Qualys Endpoint Detection and Response v1.x

Release Notes

Version EDR 1.0.1

October 12, 2020

Here is what you get with Qualys EDR 1.0.1!

Roles and Permissions
Added Certificate Information for File Events
Malware Details added to Event Datalist report
Event Tree for File and Registry Events

Note: You must upgrade to Cloud Agent version 4.1 and above to utilize all the EDR functionality.

Roles and Permissions

With this release, we introduce new EDR roles and associated permissions. Depending on the roles and permissions assigned, the user can perform actions like creating, editing, or deleting rules and actions.

Using the **Administration** module, the Manager user for the subscription can assign these roles and permissions for all the other users.

Note: EDR users created before version 1.0.1 will continue to have the same permissions.

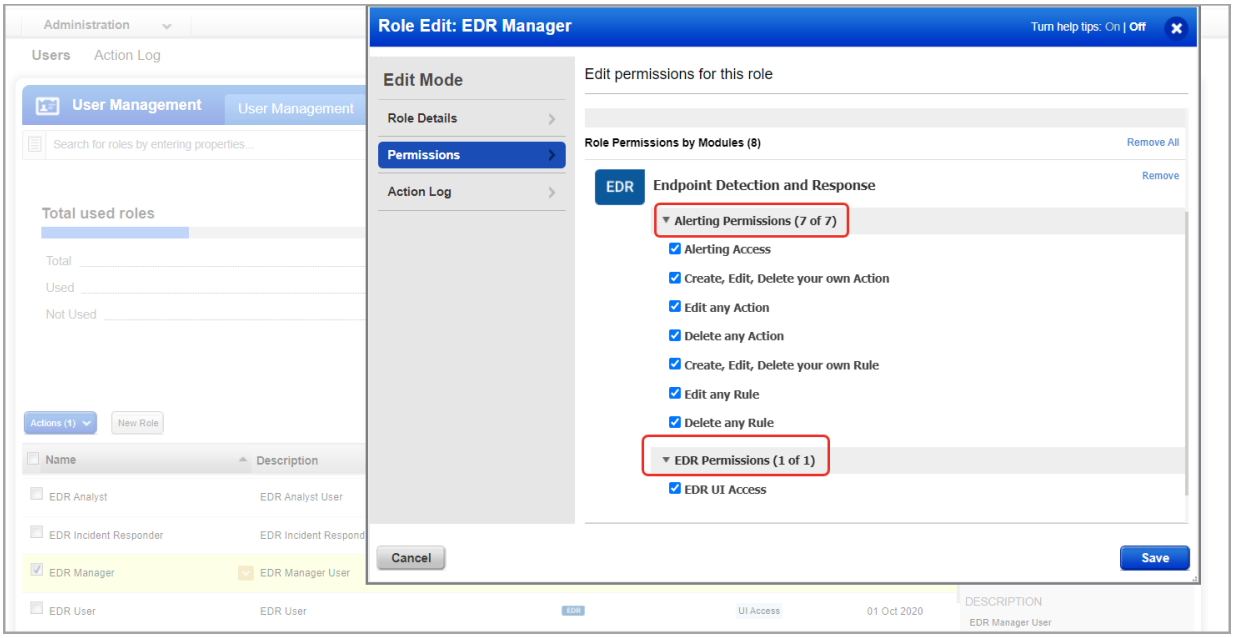
Manager: A user with the Manager role is considered a super-user and has all the available permissions. They have full privileges and access to all modules in the subscription. Only users with Manager role can create other users and assign roles.

EDR User: By default, the EDR users have EDR UI permissions only.

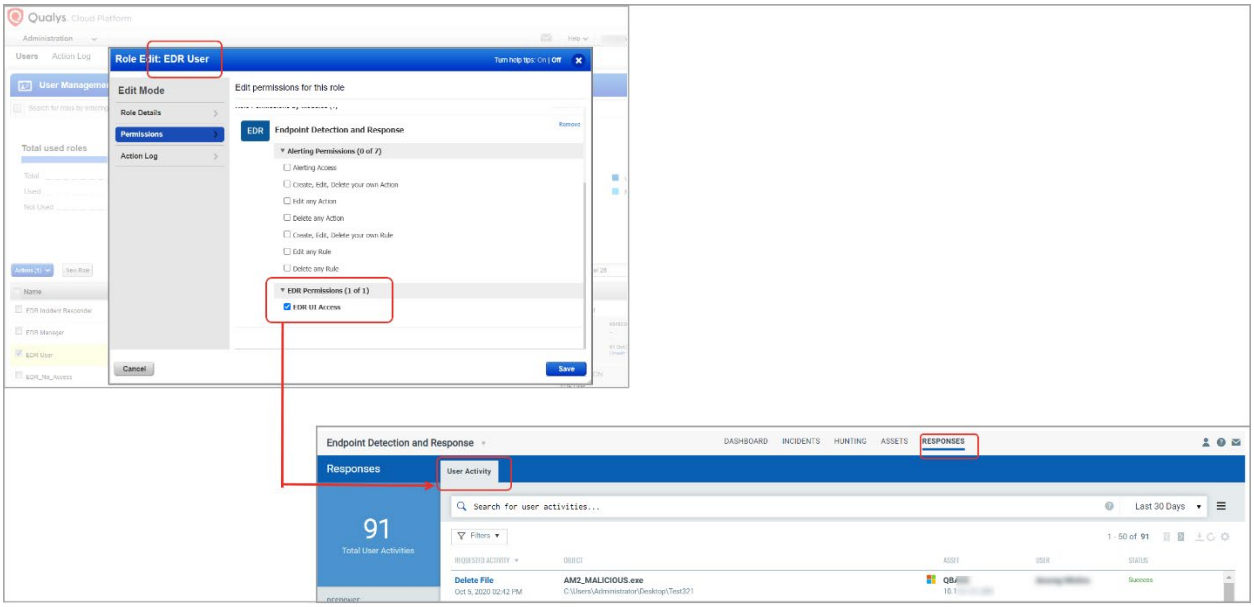
EDR Analyst, **EDR Incident Responder**, and **EDR Manager**: By default, these users have EDR UI and Alerting permissions.

Note: The Manager user can customize the permissions for all the roles.

Example: The default permissions for EDR Manager:



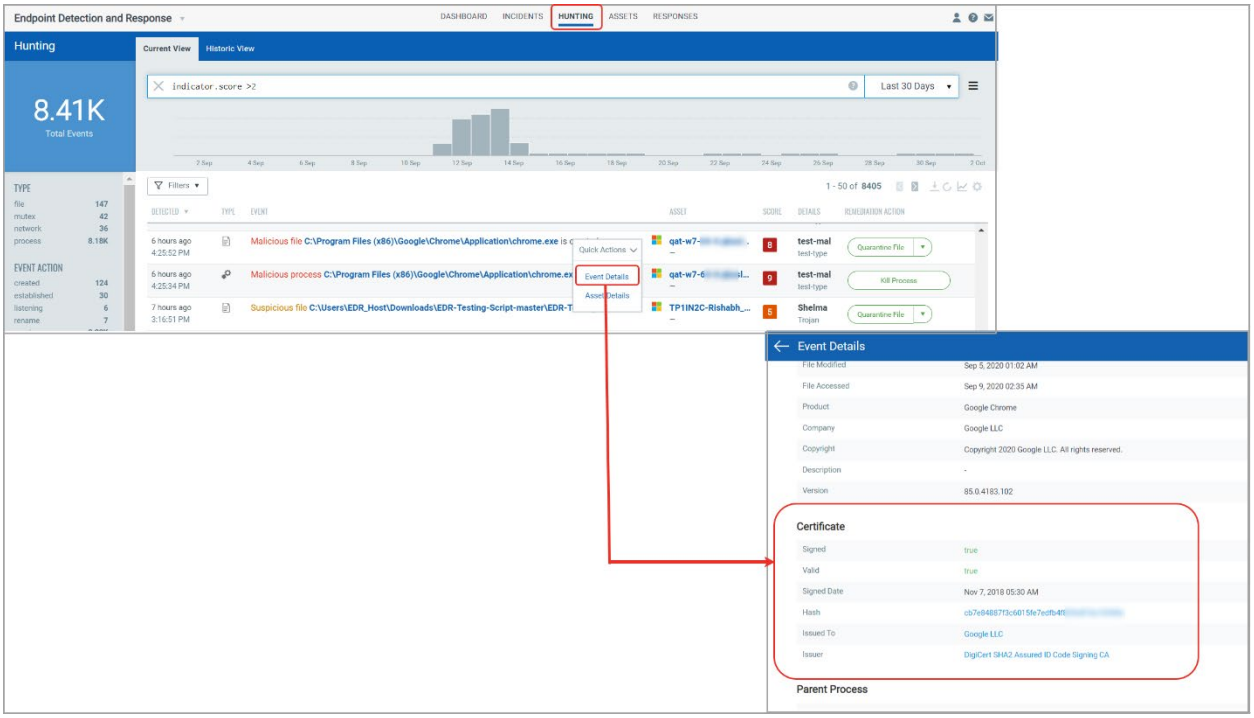
Example: As the EDR user has UI access permission only, the user can only see the **User Activity** tab under **Responses**.



Added Certificate Information for File Events

We have now added certificate information for the file events. This information will help you verify the authenticity of the file on which an event is registered.

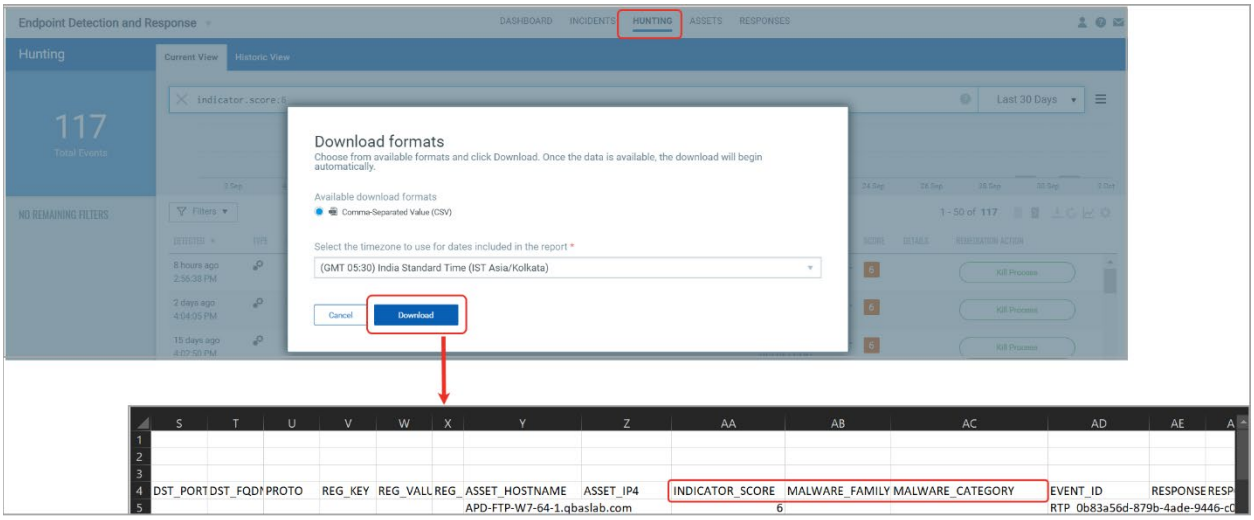
Want to view the certification information for a file event? Select the required file event from the **Hunting** tab. Click **Quick Actions** > **Event Details** and scroll to the **Certificate** section.



Malware Details Added to Event Datalist Report

To give you more information about the detected malware, we have now added the following three columns to the Event Datalist report.

- INDICATOR_SCORE
- MALWARE_FAMILY
- MALWARE_CATEGORY



Event Tree for File and Registry Events

To give you a detailed picture about the events related to a File and Registry events, we have added the event tree for File and Registry events.

Example: Registry Event Tree

Example: File Event Tree