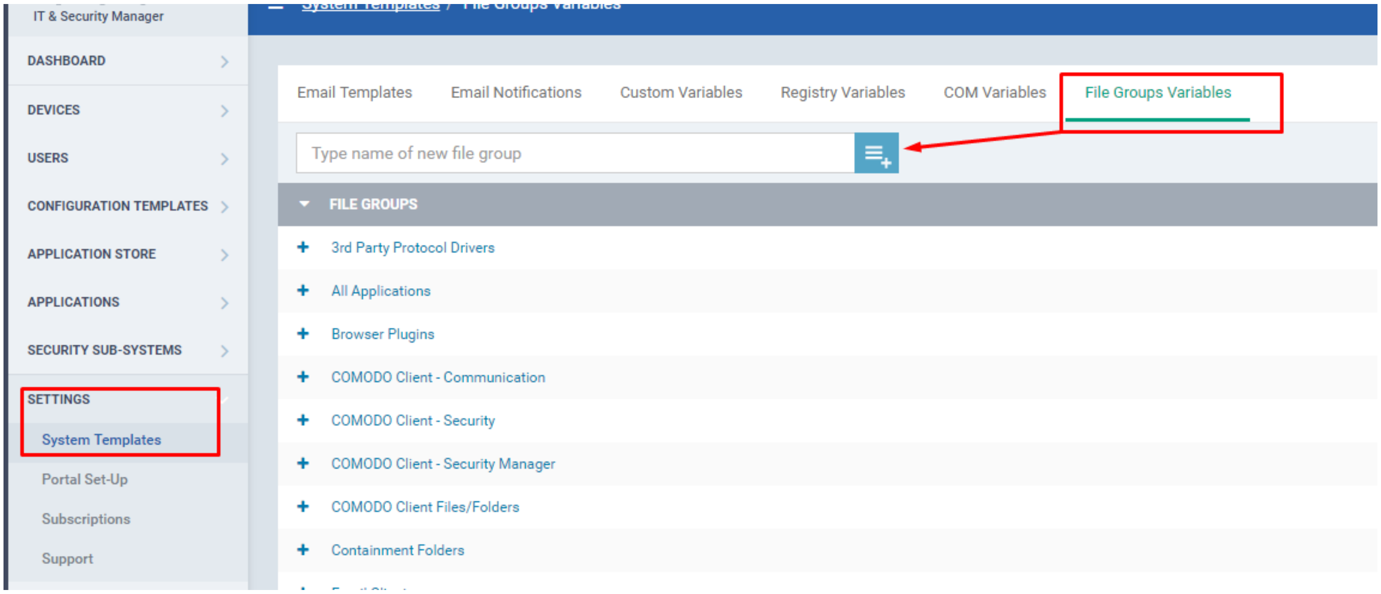
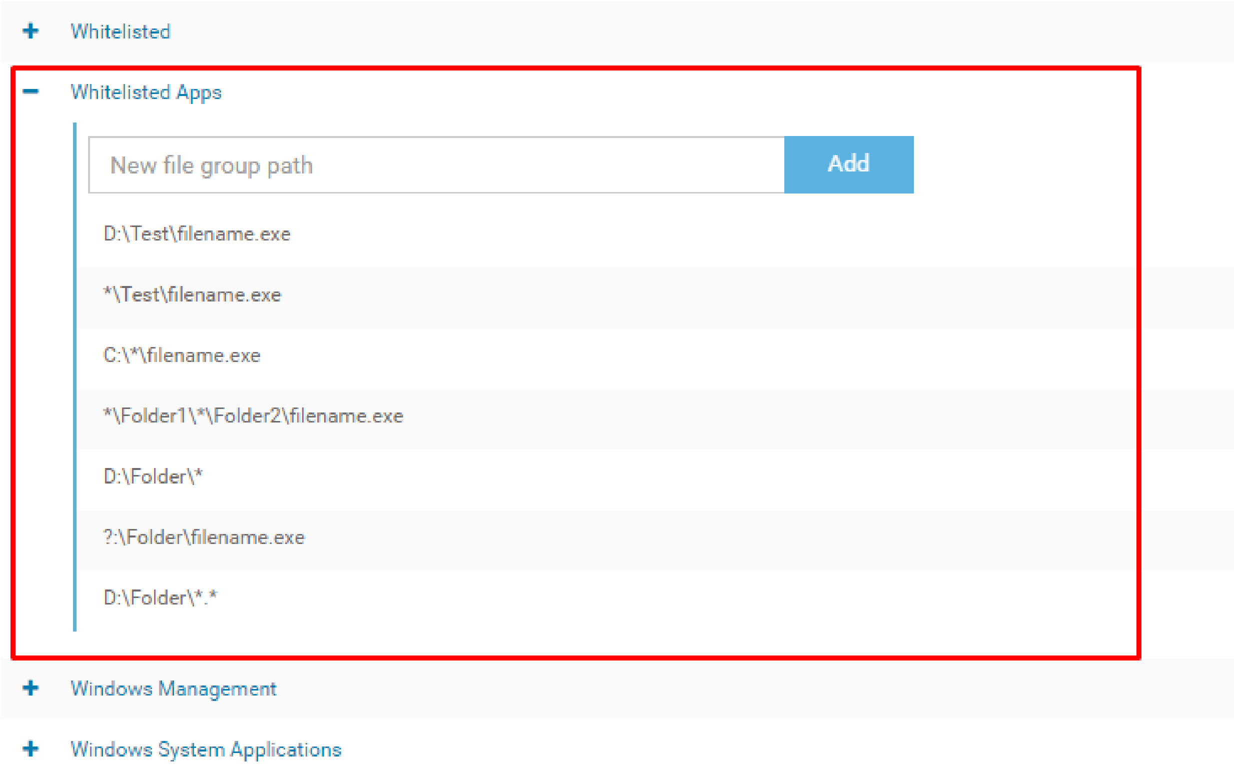
ITSM white-listing by path

1. Go to "Settings > System Templates > File Groups Variables" and create a new file group:



2. Expand the previously created group and add the required paths (you can use wildcards). Please decide with caution which paths you add to the file groups that you are going to white-list as these will be ignored by the correspondent scanning engines.



D:\Test\filename.exe

*\Test\filename.exe

C:\*\filename.exe

\Folder1\Folder2\filename.exe

D:\Folder\*

?:\Folder\filename.exe

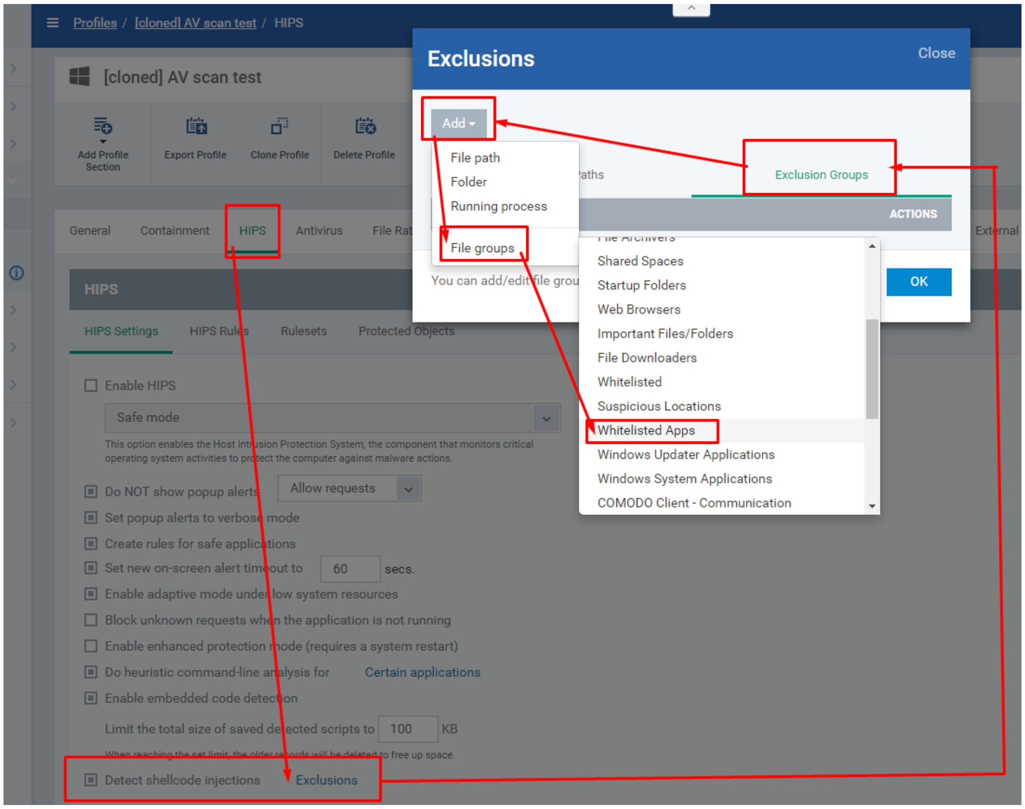
D:\Folder\*.*

Wildcards that can be used:

?:\ - this substitutes any disk drives
*\example.exe - This substitutes any folder path. It will be interpreted as all instances of example.exe regardless of the path.
*\ - This substitutes a portion in a file path that may change depending on the username for example C:\Users\*\Roaming\Microsoft\Windows
C:\random* - Will match any files in folders with names starting with "random", for example: C:\random, C:\randomname, C\randomfolder, C:\randomsomething etc. This is usually used as C:\Program Files*\ to exclude both Program Files\ and Program Files (x86) on 32 bit and 64 bit machines.
C:\folder\*.* - Will match all files in the current directory, but none in sub-directories.
C:\folder\* - Will match all files in the current directory and sub-directories.
*.exe - Will match any application with exe extension.

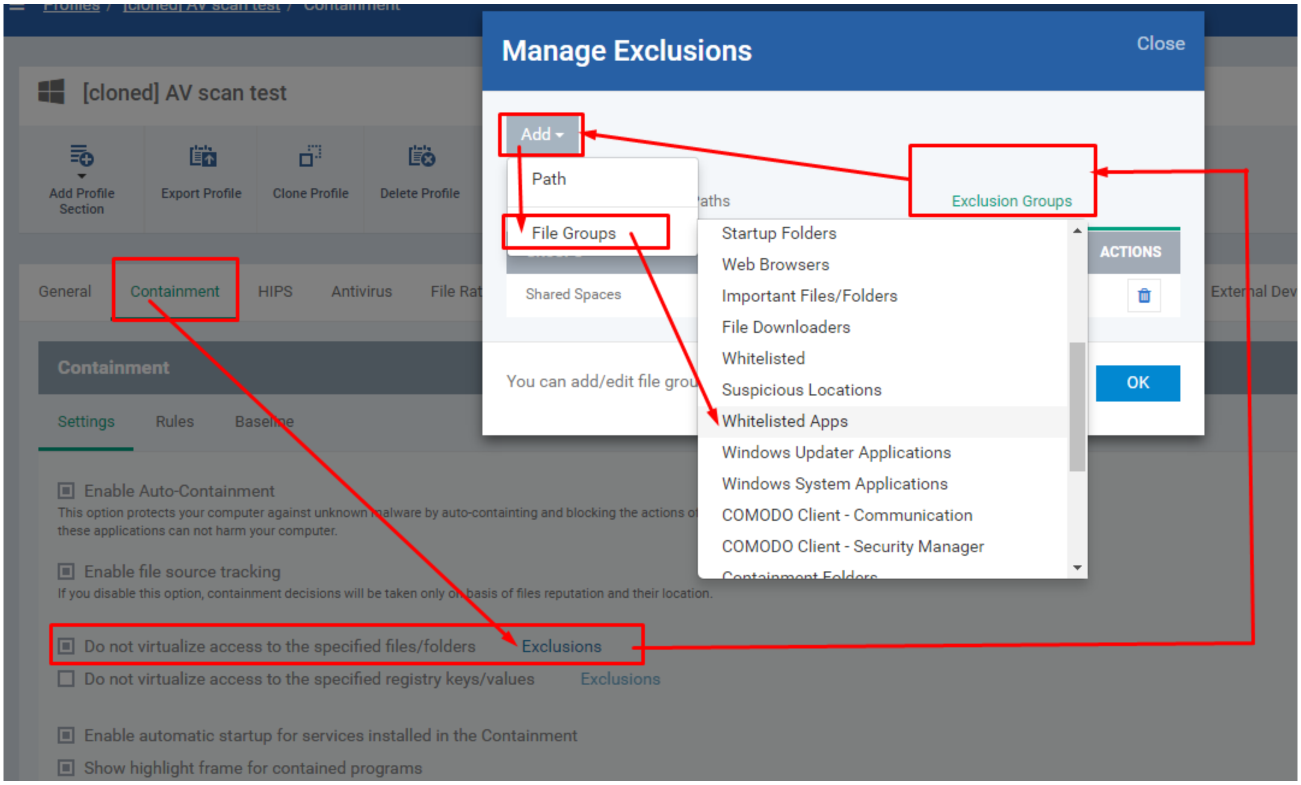
3. Edit the profile you want to use and add the file group above in the following sections:

a.) HIPS > Detect shellcode injections > Exclusions



□ Enable HIPS
Safe mode
This option enables the Host Intrusion Protection System, the component that monitors critical operating system activities to protect the computer against malware actions.
☑ Do NOT show popup alerts Allow requests
☑ Set popup alerts to verbose mode
☑ Create rules for safe applications
☑ Set new on-screen alert timeout to 60 secs.
☑ Enable adaptive mode under low system resources
□ Block unknown requests when the application is not running
□ Enable enhanced protection mode (requires a system restart)
☑ Do heuristic command-line analysis for Certain applications
☑ Enable embedded code detection
Limit the total size of saved detected scripts to 100 KB
When reaching the set limit, the older records will be deleted to free up space.
☑ Detect shellcode injections Exclusions

b.) Containment > Do not virtualize access to the specified files/folders > Exclusions



☒ Enable Auto-Containment
This option protects your computer against unknown malware by auto-containting and blocking the actions of these applications can not harm your computer.

☒ Enable file source tracking
If you disable this option, containment decisions will be taken only on basis of files reputation and their location.

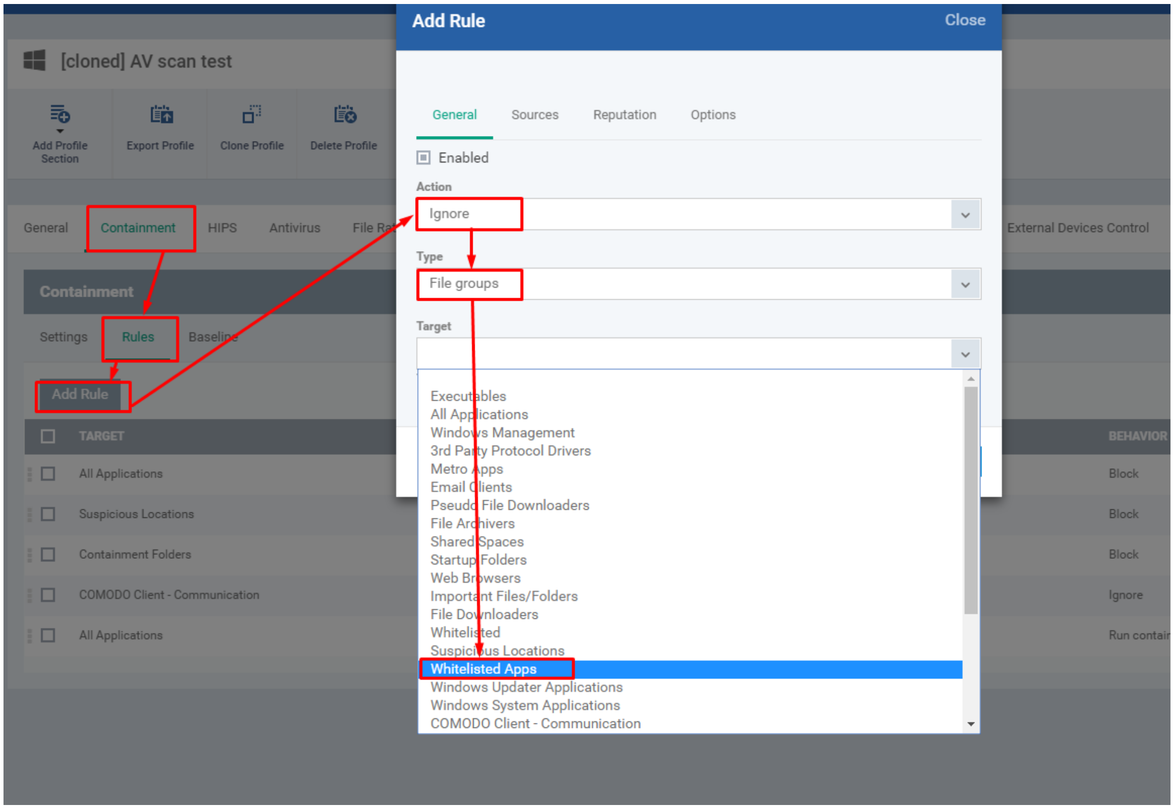
☒ Do not virtualize access to the specified files/folders Exclusions

☐ Do not virtualize access to the specified registry keys/values Exclusions

☒ Enable automatic startup for services installed in the Containment

☒ Show highlight frame for contained programs

c.) Containment > Rules - add a new rule with Action set to Ignore, Type set to File Groups and Target - select the file group. Once the rule has been created drag it to first position in the list.



☒ Enabled

Action: Ignore

Type: File groups

Target:

☐ TARGET	BEHAVIOR
☐ All Applications	Block
☐ Suspicious Locations	Block
☐ Containment Folders	Block
☐ COMODO Client - Communication	Ignore
☐ All Applications	Run contair

4. Save the Profile and apply it on the appropriate Devices.