How to block EXE files from running using Group Policy

Windows 10 & 11 Professional.

Unauthorised EXE files are often blocked for security reasons. While EXEs are the most common way for programs to run on Windows, a downloaded executable file may contain harmful software known as malware (malicious software) designed to compromise computer systems for data exfiltration, ransomware, and other cyber attacks.

To block exe files from running using Group Policy in Windows 11/10 PRO, do the following:

- Press Windows key + R to invoke the Run dialog Press Windows key + R to invoke the Run dialogue.
- In the Run dialog box type gpedit.msc and press Enter to open Group Policy Editor.
- Inside the Local Group Policy Editor, use the left pane to navigate to the path below:

Computer Configuration > Windows Settings > Security Settings > Software Restriction Policies > **ADDITIONAL RULES**

Next, right-click Additional Rules node and in the popup menu select

NEW PATH RULE

Now, enter the path to the folder that you want to prevent executable files to run from and make sure to suffix the *.exe at the end, so that you will only block executable files.

You can block (at least) the following:

C:\Windows\Temp*.exe
C:\Windows\Temp**.exe
%USERPROFILE%\AppData\Local*.exe
%USERPROFILE%\AppData\Local**.exe
%USERPROFILE%\AppData\Roaming*.exe
%USERPROFILE%\AppData\Roaming**.exe

It was possible to install Group Policy on Home versions of Windows but Microsoft has disable this function.

There is a Third-Party application that works very well at blocking EXE's and other applications from running. It is easy to install; easy to LOCK and Unlock. The Default settings don't need to be changed.

Simple Software Restriction Policy