

How to define exclusions for Shellcode Injection Protection in a Windows profile

- A shellcode injection is an attack which exploits software vulnerabilities to give attackers control of a compromised machine.
- For example, shellcode attacks are often used to create buffer-overflows on victim machines.
- By default, Comodo Client Security (CCS) monitors all applications to make sure they do not suffer shellcode attacks.
- However, you may want to omit certain applications from protection for compatibility reasons.
- This tutorial explains how to exclude items from shellcode protection on managed Windows devices.

Process in brief

- Log into Comodo One / Dragon platform
- Click 'Applications' > 'Endpoint Manager'
- Click 'Configuration Templates' > 'Profiles'
- Open the Windows profile applied to your target devices
 - Open the 'HIPS' tab (if the section has been added to the profile)
- OR
- Click 'Add Profile Section' > 'HIPS' (if it hasn't yet been added)
- Click the 'HIPS Settings' tab
- Scroll down to 'Detect shellcode injections' and ensure it is selected
- Click the 'Exclusions' link
- Click the 'Add' button. You can exclude applications by path, folder, running process, or filegroup.
- Click 'Ok' then 'Save' to apply your changes

Process in detail

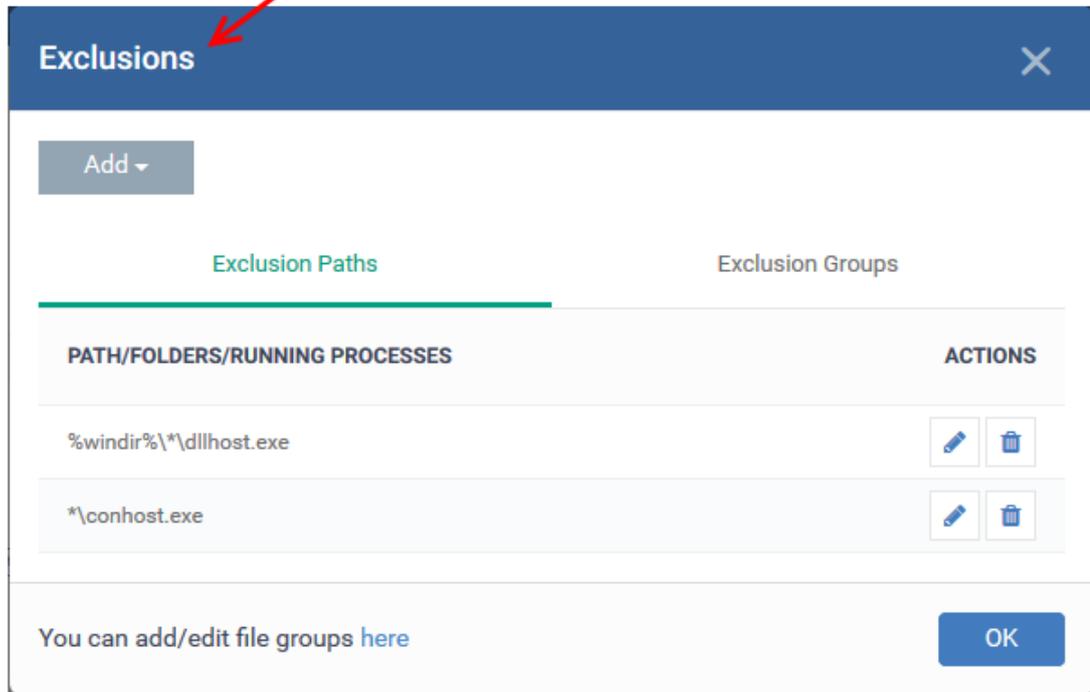
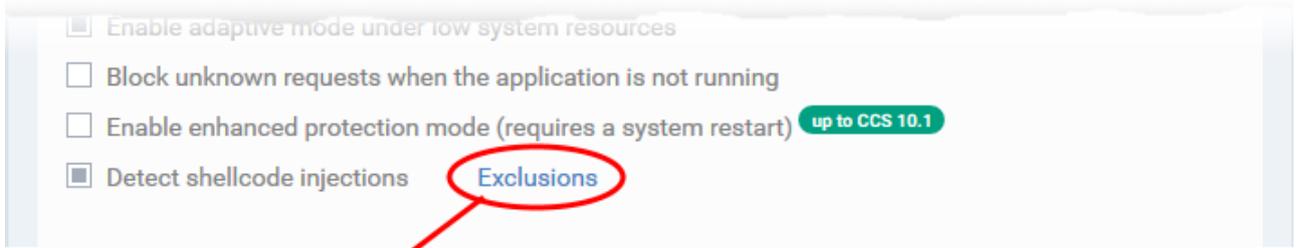
- Login to Comodo One / Dragon platform
- Click 'Applications' > 'Endpoint Manager'
- Click 'Configuration Templates' > 'Profiles'

- Open the Windows profile applied to your target devices
 - Open the 'HIPS' tab (if the section has been added to the profile)
- OR
- Click 'Add Profile Section' > 'HIPS' (if it hasn't yet been added)
- Click the 'HIPS Settings' tab
- Scroll down to 'Detect shellcode injections'

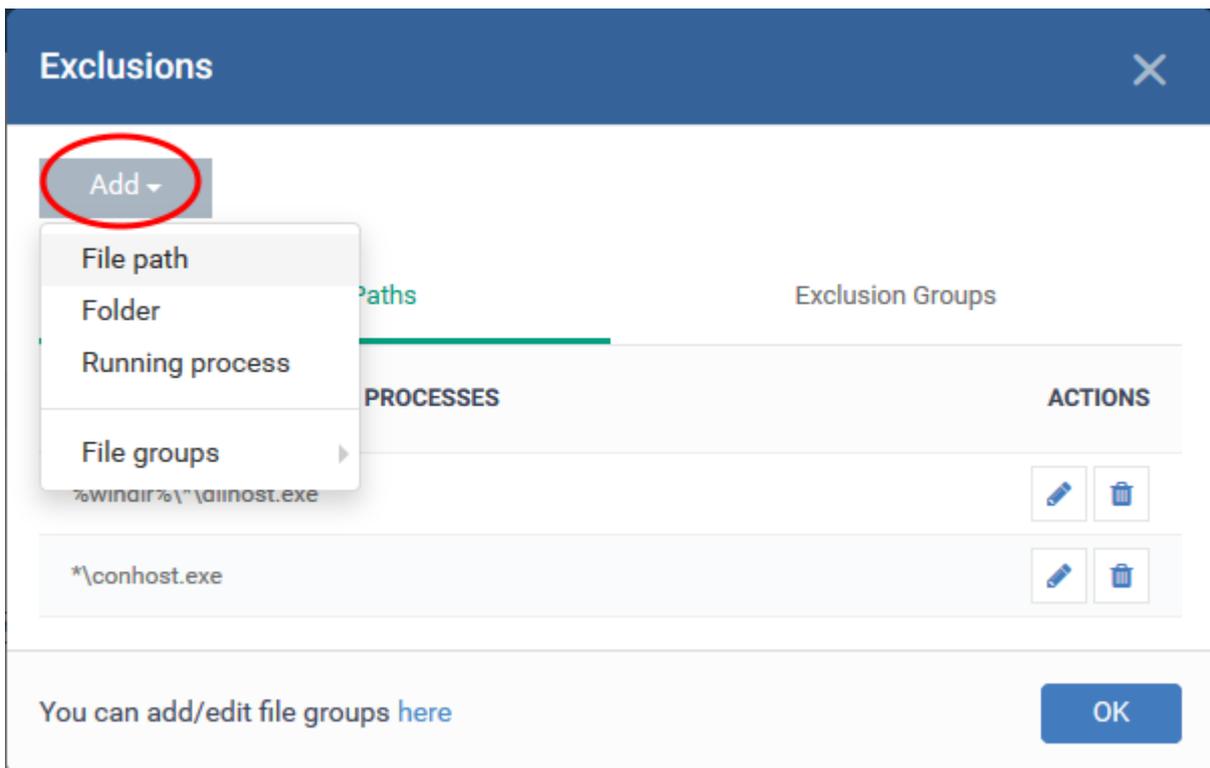
The screenshot shows the Windows Security application interface for a profile named 'Field Workers Laptops'. At the top, there are five action buttons: 'Add Profile Section', 'Export Profile', 'Clone Profile', 'Delete Profile', and 'Make Default'. Below these is a navigation bar with tabs for 'General', 'Antivirus', 'UI Settings', and 'HIPS'. The 'HIPS' tab is selected and circled in red. Underneath, there is a sub-navigation bar with 'HIPS Settings', 'HIPS Rules', 'Rulesets', and 'Protected Objects'. The 'HIPS Settings' sub-tab is active. The main content area shows the following settings:

- Enable HIPS
 - Safe mode (dropdown menu)
 - This option enables the Host Intrusion Protection System, the component that monitors critical operating system activities to protect the computer against malware actions.
- Monitoring settings**
 - Temporarily switch HIPS to training mode CC 6.27+
 - This option switches HIPS to training mode for the selected time period and starts the timer. When the time elapses, HIPS will be automatically switched to the mode set above.
 - Do NOT show popup alerts Allow requests (dropdown menu)
 - 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) up to CCS 10.1
 - Detect shellcode injections Exclusions (This entire row is circled in red)

- Ensure that 'Detect shellcode injections' is enabled, then click the 'Exclusions' link:

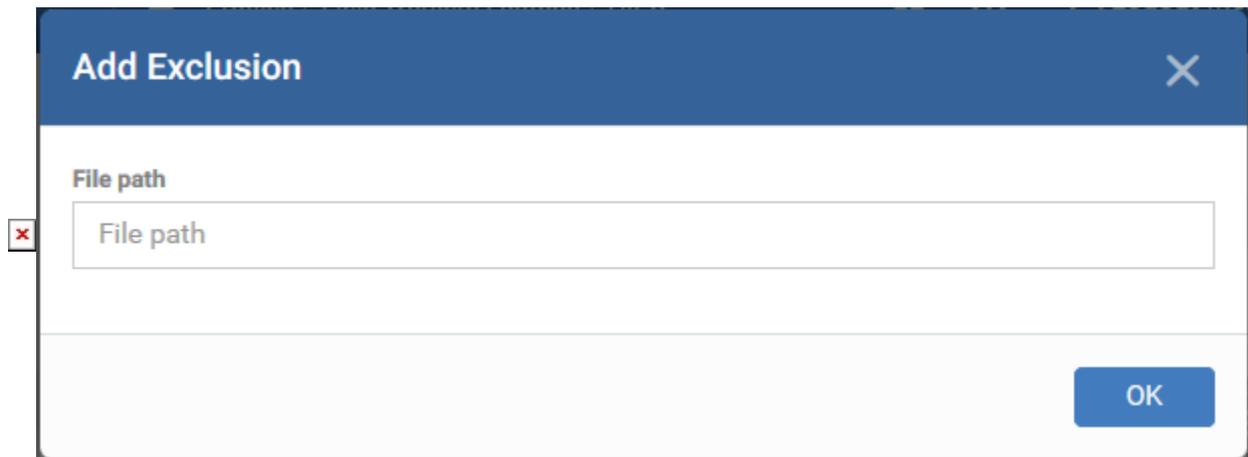


- Click the 'Add' button.



There are four ways you can select the application you want to exclude:

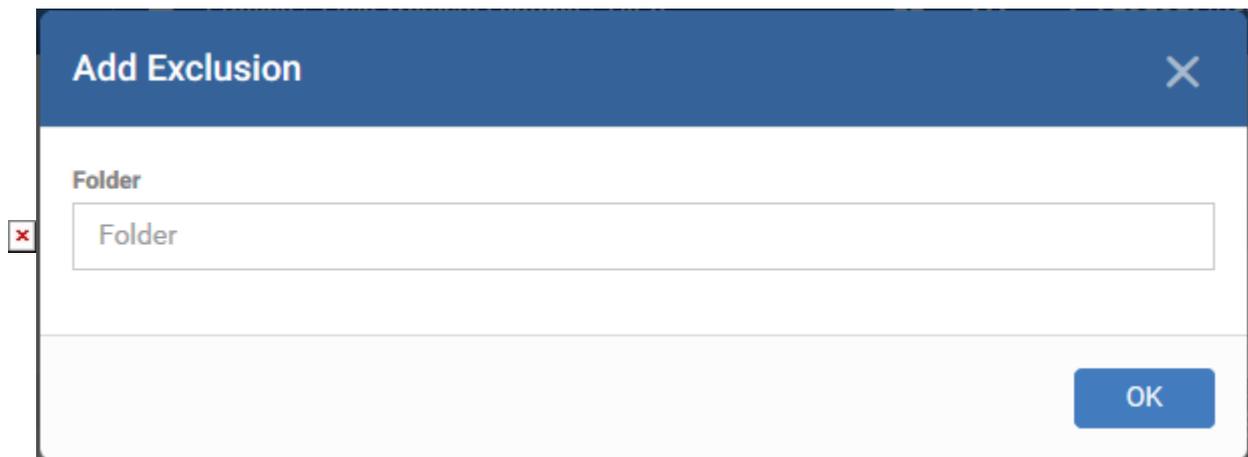
- **File Path** -Location of the file you want to exclude. Provide the file path name and click 'OK'.



The screenshot shows a dialog box titled "Add Exclusion" with a close button (X) in the top right corner. Below the title bar, there is a label "File path" above a text input field containing the placeholder text "File path". A small red 'x' icon is visible to the left of the input field. At the bottom right of the dialog, there is a blue button labeled "OK".

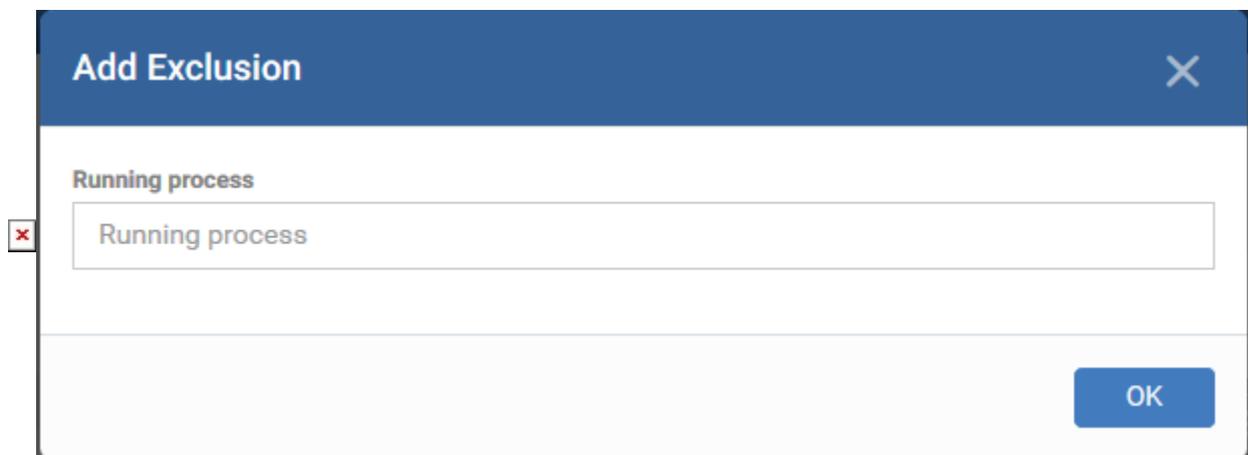
- Repeat the process to add more applications

- **Folder** - Exclude all applications in a specific folder. Enter the folder path and click 'OK':



The screenshot shows a dialog box titled "Add Exclusion" with a close button (X) in the top right corner. Below the title bar, there is a label "Folder" above a text input field containing the placeholder text "Folder". A small red 'x' icon is visible to the left of the input field. At the bottom right of the dialog, there is a blue button labeled "OK".

- **Running process** – Exclude an application by selecting its running process. The parent application of the process is added to exclusions:

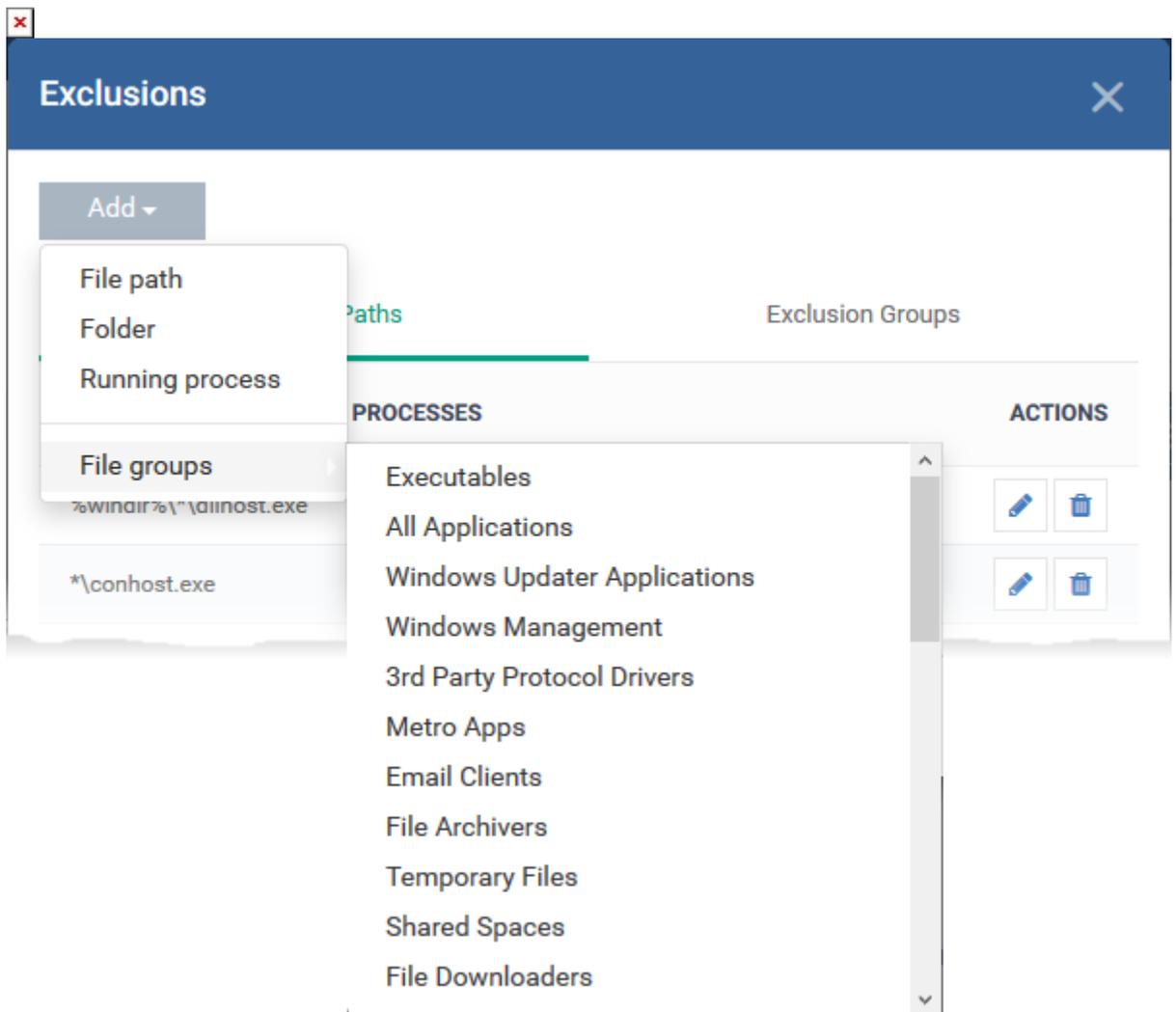


The screenshot shows a dialog box titled "Add Exclusion" with a close button (X) in the top right corner. Below the title bar, there is a label "Running process" above a text input field containing the placeholder text "Running process". A small red 'x' icon is visible to the left of the input field. At the bottom right of the dialog, there is a blue button labeled "OK".

Enter the path of the process and click 'OK'

- **File Groups** - Exclude a specific file category.

- File groups are collections of one or more files. The files in each group usually have similar functionality and characteristics.
- Example file groups included 'Executables', 'Important Files/Folders', 'Email Clients', and 'Browser Plugins'.
- Click 'Settings' > 'System Templates' > 'File Group Variables' to view and create filegroups



- Select the group you want to exclude then click 'OK'.
- Click 'Save' to apply your changes.