

How to view every threat appeared on your managed Android devices

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 Xcitium
 - 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 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.

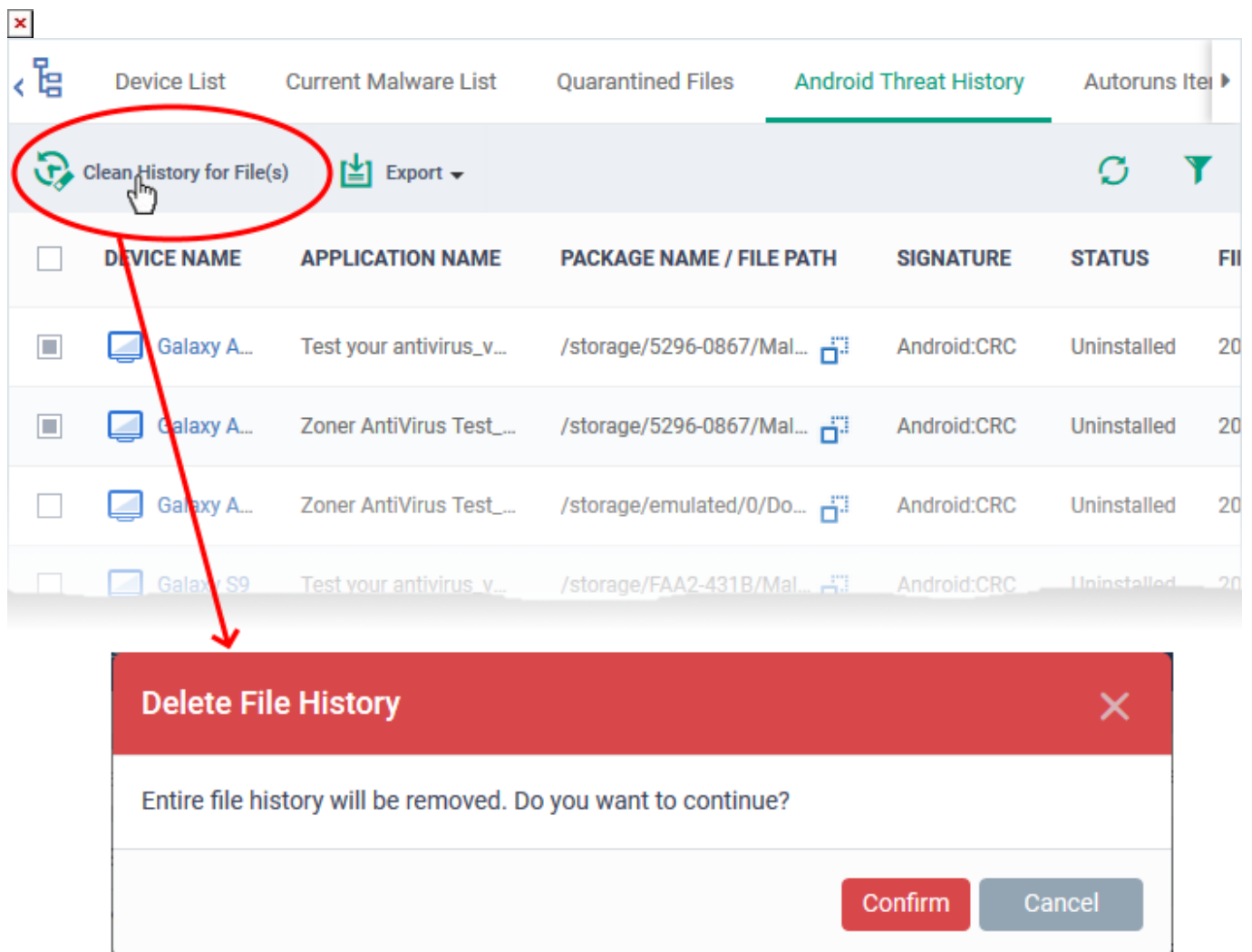
Last Detection - Date and time of the last scan to discover the malware.

- 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:



The screenshot shows the 'Android Threat History' tab in an application. At the top, there are navigation tabs: 'Device List', 'Current Malware List', 'Quarantined Files', 'Android Threat History' (selected), and 'Autoruns Items'. Below the tabs, there is a toolbar with a 'Clean History for File(s)' button (circled in red), an 'Export' button, a refresh icon, and a filter icon. Below the toolbar is a table with columns: 'DEVICE NAME', 'APPLICATION NAME', 'PACKAGE NAME / FILE PATH', 'SIGNATURE', 'STATUS', and 'FILE'. The table contains several rows of data, including entries for 'Galaxy A...' and 'Galaxy S9'. A red arrow points from the 'Clean History for File(s)' button to a dialog box titled 'Delete File History'. The dialog box contains the text 'Entire file history will be removed. Do you want to continue?' and two buttons: 'Confirm' and 'Cancel'.

- 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