

Open Endpoint Manager > Click 'Security Sub-Systems' > 'Antivirus' > 'Current Malware List' tab

- The 'Current Malware List' shows malicious items which have been blocked, but are still resident on the target device.
- You can use this interface to clean (delete), ignore, or quarantine the items.
- You can also assign a 'Trusted' rating to a file. Use this option if you think the item is a false positive. It will not be flagged by future scans.

[Background – How do files get on this list?](#)

[Overview of the current malware list area](#)

[Take actions on files in the list](#)

## Background - How do files get on this list?

- A file arrives on this list if the security client blocked the malware from running, but it was neither quarantined nor deleted.
- This can happen because of settings in the 'Antivirus' section the device profile, or because of a user's response to an alert.
- The following explains the profile settings and conditions for a file to appear in the 'Current Malware List'

### Windows devices

- [Real-time virus monitoring](#) - 'Show antivirus alerts' is *disabled* in the profile with 'Block Threats' set as the default action

...or 'Show antivirus alerts' is *enabled*, and the end-user blocked the threat at the alert.

- [Scheduled and manual scans](#) - 'Automatically clean threats' is *disabled* in the active profile.

**MAC devices** - ['Automatically Quarantine'](#) is *disabled* in the profile on the device.

**Linux devices** - ['Automatically Quarantine'](#) is *disabled* in the profile on the device.

**Android devices** - ['Automatically uninstall'](#) is *not enabled* in the profile on the device.

## Overview of the current malware list area

- Log into ITarian
- Click 'Applications' > 'Endpoint Manager'
- Click 'Security Sub-Systems' > 'Antivirus'
- Click the 'Current Malware List' tab:

Endpoint Manager

DASHBOARD

DEVICES

USERS

CONFIGURATION TEMPLATES

NETWORK MANAGEMENT BETA

APPLICATION STORE

APPLICATIONS

SECURITY SUB-SYSTEMS

Security Dashboards

Containment

Application Control

Valkyrie

Antivirus

Device Control

Antivirus / Current Malware List

Device List

Current Malware List

Quarantined Files

Threat History

Autoruns Items

Delete Malware

Ignore Malware

Quarantine Malware

Rate as Trusted

Export

	OS	DEVICE NAME	APPLICATION NAME	PACKAGE NAME / FILE PATH	FILE HASH	SIGNATURE	DETECTION DATE
<input type="checkbox"/>		<div><div></div><div>susan-Virtual...</div></div>	4c1dc737915d76b7ce5...	/home/susan/Doubtful/Files...		Malware	2019/07/02 10:32:2...
<input type="checkbox"/>		<div><div></div><div>susan-Virtual...</div></div>	grandcab.bin	/home/susan/Doubtful/Files...		Malware	2019/07/02 10:32:2...

Results per page: 

20

Displaying 1-2 of 2 results

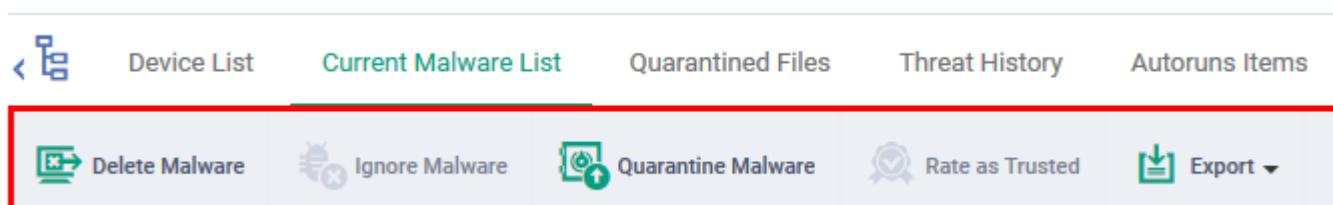
Each row shows a piece of malware on a specific device. The same file might be present on multiple devices.

Information about each file includes:

- The name and operating system of the device on which it was found.
- The location, name, and signature of the malware.
- The date it was detected.

## Take actions on files in the list

The controls above the list let you take various actions on selected files:



- **Delete Malware** - Removes the file from the device.
- **Ignore Malware** - The item is allowed to remain on the device. This action only applies to Android devices.
- **Quarantine Malware** - Moves the file to quarantine on the device. Files in quarantine cannot execute. You can review these files in the '[Quarantined Files](#)' tab.
- **Rate as Trusted** - The file is allowed to run on the device and will not be flagged as malware in future scans. Use this action only if you think the file is a false positive. You can read more about the file rating system in [this wiki](#).
- **Export** - Export the current malware list to a .csv file.

## Related topics -

- [How to manage quarantined items in Endpoint Manager](#)
- [How to manage autorun items in Endpoint Manager](#)
- [How to view security events on Windows endpoints](#)