



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.

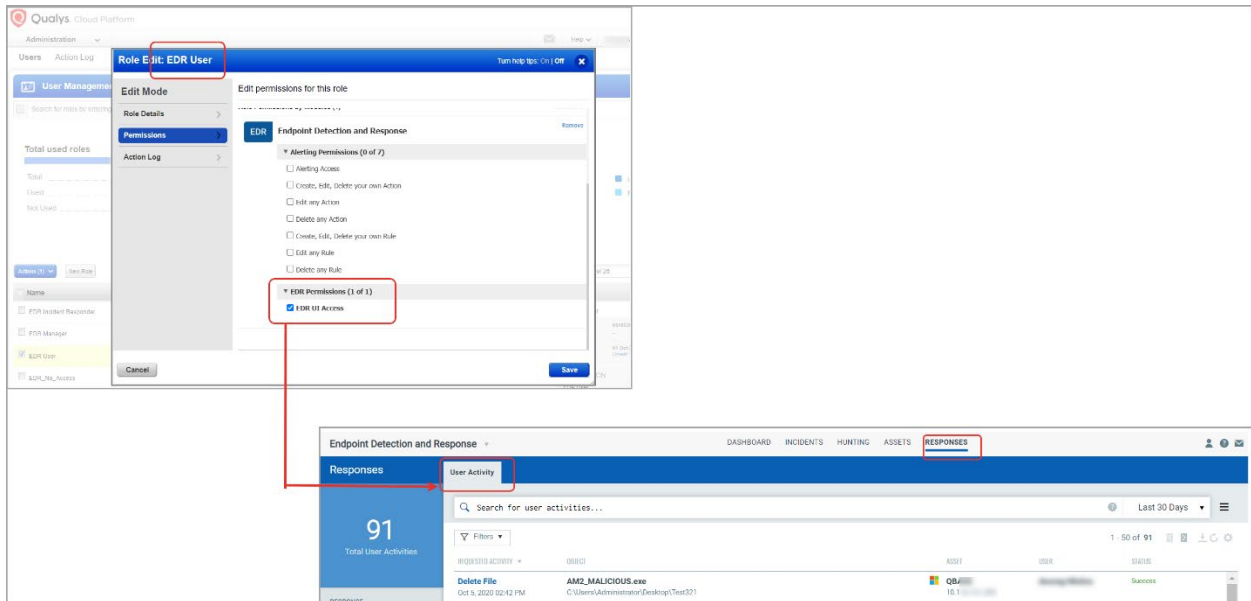
EDR Analyst, EDR Incident Responder, and EDR Manager: By default, these users have EDR UI and Alerting permissions.

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

Example: The default permissions for EDR Manager:

The screenshot displays the 'Role Edit: EDR Manager' interface. On the left, a sidebar shows 'Users' and 'Action Log' tabs, with 'User Management' selected. Below this, there's a search bar and a table of roles. The 'EDR Manager' role is selected and highlighted in yellow. The main area shows the 'Edit Mode' for the 'EDR Manager' role. It lists 'Edit permissions for this role' and 'Role Permissions by Modules (8)'. Under the 'EDR' module, there are two sections: 'Alerting Permissions (7 of 7)' and 'EDR Permissions (1 of 1)'. The 'Alerting Permissions' section includes: 'Alerting Access', 'Create, Edit, Delete your own Action', 'Edit any Action', 'Delete any Action', 'Create, Edit, Delete your own Rule', 'Edit any Rule', and 'Delete any Rule'. The 'EDR Permissions' section includes: 'EDR UI Access'. A 'Save' button is visible at the bottom right.

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.

The screenshot displays the EDR interface with the 'Hunting' tab selected. A search filter 'indicator.score >2' is applied. The main table lists several events, including a 'Malicious file' and a 'Suspicious file'. A red box highlights the 'Event Details' link for the 'Malicious file' event. A red arrow points from this link to the 'Event Details' panel on the right. In this panel, the 'Certificate' section is highlighted with a red box, showing the following information:

Property	Value
Signed	true
Valid	true
Signed Date	Nov 7, 2018 05:30 AM
Hash	c87484887f3c56156e7ccfb41...
Issued To	Google LLC
Issuer	DigiCert SHA2 Assured ID Code Signing CA

Below the certificate information, the 'Parent Process' section is partially visible.

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

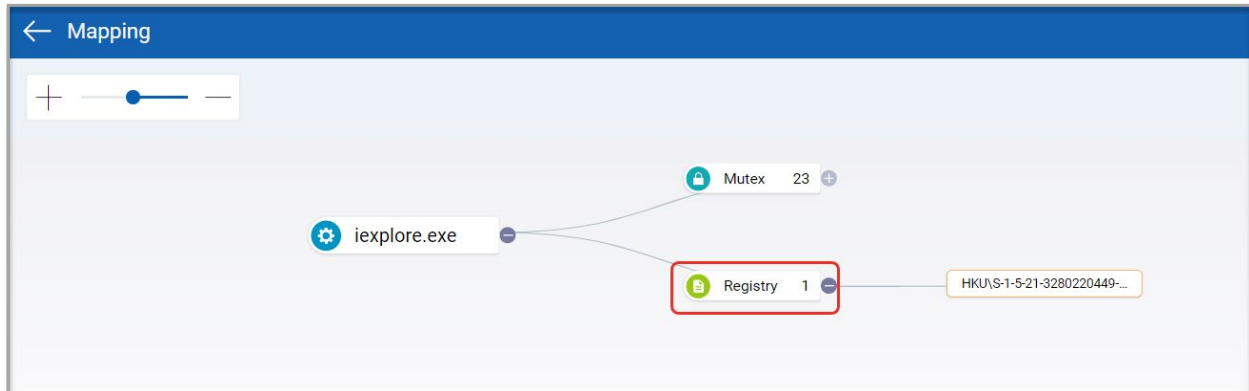
The screenshot shows the EDR interface with a 'Download formats' dialog box. The dialog box is open over a table of event data. The 'Download' button in the dialog box is highlighted with a red box, and a red arrow points from it to the 'INDICATOR_SCORE', 'MALWARE_FAMILY', and 'MALWARE_CATEGORY' columns in the table below. The table has columns for various event attributes, including 'INDICATOR_SCORE', 'MALWARE_FAMILY', and 'MALWARE_CATEGORY'.

	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	A
1														
2														
3														
4	DST_PORT	DST_FQDN	PROTO	REG_KEY	REG_VAL	REG_ASSET_HOSTNAME	ASSET_IP4		INDICATOR_SCORE	MALWARE_FAMILY	MALWARE_CATEGORY	EVENT_ID	RESPONSE	RESP
5						APD-FTP-W7-64-1.qbaslab.com			6			RTP_0b83a56d-879b-4ade-9446-c0		

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

