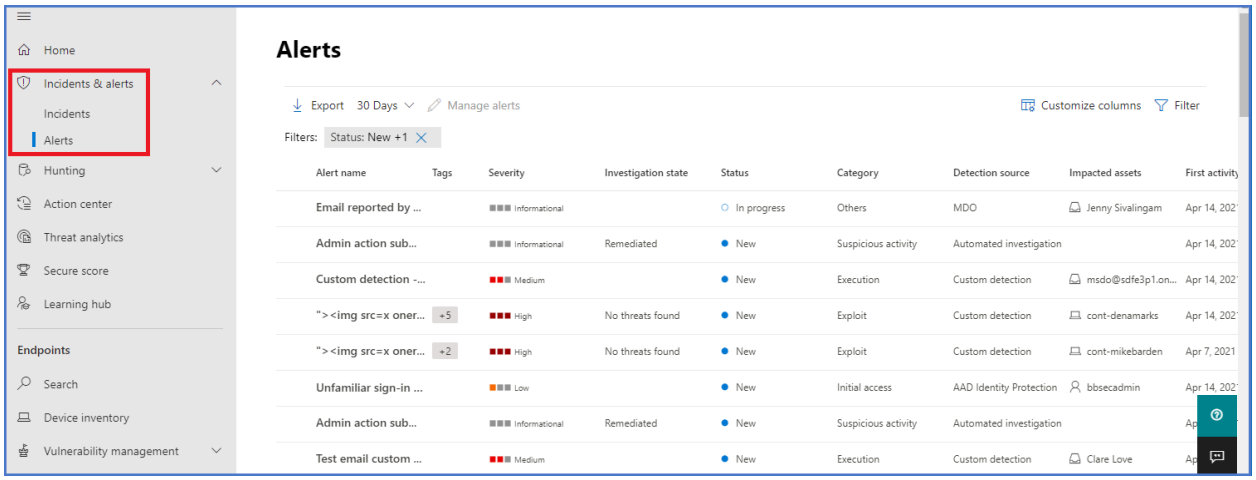
Manage and investigate alerts

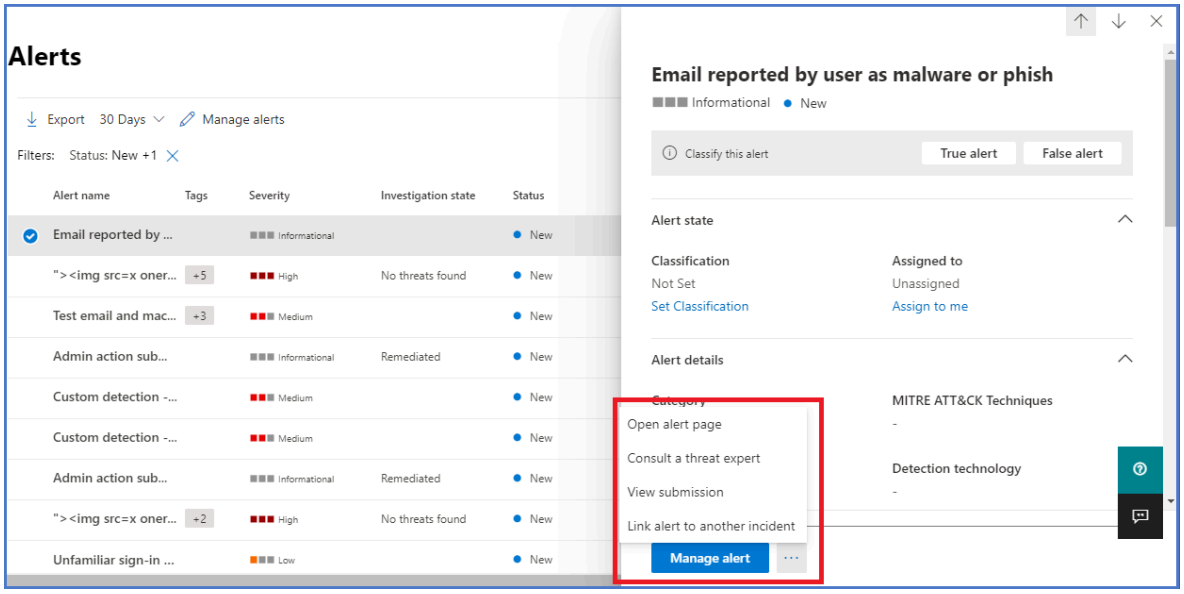
By: Ryan Stewart

You can manage alerts by selecting an alert in the Alerts queue or the Alerts tab of the Device page for an individual device. Selecting an alert in either of those places brings up the Alert management pane.



Alert management

You can view and set metadata about the Alert preview or Alert details page.



The metadata fields include and actions include:

Severity

- **High (Red)** - Alerts commonly seen associated with **advanced persistent threats** (APT). These alerts indicate a high risk because of the severity of damage they can inflict on devices. Examples include credential theft tools activities, ransomware activities not associated with any group, tampering with security sensors, or any malicious activities indicative of a human adversary.

- **Medium (Orange) -** Alerts from endpoint detection and response post-breach behaviors that **might** be a part of an advanced persistent threat (APT). This includes observed behaviors typical of attack stages, **anomalous registry change**, execution of suspicious files, and so forth. Although some might be part of internal security testing, it requires investigation as it might also be a part of an advanced attack.

- **Low (Yellow)** - Alerts on threats associated with prevalent malware. For example, hack-tools, non-malware hack tools, such as running exploration commands, clearing logs, etc. often don't indicate an advanced threat targeting the organization. It could also come from an isolated security tool testing by a u ser in your organization.

- **Informational (Grey)** - Alerts that might not be considered harmful to the network but can drive organizational security awareness on potential security issues.

Microsoft Defender Antivirus (Microsoft Defender AV) and Defender for Endpoint alert severities are **different** because they **represent different scopes**. The Microsoft Defender AV threat severity represents the absolute severity of the detected threat (malware) and is assigned based on the potential risk to the individual device if infected.

The Defender for Endpoint alert severity represents the severity of the detected behavior, the actual risk to the device, and most importantly, the potential risk to the organization.

So, for example:

- The severity of a Defender for Endpoint alert about a Microsoft Defender AV detected threat that was prevented and didn't infect the device is categorized as "Informational" because there was no actual damage.

- An alert about a commercial malware was detected while executing, but blocked and remediated by Microsoft Defender AV, is categorized as "Low" because it may have caused some damage to the individual device but poses no organizational threat.

- An alert about malware detected while executing which can pose a threat not only to the individual device but to the organization, regardless if it was eventually blocked, may be

ranked as "Medium" or "High".

- Suspicious behavioral alerts, which weren't blocked or remediated will be ranked "Low", "Medium" or "High" following the same organizational threat considerations.

Categories

The alert categories align closely with the attack tactics and techniques in the **MITRE ATT&CK Enterprise matrix.**

The alert categories also include items (like `Unwanted Software`) that are not part of the ATT&CK matrices.

The categories are:

- **Collection** - Locating and collecting data for exfiltration
- **Command and control** - Connecting to attacker-controlled network infrastructure to relay data or receive commands
- **Credential access** - Obtaining valid credentials to extend control over devices and other resources in the network
- **Defense evasion** - Avoiding security controls by, for example, turning off security apps, deleting implants, and running rootkits
- **Discovery** - Gathering information about important devices and resources, such as administrator computers, domain controllers, and file servers
- **Execution** - Launching attacker tools and malicious code, including RATs and backdoors
- **Exfiltration** - Extracting data from the network to an external, attacker-controlled location
- **Exploit** - Exploit code and possible exploitation activity
- **Initial access** - Gaining initial entry to the target network, usually involving password-guessing, exploits, or phishing emails
- **Lateral movement** - Moving between devices in the target network to reach critical resources or gain network persistence
- **Malware** - Backdoors, trojans, and other types of malicious code

- **Persistence** - Creating autostart extensibility points (ASEPs) to remain active and survive system restarts

- **Privilege escalation** - Obtaining higher permission levels for code by running it in the context of a privileged process or account

- **Ransomware** - Malware that encrypts files and extorts payment to restore access

- **Suspicious activity** - Atypical activity that could be malware activity or part of an attack

- **Unwanted software** - Low-reputation apps and apps that impact productivity and the user experience; detected as potentially unwanted applications (PUAs)

Link to another incident

You can create a new incident from the alert or link to an existing incident.

Assign alerts

If an alert isn't **yet assigned,** you can select Assign to me to assign the alert to yourself.

Suppress alerts

There might be scenarios where you need to suppress alerts from appearing in Microsoft Defender Security Center. Defender for Endpoint lets you create suppression rules for specific alerts that are known to be innocuous, such as known tools or processes in your organization.

Suppression rules can be created from an existing alert. They can be disabled and re-enabled if needed.

When a suppression rule is created, it takes effect from the point when the rule is created. The rule won't affect existing alerts already in the queue prior to the rule creation. The rule will only be applied to alerts that satisfy the conditions set after the rule is created.

There are two contexts for a suppression rule that you can choose from:

- Suppress alert on this device

- Suppress alert in my organization

The context of the rule lets you tailor what gets surfaced into the portal and ensure that only real security alerts are surfaced into the portal.

Change the status of an alert

You can categorize alerts as New, In Progress, or Resolved by changing their status as your investigation progresses. This helps you organize and manage how your team can respond to alerts.

For example, a team leader can review all New alerts, and decide to assign them to the In Progress queue for further analysis.

Alternatively, the team leader might assign the alert to the Resolved queue if they know the alert is benign, coming from an irrelevant device (such as one belonging to a security administrator), or is being dealt with through an earlier alert.

Alert classification

You can choose not to set a classification or specify whether an alert is a true alert or a false alert. It's important to provide the classification of true positive/false positive because it is used to monitor alert quality and make alerts more accurate. The "determination" field defines extra fidelity for a "true positive" classification.

Add comments and view the history of an alert

You can add comments and view historical events about an alert to see previous changes made to the alert. Whenever a change or comment is made to an alert, it's recorded in the Comments and history section. Added comments instantly appear on the pane.

Alert investigation

Investigate alerts that are affecting your network, understand what they mean, and how to resolve them.

Select an alert from the alerts queue to go to alert page. This view contains the alert title, the affected assets, the details side pane, and the alert story.

Investigate using the alert story

The alert story details why the alert was triggered, related events that happened before and after, and other related entities.

Entities are clickable, and every entity that isn't an alert is expandable using the expand icon on the right side of that entity's card. The entity in focus will be indicated by a blue stripe to the left side of that entity's card, with the alert in the title being in focus at first.

Selecting an entity switches the context of the details pane to this entity, and will allow you to review further information, and manage that entity. Selecting ... to the right of the entity card reveals all actions available for that entity. These same actions appear in the details pane when that entity is in focus.

Take action from the details pane

Once you've selected an entity of interest, the details pane changes to display information about the selected entity type, historic information when it's available, and offer controls to take action on this entity directly from the alert page.

Once you're done investigating, go back to the alert you started with, mark the alert's status as Resolved and classify it as either False alert or True alert. Classifying alerts helps tune this capability to provide more true alerts and fewer false alerts.

If you classify it as a true alert, you can also select a determination.

If you're experiencing a false alert with a line-of-business application, create a suppression rule to avoid this type of alert in the future.