

Open Endpoint Manager > Click 'Security Sub-Systems' > 'Antivirus' > 'Android Threat History'

- The 'Android Threat History' area shows all malicious events found on managed Android devices over time.
- The list shows items that have been removed from devices and those which are still present.
- The list is useful for auditing, troubleshooting and analyzing customer devices.
- You can filter the list by various criteria, export the list to .csv, and clear history items you no longer require.

Use the links below to jump to the section you need help with:

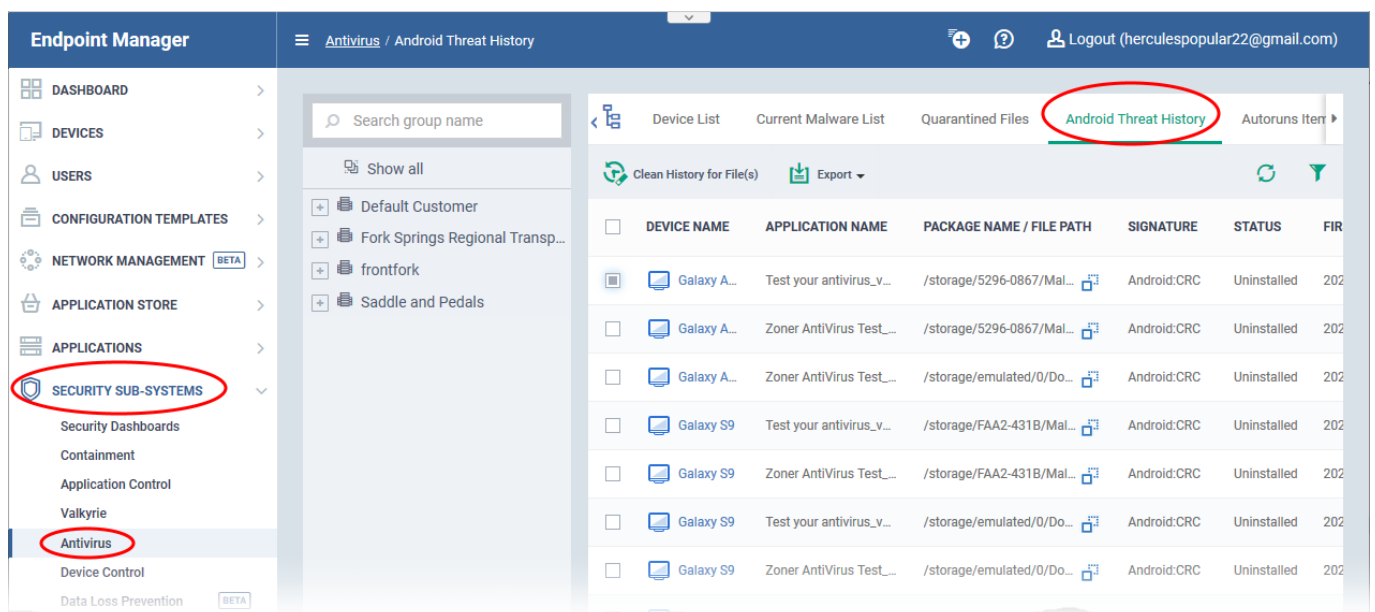
- [View Android threat history](#)
  - [Remove unwanted entries](#)
  - [Generate report of Android threat history](#)

## View Android threat history

- Login to ITarian
- Click 'Applications' > 'Endpoint Manager'
- Click 'Security Sub-systems' > 'Antivirus'
- Click the 'Android Threat History' tab
  - Select a company or a group to view threats identified on their devices

Or

- Select 'Show All' on to view threats identified on all devices added to EM



The screenshot shows the Endpoint Manager interface. The left sidebar has 'SECURITY SUB-SYSTEMS' and 'Antivirus' circled in red. The main content area shows the 'Android Threat History' page with a table of threat entries. The table has columns for DEVICE NAME, APPLICATION NAME, PACKAGE NAME / FILE PATH, SIGNATURE, STATUS, and FIR. The entries are for various Galaxy devices (Galaxy A..., Galaxy S9) and applications (Test your antivirus\_v..., Zoner AntiVirus Test...). The 'STATUS' column shows 'Uninstalled' for all entries.

DEVICE NAME	APPLICATION NAME	PACKAGE NAME / FILE PATH	SIGNATURE	STATUS	FIR
Galaxy A...	Test your antivirus_v...	/storage/5296-0867/Mal...	Android:CRC	Uninstalled	202
Galaxy A...	Zoner AntiVirus Test...	/storage/5296-0867/Mal...	Android:CRC	Uninstalled	202
Galaxy A...	Zoner AntiVirus Test...	/storage/emulated/0/Do...	Android:CRC	Uninstalled	202
Galaxy S9	Test your antivirus_v...	/storage/FAA2-431B/Mal...	Android:CRC	Uninstalled	202
Galaxy S9	Zoner AntiVirus Test...	/storage/FAA2-431B/Mal...	Android:CRC	Uninstalled	202
Galaxy S9	Test your antivirus_v...	/storage/emulated/0/Do...	Android:CRC	Uninstalled	202
Galaxy S9	Zoner AntiVirus Test...	/storage/emulated/0/Do...	Android:CRC	Uninstalled	202

The interface shows the list of malware identified on the Android devices:

**Device Name** - The label assigned to the device. If no name was assigned by the end-user, the model number of the device is used. A gray text color indicates the device has been offline for the past 24 hours.

- Click the device name to view granular details about the device.

**Application Name** - The label of the infected application.

**Package Name / File Path** - The Android package name or identifier of the package from which the app was installed.

**Signature** - The name of the identified malware.

**Status** - Whether the malware was uninstalled or is yet to be uninstalled.

**First Detection** - Date and time of the scan which first discovered the malware on the device.

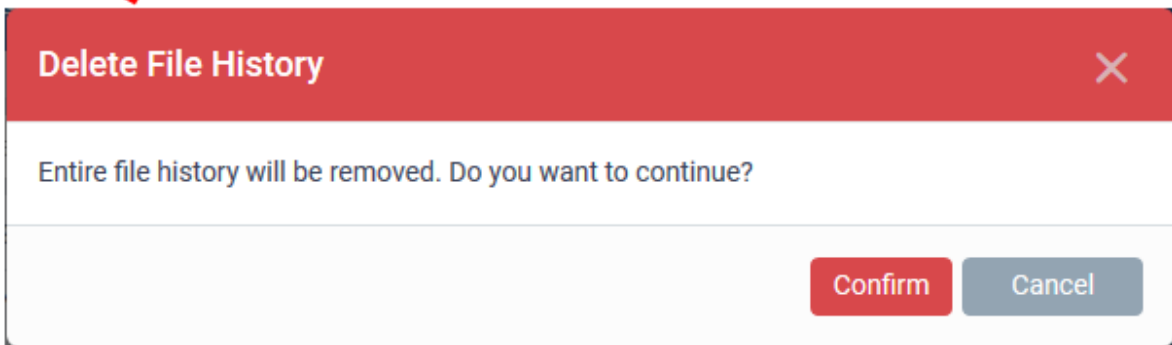
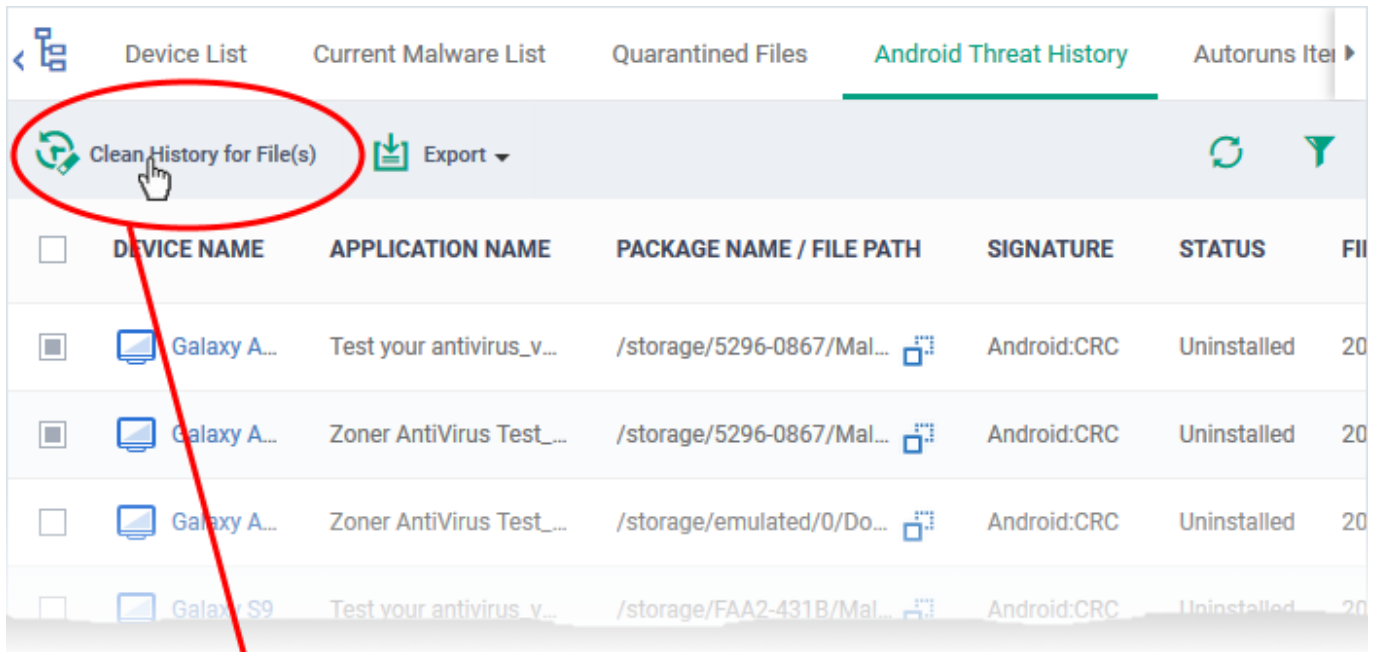
**Last Detection** - Date and time of the last scan to discover the malware.

- Click any column header to sort items in ascending/descending order of the entries in that column.
- Click the funnel icon on the right to filter items by various criteria. You can filter by device name, application name, package name/file path, signature, status and first/last detection date.

### **Remove unwanted entries**

Deleting file history will only remove the log entry. The file will not be removed from the device or from any other interfaces in which it is listed.

- Click 'Security Sub-systems' > 'Antivirus'
- Click the 'Android Threat History' tab
- Select the events you want to remove then click 'Clean History for File(s)' at the top:



- Click 'Confirm' to remove the entries from the list

### Export threat history as a CSV file

- Click 'Security Sub-systems' > 'Antivirus'
- Click the 'Android Threat History' tab
- Click the funnel icon to filter which records are included in the report
- Click the 'Export' > 'Export to CSV':



- Click 'Dashboard' > 'Reports' to view the report
- See [this wiki page](#) if you need help to download the report