

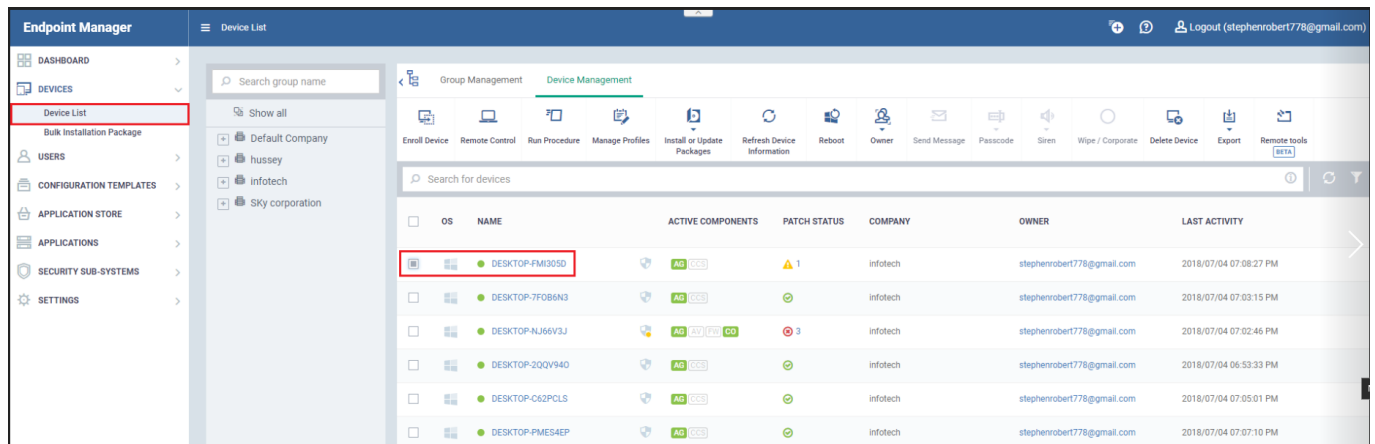
How to view antivirus scan result history for a device

Antivirus scan history helps to display the identified malware files on your endpoint.

Step [1]: Go to **Device List** on that choose a device where you need to view the malware file history of your endpoint.

For Example:

DESKTOP-FM1305D



OS	NAME	ACTIVE COMPONENTS	PATCH STATUS	COMPANY	OWNER	LAST ACTIVITY
Windows	DESKTOP-FM1305D	AG CCS	1	infotech	stephenrobert778@gmail.com	2018/07/04 07:08:27 PM
Windows	DESKTOP-7F0B6N3	AG CCS	0	infotech	stephenrobert778@gmail.com	2018/07/04 07:03:15 PM
Windows	DESKTOP-4J66V3J	AG AV PM CC	3	infotech	stephenrobert778@gmail.com	2018/07/04 07:02:46 PM
Windows	DESKTOP-2QQV94Q	AG CCS	0	infotech	stephenrobert778@gmail.com	2018/07/04 06:53:33 PM
Windows	DESKTOP-C62PCLS	AG CCS	0	infotech	stephenrobert778@gmail.com	2018/07/04 07:05:01 PM
Windows	DESKTOP-PMES4EP	AG CCS	0	infotech	stephenrobert778@gmail.com	2018/07/04 07:07:10 PM

Note:

In order to view the history of antivirus for a device, **Comodo client security** needs to be installed on your endpoint.

Step [2]: Select **Antivirus Scan History** tab, It will display the list of affected files which are handled by Comodo Client Security. You can sort the following details with Malware name, Path, Action Taken, Action Status, Scan Identification Number along with date.

Endpoint Manager | Device List / cobra / Summary

DESKTOP-FM305D
Owner: stephenrobert77@gmail.com

Manage Profiles Remote Control Run Procedure Install or Update Packages Refresh Device Information Reboot Export Security Configuration Delete Device Owner

Device Name Summary Networks Associated Profiles Software Inventory File List Exported Configurations MSI Installation State Patch Management **Antivirus Scan History** Groups Logs

Device Summary

Custom device name	DESKTOP-FM305D
Name	DESKTOP-FM305D
Logged user	shines4
AD/LDAP	N/A
Domain/Workgroup	WORKGROUP
Formfactor	PC
Model	VirtualBox
Comodo Client - Communication version	6.19.12672.18060
Processor	Intel(R) Core(TM) i3-2120 CPU @ 3.30GHz
Serial number	0
System model	VirtualBox
System manufacturer	Intel(R) G33M
Ownership type	Not specified
Last connection	2018/07/04 07:03:35 PM
Registered	2018/07/04 04:35:29 PM
External IP	192.74.23.22

OS Summary

OS	Windows
OS name	Microsoft Windows 8.1 Pro (x86)
OS version	6.3.9600
Service pack	N/A
Build version	9600
Reboot time	2018/07/05 06:29:18 AM
Reboot reason	The process C:\Windows\system32\winlogon.exe (COBRA) has initiated the restart of computer COBRA on behalf of user cobrarobert77 for the following reason: No title for this reason could be found Reason Code: 0x50007 Shutdown Type: restart Comment:

Endpoint Manager | Device List / cobra / Antivirus Scan History

DESKTOP-FM305D
Owner: stephenrobert77@gmail.com

Manage Profiles Remote Control Run Procedure Install or Update Packages Refresh Device Information Reboot Export Security Configuration Delete Device Owner

Device Name Summary Networks Associated Profiles Software Inventory File List Exported Configurations MSI Installation State Patch Management **Antivirus Scan History** Groups Logs

MALWARE NAME	PATH	ACTION TAKEN	ACTION STATUS	SCAN IDENTIFICATION NUMBER	DATE
ApplicUnwin@#2975a8b82pc1	C:\Users\mnew\AppData\Local\Temp\50316a05.txt.part1	Moved to quarantine	Success	(00000000-0000-0000-0000-000000000000)	2018/07/05 06:24:38 AM
ApplicUnwin@#2975a8b82pc1	C:\Users\mnew\AppData\Local\Temp\50316a05.txt.part1	Detected	Success	(00000000-0000-0000-0000-000000000000)	2018/07/05 06:24:38 AM
ApplicUnwin@#2975a8b82pc1	C:\Users\mnew\AppData\Local\Temp\DAJH8a5s.com.part1	Detected	Success	(00000000-0000-0000-0000-000000000000)	2018/07/05 06:24:38 AM
ApplicUnwin@#2975a8b82pc1	C:\Users\mnew\AppData\Local\Temp\DAJH8a5s.com.part1	Moved to quarantine	Success	(00000000-0000-0000-0000-000000000000)	2018/07/05 06:24:38 AM
Malware@#278dewoods1vr	C:\Users\mnew\AppData\Local\Temp\7W6X9H1.zip.part1	Moved to quarantine	Success	(00000000-0000-0000-0000-000000000000)	2018/07/05 06:24:29 AM
Malware@#278dewoods1vr	C:\Users\mnew\AppData\Local\Temp\7W6X9H1.zip.part1	Detected	Success	(00000000-0000-0000-0000-000000000000)	2018/07/05 06:24:29 AM
CloudScanner.Trojan.Genp2	C:\Program Files\Desktop Restore\uninst000.exe	Detected	Success	(7592DE53-8D4E-4C3E-8B06-0718D647275D8)	2018/07/03 10:00:04 AM
CloudScanner.Trojan.Genp2	C:\Program Files\CrystalDiskInfo\uninst000.exe	Detected	Success	(7592DE53-8D4E-4C3E-8B06-0718D647275D8)	2018/07/03 10:00:04 AM

Options Explanation,

Malware name - It displays the name of the malicious file.

Path - It shows the affected file path where it is located.

Action Taken - It depicts the action performed for the handled malware file i.e, Detected and Moved to quarantine.

Action Status - On successful handling of the file, status will be success.

Scan Identification Number - The identification number of the file will be displayed.

Date - The date at which the comodo client security has tracked the occurrence of the malicious file.