Simple Windows Hardening - Manual

Version 2.1.1.1

Dev. Website:
https://github.com/AndyFul/Hard_Configurator/tree/master/Simple_Windows_Hardening

H_C_HardeningTools repository:
ConfigureDefender/H_C_HardeningTools at master · AndyFul/ConfigureDefender · GitHub

TABLE OF CONTENTS

INTRODUCTION

Simple Windows Hardening (**SWH**) works on Windows 10 and 11. It is a portable application that allows configuring Windows built-in features to support antivirus and prevent fileless malware.
SWH is adjusted to the home environment. After the initial configuration, it can be closed and all protection comes from the Windows built-in features.

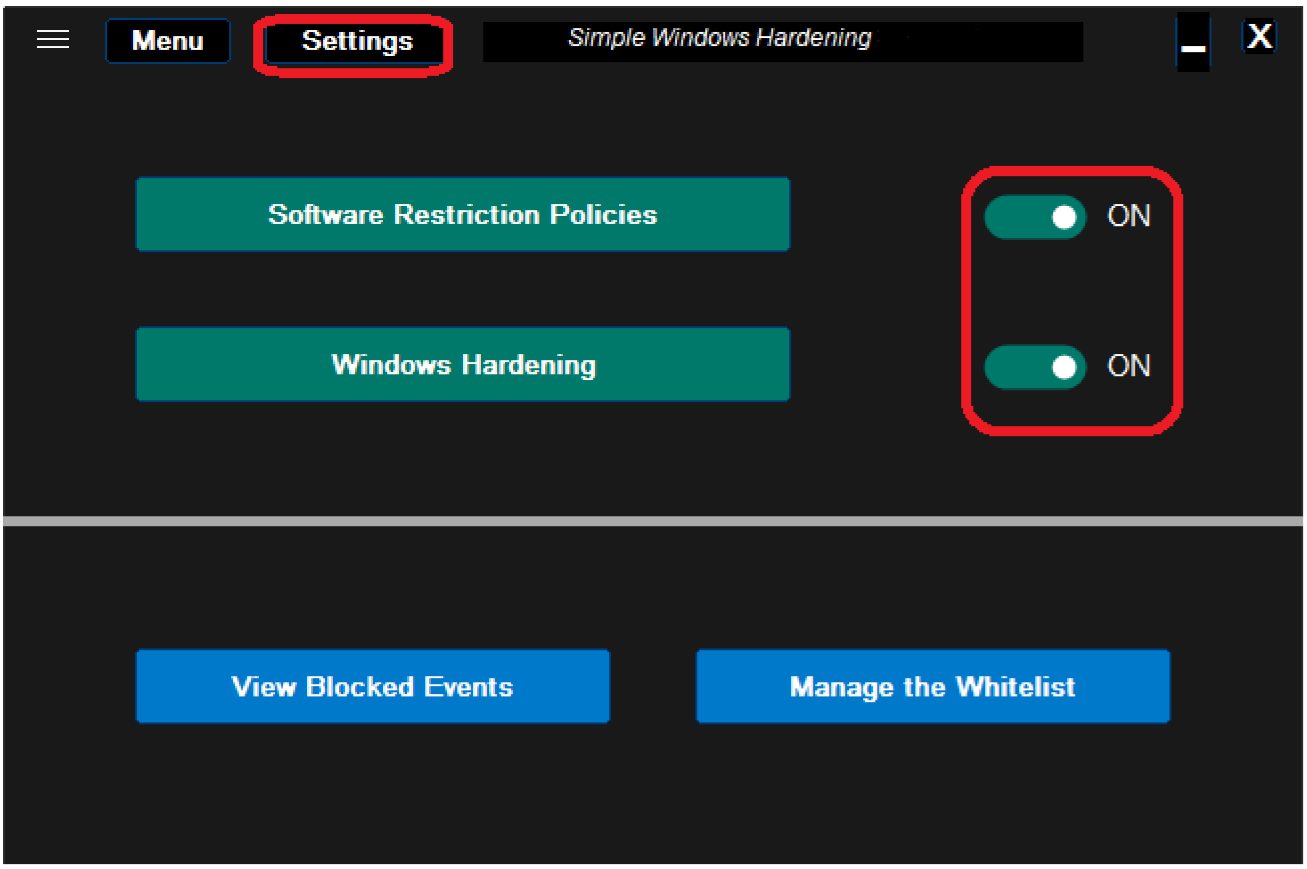
SWH is based on Software Restriction Policies (SRP) and some useful Windows Policies.
Users on Windows 11 should bear in mind that Microsoft stopped the development of SRP a few years ago. One cannot exclude the possibility that some problems related to SRP may arise in the future on Windows 11. It is also possible that Microsoft will remove SRP on Windows 12.
SWH is tested via Windows Insider program, so any possible problem is recognized in advance and reported on the Dev. Website.

SWH is a simplified version of Hard_Configurator. The below Hard_Configurator restrictions are set to Windows default values and cannot be configured in SWH: <Block Sponsors>, <Update Mode>, <Hide 'Run As Administrator>, <Forced SmartScreen>, <Shell Extension Security>, <MSI Elevation>, <UAC CTRL_ALT_DEL>, and <Disable Elevation on SUA>.

Generally, SWH applies the Hard_Configurator Windows_10_Basic_Recommended_Settings (without Forced SmartScreen). These settings can be modified in SWH.

The restrictions can be switched OFF/ON by using two switches on the right of the green buttons:
Software Restriction Policies and **Windows Hardening**.

In the OFF position, the restrictions are remembered and next removed - Windows default settings are applied for previously restricted features. When switching ON, the remembered settings are restored. **Furthermore, in the ON position the configurable settings can be changed by the user from the Settings menu.**



The security setup is adjusted to keep usability and prevent fileless malware in the home environment. So, the EXE and MSI files are not restricted in SWH, except when executed from archives and email clients. But non-executable files like scripts, shortcuts, and other files with unsafe extensions are restricted. Such a setup can be very efficient because nowadays, many initial vectors of attack are performed via non-executable files.

THE EXE / MSI 0-DAY MALWARE.

SWH does not apply restrictions to EXE and MSI files, because these files are often used to install/update applications. Nowadays, many antivirus solutions can provide strong protection against EXE/MSI malware. But still, the antivirus proactive features can have a problem with 0-day malware.

The user has to be very careful when running EXE/MSI files originated from:
1. Internet web links embedded in the emails.
2. Attachments embedded in the emails.
3. Flash drives (USB drives) shared with other people.

When using SWH restrictions, the **RunBySmartScreen** tool can be helpful. It allows checking any EXE/MSI file against the Microsoft SmartScreen Application Reputation service in the cloud. Many such files are accepted by SmartScreen, and this is the best way to avoid a 0-day malware. If the EXE/MSI file is not recognized by SmartScreen as safe or malicious, then the simplest method is waiting a minimum one day before running the unsafe file. After one day most of the malicious links are dead and most of the 0-day malware are properly detected by a good antivirus.

SWH supports especially well Antivirus solutions with enabled reputation file lookup:
1. Microsoft Defender (ASR prevalence rule / ConfigureDefender).
2. Norton 360 (Download Insight).
3. Avast (Hardened Mode).
4. Comodo (Autosandbox).
5. SAC (on Windows 11) + any AV.

In these cases, one can skip the RunBySmartscreen tool.

QUICK CONFIGURATION

1. Run SWH - the restrictions are automatically configured.
2. Log OFF the account or reboot is required, depending on what restrictions were applied in SWH.
3. **If MS Office (or Adobe Acrobat Reader) is installed, then it is recommendable to apply additional hardening by using DocumentsAntiExploit tool.**

Please keep updated your system/software. Use SWH on the default settings for some time, until you will be accustomed to it. Most users will probably do not see any difference, but rarely a legal script or file with unsafe extension will be blocked by SWH settings.
The blue buttons **View Blocked Events** and **Manage the Whitelist** can help to recognize and whitelist the blocked files. Please be careful, if you are not certain that the blocked file is safe, then wait one day or two before whitelisting it.

SOFTWARE INCOMPATIBILITIES

Windows built-in SRP cannot work with **AppLocker** (introduced via GPO or MDM WMI Bridge). In such a case, SimpleWindowsHardening shows an alert. Furthermore, the options related to SRP are **Switched OFF** and removed from the **Settings**.

From the year 2022, AppLocker (GPO) policies can work on Windows 10/11 Home and Pro. AppLocker is activated by default on Windows 11 ver. 22H2 or later (also on Windows Home), so SRP is disabled in the default configuration.

SimpleWindowsHardening ver. 2.1.1.1 can enable SRP on Windows 11, and SRP can also work with enabled Smart App Control (SAC).

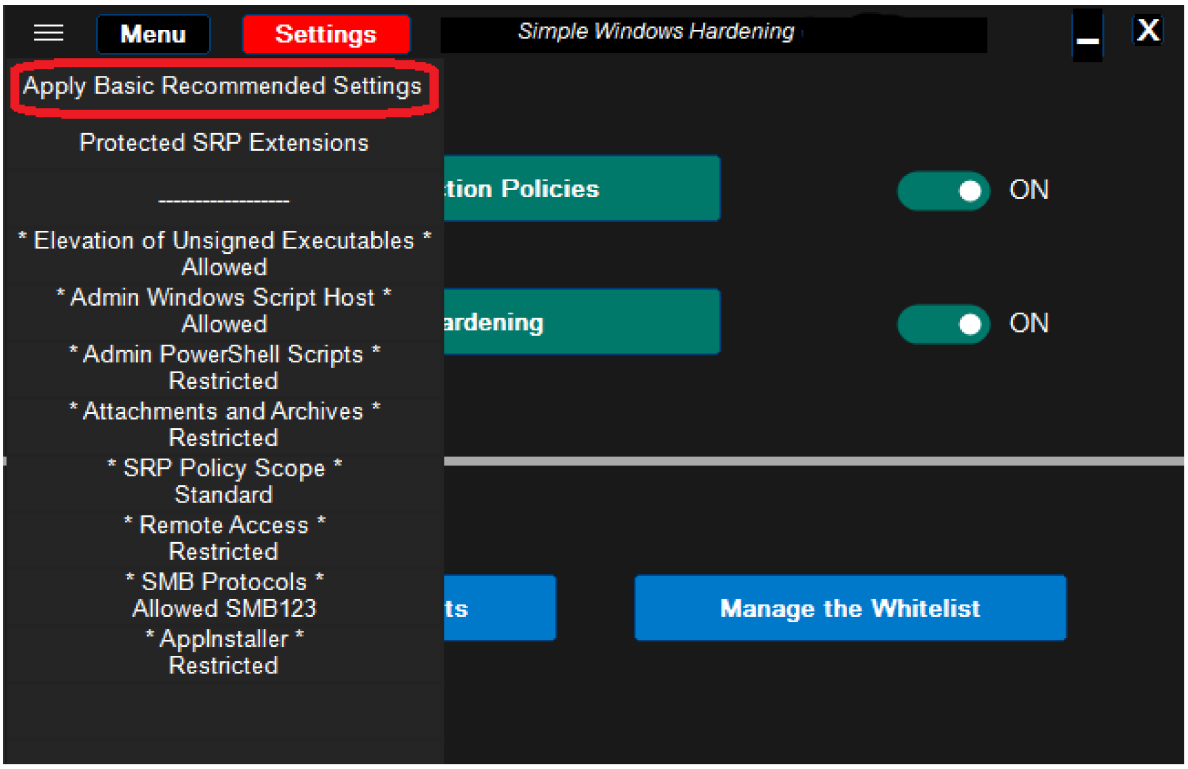
Windows built-in SRP is incompatible with **Child Account** activated on Windows 10+ via Microsoft Family Safety. Child Account adds some Ap-

pLocker rules (via MDM), so SRP cannot work. Unfortunately, after removing Child Account, the AppLocker Policy files are not removed (unpleasant bug)! These policy files have to be removed manually to recover the SRP functionality.

SimpleWindowsHardening settings are not compatible with **SRP introduced via Group Policies Object (GPO)** available in Windows Pro, Education, and Enterprise editions. The GPO refresh feature will overwrite the SimpleWindowsHardening settings. So, before installing SimpleWindowsHardening, SRP has to be removed from GPO.

SimpleWindowsHardening will also conflict with **any software which uses SRP**, but such applications are rare (CryptoPrevent, SBGuard, AskAdmin, Ultra Virus Killer). Before installing SimpleWindowsHardening it will be necessary to uninstall the conflicting application.

Basic Recommended Settings



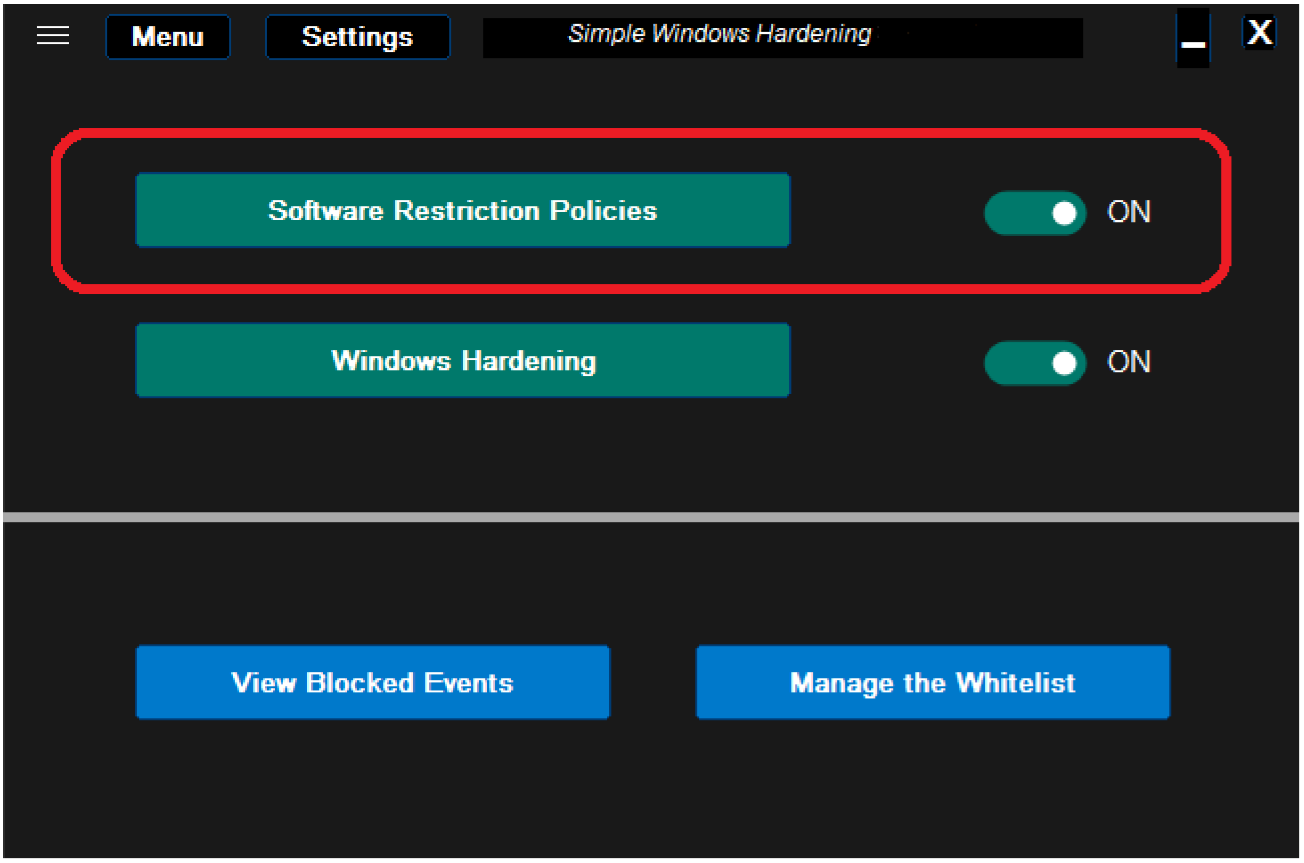
The default SWH restrictions can be always restored by choosing: Settings >> Apply Basic Recommended Settings.
These settings are applied automatically after starting the SWH application, if Windows SRP has not been yet installed or the settings have been tampered by another application.

In the Basic Recommended Settings, the features are configured as follows:

1. PowerShell is restricted by Constrained Language Mode (non-configurable in SWH).
2. The %WinDir% folder (usually c:\Windows\) is hardened by adding the writable subfolders to UserSpace (non-configurable in SWH).
3. The shortcuts are blocked in UserSpace, except some standard locations like Desktop or Menu Start. If necessary, then shortcucts in non-standard locations can be whitelisted (Manage the Whitelist >> Whitelist By Path >> Add Path*Wildcards).
4. SRP blocks by default unsafe files in UserSpace, except EXE and MSI files. The unsafe files are recognized by the file extensions. These extensions can be added/removed from the **Settings** menu (Settings >> Protected SRP Extensions).
5. Execution of EXE and MSI files is disallowed from the archiver applications and email clients. This option can be configured from the **Settings** menu (Settings >> * Attachments and Archivers *).
6. * Elevation of Unsigned Executables * is set to Allowed by default, but the user can set it manually to Restricted.
7. * Admin Windows Script Host * is set to Allowed by default, but the user can set it manually to Restricted.
8. * Admin PowerShell Scripts * is set to Restricted by default.
9. * Remote Access * is set to Restricted by default.
10. * SMB Protocols * is set to Allowed by default, but the user can set it manually to restrict SMB1 Protocol or all SMB 1,2,3 Protocols.
11. * AppInstaller * is set to Restricted by default.
12. Cached Logons are disabled (non-configurable in SWH).
13. Execution of 16-bit processes is disabled (non-configurable in SWH).

The features 3-11 (green background) are configurable in the SWH application. Other features (grey background) cannot be configured in SWH.

Software Restriction Policies



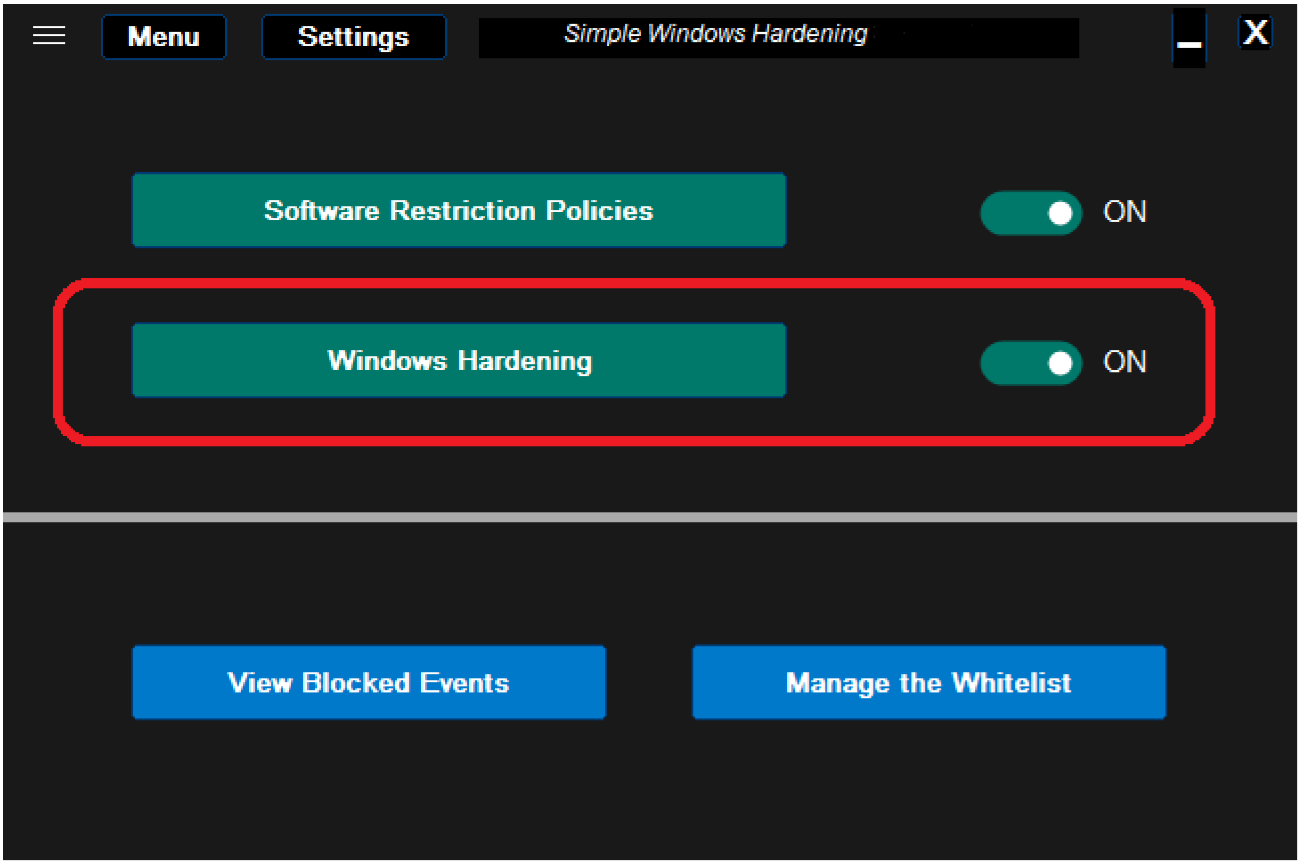
When the switch is ON, the below SRP setup can be applied:

1. PowerShell works restricted by Constrained Language Mode in SWH).
2. The %WinDir% folder (usually c:\Windows\) is hardened by adding the writable subfolders to UserSpace (non-configurable in SWH).
3. The shortcuts are blocked in UserSpace by default, except some standard locations like Desktop or Menu Start. If necessary, then shortcucts in non-standard locations can be whitelisted (Manage the Whitelist >> Whitelist By Path >> Add Path*Wildcards).
4. SRP blocks by default unsafe files in UserSpace, except EXE and MSI files. The unsafe files are recognized by the file extensions. These extensions can be added/removed from the **Settings** menu (Settings >> Protected SRP Extensions).
5. Execution of EXE and MSI files from the archiver applications and email clients can be Allowed/Restricted. This option can be configured from the **Settings** menu (Settings >> * Attachments and Archivers *).

6. The installation of Universal Windows Platform (UWP) apps can be done only via Microsoft Store. On the contrary, the installation of desktop applications from Microsoft Store is disabled. This option can be configured from the **Settings** menu (Settings >> * AppInstaller *).

After switching OFF, all the above restrictions are remembered and removed - Windows default values are applied for them.
The user can restore the remembered restrictions by switching ON again.
When the switch is ON, the options 3-6 can be manually configured from the Settings menu.

Windows Hardening



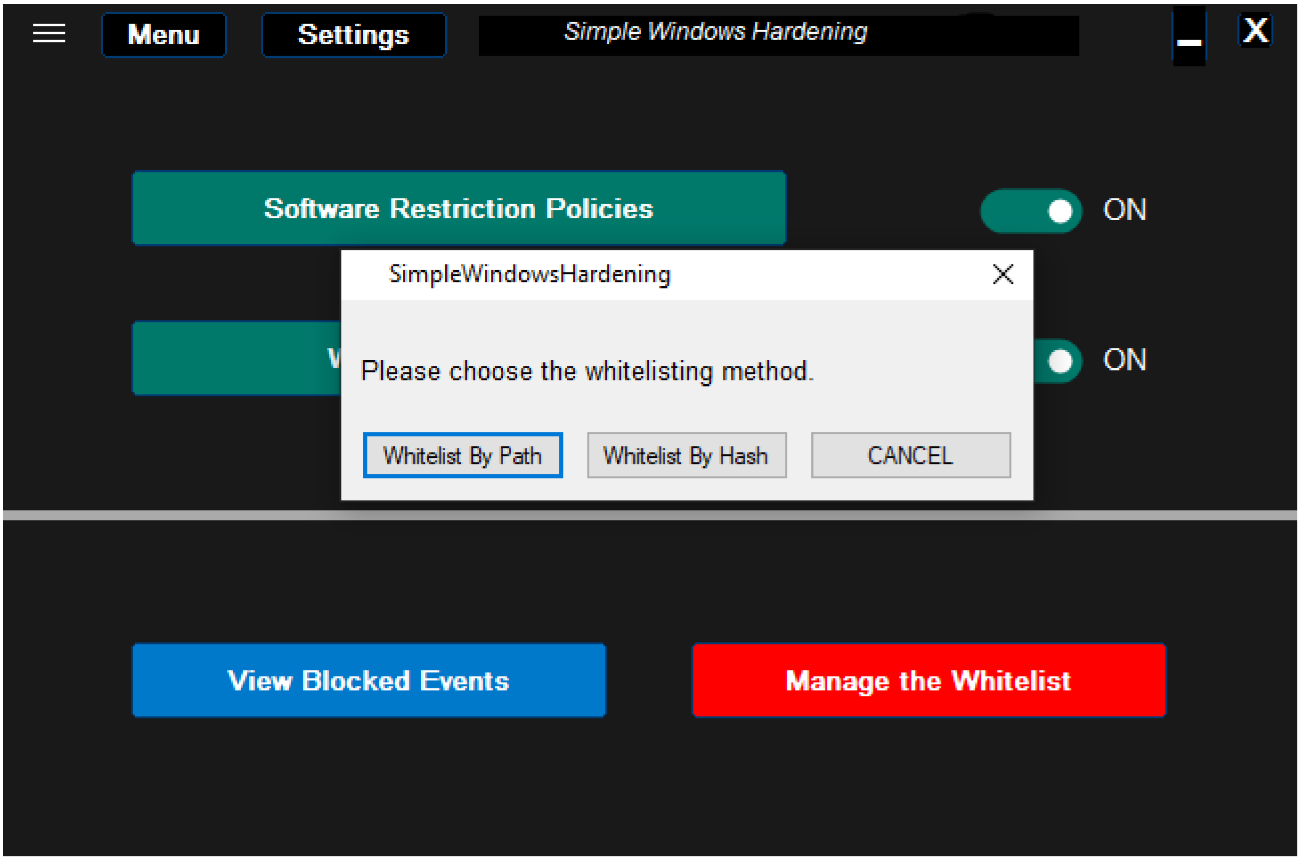
When the switch is ON, the below hardening setup can be applied:

1. * Elevation of Unsigned Executables * set to Allowed/Restricted.
2. * Admin Windows Script Host * set to Allowed/Restricted.

3. * Admin PowerShell Scripts * set to Allowed/Restricted.
4. * Documents Anti-Exploit * set to Adobe + VBA |VBA | OFF.
5. * Remote Access * set to Allowed/Restricted.
6. * SMB Protocols * set to Allowed SMB123 | Restricted SMB1 | Restricted SMB123.
7. Cached Logons are disabled (non-configurable in SWH).
8. Execution of 16-bit processes is disabled (non-configurable in SWH).

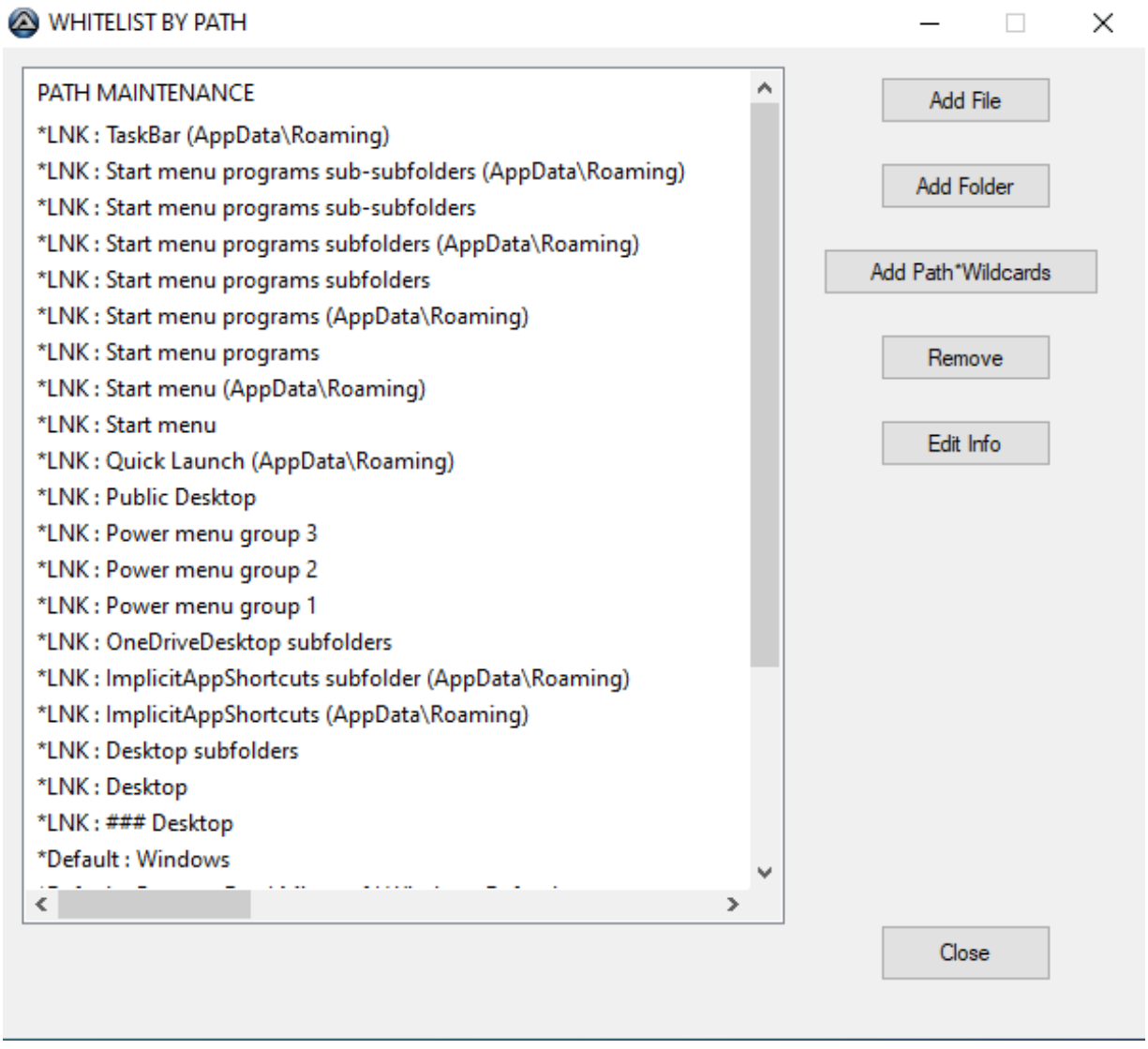
After switching OFF, all the above restrictions are remembered and removed - Windows default values are applied for them. The user can restore the remembered restrictions by switching ON again.
When the switch is ON, the options 1-6 can be manually configured from the Settings menu.

Manage the Whitelist



This button, can be used to whitelist the processes blocked by SRP (events ID 865-868, 882, 1007, 1008) and the PowerShell scripts restricted by Constrained Language mode.

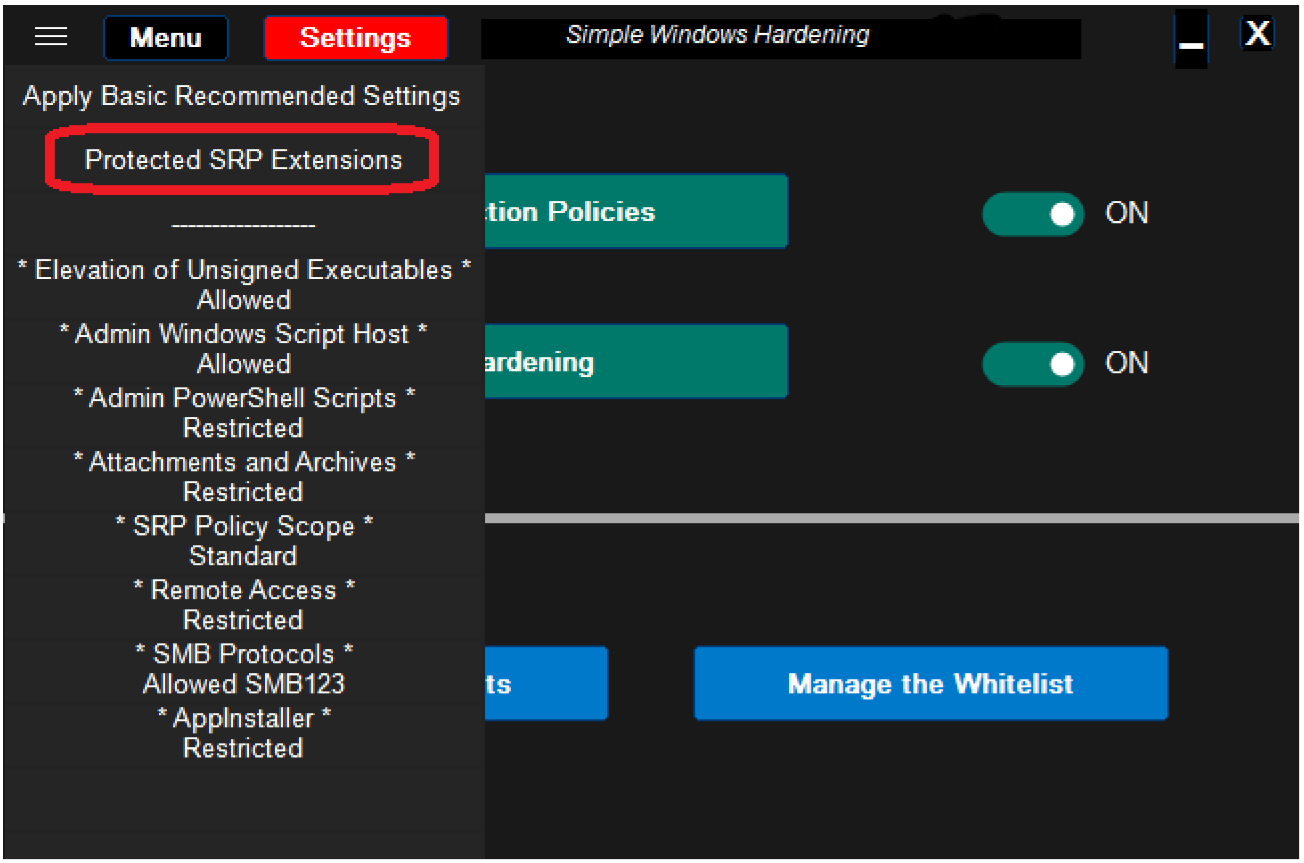
After pressing the button, the user is asked to choose the whitelisting method <Whitelist By Path> or <Whitelist By Hash> .
Whitelisting is very useful when running files located in UserSpace (outside of the system folders: 'Windows', 'Program Files ...'). It has to be done with caution because SRP will not block the malware running from the whitelisted path. If necessary, then < Whitelist By Hash> can be used for more security. The file whitelisted by hash can be used in any location. This whitelisting method prevents running the file if it would be replaced or modified by malware, but also will block the application updates.



Whitelisting by path with wildcards is only possible when using the option <Add Path*Wildcards>. **This option does not support the paths with quotation marks and does not support environment variables.**

Whitelisting by path a shortcut (LNK file) has to be done by using the option <Add Path*Wildcards>, too. But in this case, the path to shortcut file cannot include wildcards!

Protected SRP Extensions

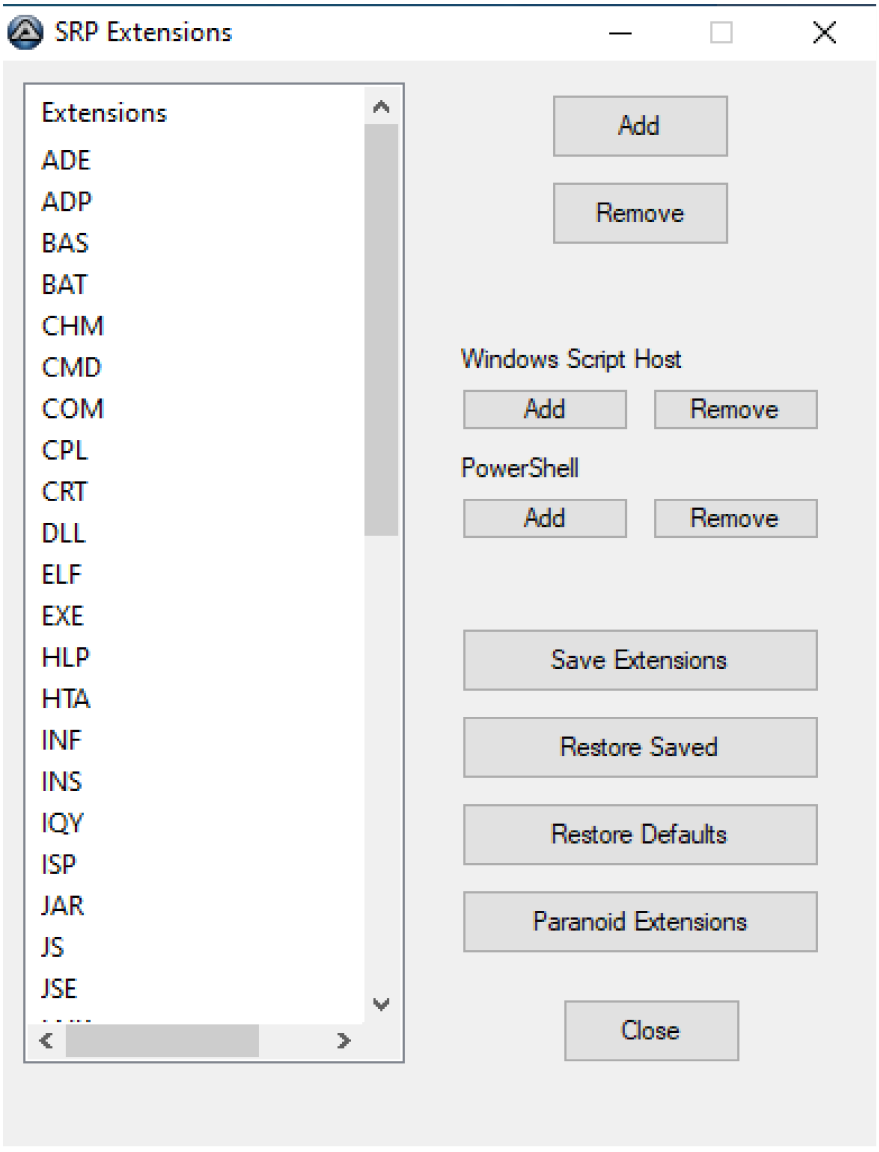


This option opens ADD/REMOVE window with the list of actually protected extensions.

The default extensions are as follows:
ACCDA, ACCDU, ADE, ADP, BAS, BAT, CHM, CMD, COM, CPL, CRT, CSV, DLL, DQY, ECF, ELF, EXE, HLP, HTA, INF, INS, IQY, ISP, JAR, JS,

JSE, LNK, MDA, MDB, MDE, MSC, MSP, MST, OCX, OQY, PA, PCD, PIF, PPA, PPAM, REG, RQY, RTF, SCR, SCT, SETTINGCONTENT-MS, SHS, SLK, URL, VB, VBE, VBS, WLL, WS, WSC, WSF, WSH, WWL, XLA, XLAM, XLL, XLM.

The PowerShell script extensions are not on the list, because of the default PowerShell Execution Policy set to Restricted. Furthermore, the SWH default settings block PowerShell script files also for Administrators.



Paranoid Extensions include an extended number of potentially dangerous file extensions (about 300 entries), which were abused in the wild.

You can customize the list of extensions via <Add> and <Remove> buttons. When using a custom list, it is good to save it (<Save Extensions>). The list can be restored by using <Restore Saved> button.

PROTECT 'WINDOWS' FOLDER

This setting is non-configurable in SWH. The restriction is applied to prevent the execution of native Windows executables, Windows CMD, Windows Script Host, and MSI Installer from writable 'Windows' subfolders. So, the execution of EXE, COM, SCR, BAT, CMD, JS, JSE, VBS, VBE, WSF, WSH, and MSI files is blocked, when they are run directly or via command lines with Sponsors: cmd.exe, wscript.exe, cscript.exe, or msiexec.exe.
The execution is denied even if these file extensions are not on the list of **Protected SRP Extensions**.

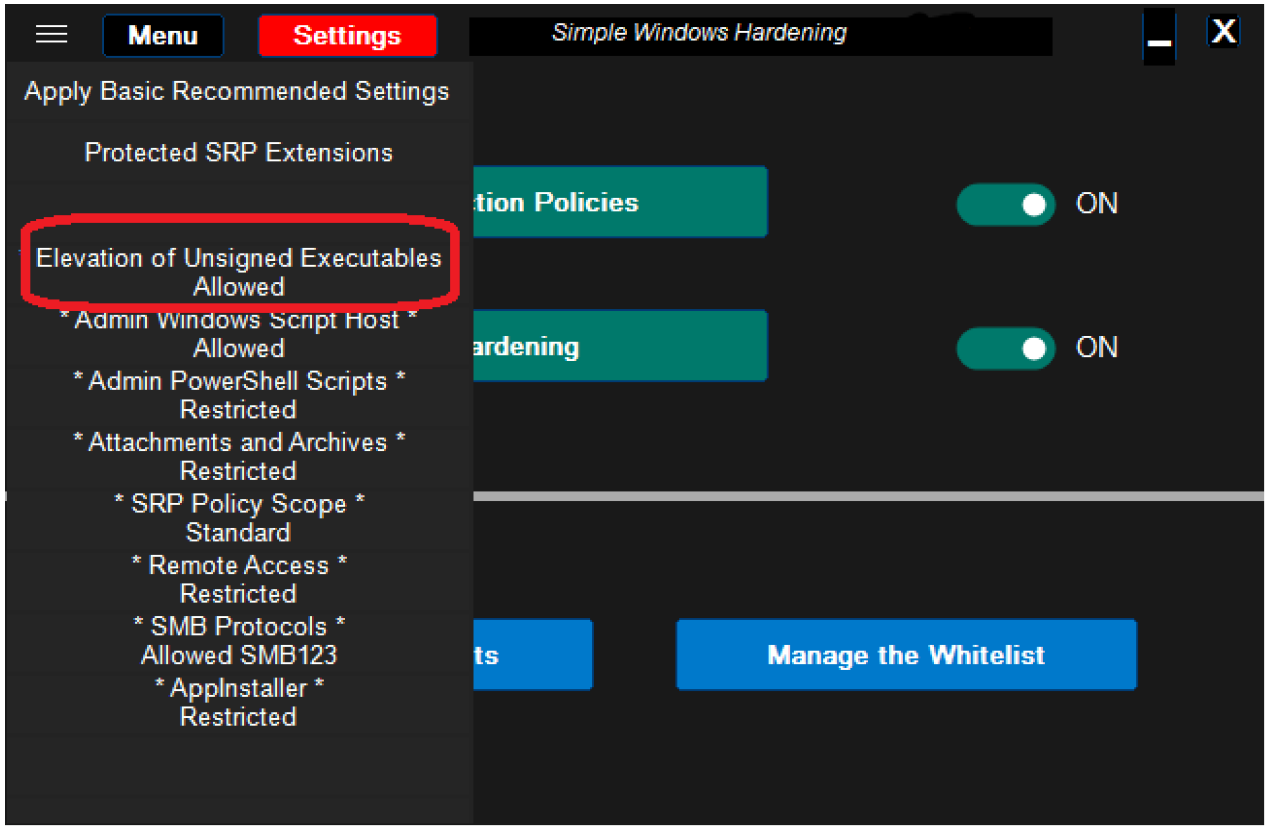
PROTECT SHORTCUTS

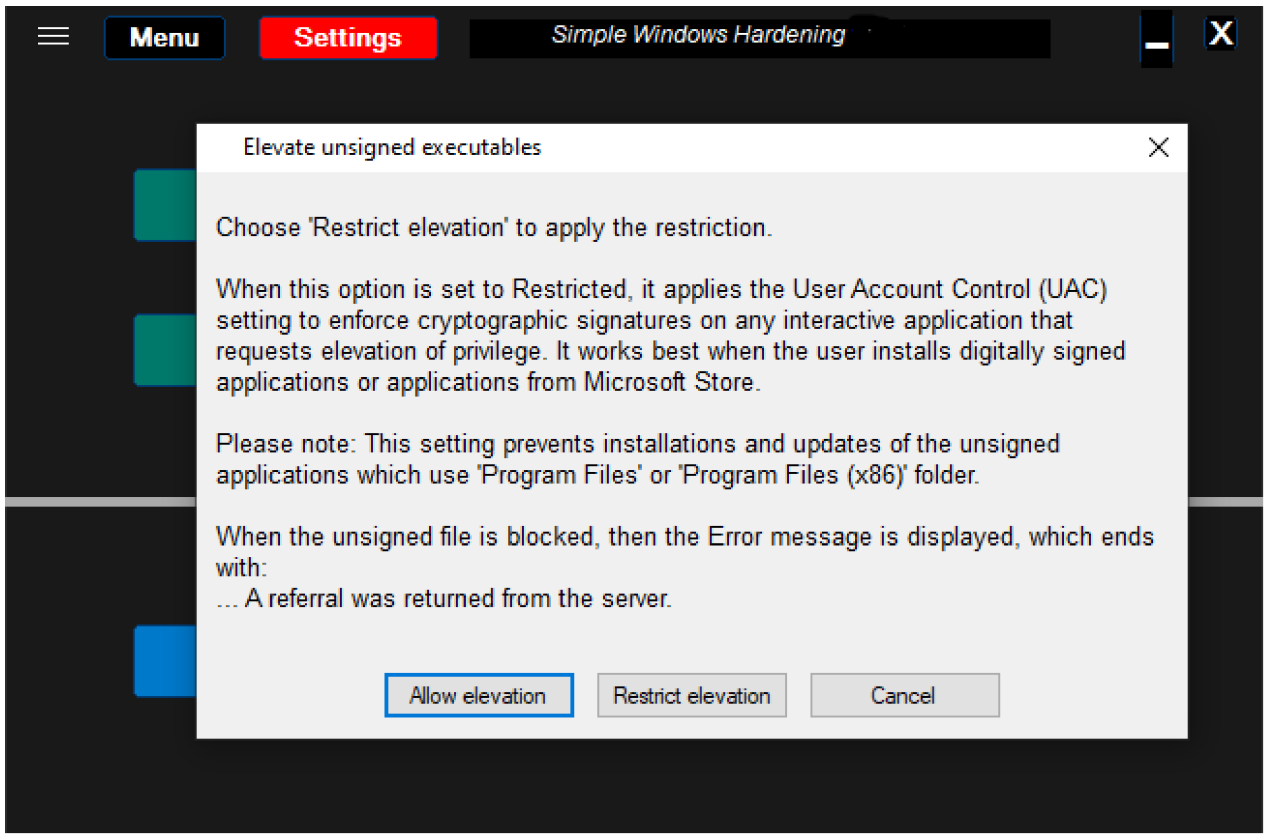
The SWH restrictions prevent the execution of shortcuts in UserSpace.
Shortcuts can be executed when:

1. They are located in SystemSpace ('Windows', 'Program Files', Program Files (x86)) and in some standard shortcut locations: 'Desktop', 'Power Menu', 'Start Menu', 'Quick Launch', 'Taskbar', and 'Public Desktop'.
2. They are whitelisted by path - Manage the Whitelist >> Whitelist by path >> Add Path*Wildcards.

So, this restriction is partially configurable via whitelisting. It is applied because specially crafted shortcuts can bypass Software Restriction Policies.

* Elevation of Unsigned executables *





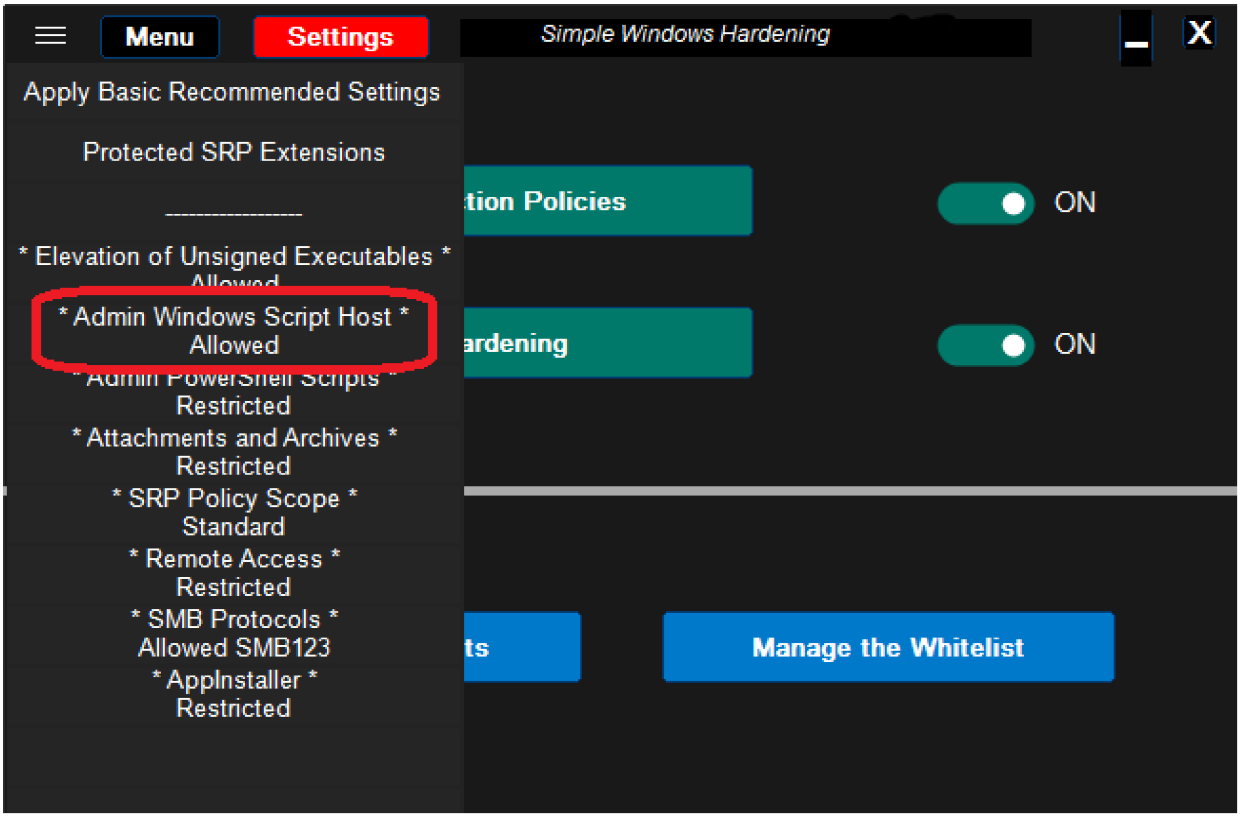
If Restricted, then the User Account Control (UAC) enforces cryptographic signatures on any interactive application that requests elevation of privilege. If unsigned application requests elevation, then it will be blocked.
Most malware files are usually unsigned and want to elevate, so this option is a good preventive feature. Yet, it is the UAC setting, so if the UAC is bypassed then this restriction is bypassed too. It is stronger on the Standard User type of account (SUA) as compared to the default Admin account, because SUA has a stronger design to prevent such bypasses.

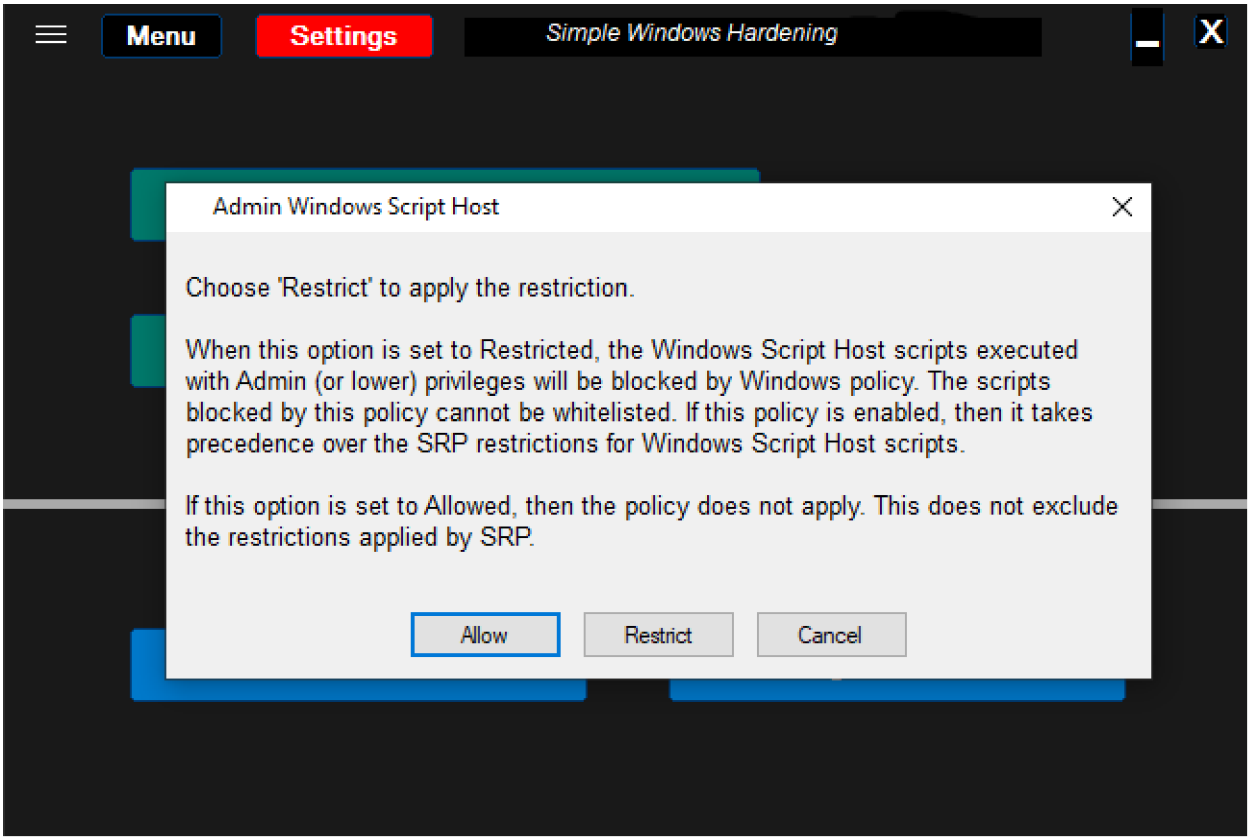
This restriction does not support whitelisting, so it will prevent auto-updates of the unsigned applications even when they are installed in 'Program Files' or 'Program Files (x86)' system folder. Such applications have to be installed/updated without this restriction ("Allow elevation" has to be chosen).

This restriction works best when the user installs digitally signed applications, or unsigned applications which do not require Administrative rights.

When the unsigned file is blocked, then the Error message is displayed, which ends with: ***"... A referral was returned from the server".***

* Admin Windows Script Host *



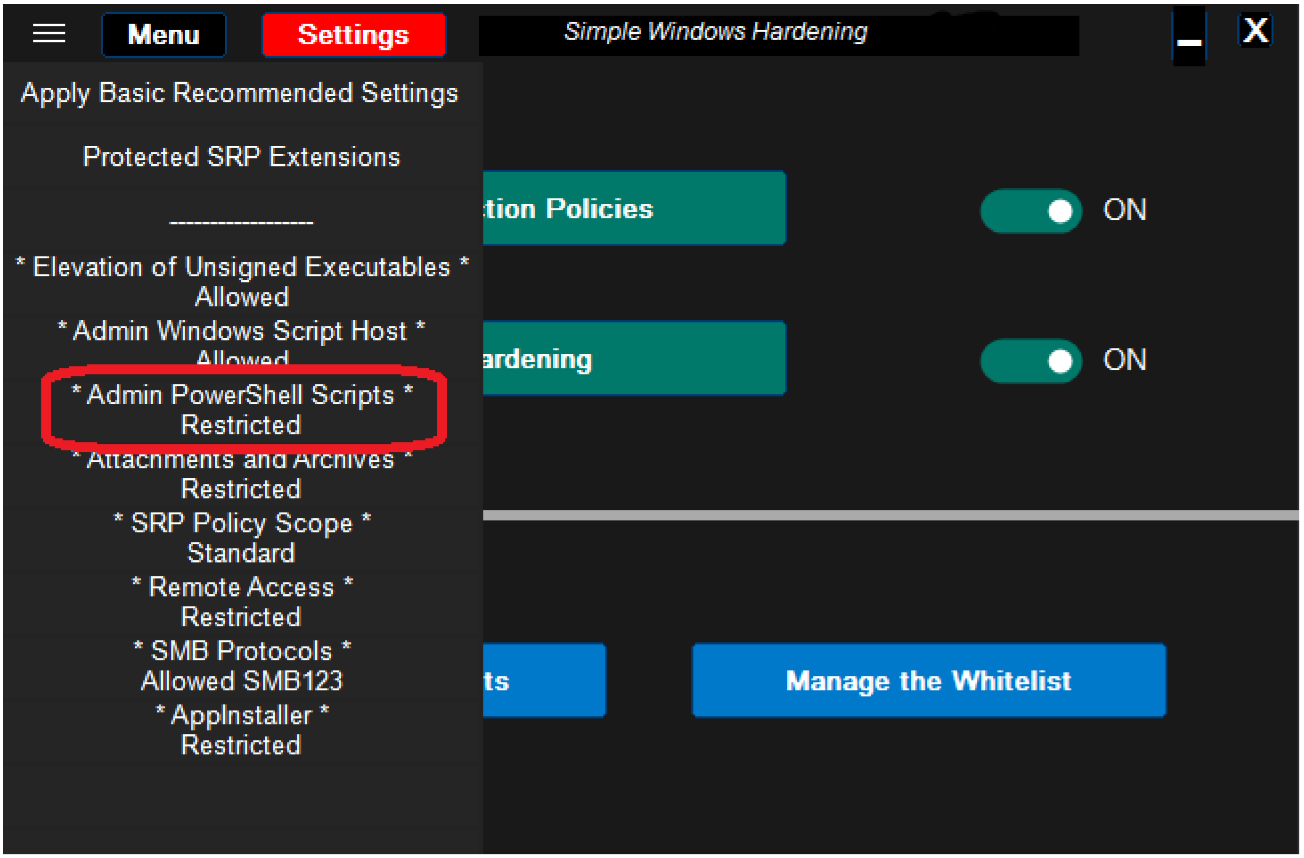


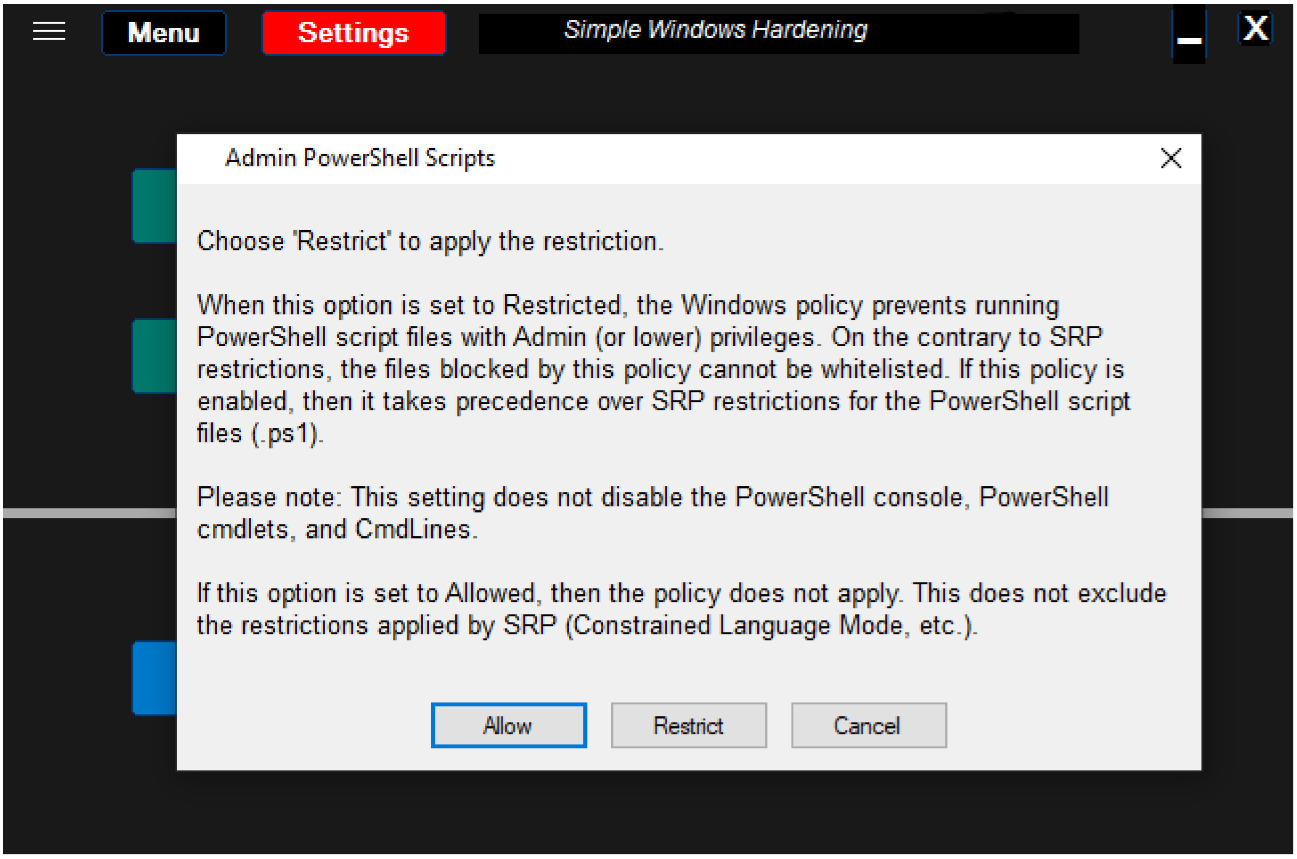
If Restricted, then this option disables Windows Script Host for all processes (also with high privileges). So, the execution of JS, JSE, VBS, VBE, WSF, and WSH scripts is blocked both in UserSpace and SystemSpace. The script whitelisting is not possible.

This option is not Restricted in the SWH default settings, because Windows Script Host is already restricted for standard processes by SRP (which allows whitelisting).

When it is Restricted, some scripts from the system folder: %SYSTEMROOT%\system32\ may be blocked at the boot time, for example: gathernetworkinfo.vbs, gathernetworkinfo.vbs, gatherwiredinfo.vbs, etc. The above scripts are not essential for the Windows system in the home environment, so they may be blocked without issues.

* Admin PowerShell Scripts *

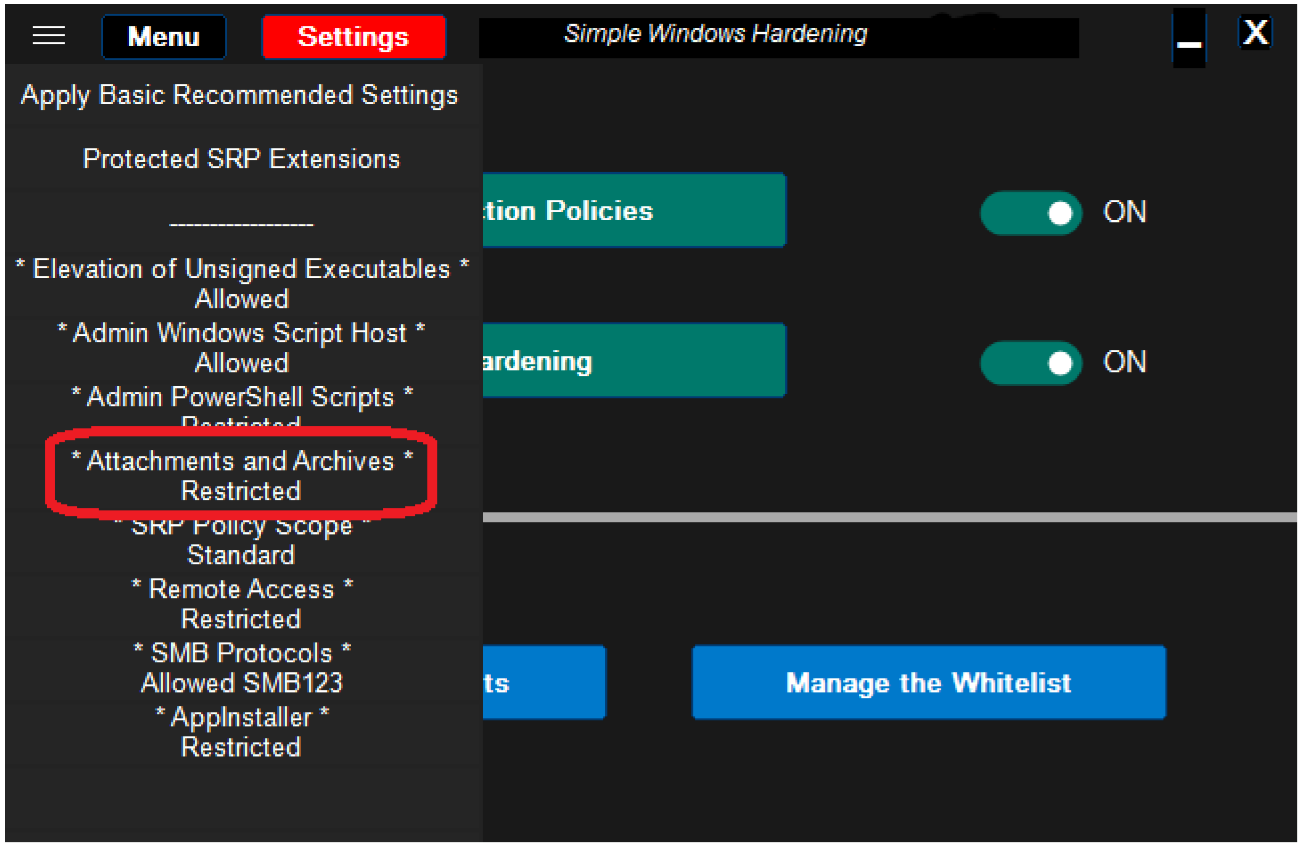


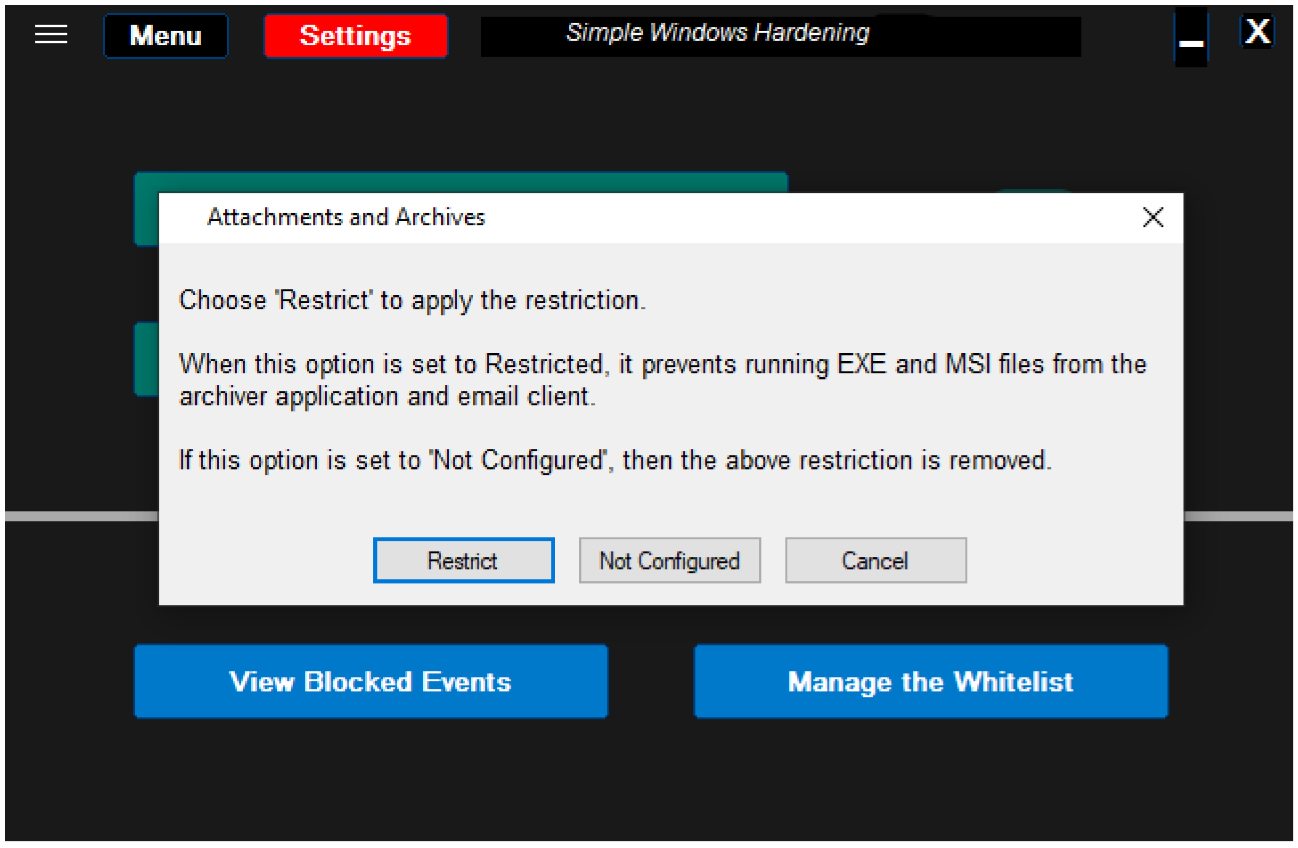


If this option is Restricted, then script file execution is blocked, but the user can still execute PowerShell **commands and cmdlets.** The cons are that PowerShell scripts cannot be whitelisted. Keep this option Restricted, because scripts are the weak point of most antimalware programs.

It is worth remembering that this option is stronger than Windows Execution Policy set to Restricted or adding .ps1 file extension to Protected SRP Extensions. These methods can be bypassed by using command-lines with PowerShell Sponsors (pwershell.exe or powershell_ise.exe), that will be blocked when * **Admin PowerShell Scripts** * feature is set to Restricted.

* Attachments and Archives *



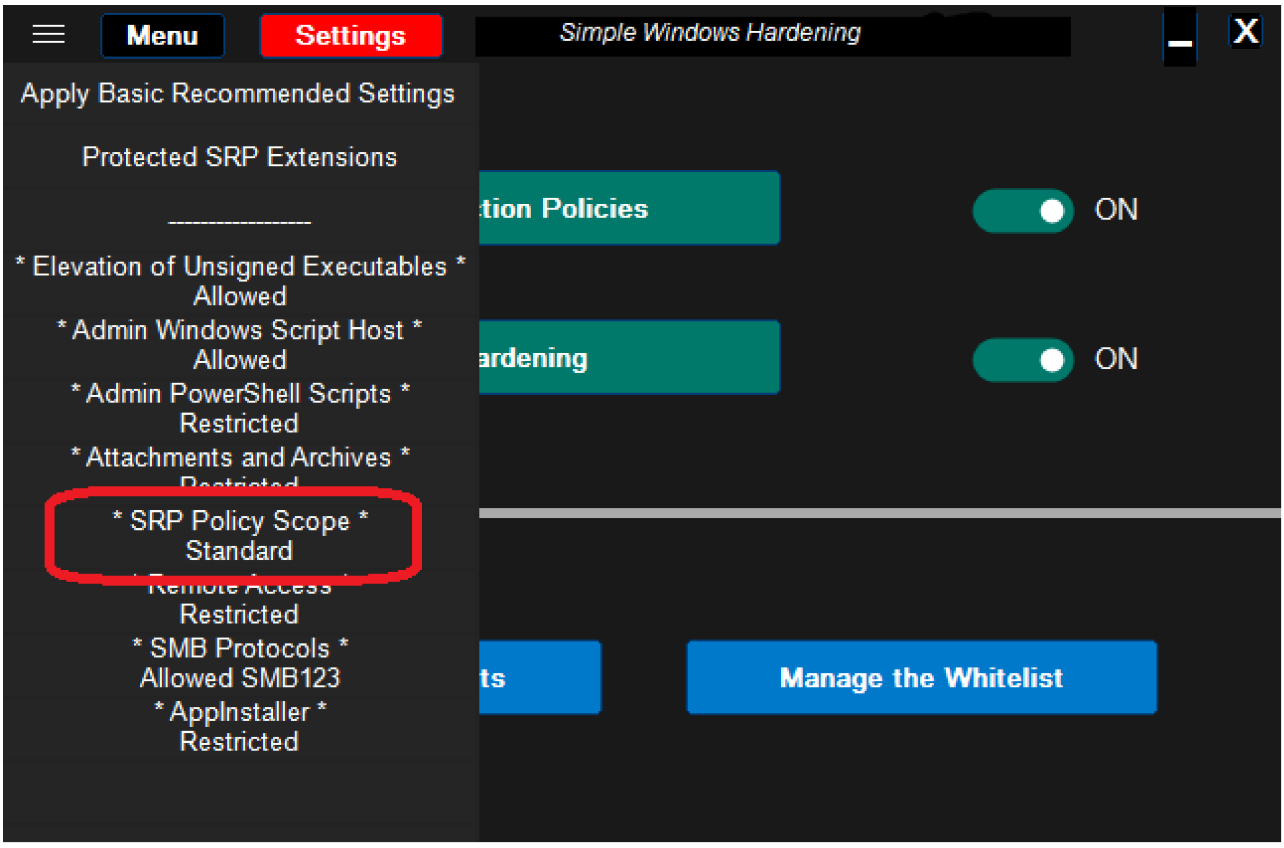


Supported archiver applications:
Windows built-in Zip, 7-Zip, ALZip, Bandizip, B1 Free Archiver, Explzh, ExpressZip, IZArc, PeaZip, PKZip, PowerArchiver, WinRar, WinZip.

Supported email clients:
Mail for Windows 10, Outlook, Claws-mail, eM Client, Foxmail, Hiri, Mailspring, PostBox, Spike, Thunderbird, and any online email client

This restriction can prevent bypassing the SmartScreen Application Reputation feature by accidentally opening EXE or MSI attachments directly from the archiver application or email client. To execute such files, the archive has to be first unpacked and email attachments have to be downloaded to the computer. It is recommended to use the RunBySmartscreen application to check such files against SmartScreen Reputation Service. Such files can be often dangerous - if the file is not accepted by SmartScreen, then it is better to wait a day or more before executing the files.

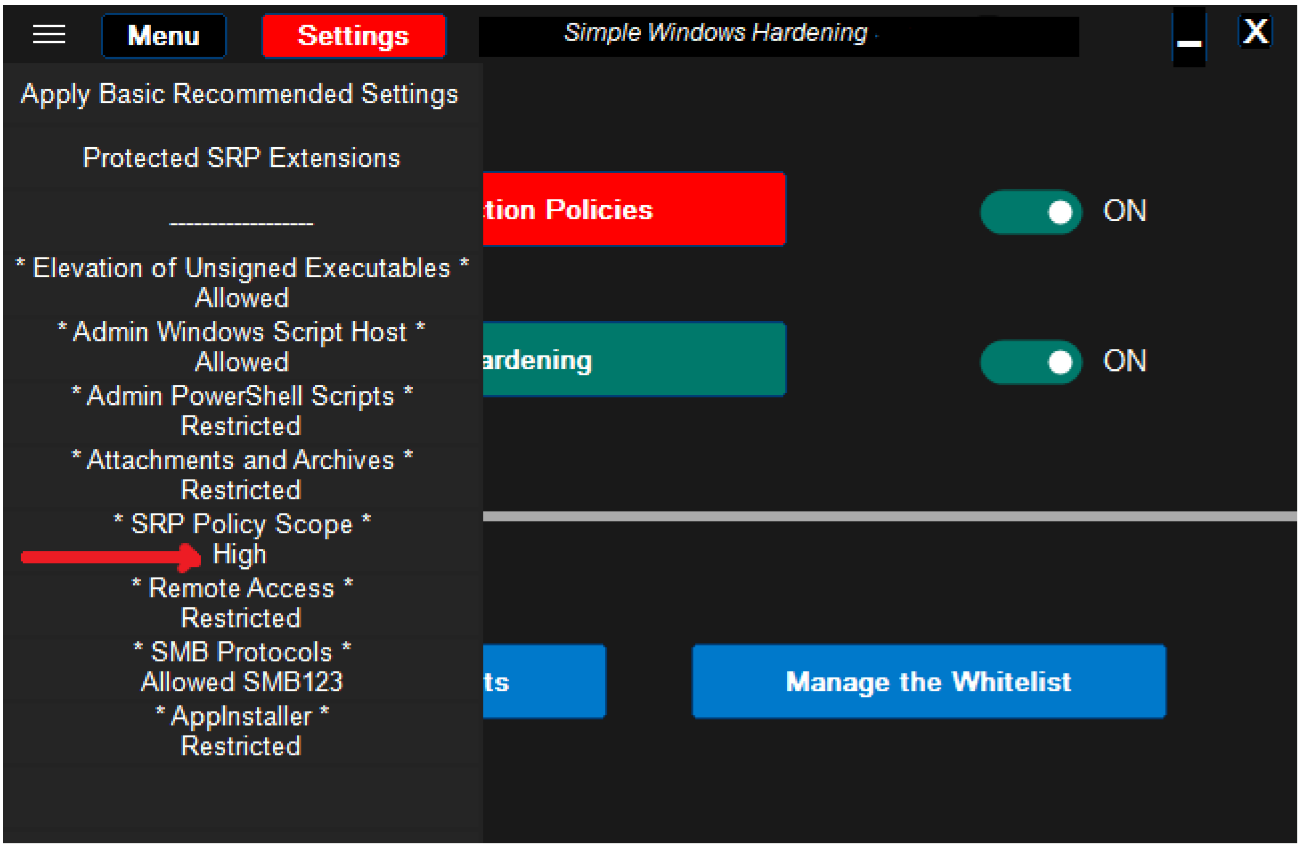
* SRP Policy Scope *



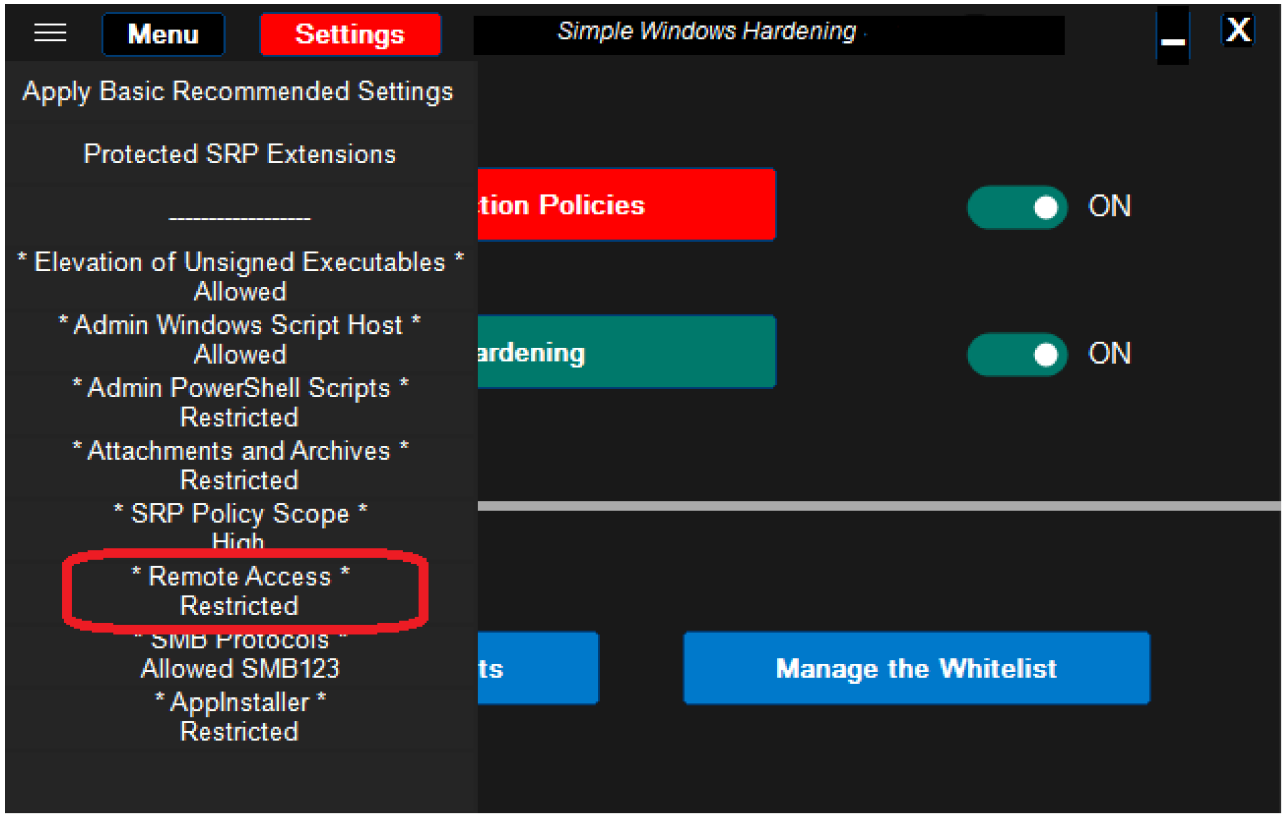
The option * SRP Policy Scope * can apply the SRP restrictions to high privileged processes. Normally, this option is set to Standard, so the restrictions are applied to processes with standard rights and skipped for processes with higher privileges. This is a default SRP setting that does not disrupt administrative processes running from UserSpace.

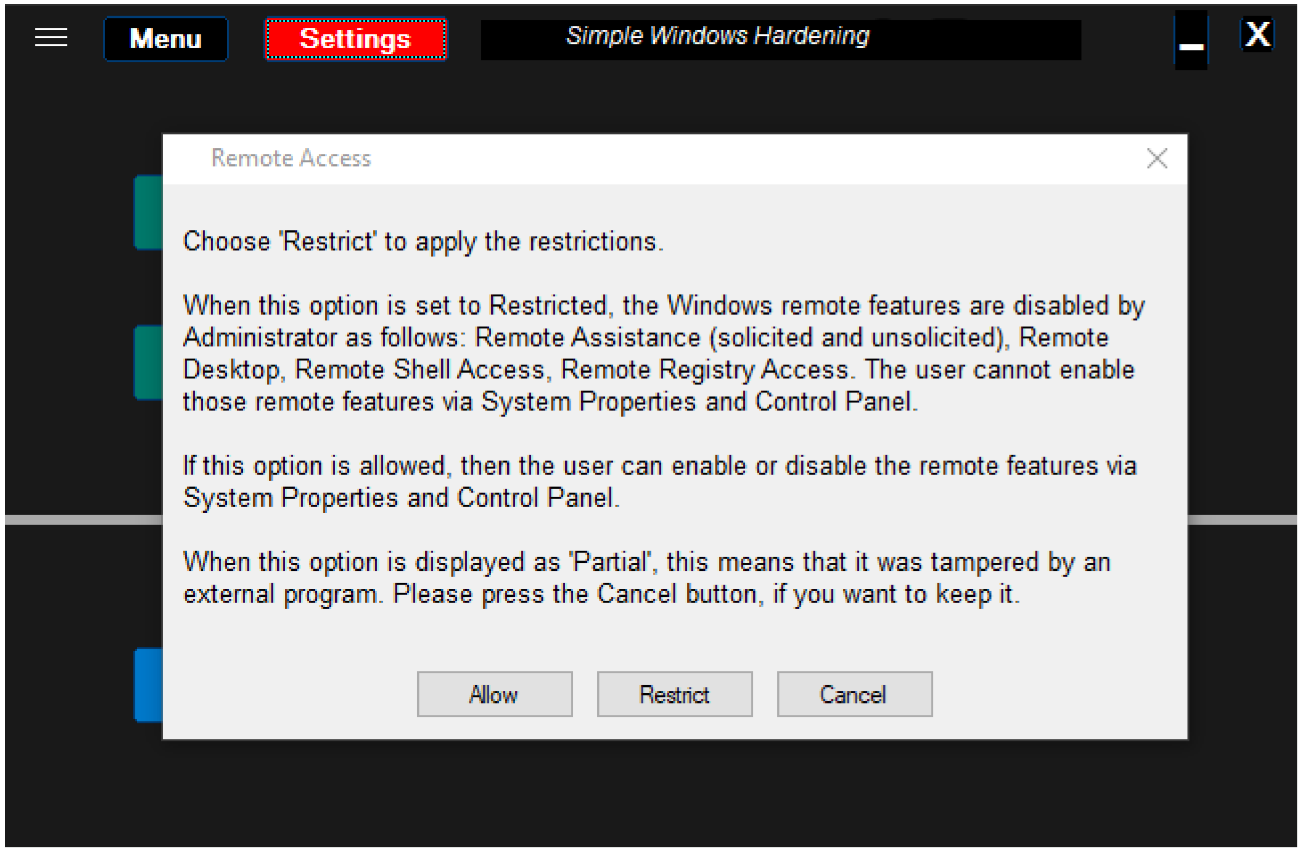
The advanced users can set SRP to apply restrictions to standard and higher privileged processes. This can be done with * SRP Policy Scope * set to High. It is recommended when the computer is used both in the Home environment and in the Business local network.
Applying restrictions for high privileged processes makes also sense when using older Windows versions or vulnerable software.

When the High setting is applied, the **< Software Restriction Policies>** button changes its color to red.



* Remote Access *

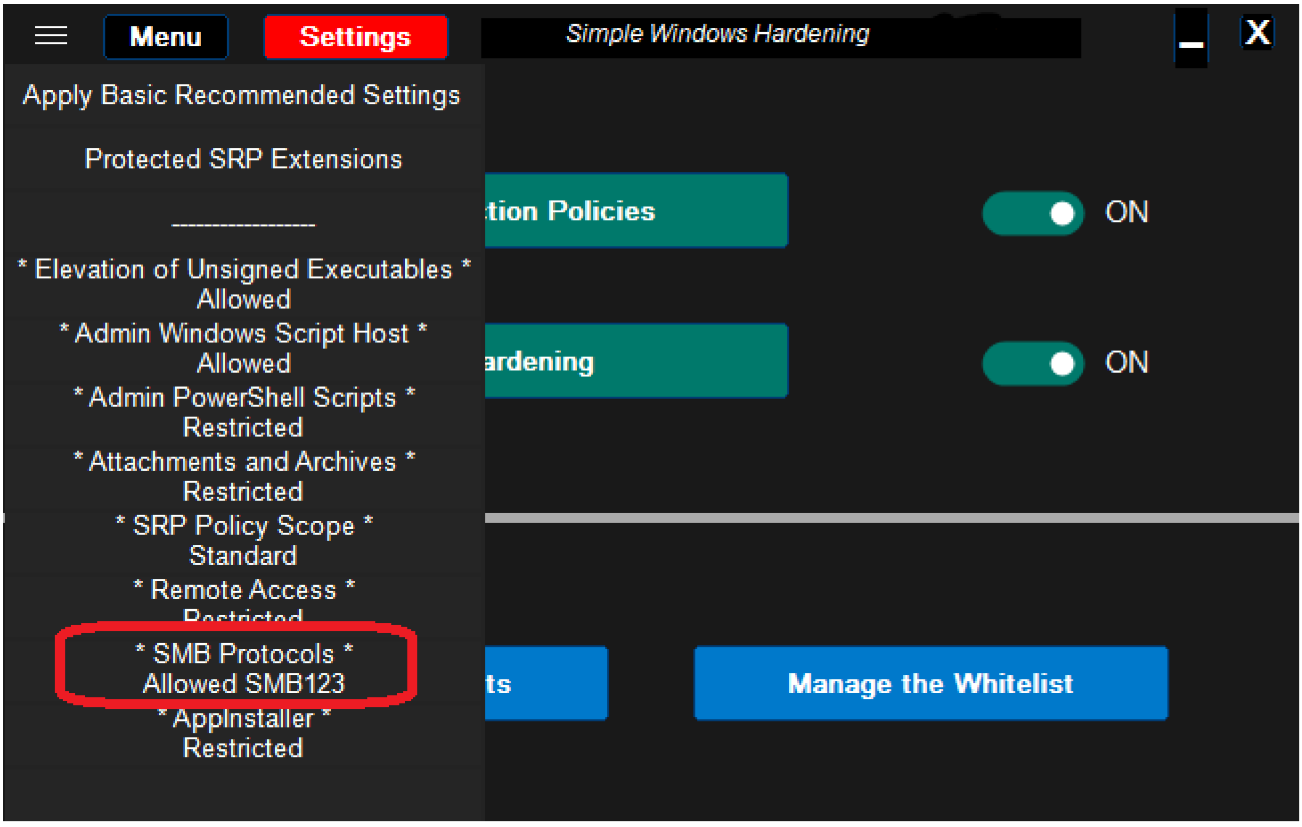


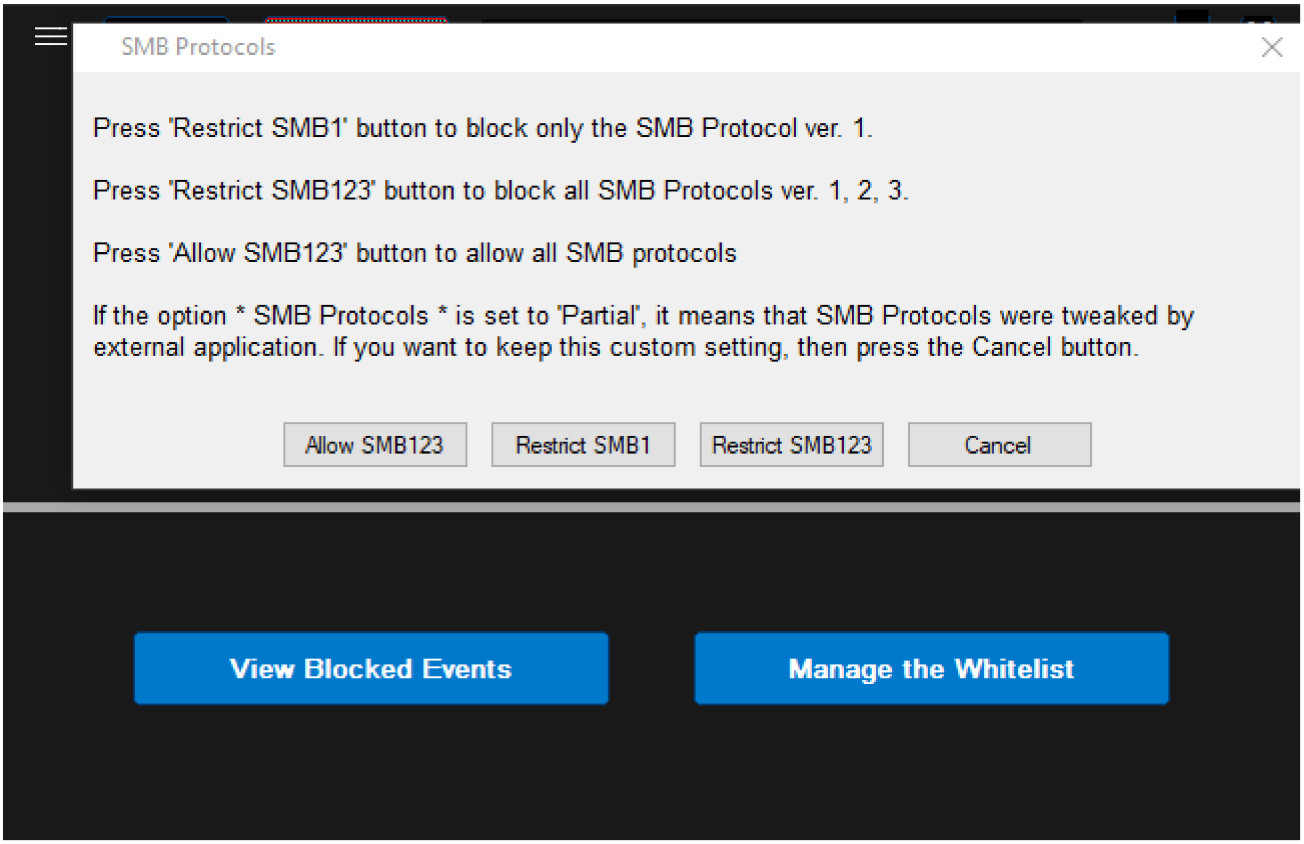


It is recommended for home users to keep <Remote Access> Restricted.
The remote connections are frequently exploited by malware and hackers.
Changing this option always stops 'Remote Registry' service, if it was started.

The events related to Remote Access cannot be whitelisted and are not included in the SWH log. This requires attention because disabling Remote Access can cause silent blocks.
Some problems may occur after disabling Remote Acess, especially in the business environment. For example, some functions of print spooler and directory services replication may require access through the remote registry service. Other custom applications may also depend on Remote Acess features.

* SMB Protocols *





The events related to * SMB Protocols * cannot be whitelisted and are not included in the SWH log. This requires attention because disabling SMB can cause silent blocks.

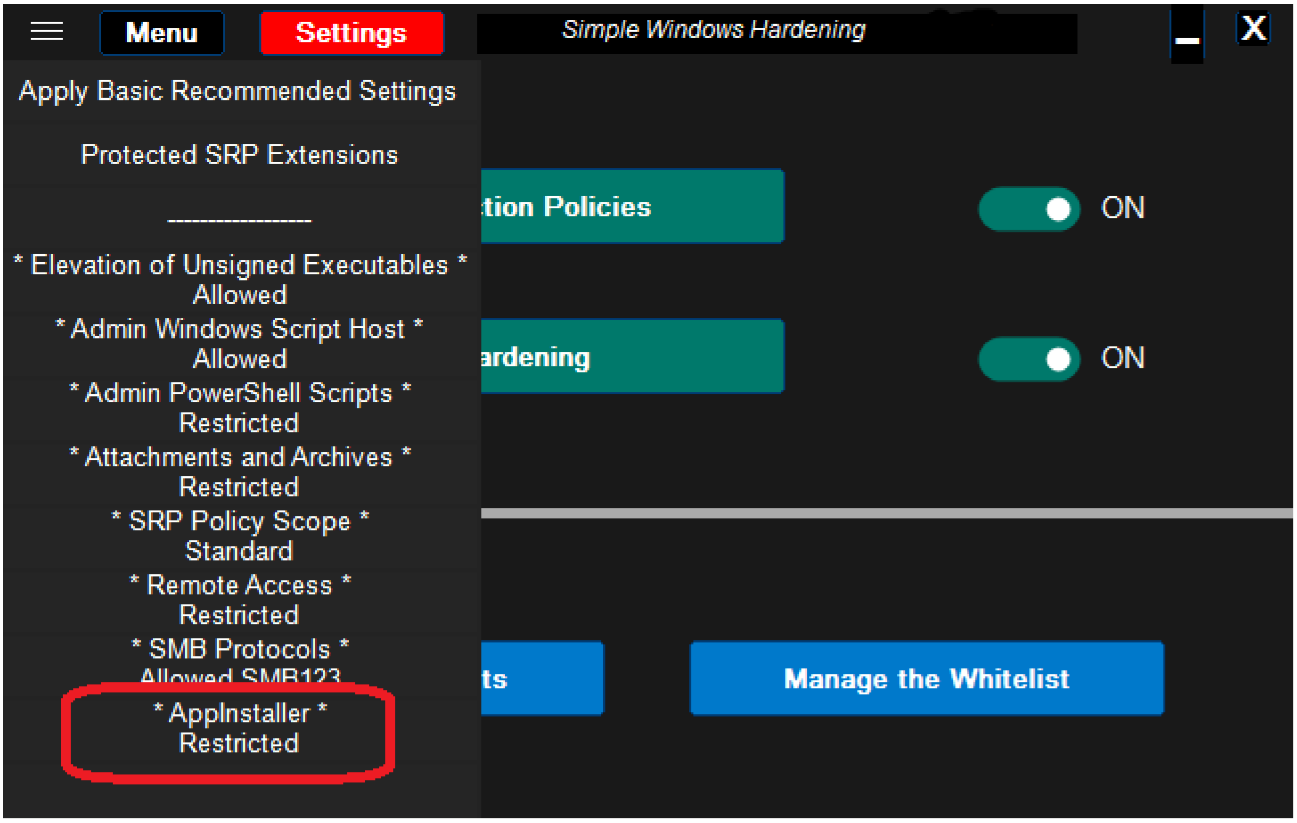
Disabling SMB 1.0, 2.0, 3.0 does not mean that these features are uninstalled from Windows. The 'Allow SMB123' setting is available only when SMB 1.0 is installed. SMB 1.0 can be installed/uninstalled as follows:
Programs and Features >> Turn Windows Features On or Off >> 'SMB 1.0/CIFS File Sharing Support'
or using the Windows system tool: OptionalFeatures.exe.

This option is usually displayed as Restricted SMB1, because the fresh installation of Windows 10/11, does not install the protocol SMB 1.0.
The SMB protocols can be used sometimes (rarely) in the home network for sharing folders/files/printers.

Anyway, in the home environment, one should try disabling SMB 1.0 (if not disabled after upgrading Windows), because it is most vulnerable. Sharing devices (network printers, NAS) mostly use SMB 2.0 or 3.0. Home users

who do not use local network devices, and sharing services in a home local network, can probably disable all SMB protocols, without any issues. In public networks, one can temporarily disable SMB to harden the system against 0-day remote exploits (like EternalBlue).

* AppInstaller *

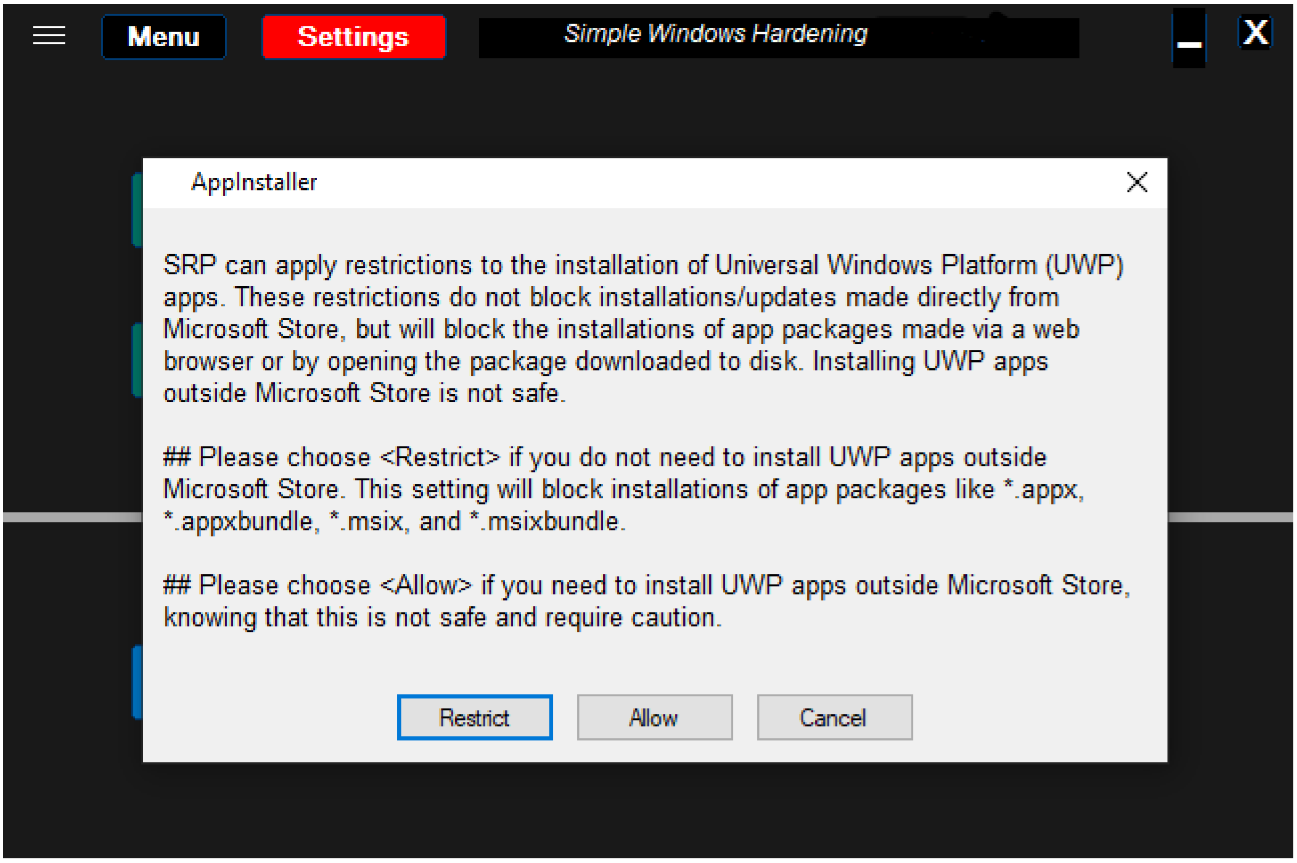


When Appinstaller is restricted, it applies some SRP restrictions to the application installations:

1. Universal Windows Platform (UWP) app installations are allowed only via Microsoft Store.
2. Desktop application installations are not allowed via Microsoft Store.

This will block the installations/updates of UWP app packages (*.appx, *.msix, *.appxbundle, and *.msixbundle) done via a web browser or by opening the package downloaded to disk. The user will be forced to use Microsoft Store to install UWP apps.

Microsoft Store expanded the offer and included the possibility to publish both UWP apps and desktop applications. So, the users can install also desktop applications directly from Microsoft Store. Yet, this possibility will be blocked when <Block AppInstaller> = ON.



It is recommendable to restrict AppInstaller because installing UWP apps outside Microsoft Store is not safe.
If you need to use UWP apps outside Microsoft Store, then the <Block AppInstaller> option can be set to OFF, while knowing that precautions should be taken when installing / updating such app packages.

When AppInstaller is restricted, SWH uses SRP to block the execution from the folder: **%ProgramFiles%\WindowsApps\Microsoft.DesktopAppInstaller***
The wildcard at the end of the folder path is required because the folder path includes the version number which can change after the update.

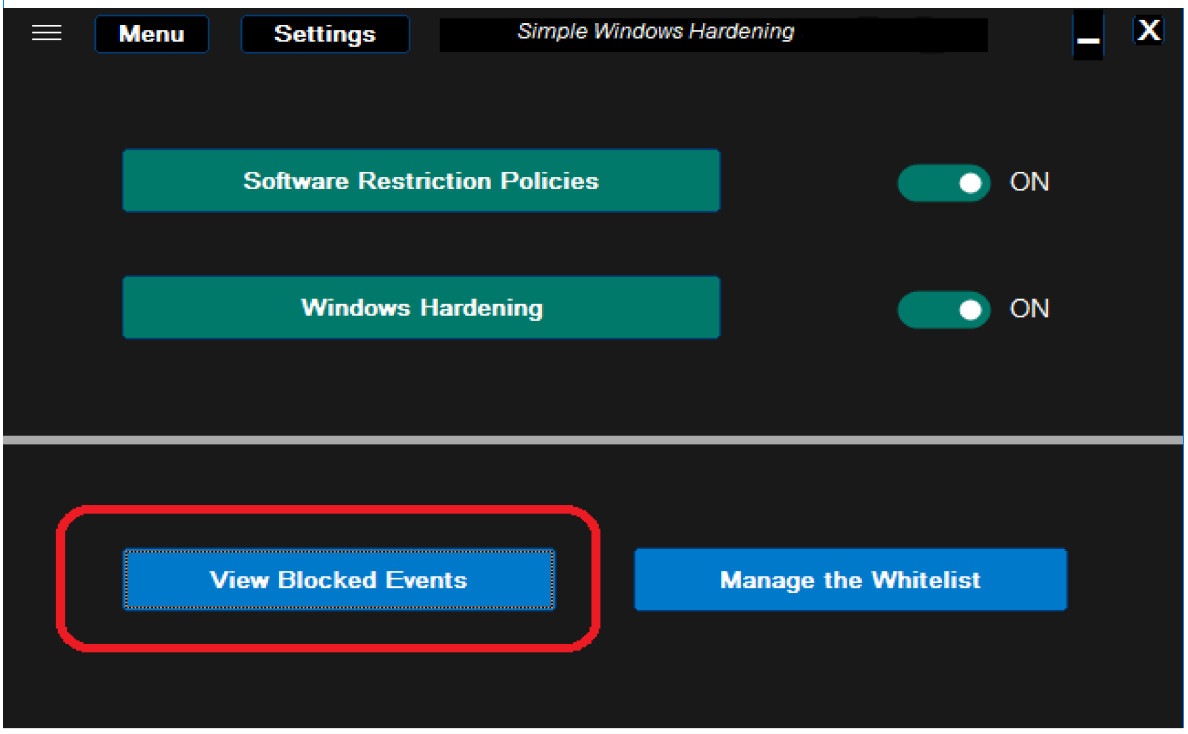
DISABLE 16-BIT APPLICATIONS

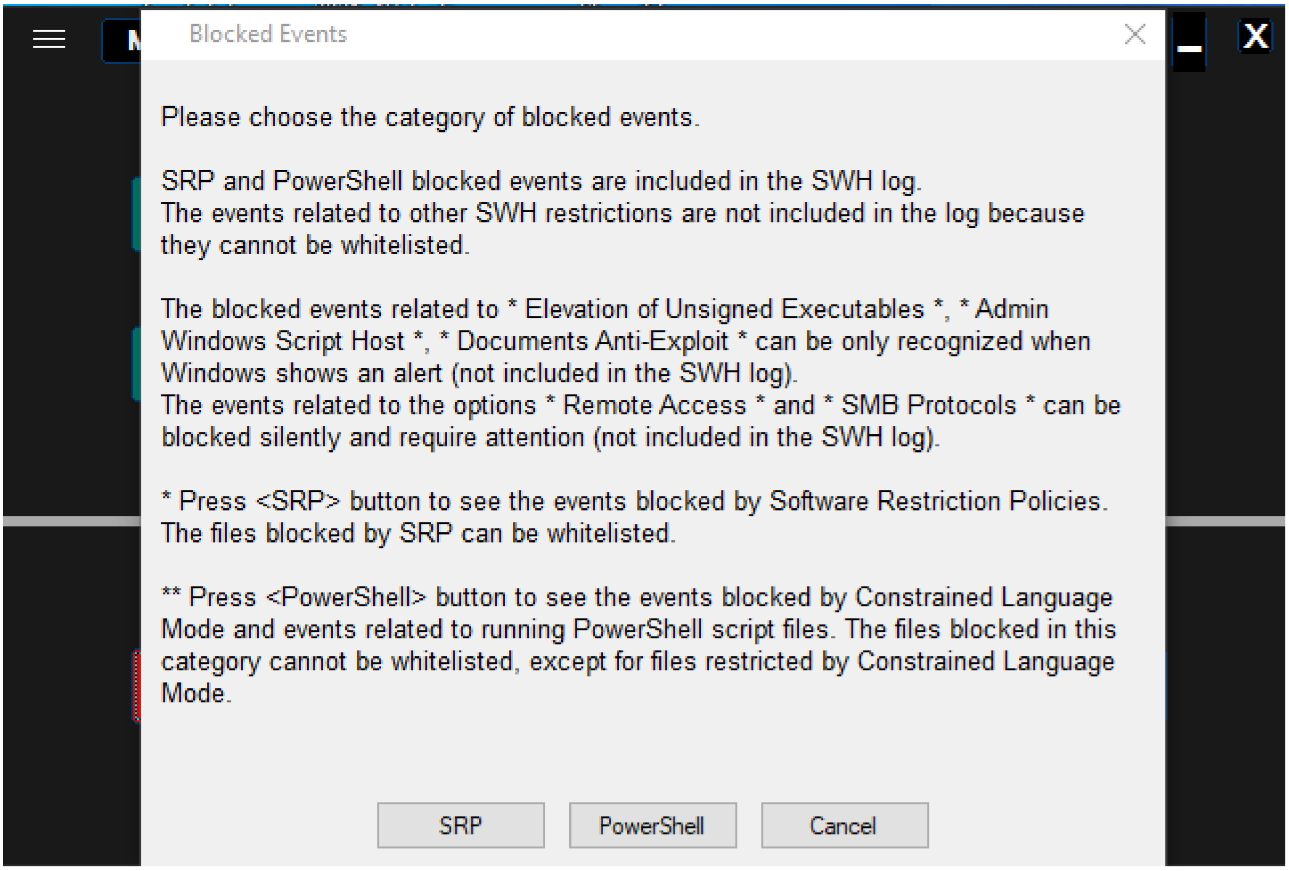
This option is non-configurable in SWH and the execution of 16-bit applications is disabled. Windows 64-bit has not got the NTVDM subsystem, so 16-bit applications cannot run (yet, there are 64-bit NTVDM alternatives available on GitHub).

CACHED LOGONS

This option is non-configurable in SWH and cached logons are Restricted. This setting is related to Active Directory Domain (ADD) credential caching. The default Windows configuration caches the last logon credentials for users who log on interactively to ADD. Caching the credentials, let users log on to the domain when no domain controllers are available or when the machine is disconnected from the network. Normally, home networks don't use Active Directory. Typically, in the home networks (even with Active Directory), the Cached Logons feature can be disabled.

View Blocked Events





When the program/script is blocked by SRP, the information is usually written in the Windows Event Log. This option uses event IDs as follows:

★ **SRP** - provider: Microsoft-Windows-SoftwareRestrictionPolicies

- 865 - restricted by policy level
- 866 - restricted by path rule
- 867 - restricted by certificate rule
- 868 - restricted by hash or zone rule
- 882 - other

★ **SRP** - provider: MsiInstaller

- 1007 - MSI (MST) file is blocked by SRP
- 1008 - MSI (MST) file is blocked due to an error in SRP

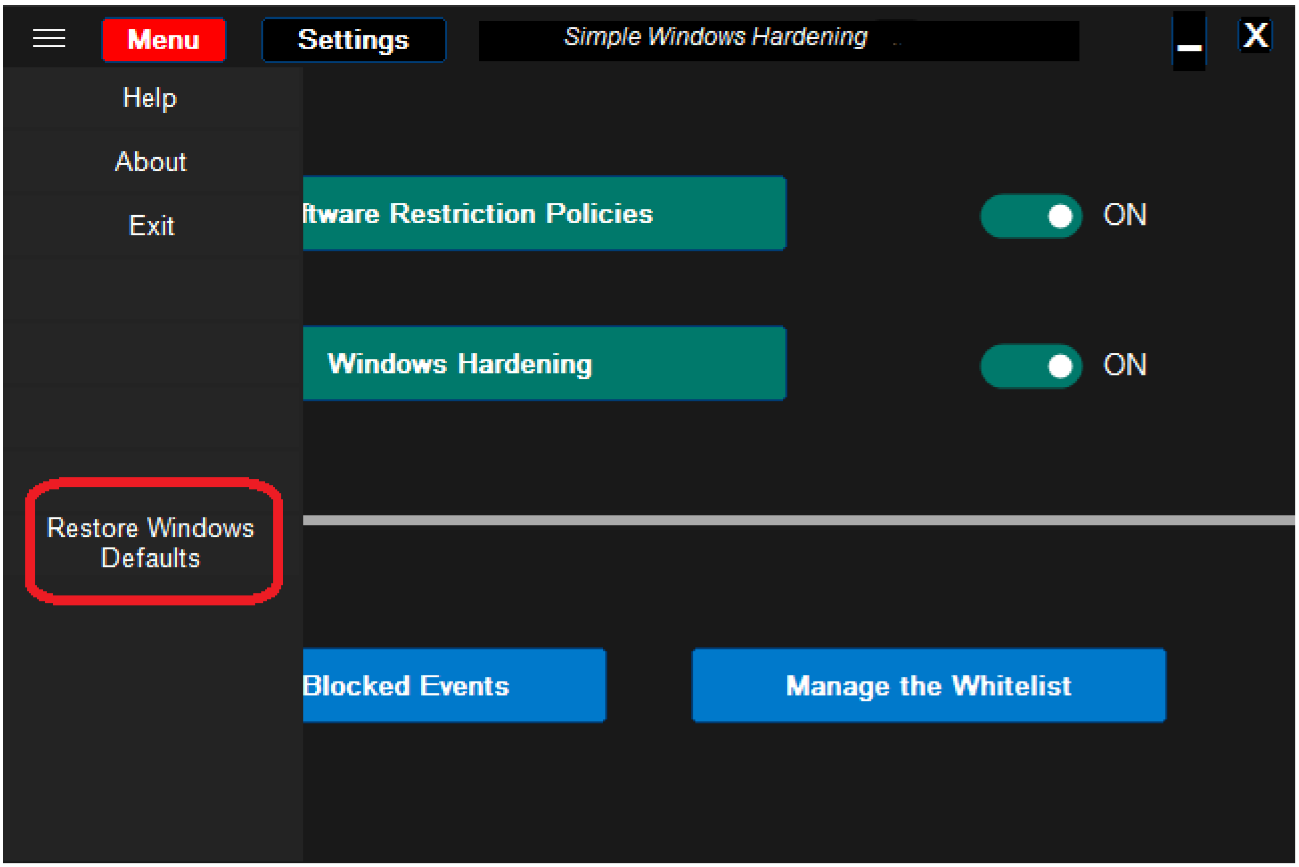
SRP events can be whitelisted.

★ **PowerShell (non-SRP)** - provider: Microsoft-Windows-PowerShell

- 4100 - PowerShell encounters an error (also when script execution is disabled via Administrator policy or default execution policy).

Only events related to PowerShell Constrained Language Mode can be whitelisted.

Restore Windows Defaults



This option allows removing SRP and all Windows Policies that might have been changed by SWH - Windows default values are applied (computer re-boot is required).
Yet, the restrictions made via external tools (like DocumentsAntiExploit) will not be removed.