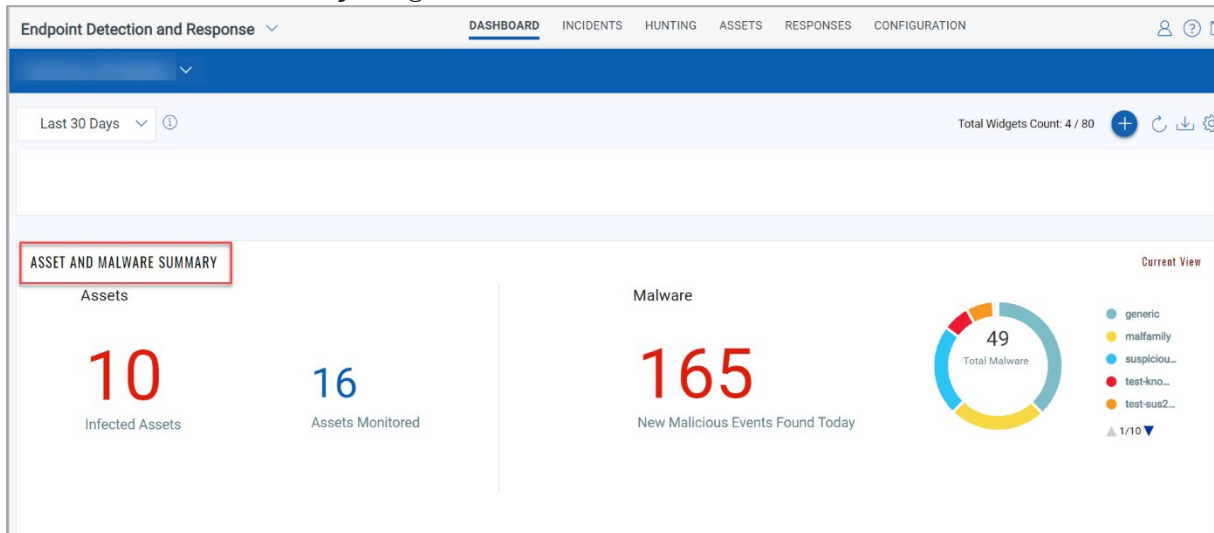
New Asset and Malware Summary Widget

With this release we have added Asset and Malware Summary widget that displays the details of the infected assets and malware. To add the widget in your dashboard perform the following steps:

1. On the **Dashboard** page, click 
2. From the list of modules, select **Endpoint Detection and Response**



3. In the Qualys Defined Templates section, click **Add to Dashboard** from the **Asset and Malware Summary** widget.



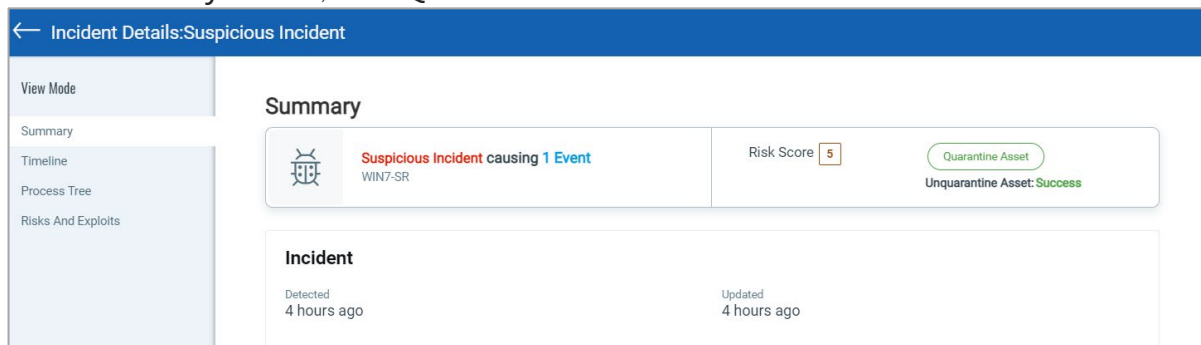
Quarantine an Asset

In case of any malicious event, the Quarantine Asset feature restricts the infected host machine from performing any network communication. You can quarantine an asset if its agent version is 4.9.0 and above. You can Quarantine an Asset from the Incidents or Asset tab.

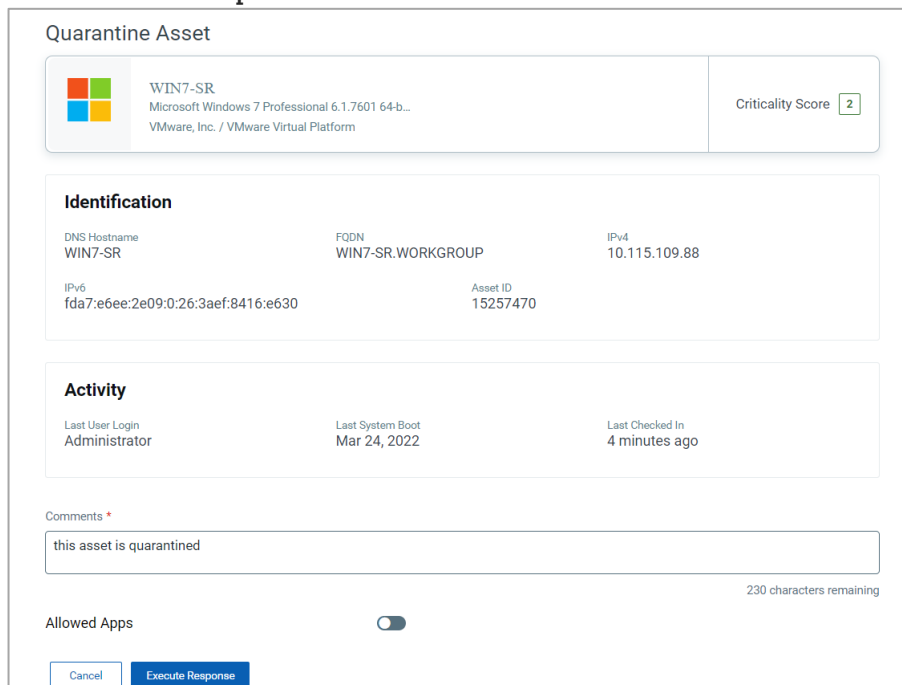
Quarantine an Asset from Incidents Tab

To quarantine an asset based on the incident description, perform the following steps:

1. Click the Incident description that you want to quarantine.
2. In the **Summary** section, click **Quarantine Asset**.

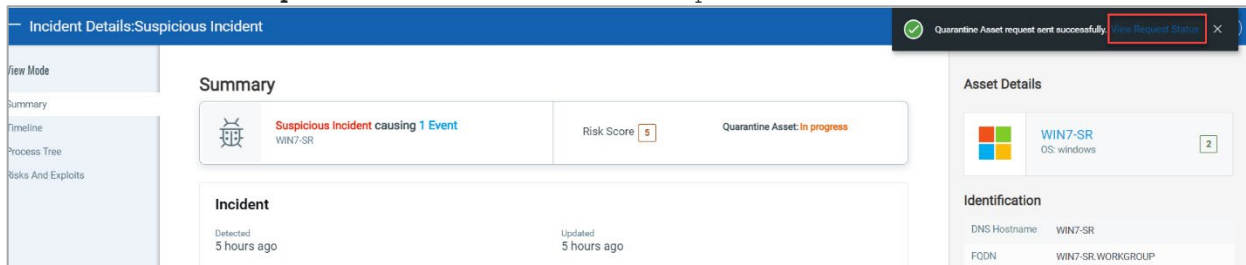


3. In the **Quarantine Asset** window, add your comments. Optionally, you can toggle **Allowed Applications** and add the app name you prefer to be accessible while quarantining the asset.
4. Click **Execute Response**.

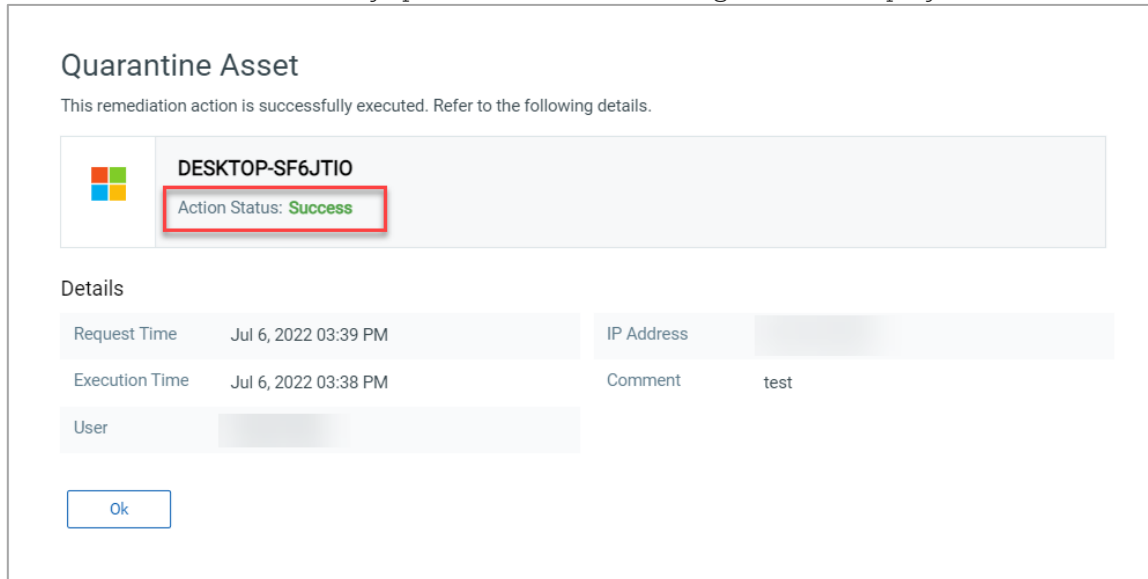


A notification **Quarantine Asset request sent successfully. View Request Status** is generated.

5. Click the **View Request Status** to follow the asset quarantine status.



Once the asset is successfully quarantined the following status is displayed:

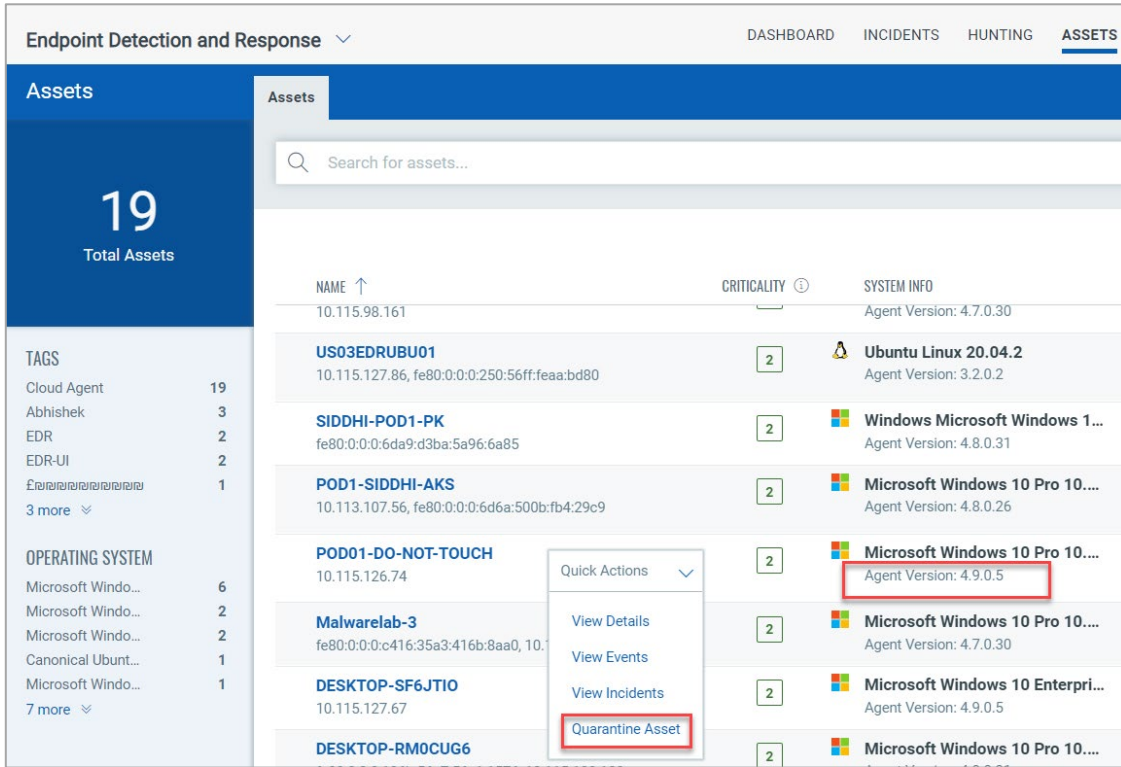


Quarantine an Asset from the Assets Tab

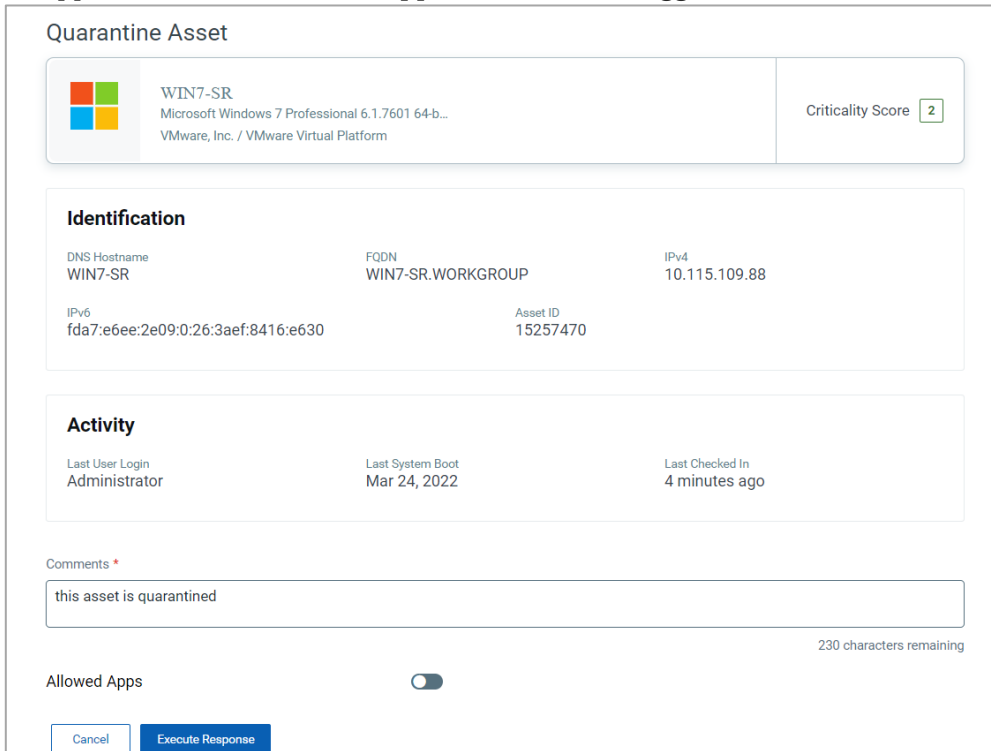
To quarantine an asset from the Assets tab, perform the following steps:

1. In the **Assets** tab select the Asset that you want to quarantine. The Agent version should be 4.9.0 and above.

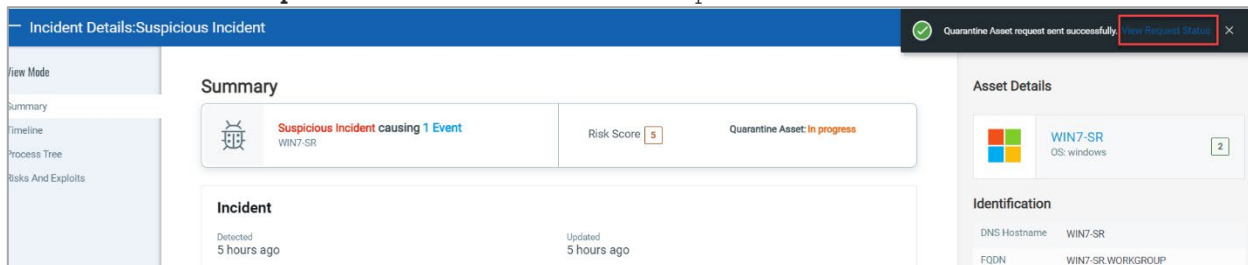
- From the **Quick Actions** menu, click **Quarantine Asset**.



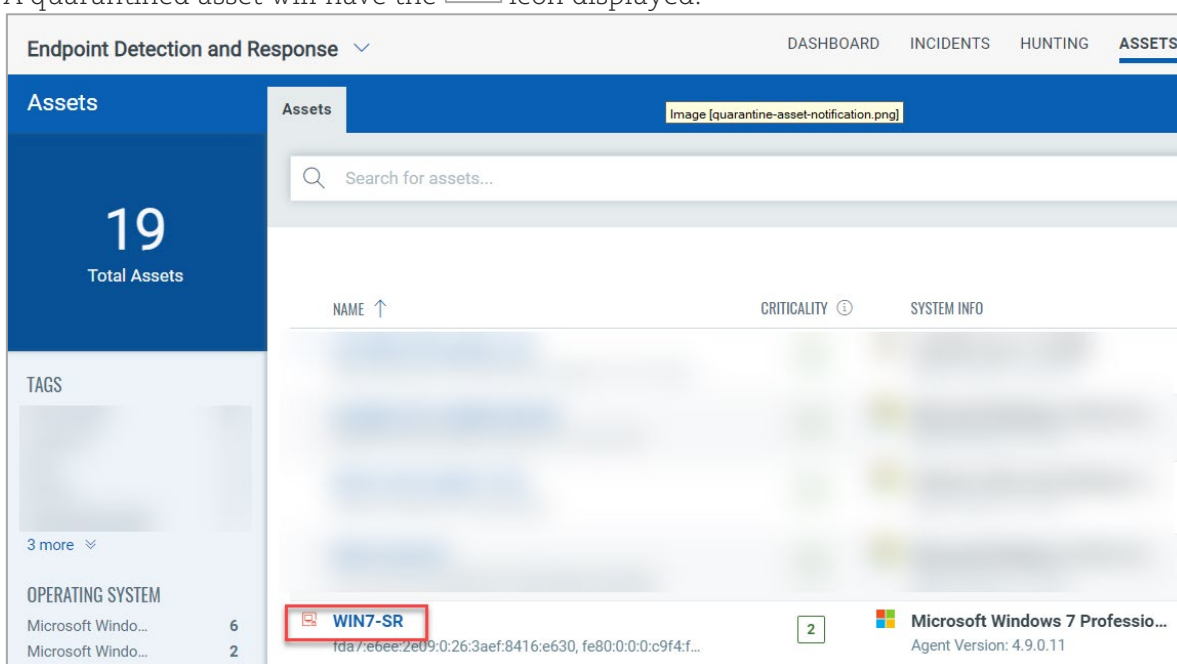
- In the **Quarantine Asset** window, add your comments. Optionally, you can toggle **Allowed Applications** and add the app name you prefer to be accessible while quarantining the asset. Applications listed in the Quarantine Asset Configuration will be applicable in the **Allowed Applications** if this toggle is enabled.



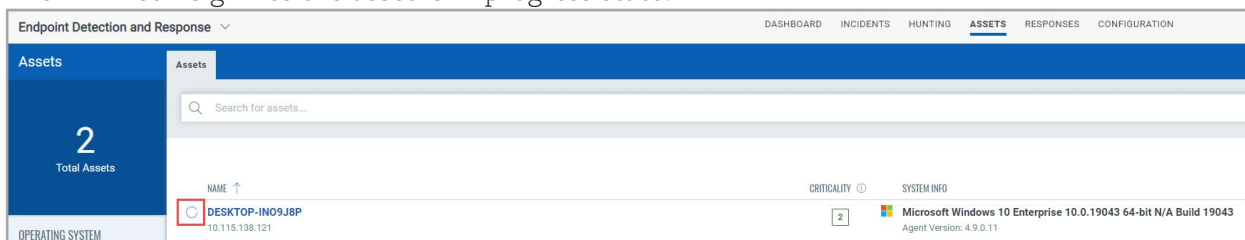
- Click **Execute Response**.
A notification **Quarantine Asset request was sent successfully. View Request Status** is generated.
- Click the **View Request Status** to follow the asset quarantine status.



A quarantined asset will have the  icon displayed.



The  icon signifies the asset is in progress state.



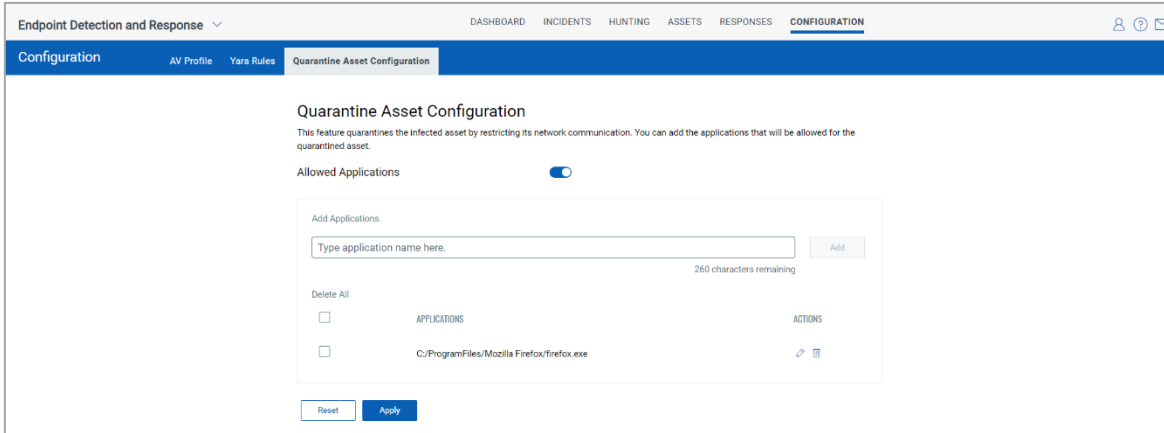
Quarantine Asset Configuration from the Configuration Tab

From the **Configurations** tab, you can whitelist the applications that will be allowed while the asset is quarantined.

Perform the following steps to whitelist applications for the Quarantined asset:

- In the **Configuration** tab, select **Quarantine Asset Configuration**.

2. Toggle **Allowed Applications**.
3. In the **Add Applications** field, provide the complete path of the application. You can provide environmental variables in the field. Wild card inputs are not supported.



4. Click **Apply**.

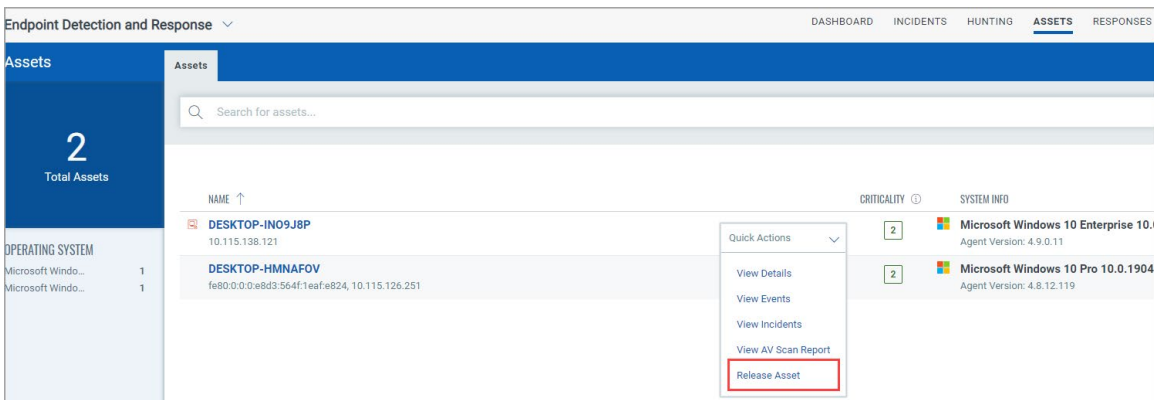
Note: To allow the Qualys Endpoint protection, add the following paths:

- C:\Program Files\Qualys\QualysEPP\downloader.exe
- C:\Program Files\Qualys\QualysEPP\EPSecurityService.exe
- C:\Program Files\Qualys\QualysEPP\ephost.integrity.legacy.exe
- C:\Program Files\Qualys\QualysEPP\EPConsole.exe
- C:\Program Files\Qualys\QualysEPP\EPIntegrationService.exe
- C:\Program Files\Qualys\QualysEPP\EPProtectedService.exe
- C:\Program Files\Qualys\QualysEPP\bdredline.exe

Release an Asset

To release a quarantined asset, perform the following steps:

1. In the **Assets** tab, select the quarantined asset. From the **Quick Actions** menu select **Release Asset**.



2. In the **Release Asset** window add your comments.

Release Asset

DESKTOP-SF6JTIO
Microsoft Windows 10 Enterprise
VMware, Inc. / VMware Virtual Platform

Criticality Score 2

Identification

DNS Hostname: DESKTOP-SF6JTIO
FQDN: DESKTOP-SF6JTIO.WORKGROUP
IPv4: [redacted]
IPv6: -
Asset ID: 15197045

Activity

Last User Login: Administrator
Last System Boot: Jun 15, 2022
Last Checked In: 8 minutes ago

Comments *

Type comments here

255 characters remaining

Allowed Apps

Cancel Execute Response

3. Click **Execute Response**.

A notification **Release Asset request sent successfully. View Request Status** is generated.

4. Click the **View Request Status** to follow the release asset status.



Search Bar in the Incidents Timeline

With this release, we have introduced the Search Bar in the **Incidents** tab under the **Timeline** option. You can use the Events Search Token to view the detected events from the search bar.

Incident Details: fam_trojan

View Mode

Summary

Timeline

Process Tree

Risks And Exploits

Timeline

fam_trojan causing 5 Events
POD01-DO-NGF-TOUGH

Risk Score B

Quarantine Asset
Unquarantine Asset
Success

Timeline of Detected Events

Search for events...

1 - 6 of 6

4 hours ago 01:29 PM Process C:\Windows\system32\cmd.exe is executed by svchost.exe PID:12464 No Action Required

4 hours ago 01:29 PM Process C:\Windows\system32\cmd.exe is terminated by svchost.e... PID:12464 No Action Required

3 hours ago 01:30 PM File C:\Users\Administrator\AppData\Roaming\edr\AM2_MALICIOU... Quarantine File

3 hours ago 01:30 PM File C:\Users\Administrator\edr\AM2_SUSPICIOUS_20220705-1329... Quarantine File

3 hours ago 01:30 PM File C:\Users\Administrator\edr\Mobile_Fraud_1_20220705-132952... Quarantine File

EVENT DETAILS View All Details

Process cmd.exe is executed

Threat details

Threat Name -
AV -
Family -
Category -
Score 0

Process

State RUNNING
Name cmd.exe
Full Path C:\Windows\system32\cmd.exe
Arguments /c
C:\edr\UIAutomation\windows_file_data_generation_script.bat
Elevated true