How to view antivirus scan results and quarantined files on a device in Endpoint Manager

Click 'Devices' > 'Device List' > 'Device Management' > click the name of a device > 'Antivirus' tab

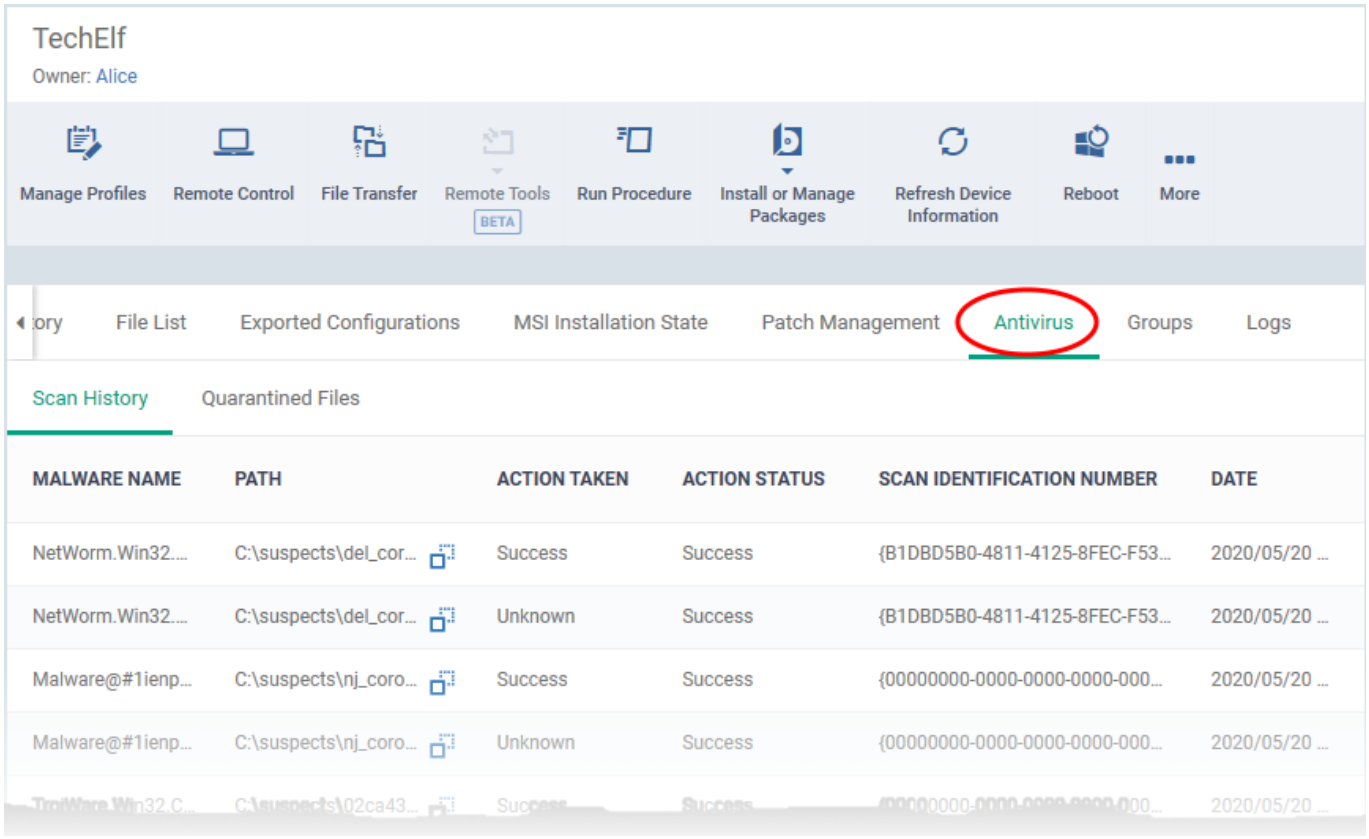
- The 'Antivirus' tab is available only for Windows and Mac OS devices, on which Xcitium Client Security is installed and 'Antivirus' is enabled in the profile active on them.
- The interface shows malware discovered on your managed endpoints by manual AV scans and automated scans ran by the profile.
- You can also view the items moved to quarantine on the device and take actions on them.
    - See this wiki for help to run manual scans on the device from Endpoint Manager
    - See this wiki for help to schedule automated scans in a Windows profile
    - See this wiki for help to schedule automated scans in a Mac OS profile

Use the following links to jump to the task you need help with:

Open the antivirus interface

- Login to Xcitium
- Click 'Applications' > 'Endpoint Manager'
- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab
    - Select a company or group on the left to view devices in the group

      Or
    - Select 'Show all' to view every device enrolled to EM
- Click the name of a Windows or Mac OS device then select the 'Antivirus' tab:



The antivirus interface has two tabs:

- **Scan History** – Windows only. Shows the list of malware identified by the scans and actions taken on them. See View scan history to read more.
- **Quarantined Files** – Windows and Mac OS devices. Shows the list of items moved to quarantine. You can remove, restore or change file trust rating of the items. See Quarantined items to read more.

View scan history

The scan history is available only for Windows devices, with CCS installed and antivirus is enabled by the profile active on them

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab
    - Select a company or group on the left to view devices in the group

      Or
    - Select 'Show all' to view every device enrolled to EM
- Click the name of a Windows or Mac OS device then select the 'Antivirus' tab
- Click the 'Scan History' tab (if it is not already open)

Malware Name - Label of the malicious item

Path - The installation location of the file containing the malware

Action Taken - The response taken by Xcitium Client Security to the malware.

Action Status - Whether the response was a success or failure

Scan Identification Number - Unique identifier assigned to the scan which found the malware

Date - Date and time at which the scan was performed.

Quarantined items

- Quarantine is a secure holding area for potentially dangerous files. Quarantined files pose no threat to your system.
- Files identified as malicious or containing threats are moved to quarantine by CCS. See How do threats get quarantined? to read more.
- You can analyze the trustworthiness of items in quarantine and delete, restore or assign a file trust rating to them.
- File ratings determine how CCS handles the file:
    - Files rated as 'Malicious' will stay in quarantine on the device.
    - Files rated as 'Unrecognized' will be restored to their original location on the device. Future virus scans may flag them as malicious again.
    - Files rated as 'Trusted' will be restored to their original locations on the device. These files are skipped in future virus scans.

View quarantined files

- Click 'Devices' > 'Device List'
- Click the 'Device Management' tab
    - Select a company or group on the left to view devices in the group

      Or
    - Select 'Show all' to view every device enrolled to EM
- Click the name of a Windows or Mac OS device then select the 'Antivirus' tab
- Click the 'Quarantined Files' tab

File Name - The file that was moved to quarantine.

File Path – The location of the identified file on the device

File Hash - The SHA1 hash value of the quarantined file

Date Quarantined - Date and time at which the malware was identified and moved to quarantine on the device.

Xcitium Rating - The file's trust level as rated by CCS.

Admin Rating - The trust rating of the file as set by the administrator. Files can be rated as trusted, malicious or unrecognized.

User's last action - The response to the quarantined item by the EM admin.

User's last action status - The current status of the response. The possible statuses are:

- Operation failed. Try again.
- Command is queued
- Command has been sent

- Click 'Request quarantined files' to import the list of most recently quarantined files from the device

The quarantine interface lets you:

- Restore False Positives from Quarantine
- Remove Malware files from the devices
- Rate files as 'Unrecognized', 'Trusted' or 'Malicious'

Restore False Positives from Quarantine

You can restore items from quarantine to their original location. This is useful if an identified item is a false positive, or a trustworthy file.

- Select the items from the list
- Click 'Restore file(s) on Device' on the top

The items are restored to its original location on the device and removed from the list.

Remove Malware files from the devices

You can permanently delete items from the device, if identified items are genuine malware.

- Select the items from the list
- Click 'Delete file(s) from Device' on the top

The items are deleted permanently from the device and removed from the list.

Rate files as 'Unrecognized', 'Trusted' or 'Malicious'

You can set a trust rating for items in quarantine as 'Admin Rating'. The admin rating supersedes the Xcitium rating for a file.

- Select the items from the list
- Click 'Rate as Unrecognized', 'Rate as Trusted' or 'Rate as Malicious' appropriate to the rating you want to assign to the items.

A confirmation is shown and the command is sent to the device.

- Files rated as 'Malicious' will stay in quarantine on the device.
- Files rated as 'Unrecognized' will be restored to their original locations on the device. Future AV scans may flag them as 'malicious' again.
- Files rated as 'Trusted' will be restored to their original locations in the device. These files will be white-listed and skipped by future antivirus scans.

How do threats get quarantined?

Windows Devices

Real time scans - Threats are placed in quarantine if:

- 'Show antivirus alerts' is disabled and 'Quarantine Threats' is set as the default action in the profile on the device. This setting is in the 'Realtime Scan Settings' area of the profile's antivirus section.
- 'Show antivirus alerts' is enabled and the end-user quarantined the threat at an alert.
- See 'Realtime Scan' in How to configure antivirus settings in a Windows Profile if you want to read more about the antivirus section of a profile.

On-demand / Scheduled scans - Threats are placed in quarantine if:

- 'Automatically clean threats' is enabled and 'Quarantine' is set as the action in the profile on the device.
- See 'On-demand / Scheduled Scans' in How to configure antivirus settings in a Windows Profile to read more.

Manual quarantine:

- Admins can move threats to quarantine from the 'Current Malware List' interface.
- End-users can move files to quarantine on their endpoint.
- See How to view and manage unprocessed malware on your endpoints for more details.

MAC OS Devices

Real time scans - Threats are placed in quarantine if:

- 'Automatically quarantine threats found during scanning' is enabled in the profile on the device. This setting is in the 'Realtime Scan Settings' area of the profile's antivirus section.
- The end-user chooses to quarantine the threat at an alert
- See 'Realtime Scanning' in How to configure antivirus settings in a Mac OS profile if you want to read more about the antivirus section of a profile.

On-demand / Scheduled scans - Threats are quarantined if:

- 'Automatically quarantine threats found during scanning' is enabled in the profile on the device

- See 'Manual Scanning' in How to configure antivirus settings in a Mac OS profile if you want to read more about the antivirus section of a profile..

Manual quarantine:

- An administrator moved a threat to quarantine from the 'Current Malware List' interface
- An end-user moved a file to quarantine on the endpoint
- See How to view and manage unprocessed malware on your endpoints for more details.