How to manage programs running in containment on your endpoints

Open Endpoint Manager > Click ‘Security Sub-Systems > ‘Containment’

- The containment interface shows all programs that are running in the container on your managed endpoints.
- From here, you can view file details and apply various actions to the file. Action include change the trust rating of the file, view the Valkyrie analysis of the file, and export the list to .csv.
- This wiki contains background information on the container, explains how files can become contained, and explains the containment interface in Endpoint Manager.

What is the container?

- The container is a secure, virtual environment in which files with an unknown trust rating are run. Unknown files are those which are neither whitelisted as safe, not blacklisted as malware.
- Contained files and applications are not permitted to modify files, user data or other processes on the host machine. This isolation prevents them from infecting the host or stealing user data.
- This process is completely transparent to the endpoint user. The program will continue to run as normal from their point of view.
- You have the option to automatically upload unknown files to Valkyrie, our advanced file analysis service. Valkyrie tests unknown files to a range of tests to establish whether the file is safe or not. It then sends the new trust verdict back to Endpoint Manager.

Why do some files run in the container?

An application could run inside the container because:

- It was auto-contained by a rule in the configuration profile applied to the endpoint. See this wiki if you want to learn about containment rules in a profile.
- It was auto-contained by a local rule in Comodo Client Security (CCS) on the endpoint. See this wiki if you want to learn about containment rules in CCS.

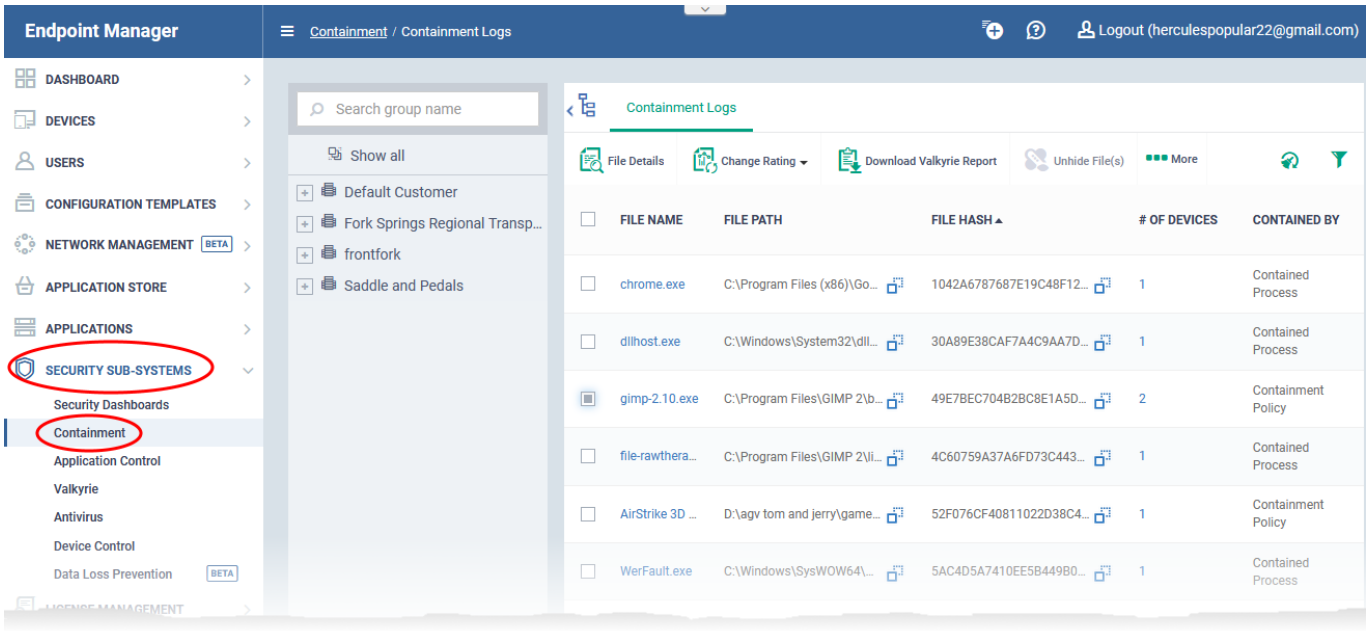
- The endpoint user ran the program inside the container on a 'one-off' basis. This can be done by right-clicking on the file then selecting ‘Run in Comodo container’.

Overview of the containment area

- Click 'Security Sub-Systems' > 'Containment'
  - Click a company or a group to view programs run inside container on their devices

    Or

  - Select 'Show All' to view programs contained on every device in EM



Note: The companies and groups available for selection in the middle pane depend on the Access Scope rights assigned to the role of the currently logged-in administrator. See this wiki to read more on assignment of company access to roles.

The column headers are as follows:

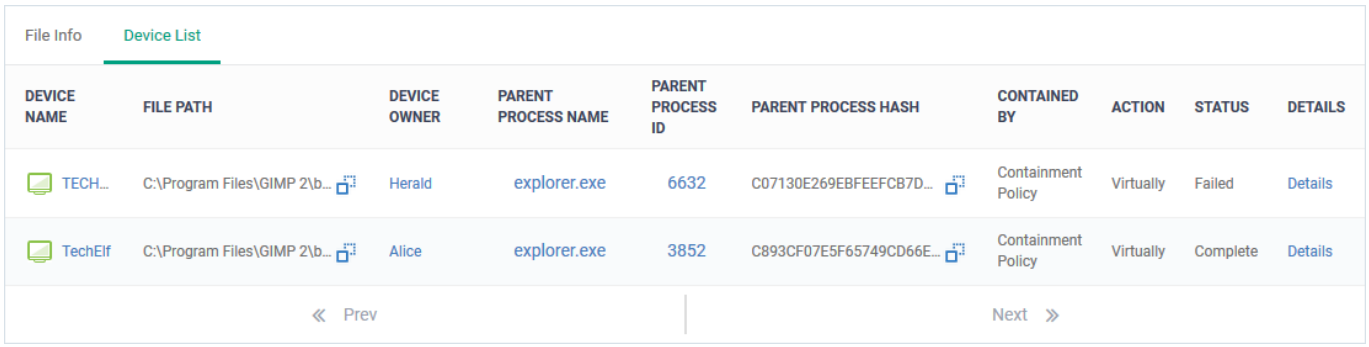
File Name - The executable is running in the container. Click the file name to view its details.

File Path - The location of the contained file on the local endpoint.

File Hash - The SHA-1 hash value of the file. Each hash uniquely identifies a specific file, even if the filename changes.

# of Devices - The quantity of endpoints on which the item is contained.

- Click the number to view a list of the affected endpoints:



Click ‘Details’ in a row to see the list of events generated by the file on the endpoint. See this wiki to read more about viewing security events.

Contained by - The reason the file was contained.

Parent Process Name - The program or service that launched the contained application.

Action - The permission level at which the file was run in the container, or the action that was taken upon it. The possible values are:

- **Restricted** - The file was run in the container but had some limited access to operating system resources.
- **Virtually** - The file was completely isolated from the operating system and files on the computer.
- **Blocked** - The file was not allowed to run at all.
- **Ignored** - The file was allowed to run outside the container without any restrictions.
- **Unknown** - The level of containment could not be determined.

Status - The execution state of the file inside the container. The possible values are:

- **Running** - The file is currently active on the endpoint
- **Complete** - The file has finished its runtime cycle
- **Failed** - The file could not execute in the container

Comodo Rating / Admin Rating - The trust rating of the file as set by Comodo and the admin respectively. Files can be rated as trusted, malicious or unrecognized.

- See this wiki to learn how this rating system works
- See this wiki to learn how to configure the rating system

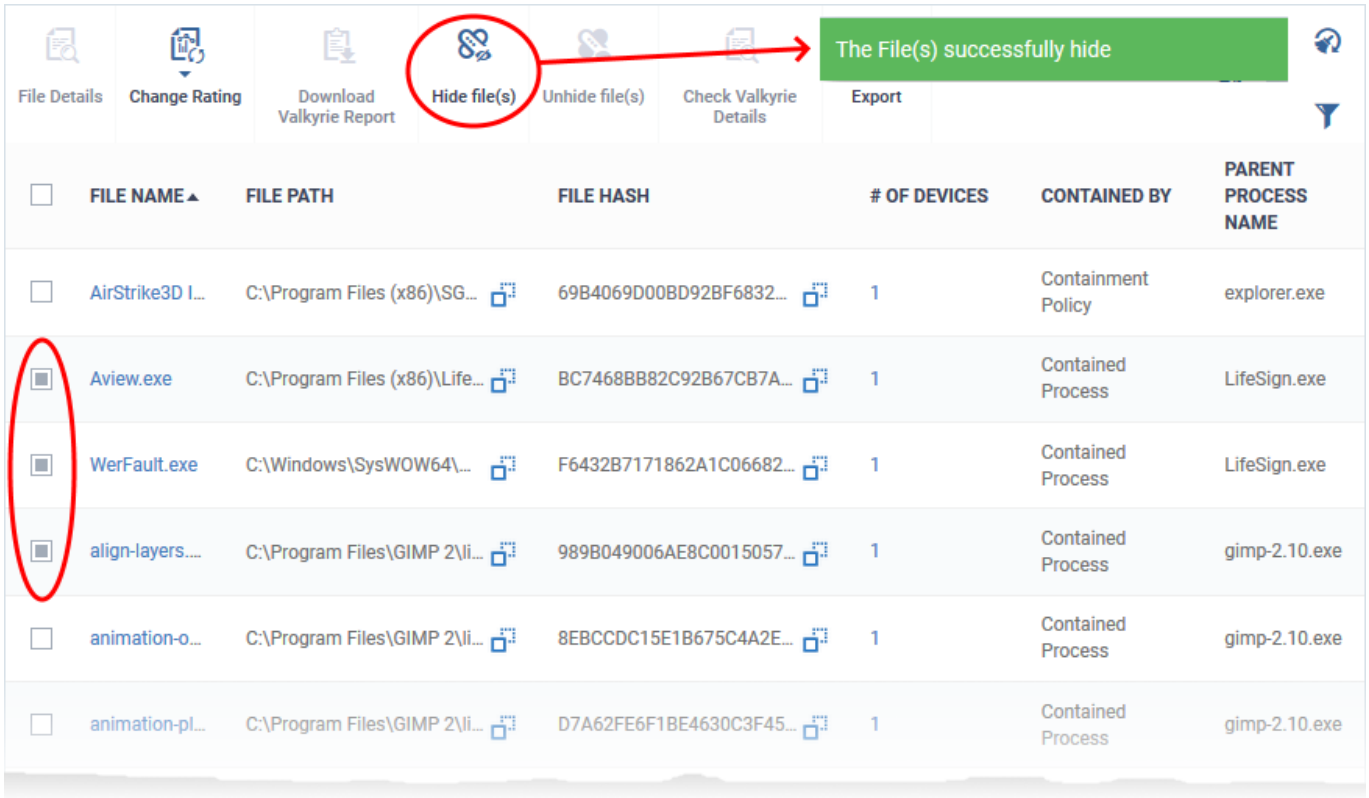
Date Contained - Date and time the file ran in the container.

Hide / unhide the file records

You can conceal file records that you do not want to see in the list. This is useful, if the list contains records of many child processes contained by a parent application run inside the container. You can restore hidden files to the list at anytime.

Hide files from the Containment interface

- Click 'Security Sub-Systems' > 'Containment'
- Select the files you want to hide from the list
- Click 'Hide file(s)'

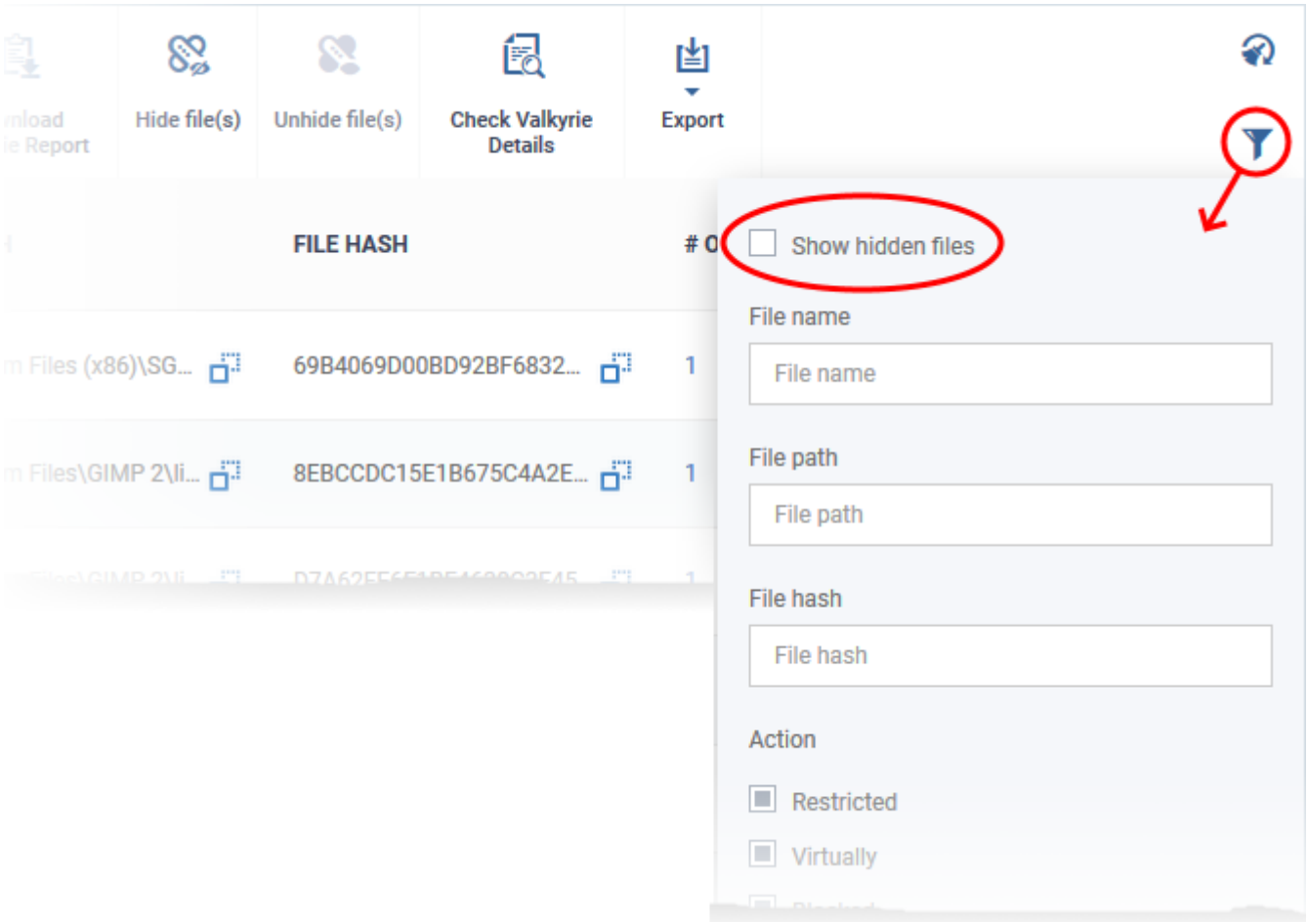


The files are removed from the list. You can restore them at anytime.

- You cannot take any actions like changing file rating on hidden files
- Hidden files are not included in the report of contained files generated from the 'Containment' interface

Restore hidden files

- Click 'Security Sub-Systems' > 'Containment'
- Click the funnel icon
- Select 'Show hidden files' and click 'Apply'



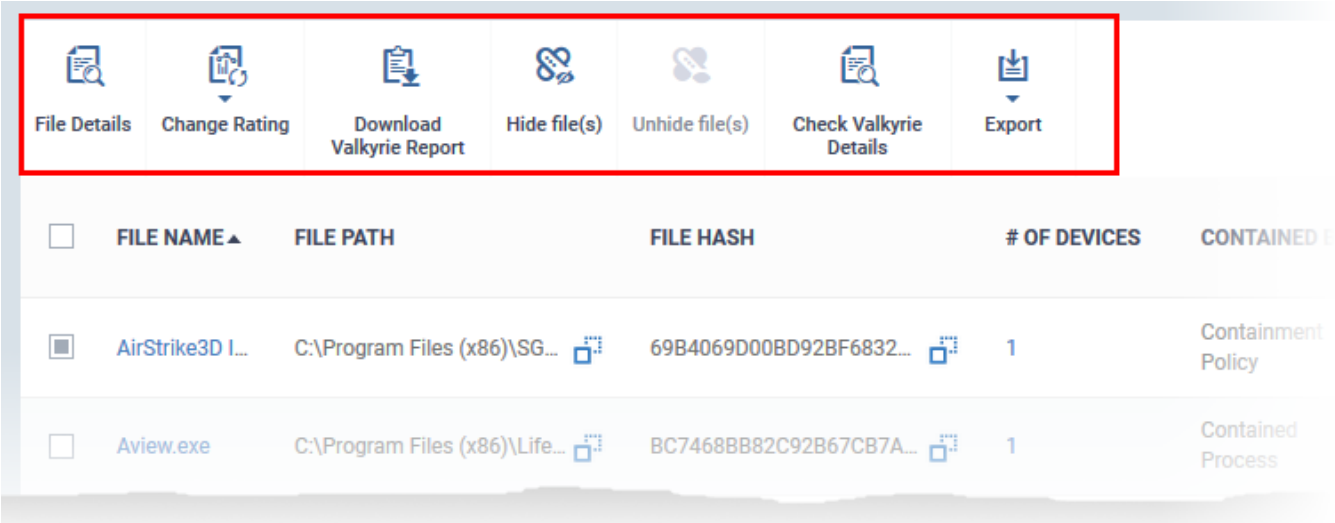
The hidden files are shown on the list with gray background:

- Select the files to be restored and click 'Unhide file(s)'

The files are restored to the list.

Take actions on contained files

The controls above the list allow you to take various actions on contained files:



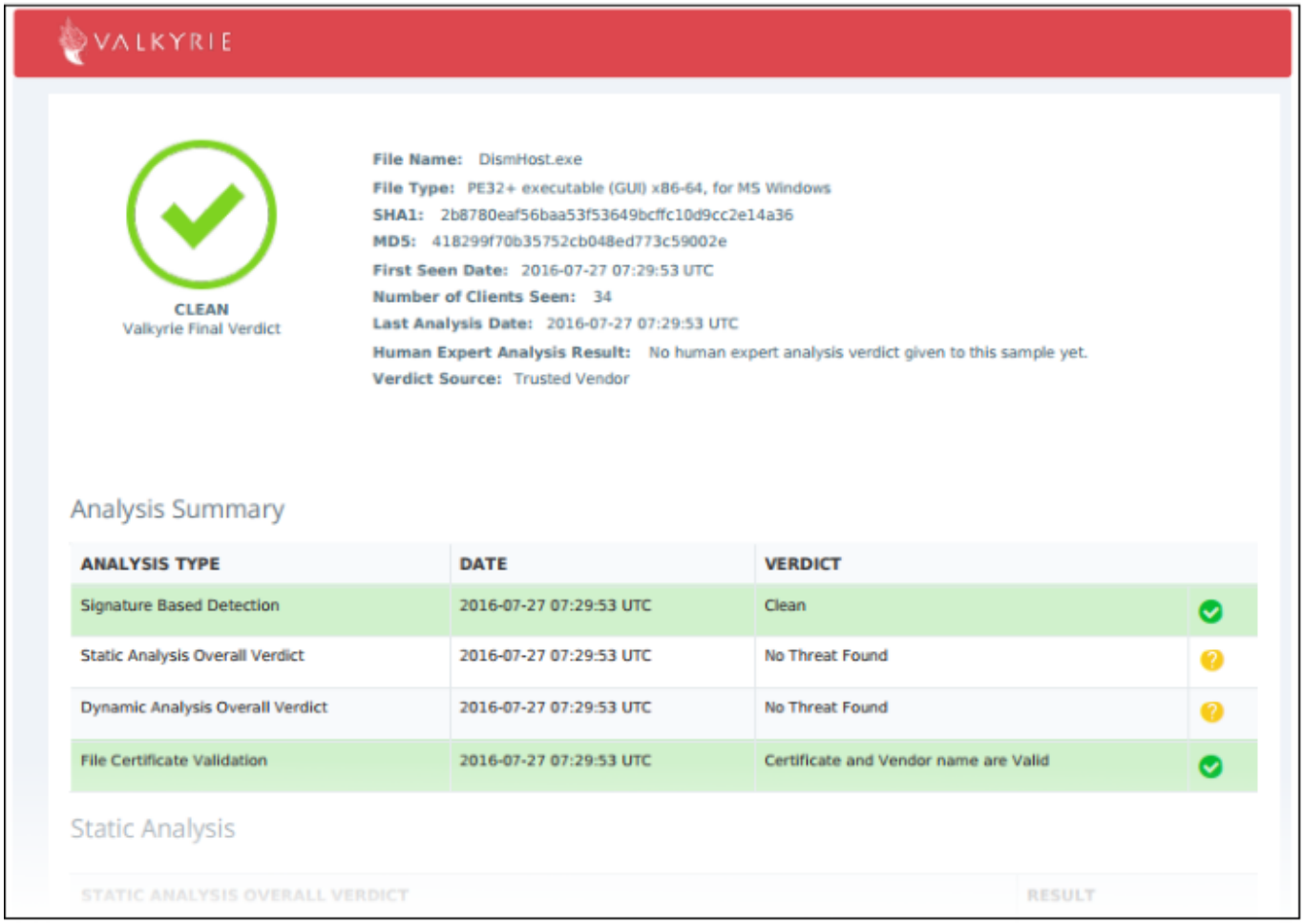
File Details -Opens the file and device information screen as explained above

Change rating – Allows you to rate contained files as unrecognized, trusted or malicious. Please be confident the file is safe before marking a file as trusted. Any new file ratings will be sent to endpoints during the next sync.

- See this wiki to learn how the rating system works
- See this wiki to learn how to configure the rating system

Export - Export the list of contained files to a .csv file. The exported file can be viewed at 'Dashboard' > 'Reports'.

Download Valkyrie report - Valkyrie is Comodo's advanced file analysis and trust-verdict system. Each pdf report contains an in-depth breakdown on the activity an unknown file, along with an overall verdict on its trustworthiness.



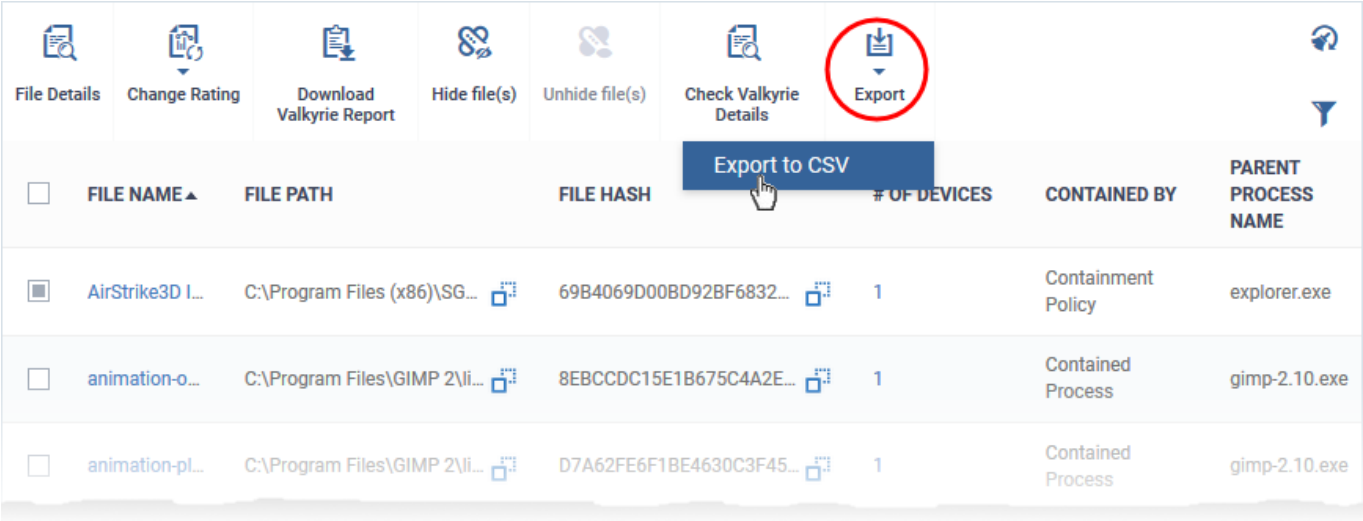
You can also download and view the report at https://valkyrie.comodo.com/ after signing into your Valkyrie account.

Check Valkyrie details - View Valkyrie analysis of the contained file at https://valkyrie.comodo.com

See https://help.comodo.com/topic-397-1-773-9563-Introduction-to-Comodo-Valkyrie.html for help to use the Valkyrie online portal.

Generate a report of contained files

- Click 'Security Sub-Systems' > 'Containment'
- Click 'Export' > 'Export to CSV'



- The CSV file is available in 'Dashboard' > 'Reports'
- See this wiki page if you need help to download the report