

# How to view full process tree of a contained application

- The container is a secure, virtual environment which is isolated from the rest of the host.
- Applications in the container pose no threat to the endpoint as they cannot write to the host system and cannot access other processes.
- Xcitium Client Security (CCS) will run a file in the container for two reasons:
  - Because it has a trust rating of 'unknown'. This means it is not yet confirmed as safe to run on the host.
  - Because the file met the conditions of an auto-containment rule which is active on the endpoint.
- Parent process information is useful for admins who need granular knowledge about the applications on their network.
- This article explains how to use both the Endpoint Manager and CCS to find the parent process of a contained application.
  - [Use Endpoint Manager to view the parent processes of a contained application](#)
  - [Use CCS to view the parent processes of a contained application](#)

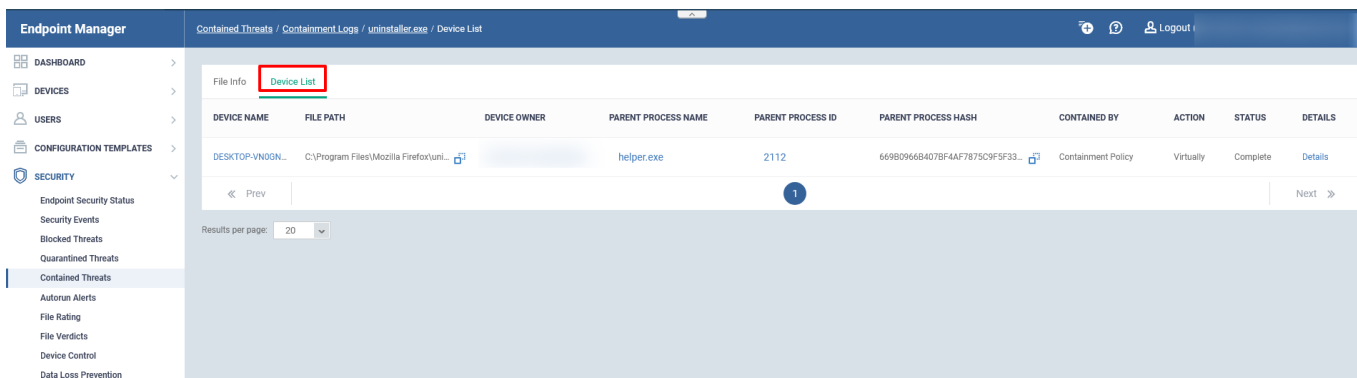
## Use Endpoint Manager to view the parent process tree of a contained application

- Login to Xcitium
- Click 'Applications' > 'Endpoint Manager'
- Click 'Security Sub-Systems' > 'Containment'
- Select the file whose parent process you want to view
- Click the 'File Details' button:

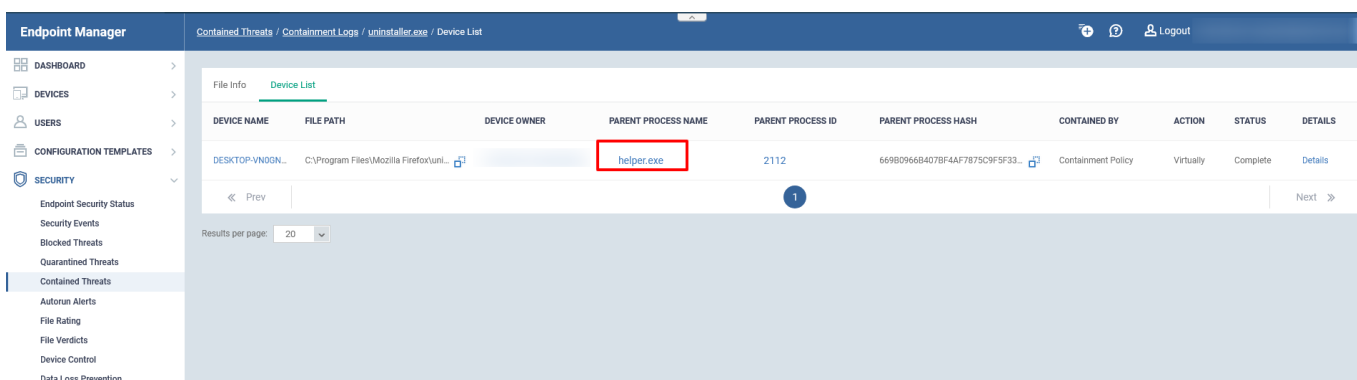
The screenshot displays the Xcitium Endpoint Manager interface. On the left, the 'SECURITY' menu is highlighted. The main area shows 'Containment Logs' with a search bar and several action buttons. The 'File Details' button is highlighted with a red box. Below the buttons is a table of containment logs.

FILE NAME	FILE PATH	FILE HASH	# OF DEVICES	CONTAINED BY	PARENT PROCESS NAME	ACTION	STATUS	XCITIUM RATING	ADMIN RATING	DATE TIME
uninstaller.e...	C:\Program Files\Mozilla FL...	5699CF18248A16DCBF40...	1	Containment Policy	helper.exe	Virtually	Complete	Unrecognized	Not set	2022/08/25 02:18:37 PM
default brow...	C:\Program Files\Mozilla FL...	7CA63532DD17D9D98275...	1	Contained Process	Url_A.exe	Virtually	Complete	Unrecognized	Not set	2022/08/23 03:30:51 PM
regsvr32.exe	C:\Windows\System32\reg...	8D7C2FD354363DAEE63E...	1	Contained Process	Url_A.exe	Virtually	Complete	Trusted	Not set	2022/08/23 03:30:50 PM

- Click the 'Device List' tab:



- Click the name of the file in the 'Parent Process' column:



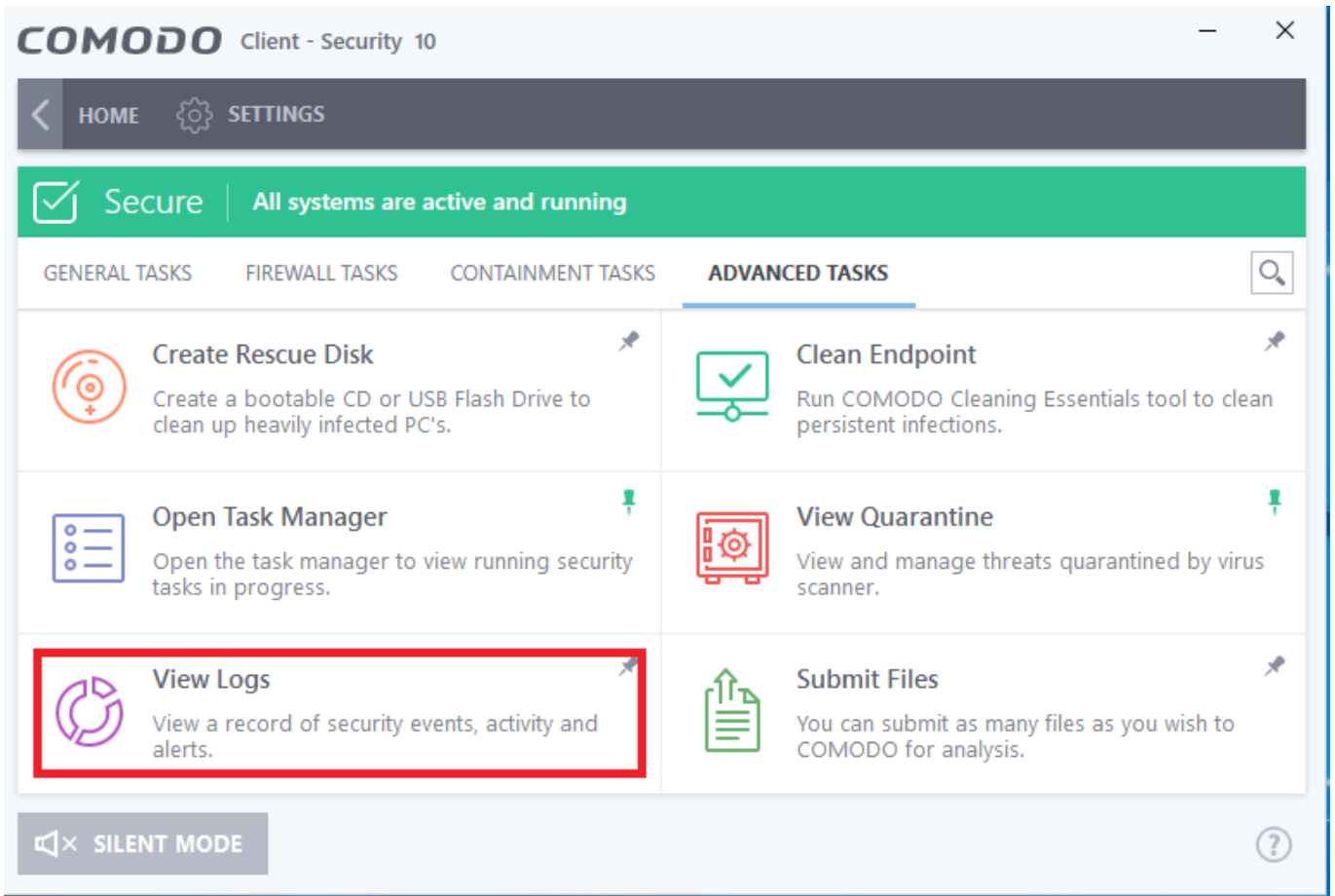
- The full process tree is shown as follows:



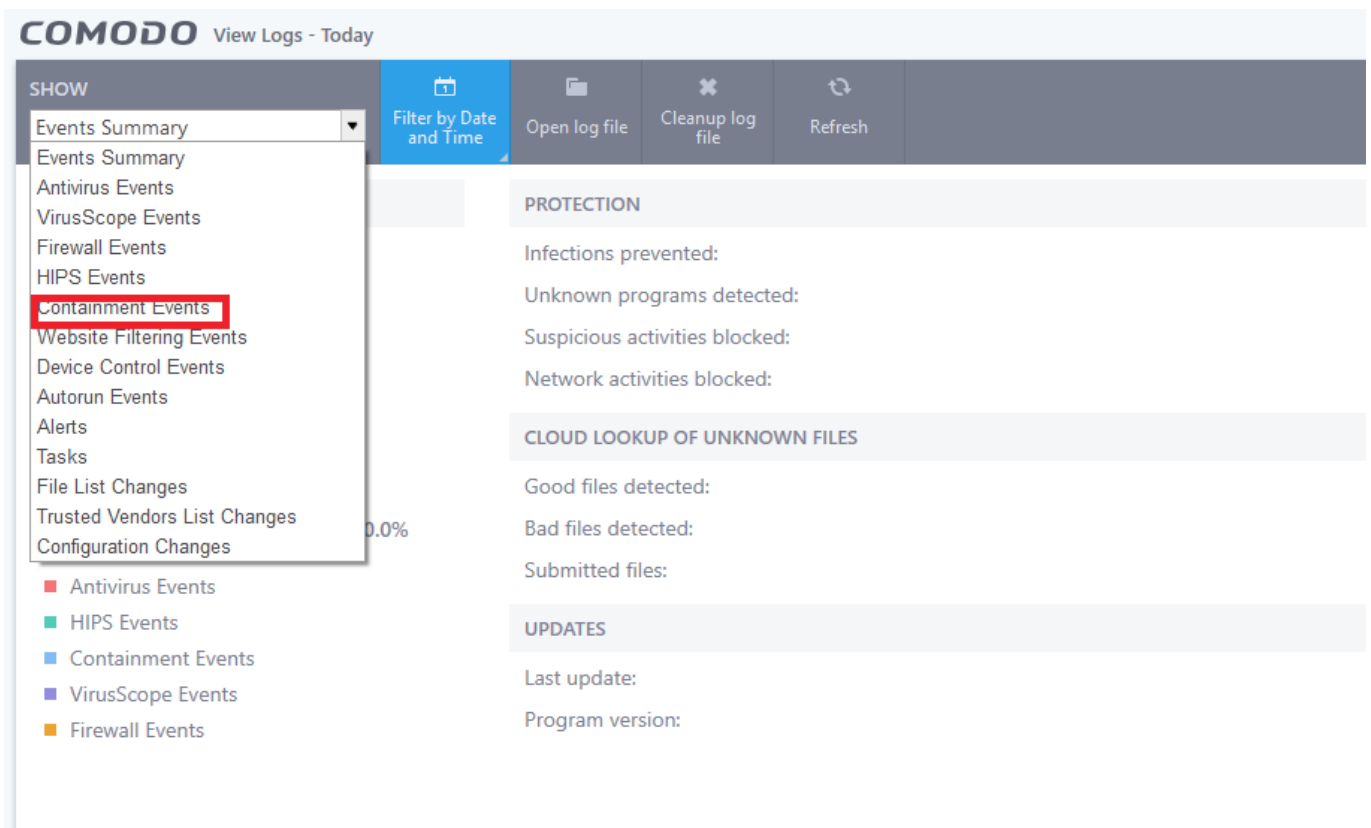
### Use CCS to view the parent process tree of a contained application

- Open Xcitium Client Security (CCS) on the endpoint
- Click 'Tasks' at the top-left of the home screen

- Click 'Advanced Tasks' > 'View Logs'



- Click the 'Show' drop-down at top-left and select 'Containment Events':



**COMODO** View Logs - Entire period

SHOW  
Containment Events

Advanced Filter Filter by Date and Time Open log file Cleanup log file Export Refresh

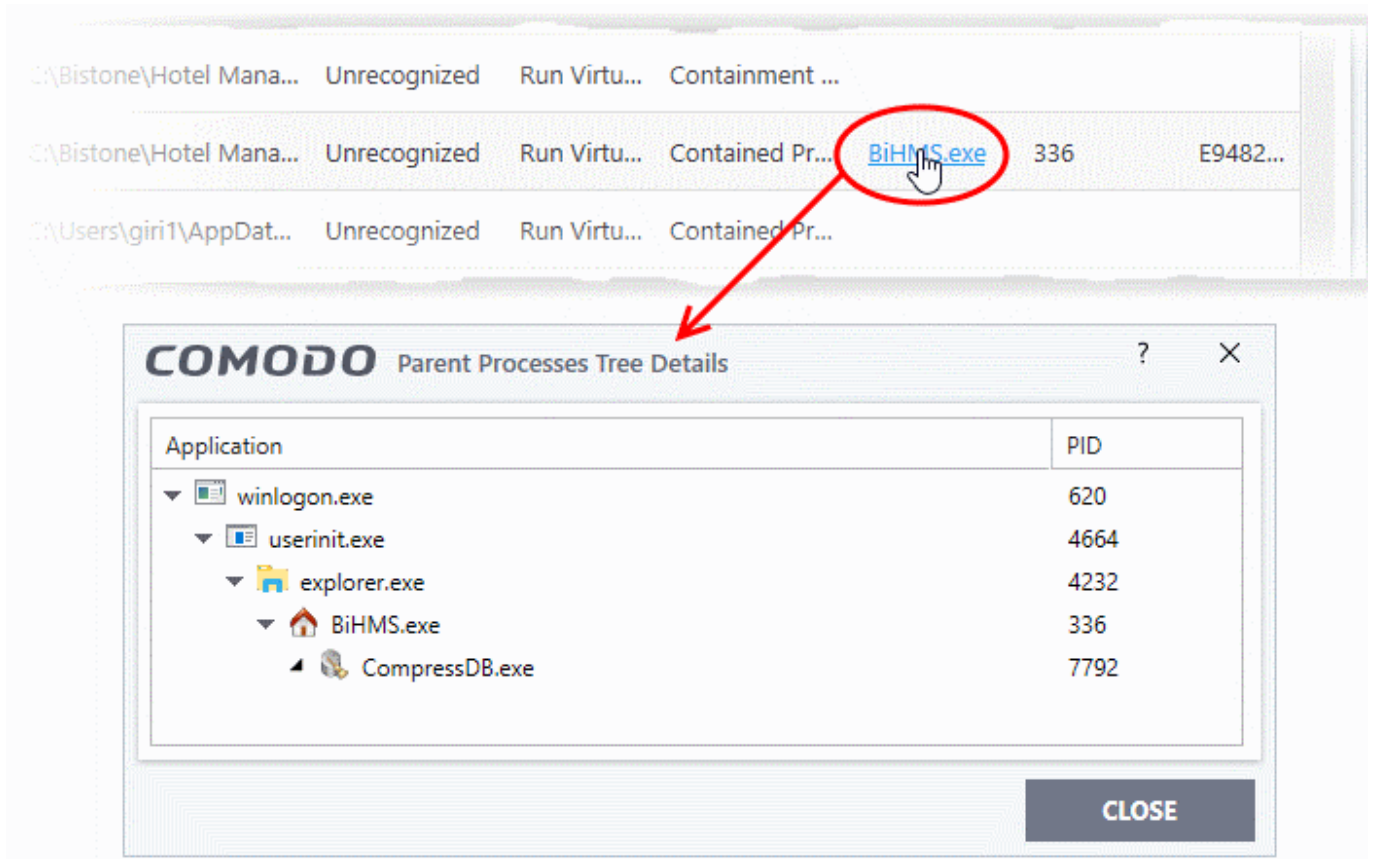
Date & Time	Application	Rating	Action	Contained by	Alert	Parent Pr...	Parent Pr...	Parent Pr...
5/31/2019 12:23...	C:\Program Files\Wind...	Trusted	Ignored	Containment ...				
5/31/2019 12:23...	C:\Program Files\Wind...	Trusted	Ignored	Containment ...		<a href="#">svchost.exe</a>	752	C02EC...
5/31/2019 12:19...	C:\Program Files (x86)\...	Trusted	Run Virtu...	Containment ...		<a href="#">cmdvirth.exe</a>	6576	54322...
5/31/2019 12:19...	C:\Windows\System32...	Trusted	Run Virtu...	Containment ...		<a href="#">cmdvirth.exe</a>	6576	54322...
5/31/2019 12:19...	C:\Windows\System32...	Trusted	Run Virtu...	Containment ...		<a href="#">cmdvirth.exe</a>	6576	54322...
5/31/2019 12:19...	C:\Windows\System32...	Trusted	Run Virtu...	Containment ...		<a href="#">cmdvirth.exe</a>	6576	54322...
5/31/2019 12:19...	C:\Windows\System32...	Trusted	Run Virtu...	Containment ...		<a href="#">cmdvirth.exe</a>	6576	54322...
5/31/2019 12:19...	C:\Bistone\Hotel Mana...	Unrecognized	Run Virtu...	Containment ...		<a href="#">explorer.exe</a>	4048	8B1EA...
5/31/2019 12:19...	C:\Program Files\COM...	Trusted	Run Virtu...	Containment ...		<a href="#">services.exe</a>	604	3848E...

CLOSE



The log viewer shows a list of containment events on the endpoints.

- **Date & Time** - When the event occurred.
- **Application** - The installation path of the application that was run in the container.
- **Rating** - The reputation of the contained application.
- **Action** - How the application was handled by CCS. This is also the restriction level imposed on the application by the container.
- **Contained by** – The CCS service, policy or user that placed the application in the container.
- **Alert** - Click 'Related Alert' to view the notification generated by the event.
  - These alerts are only shown to users if 'Do not show privilege elevation alerts' is disabled in 'Settings' > 'Containment' > 'Containment Settings'.
- **Parent Process** - The program which spawned the contained process.
  - Click the name of the parent process to view the full process tree:



- **Parent Process ID** - The unique identifier that points to the process.
- **Parent process hash** - The SHA1 hash value of the program which spawned the contained process.