Perform device investigations in Microsoft Defender for Endpoint

# Device inventory list

Device inventory shows a list of devices in your network where alerts are generated. By default the queue displays devices with alerts seen in the last 30 days. Click device to open the device page. This page can also be accessed via incidents and alerts.

**Risk level -** Risk level assesses overall risk of device. Resolving active alerts, approving remediation activities and supressing subsequent alerts can lower the risk level.

**Exposure level –** Assesses the current exposure of the device based on the cumulative impact of its pending security recommendations. The possible levels are low, medium and high. If the exposure level says “no data available” this may be because:

* The device stopped reporting for more than 30 days
* The device OS is not supported
* The device has a stale agent(unlikely)

**Health State -** The following device health states:

* Active – devices are actively reporting sensor data to the service
* Inactive - Devices that stopped sending signals for more than seven days
* Misconfigured – Devices that have impaired communications with service or are unable to send sensor data. Misconfigured devices can further be classified to:
  + No sensor data
  + Impaired communications

**Antivirus Status -** The antivirus status for Windows 10 devices only:

* Disabled – Virus & threat protection is turned off
* Not reporting – Virus & threat protection is not reporting
* Not updating – Virus & threat protection is not up to date

# Investigate the device

When you investigate a specific device, you’ll see:

* Device details
* Response actions
* Tabs(overview, alerts, timeline, security recommendations)
* Cards (active alerts, logged on users, security assessment)

# Response actions

Response actions run along the top of a specific device page and include:

* Manage tags
* Isolate device
* Restrict app execution
* Run antivirus scan
* Collect investigation package
* Initiate Live Response Session
* Initiate automated investigation
* Consult a threat expert
* Action centre

You can take response actions in the Action centre, on a specific device page, or on a specific file page.