The ITarian platform is powered by Xcitium's advanced technology for endpoint protection, is an extremely powerful platform with in-depth technologies in its stack. Some applications that have high resource usage, like Data Loss Prevention (DLP) or other applications, when used with Xcitium without proper configuration might cause higher resource usage. This is because Xcitium's powerful technology stack monitors everything for you.

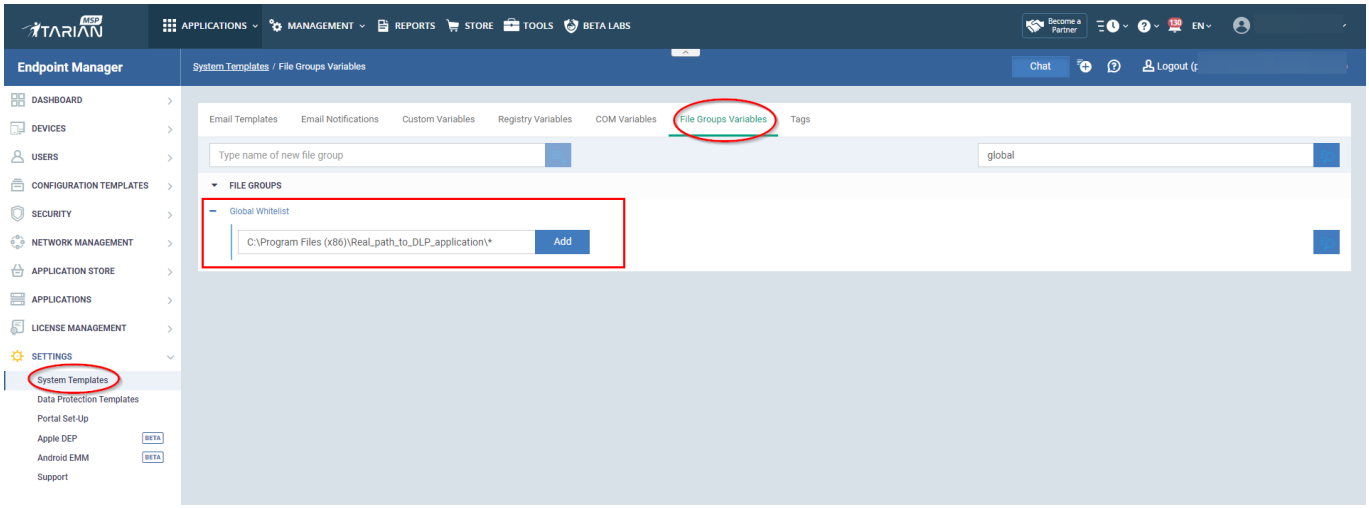
In cases where these applications are recognized as trusted and require exceptions, it is acceptable to whitelist them by following the outlined procedures below, specifically designed for DLP applications.

Note: While these processes are tailored for DLP tools, the same approach can be applied to other types of trusted applications that may require similar whitelisting adjustments.

Adding in a Global Whitelist

We can add the DLP application path in a Global Whitelist by following steps:

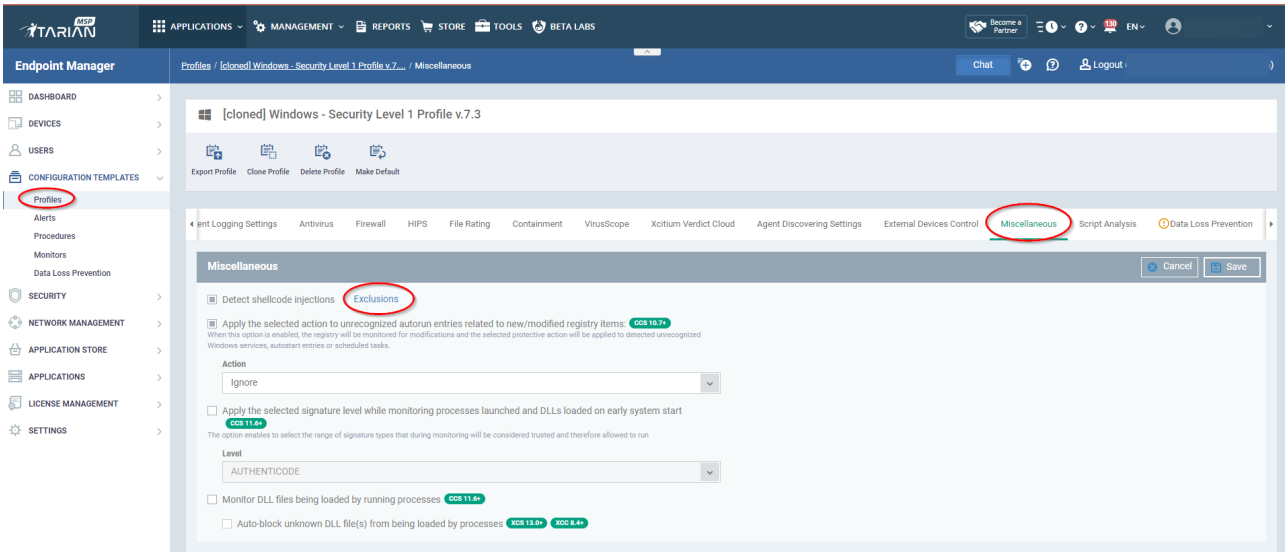
- Login to ITarian
- Click 'Applications' > 'Endpoint Manager'
- Click 'Settings' > 'System Templates'
- Select the 'File Groups Variables' tab
- Click the '+' button at the **Global Whitelist**
- Enter the full path of the DLP application path containing your target files. Click 'Add'
    - To include all files in a folder, place a wildcard '*' character after the folder name,
    - For example - **C:\Program Files (x86)\Real_path_to_DLP_application*** is just an example, and you should place a real path to that DLP application here.



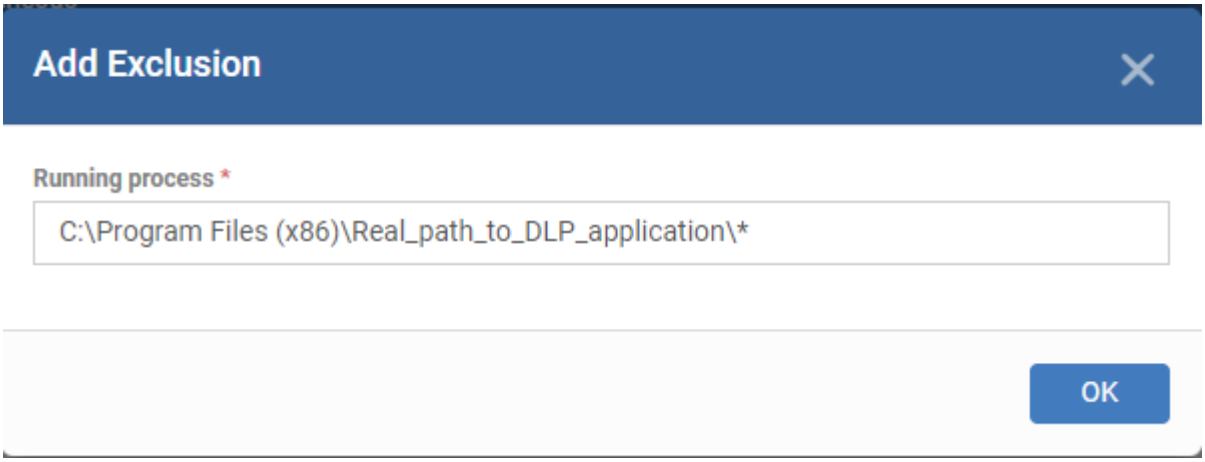
Adding as an exclusion in shellcode injection

We can the DLP application file path as exclusion in Shellcode Injection by following steps:

- Click 'Applications' > 'Endpoint Manager'
- Click 'Configuration Templates' > 'Profiles'
- Select the profile associated with the device where you want to add the exclusion
- Click 'Miscellaneous' and Edit to make the following changes
- Select 'Exclusions' under Detect Shellcode Injections

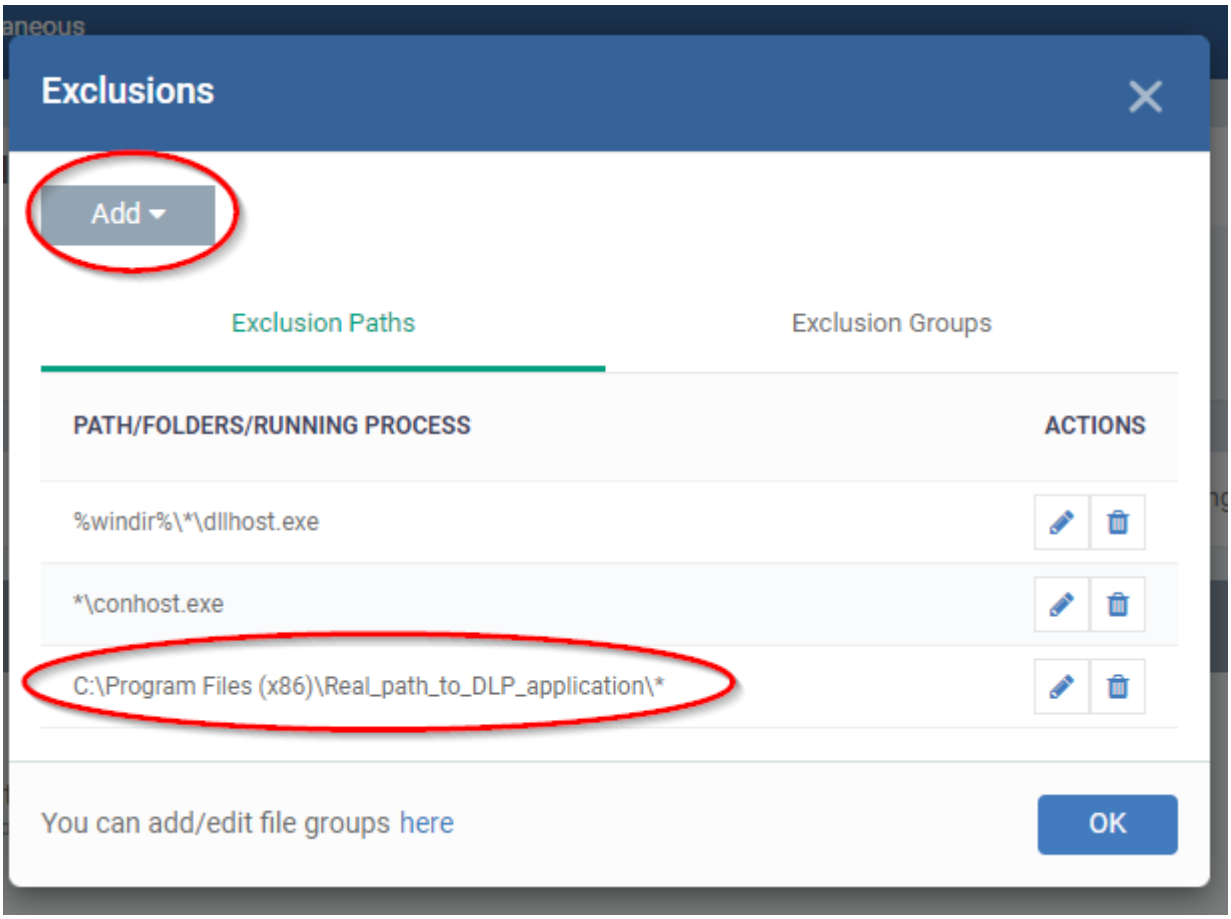


- Click 'Add' > 'Running Process' and provide the actual installation path of the DLP application



  - For example - **C:\Program Files (x86)\Real_path_to_DLP_application*** is just an example, and you should place a real path to that DLP application here.

- Click 'Ok' and 'Save' the changes in profile settings



Adding all XCS paths as exclusion

In the next step, if the DLP application supports exclusions, especially injection exclusions, we can add all XCS paths to exclusions in that DLP application

- C:\Program Files (x86)\COMODO
- C:\Program Files\COMODO\COMODO Internet Security

- C:\ProgramData\Comodo
- C:\Windows\System32\drivers\cesboot.sys
- C:\Windows\System32\drivers\ceserd.sys
- C:\Windows\System32\drivers\cesfw.sys
- C:\Windows\System32\drivers\cesguard.sys
- C:\Windows\System32\drivers\ceshlp.sys
- C:\Windows\System32\drivers\ceskbdflt.sys
- C:\Windows\System32\guard64.dll
- C:\Windows\SysWOW64\guard32.dll