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

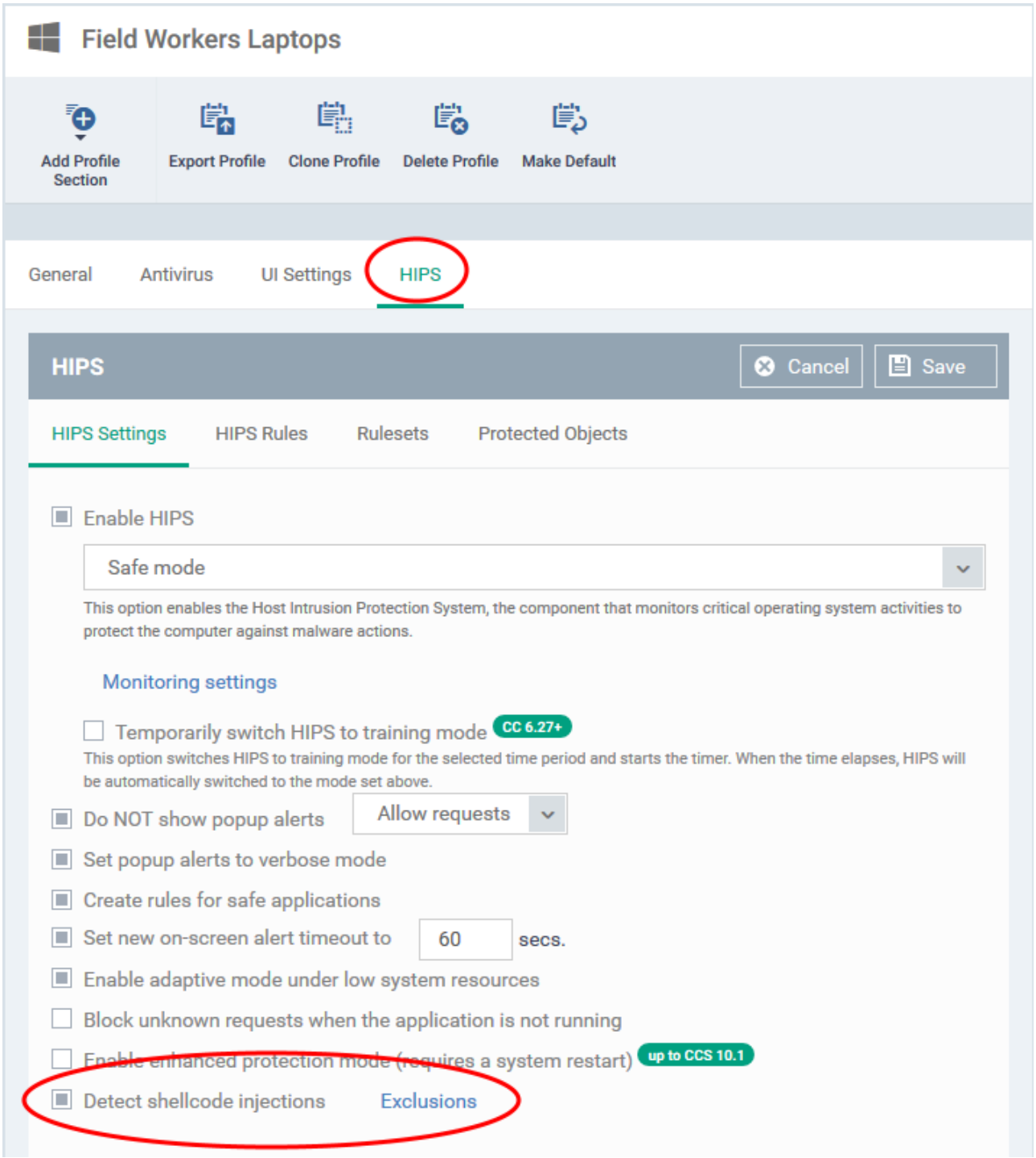
Process in detail

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

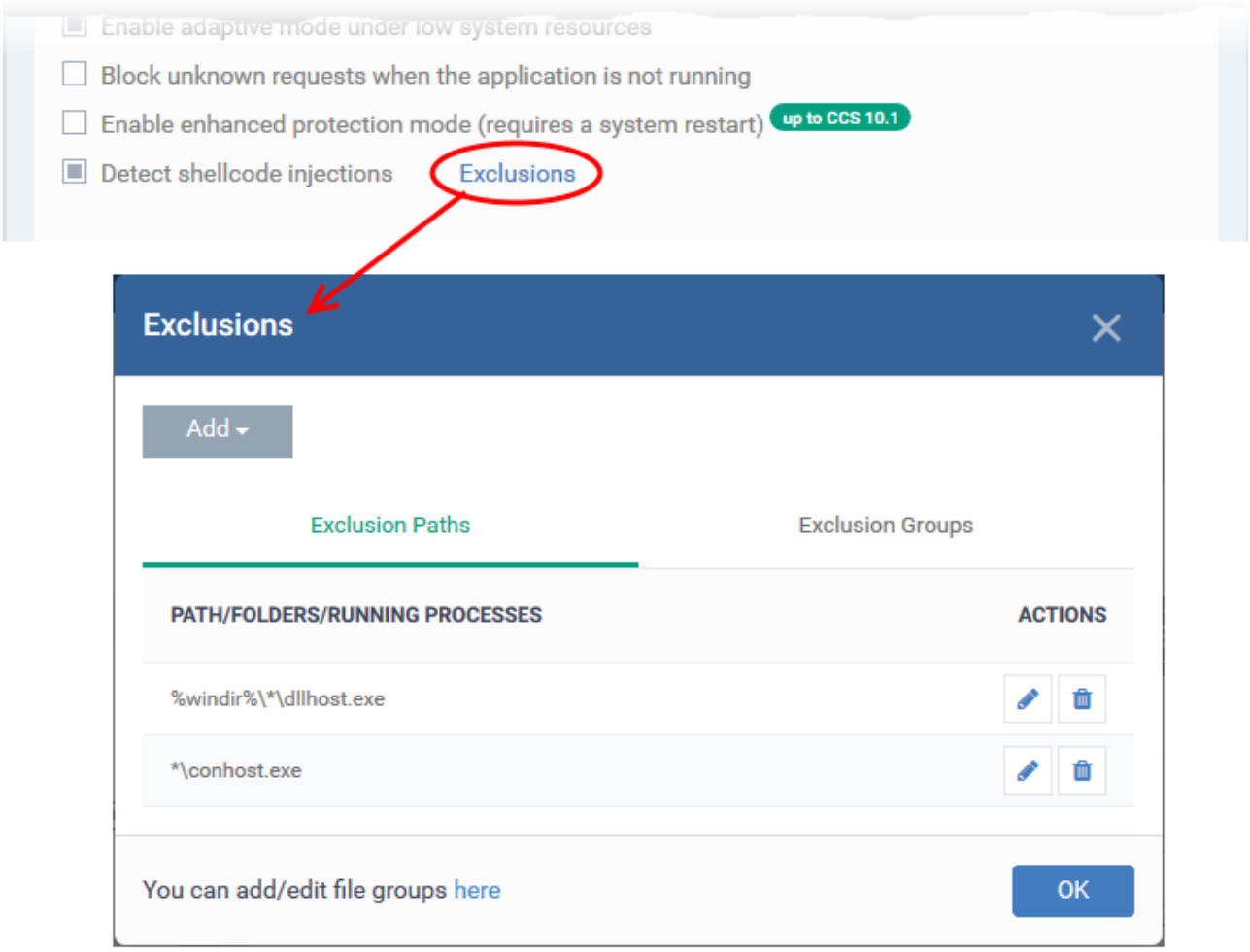
- Open the Windows profile applied to your target devices
    - Open the 'HIPS' tab (if the section has been added to the profile)

      OR

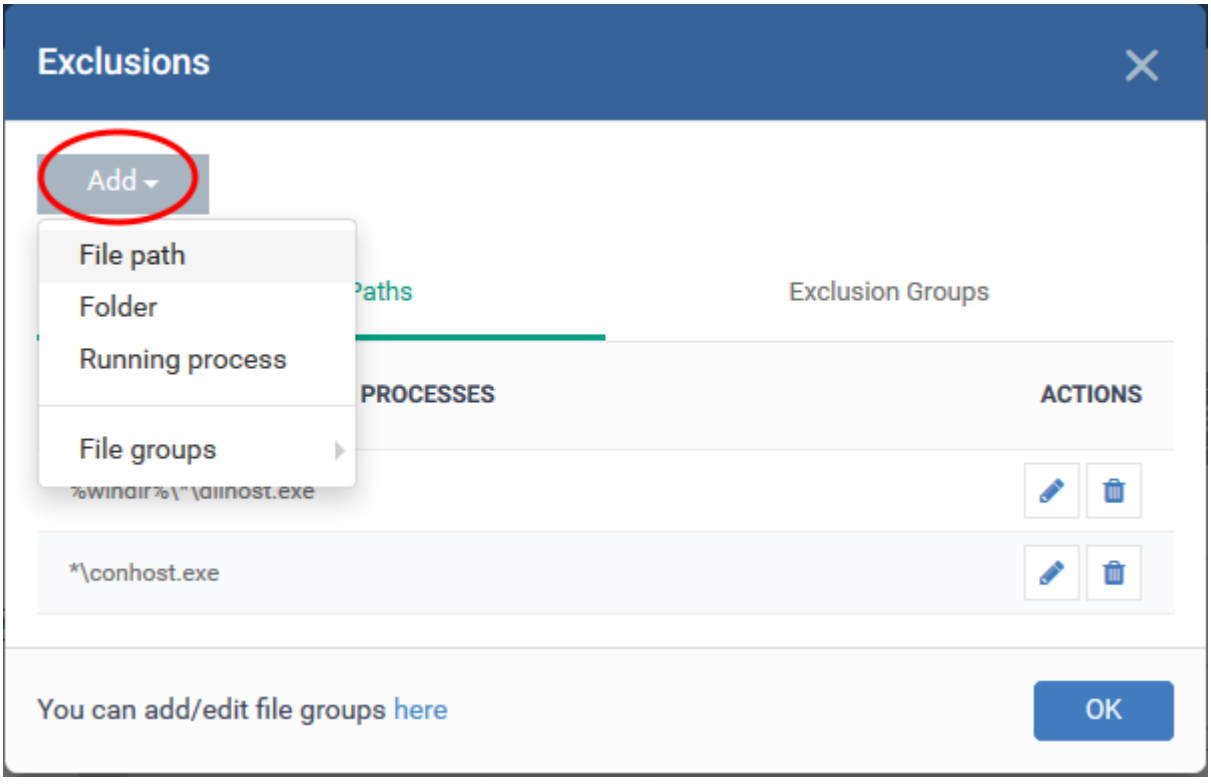
    - Click 'Add Profile Section' > 'HIPS' (if it hasn't yet been added)
- Click the 'HIPS Settings' tab
- Scroll down to 'Detect shellcode injections'



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

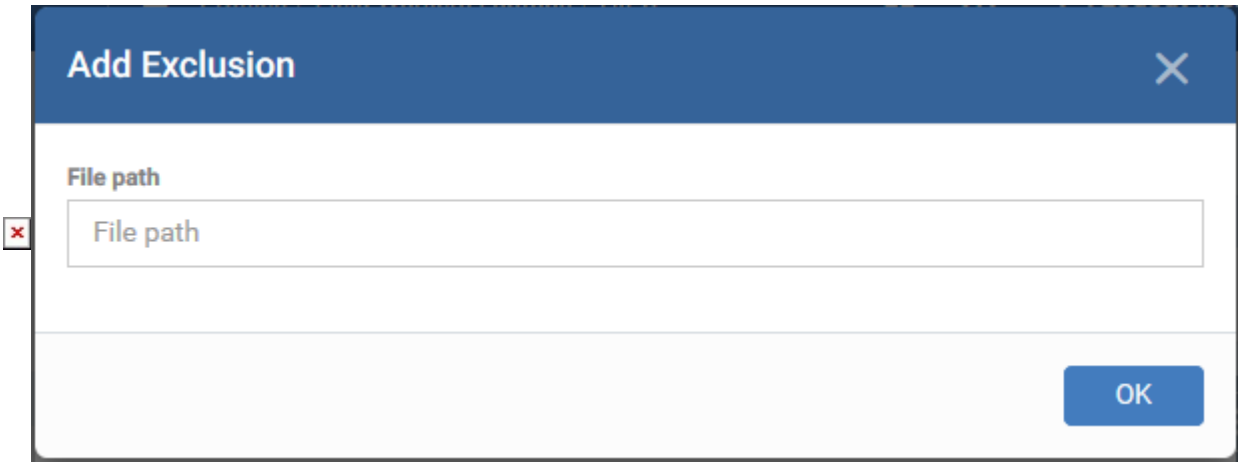


- Click the 'Add' button.



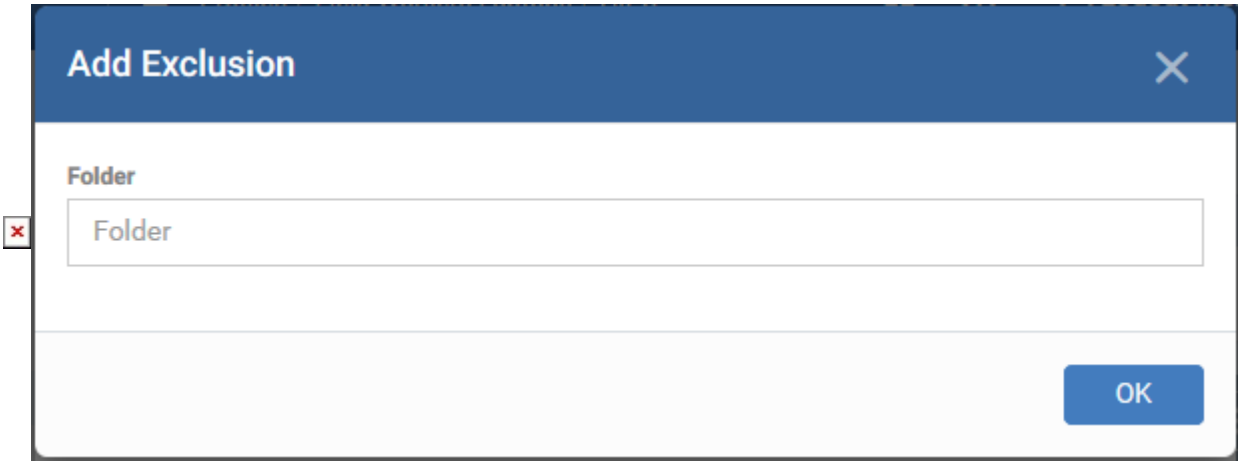
There are four ways you can select the application you want to exclude:

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

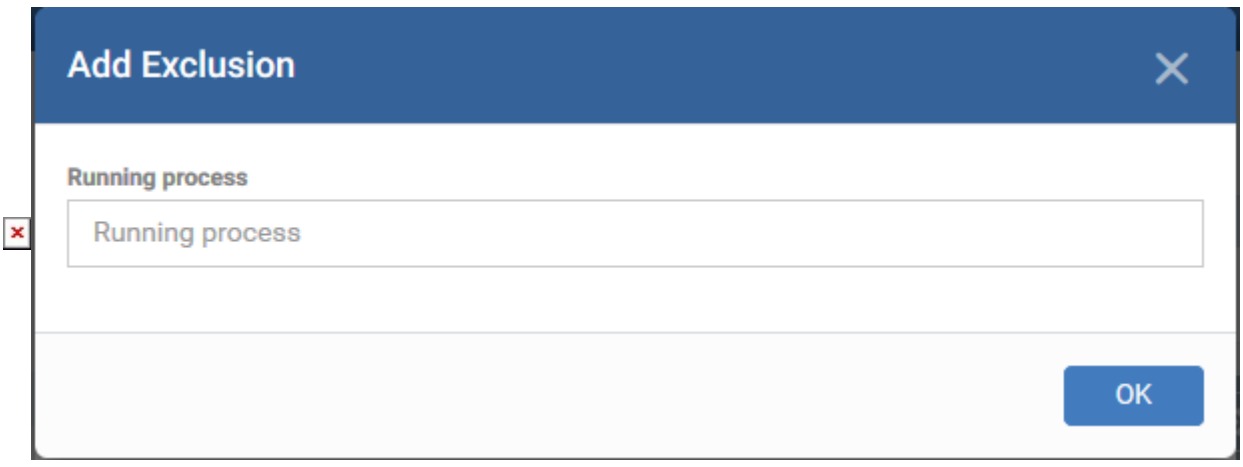


  - Repeat the process to add more applications

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

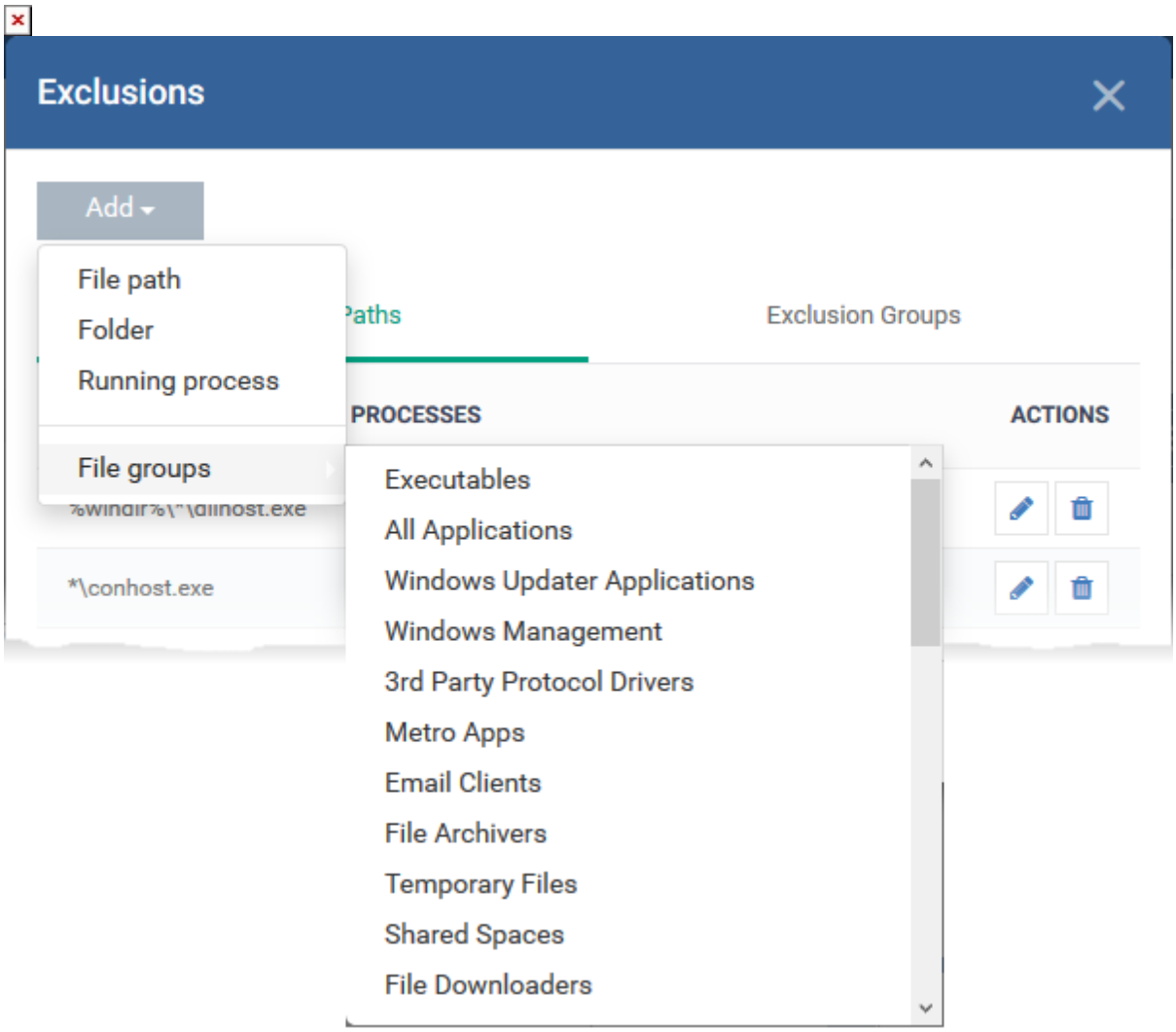


- **Running process** – Exclude an application by selecting its running process. The parent application of the process is added to exclusions:



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.