Qualys Endpoint Detection and Response v2.x

Release Notes

Version 2.1

July 25, 2022

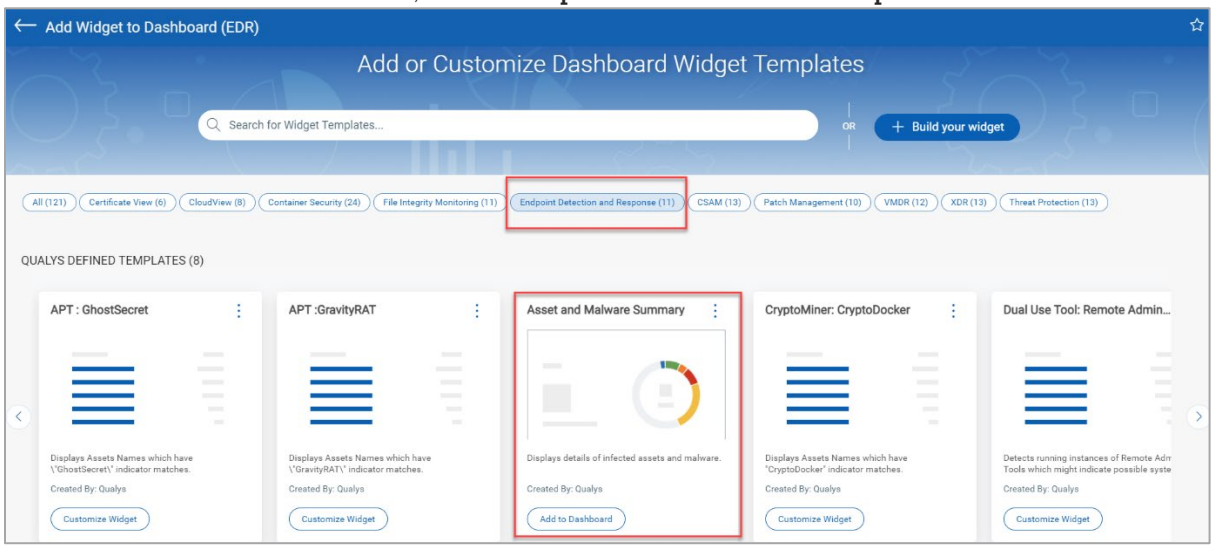
Here's what's new in Endpoint Detection and Response 2.1!

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

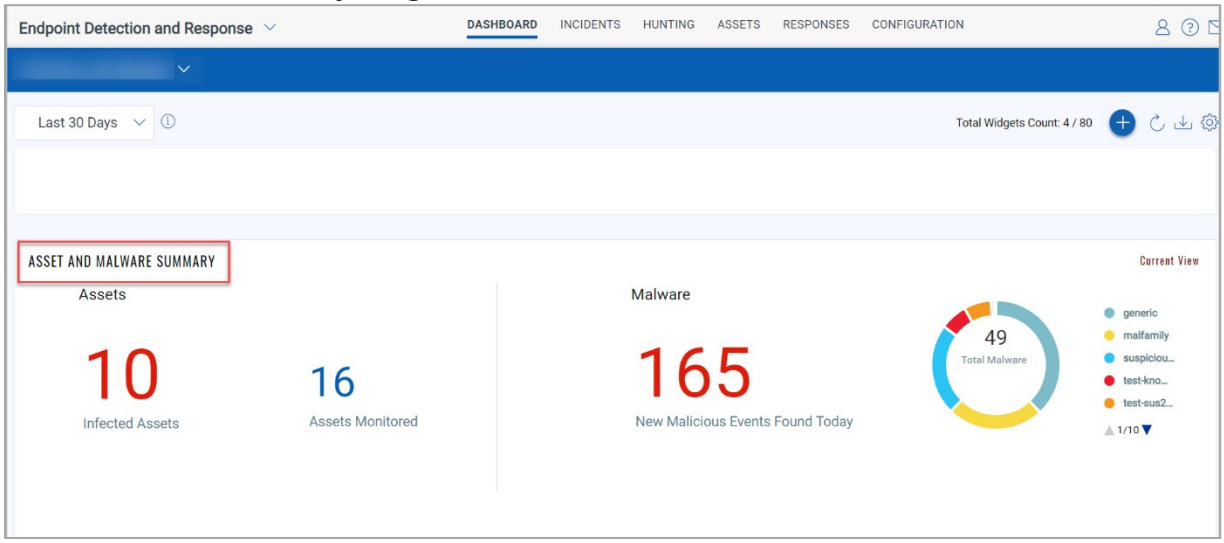
New Asset and Malware Summary Widget

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 **Dashbaord** 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.



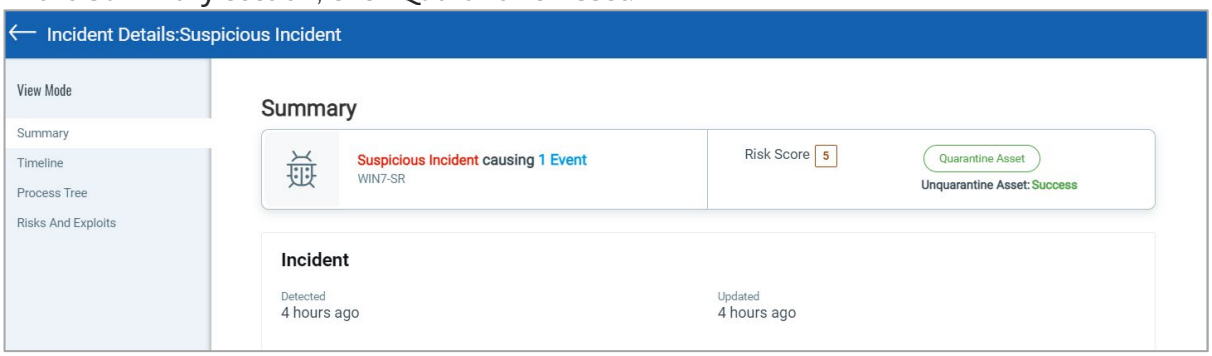
Quarantine an Asset

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.

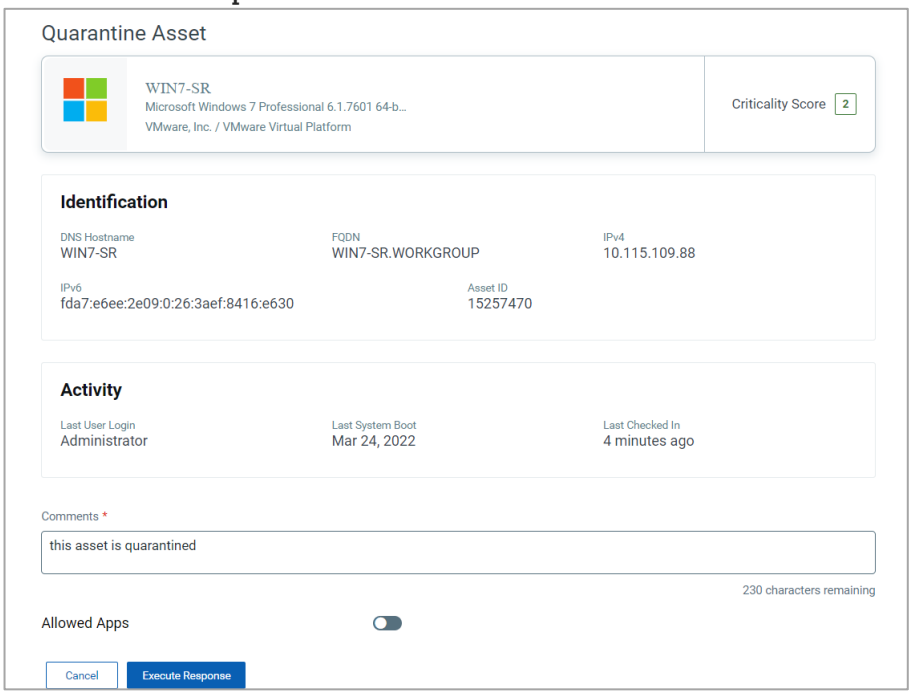
Quarantine an Asset from Incidents Tab

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**.

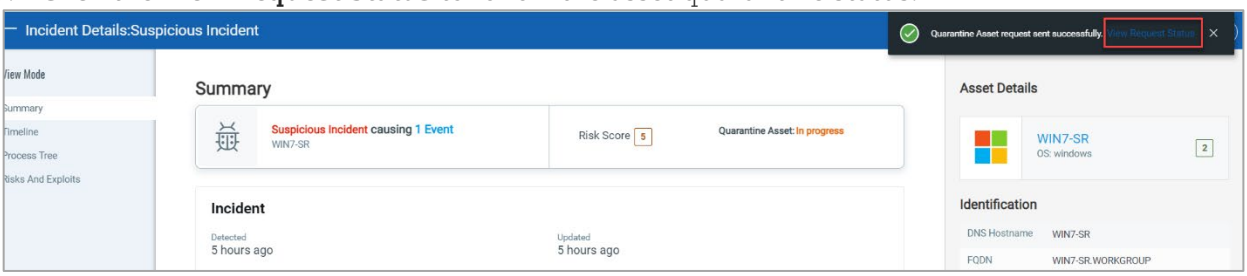


3. In the **Quarantine Asset** window, add your comments. Optionally, you can toggle **Allowed Applications** and add the app name you prefer to be accessible while quarantining the asset.
4. Click **Execute Response**.

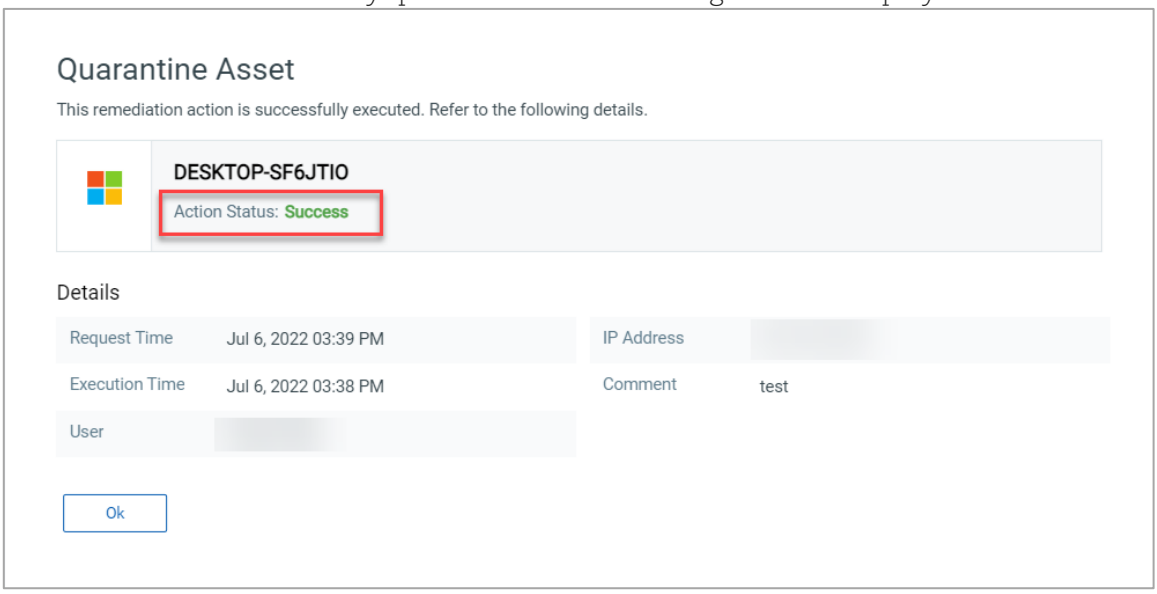


A notification **Quarantine Asset request sent successfully. View Request Status** is generated.

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



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

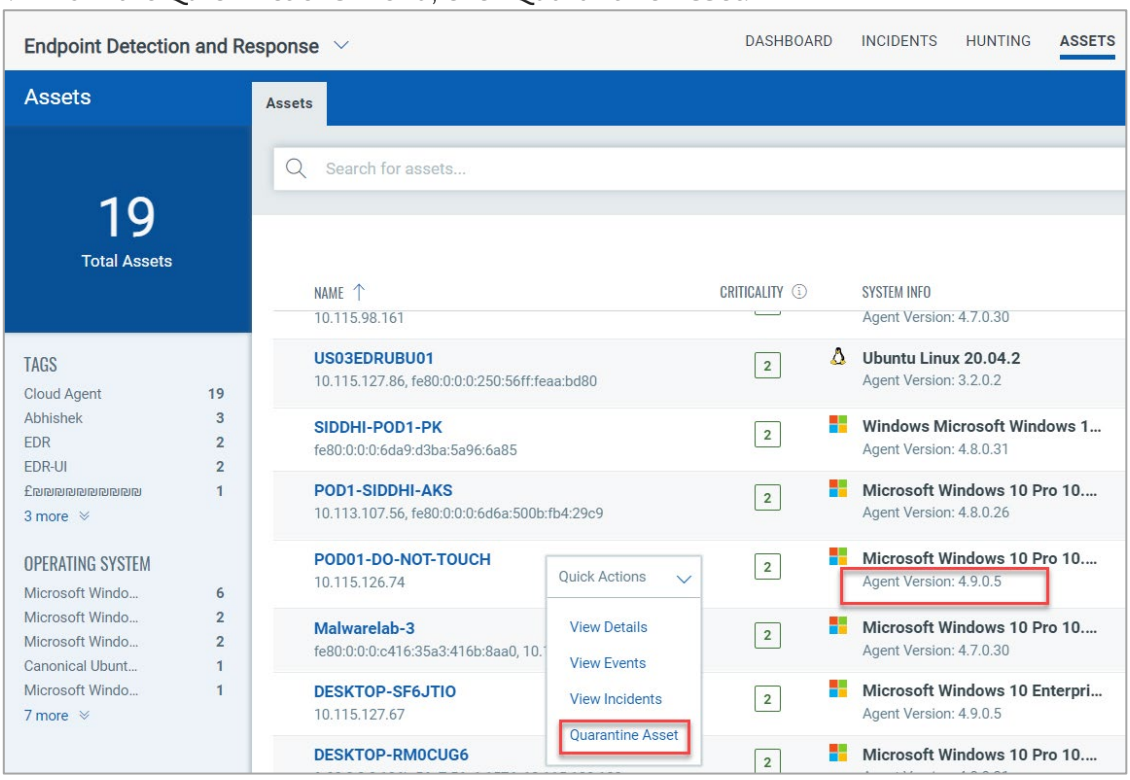


Quarantine an Asset from the Assets Tab

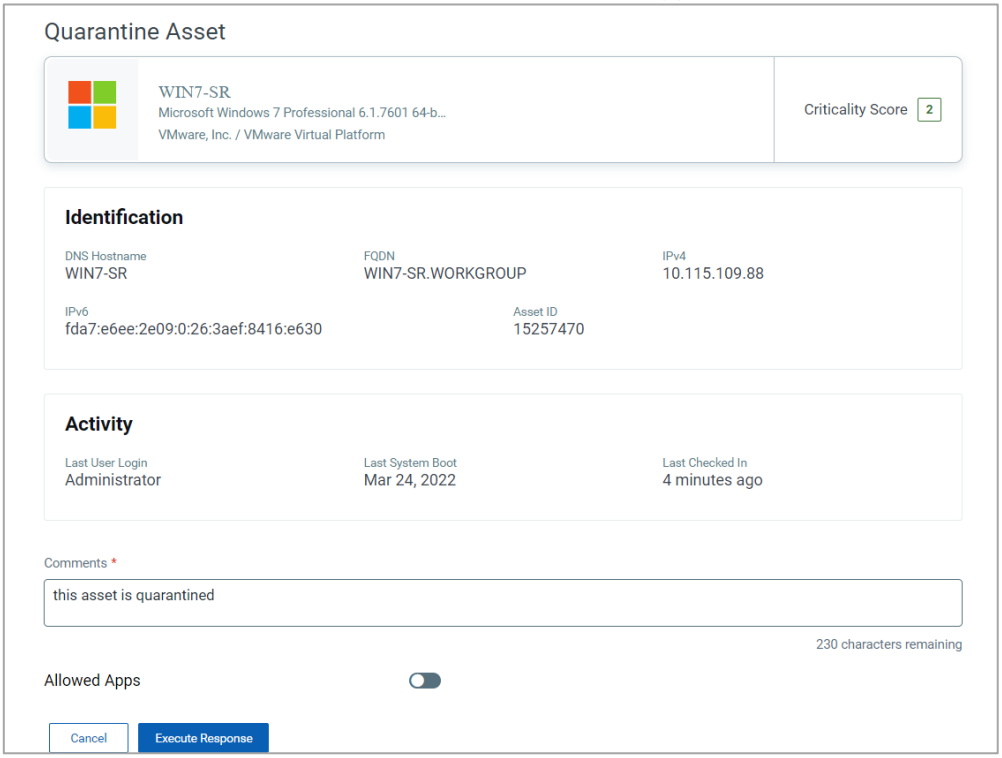
To quarantine an asset from the Assets tab, perform the following steps:

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

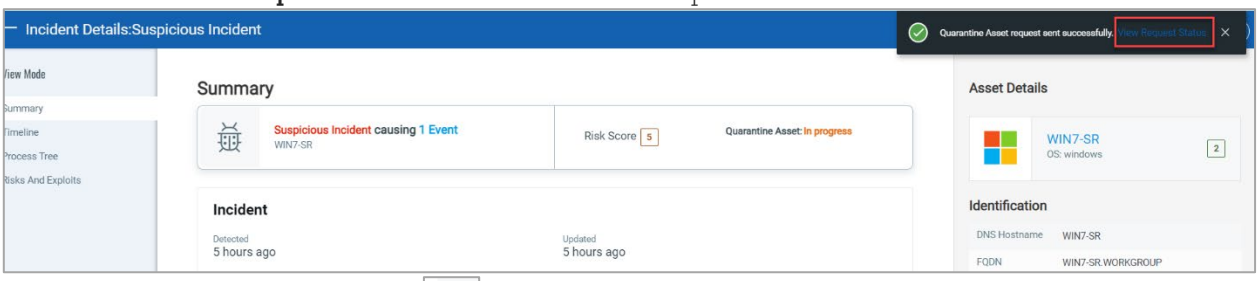
2. From the **Quick Actions** menu, click **Quarantine Asset**.



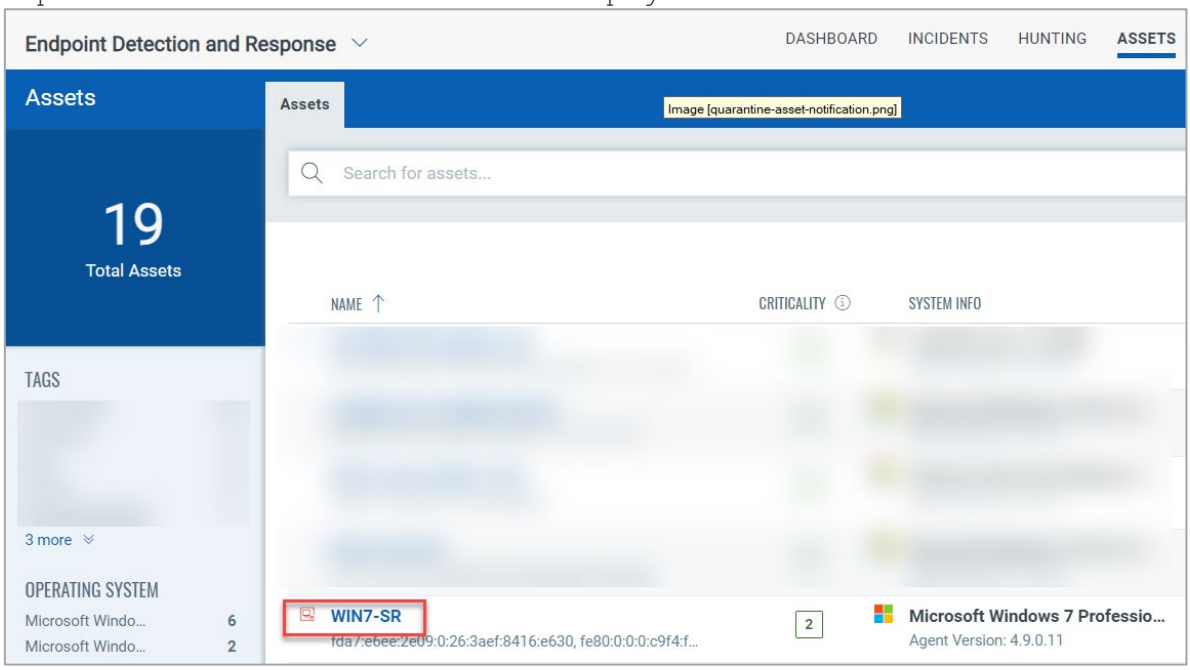
3. In the **Quarantine Asset** window, add your comments. Optionally, you can toggle **Allowed Applications** and add the app name you prefer to be accessible while quarantining the asset. Applications listed in the Quarantine Asset Configuration will be applicable in the **Allowed Applications** if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



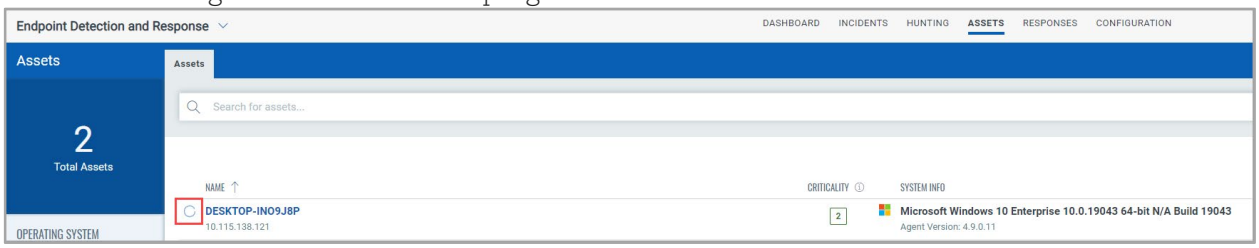
4. Click **Execute Response**.
   A notification **Quarantine Asset request was sent successfully. View Request Status** is generated.
5. Click the **View Request Status** to follow the asset quarantine status.



A quarantined asset will have the  icon displayed.



The  icon signifies the asset is in progress state.

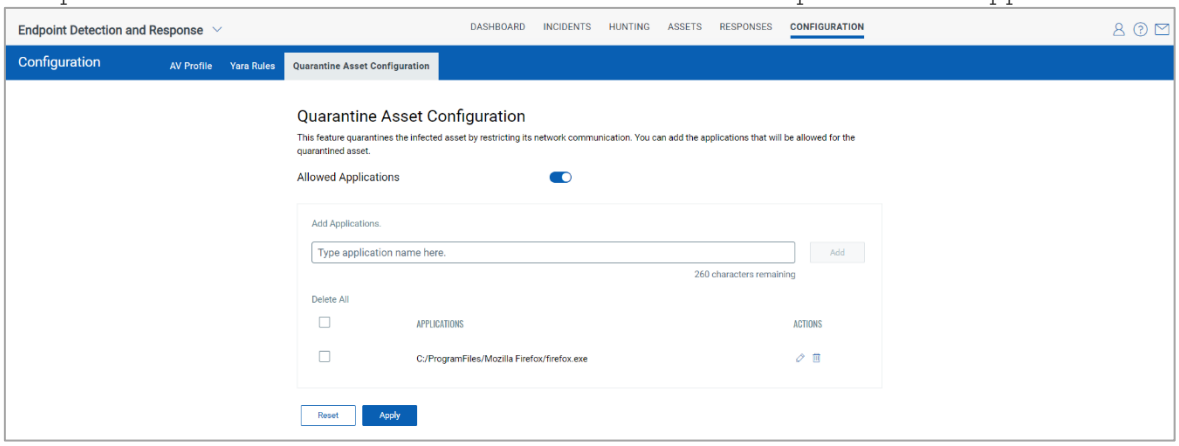


Quarantine Asset Configuration from the Configuration Tab

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:

1. 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**.

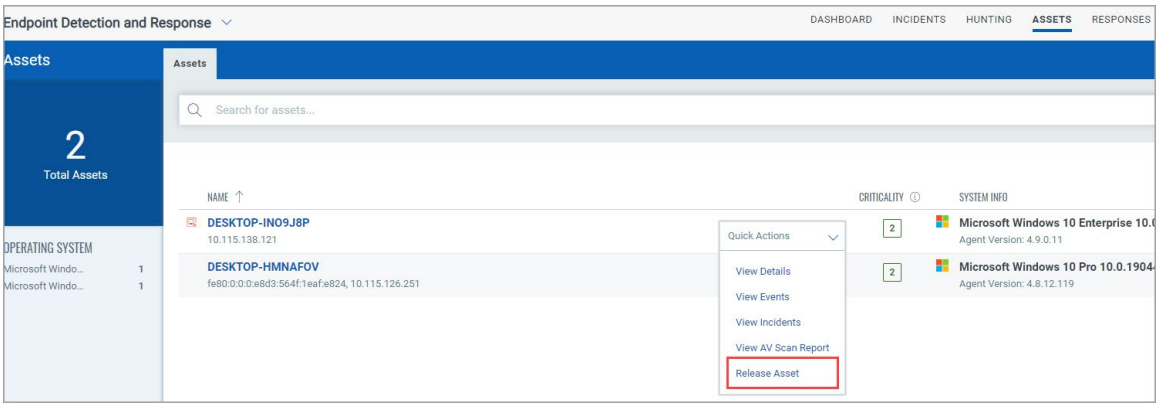
Note: To allow the Qualys Endpoint protection, add the following paths:

- 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

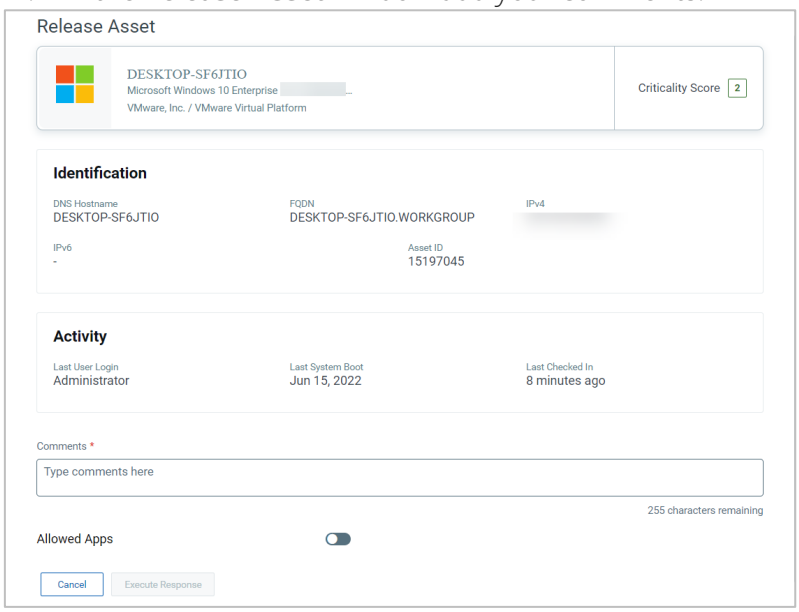
Release an Asset

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.



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.