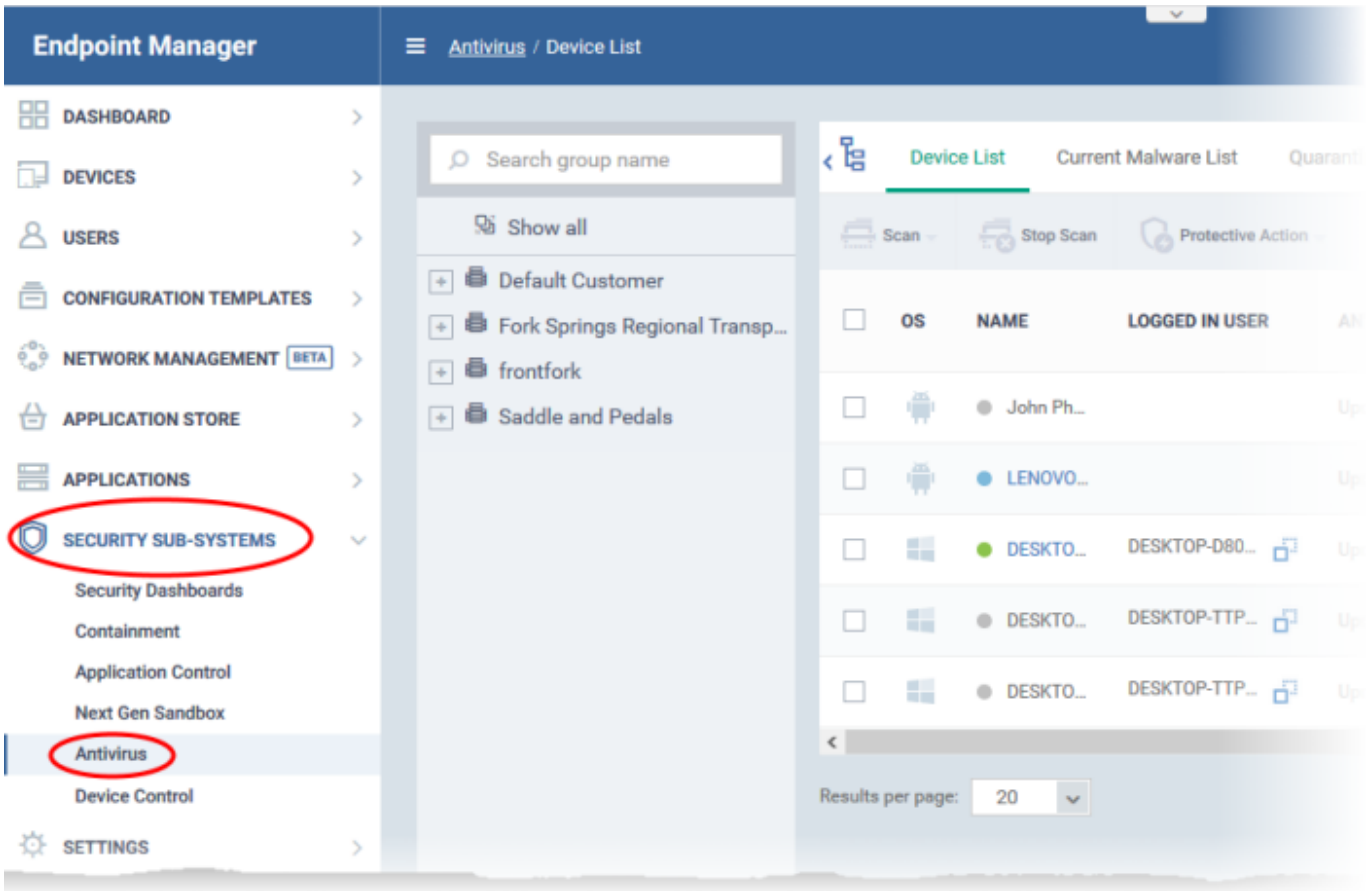
Use the ‘Antivirus’ area to run scans and track malware activity on endpoints

- Open Endpoint Manager
- Click 'Security Sub-systems' > 'Antivirus'

The antivirus area provides a detailed overview of threats on your managed endpoints. It allows you to view current and previous threats, run scans on selected or all devices, manage quarantined files, and more.



The interface has the following tabs:

- **Device List** - Shows the status of each managed device with regards to malware. This area allows you to:
    - Run virus scans on selected or all devices
    - View the date and type of the most recent virus scan
    - View whether devices have the latest virus database
    - View all infected devices
    - Clean malware from infected devices with a single click

Click for more on this tab

- **Current Malware List** - A list of all unprocessed malware on your managed devices. You can delete, ignore, quarantine or even trust malware on specific devices. You can apply these actions to specific threats, or multiple threats at once. Click for more on this tab

- **Quarantined Files** - Shows malware which has been quarantined by Xcitium Client Security on Windows, Mac and Linux devices. You can delete or restore quarantined items, or assign a new trust rating to them. Click for more on this tab

- **Threat History** - A list of all threats found on Windows, Mac, Android and Linux devices since you deployed Endpoint Manager. The list shows threats that have neutralized in the past, and threats that are still active. Click for more on this tab

- **Autorun Items** - View and take action on items that were blocked by the boot protection feature of Xcitium Client Security (CCS). CCS will disable autoruns that attempt to modify protected registry items, if so configured in the antivirus section of a profile. This tab lets you review the files, apply a new trust rating to them, or delete/restore files as required.

  Click for more on this tab