Simple Windows Hardening - Manual

Version 1.0.0.0

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

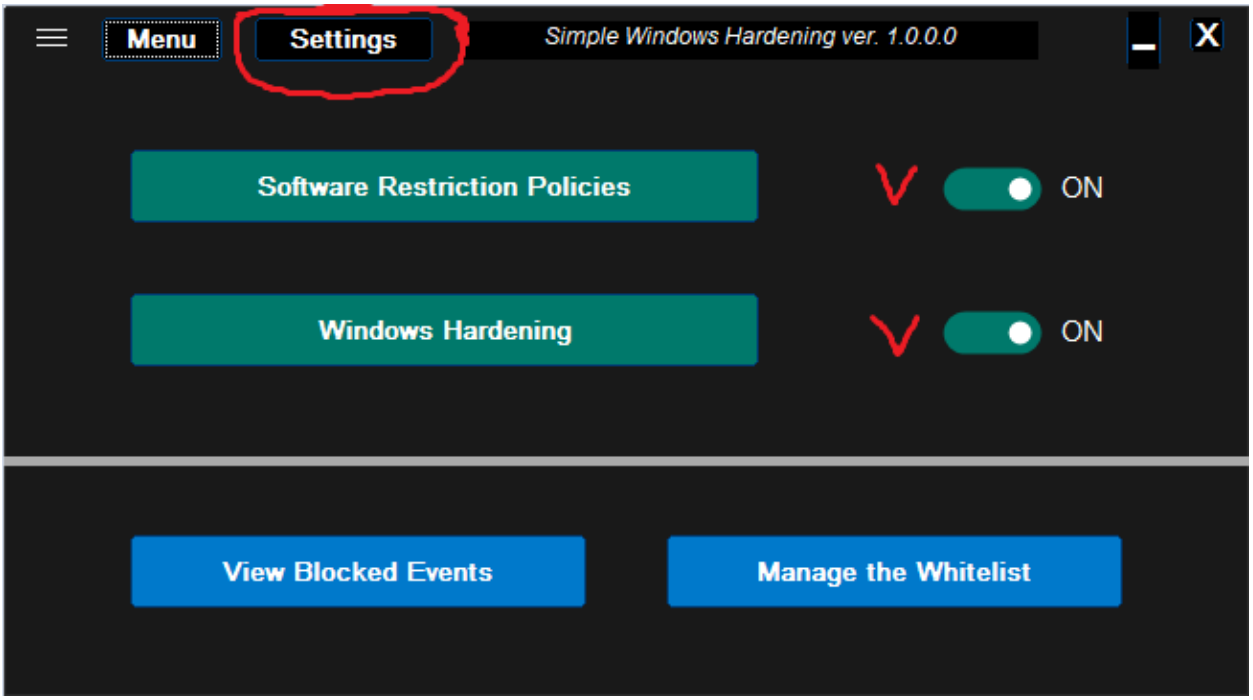
TABLE OF CONTENTS

INTRODUCTION

Simple Windows Hardening (**SWH**) is a portable application that works on Windows 10 (Home and Pro editions). It is a simple configurator (front end) of advanced security that is already present in Windows 10, but which is not activated by default. This security is based on Software Restriction Policies (SRP) and some useful Windows Policies. It is not intended to work as a standalone security solution, but to support antivirus by reducing the attack surface in the home environment. After the initial configuration made via SWH, it can be closed and all protection comes from the Windows built-in features.

SWH application is a simplified version of Hard_Configurator. When running **SWH**, the below Hard_Configurator restrictions are set to Windows default values and cannot be configured:
<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 will apply the Hard_Configurator Windows_10_Basic_Recommended_Settings (without Forced SmartScreen). These settings can be modified (in a limited way) in **SWH**, because sometimes on some computers they should be allowed for usability.



The restrictions made by **SWH** 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. So, the EXE and MSI files are not restricted in **SWH**, except when executed from archives and email clients. But, scripts, shortcuts, and other files with unsafe extensions are restricted. Such a setup can be very efficient because nowadays, most initial vectors of attack are not related to EXE or MSI files, but other files are used instead.

THE EXE / MSI 0-DAY MALWARE.

The SWH application does not apply restrictions to EXE and MSI files, because these files are often used to install/update applications. Nowadays, many antivirus solutions have very good detection of such files, as compared to the detection of scripts. But still, the antivirus proactive features can have a problem with 0-day malware. In the home environment, the main delivery vectors of 0-day malware are spam emails and flash drives (USB drives).

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 user can consider the **RunBySmartScreen** tool. 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 the 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 fi-

le. After one day most of the malicious links are dead and most of the 0-day malware are properly detected by a good antivirus.

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 before running SWH.

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. You can use blue buttons **View Blocked Events** and **Manage the Whitelist** 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

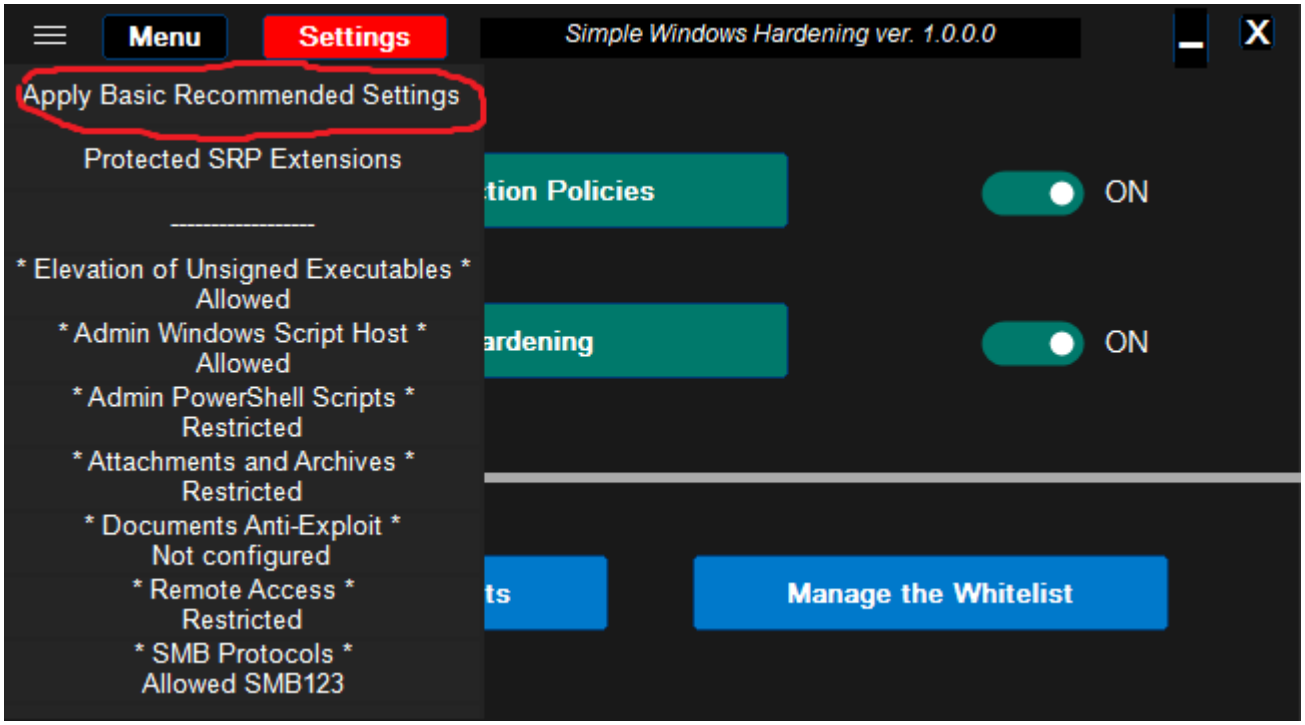
Windows built-in SRP is incompatible with Child Account activated on Windows 10 via Microsoft Family Safety. Such an account disables most SRP restrictions. This issue is persistent even after removing the Child Account. To recover SRP functionality, Windows has to be refreshed or reset.

SWH is incompatible with SRP introduced via Group Policies Object (GPO) available in Windows Pro, Education, and Enterprise editions. GPO refresh feature will overwrite the SWH settings related to SRP. So, before installing SWH, the SRP has to be removed from GPO.

SWH will also conflict with any software which uses SRP, but such applications are rare (CryptoPrevent, SBGuard, AskAdmin, Ultra Virus Killer). Before installing SWH it will be necessary to uninstall the conflicting application or it will be detected and SWH will replace the SRP settings with predefined settings.

Apply 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.

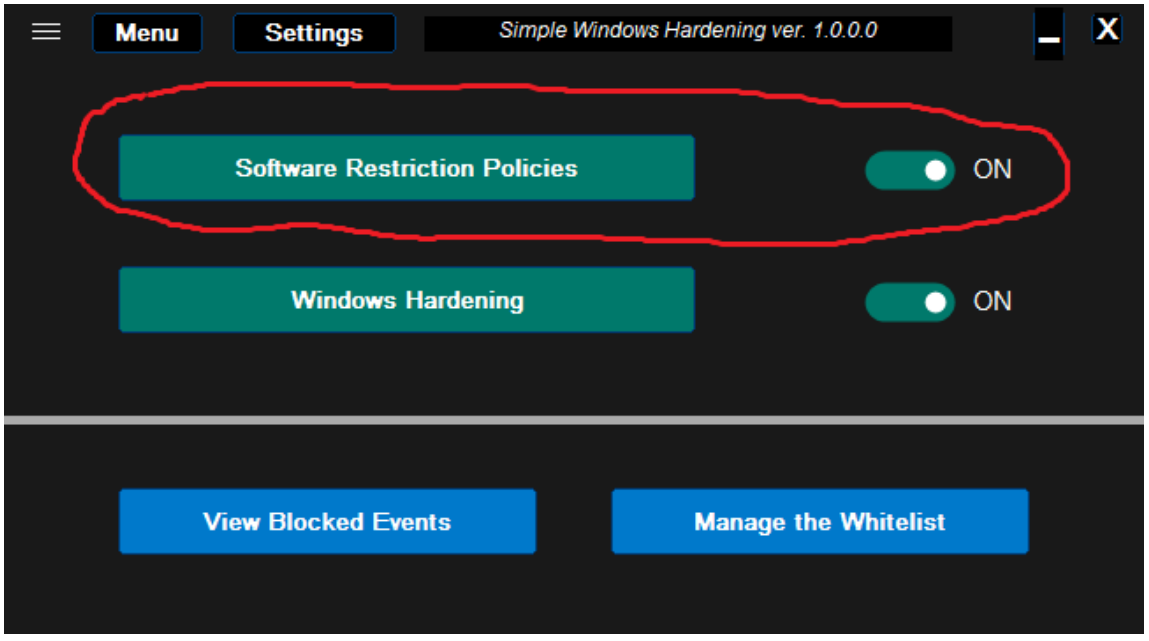
In the Basic Recommended Settings, the features are configured as follows:

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 >> Protec-

ted 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 * set to Allowed by default, but the user can set it manually to Restricted.
7. * Admin Windows Script Host * set to Allowed by default, but the user can set it manually to Restricted.
8. * Admin PowerShell Scripts * set to Restricted by default.
9. * Documents Anti-Exploit * set to "Adobe + VBA" by default.
10. * Remote Access * set to Restricted by default.
11. * SMB Protocols * set to Allowed by default, but the user can set it manually to restrict SMB1 Protocol or all SMB 1,2,3 Protocols.
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 (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 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 *).

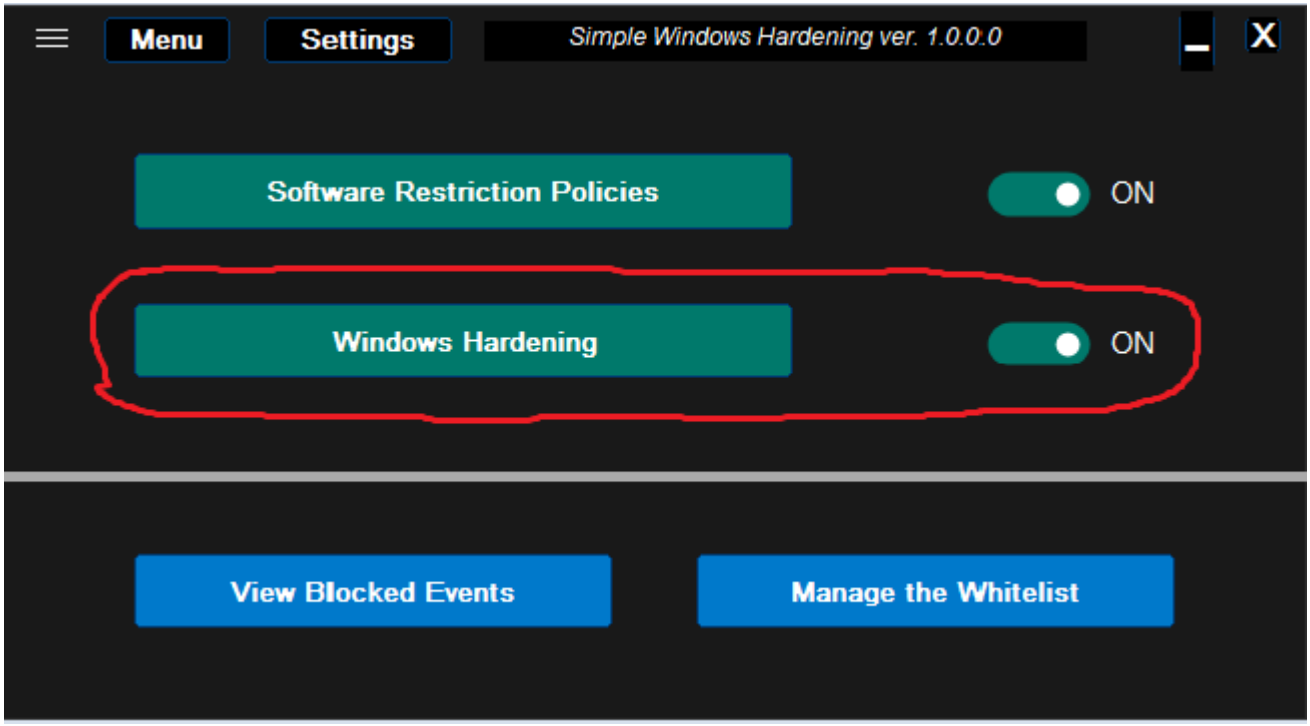
After switching OFF, all the above restrictions are remembered and removed - Windows default values are applied for them.
The user can restore the remembered restrictions by switching ON again.
When the switch is ON, the options 3-5 can be manually configured from the Settings menu.

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.

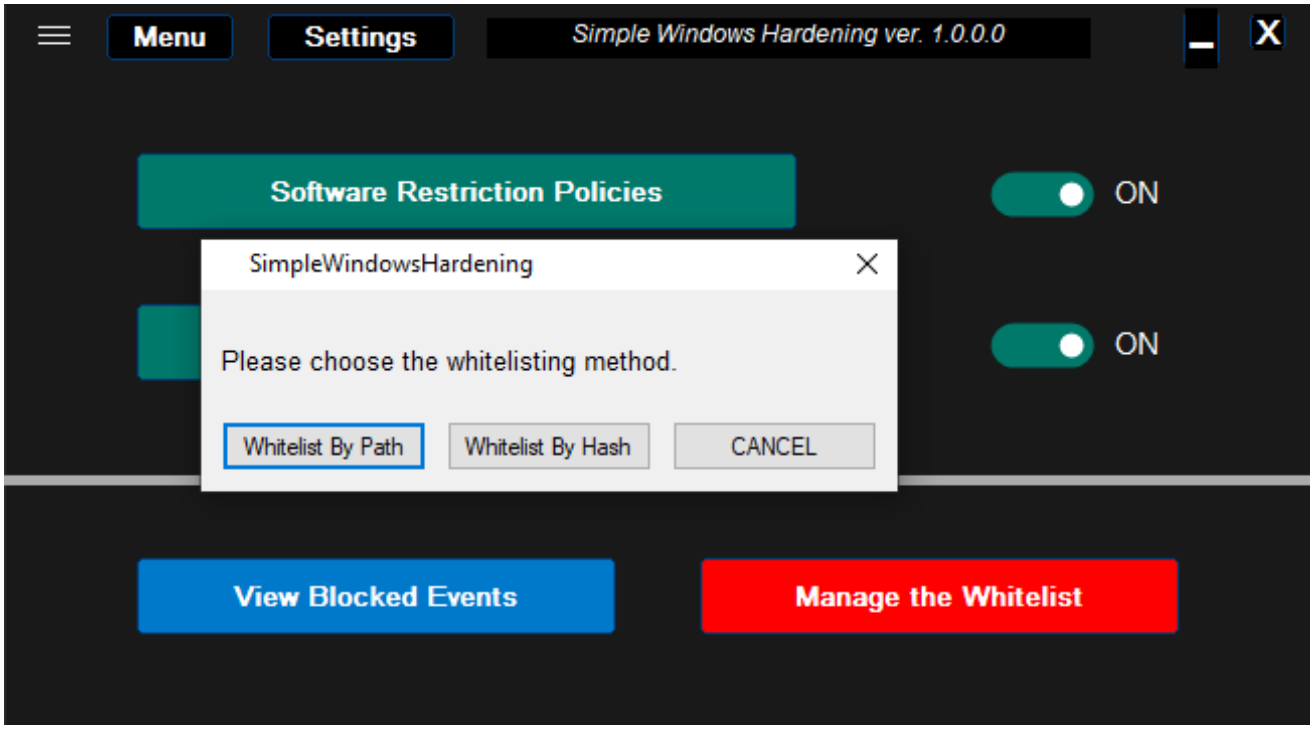
7. Cached Logons are disabled (non-configurable in SWH).
8. Execution of 16-bit processes is disabled (non-configurable in SWH).



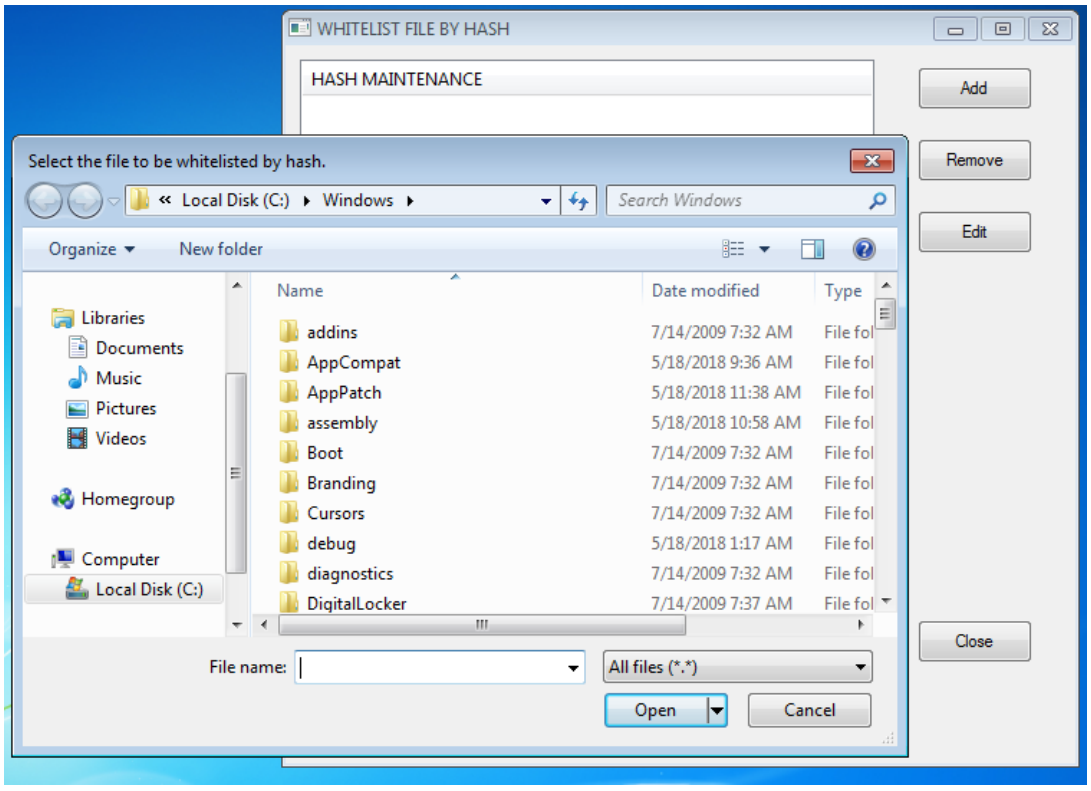
After switching OFF, all the above restrictions are remembered and removed - Windows default values are applied for them. The user can restore the remembered restrictions by switching ON again.
When the switch is ON, the options 1-6 can be manually configured from the Settings menu.

Manage the Whitelist

This button, can be used to whitelist the processes blocked by SRP (events ID 865-868, 882, 1007, 1008). Other blocked processes (events ID 1000 and 4100) cannot be whitelisted. After pressing the button, it changes color to red and the user is asked to choose <Whitelist By Path> or <Whitelist By Hash> .



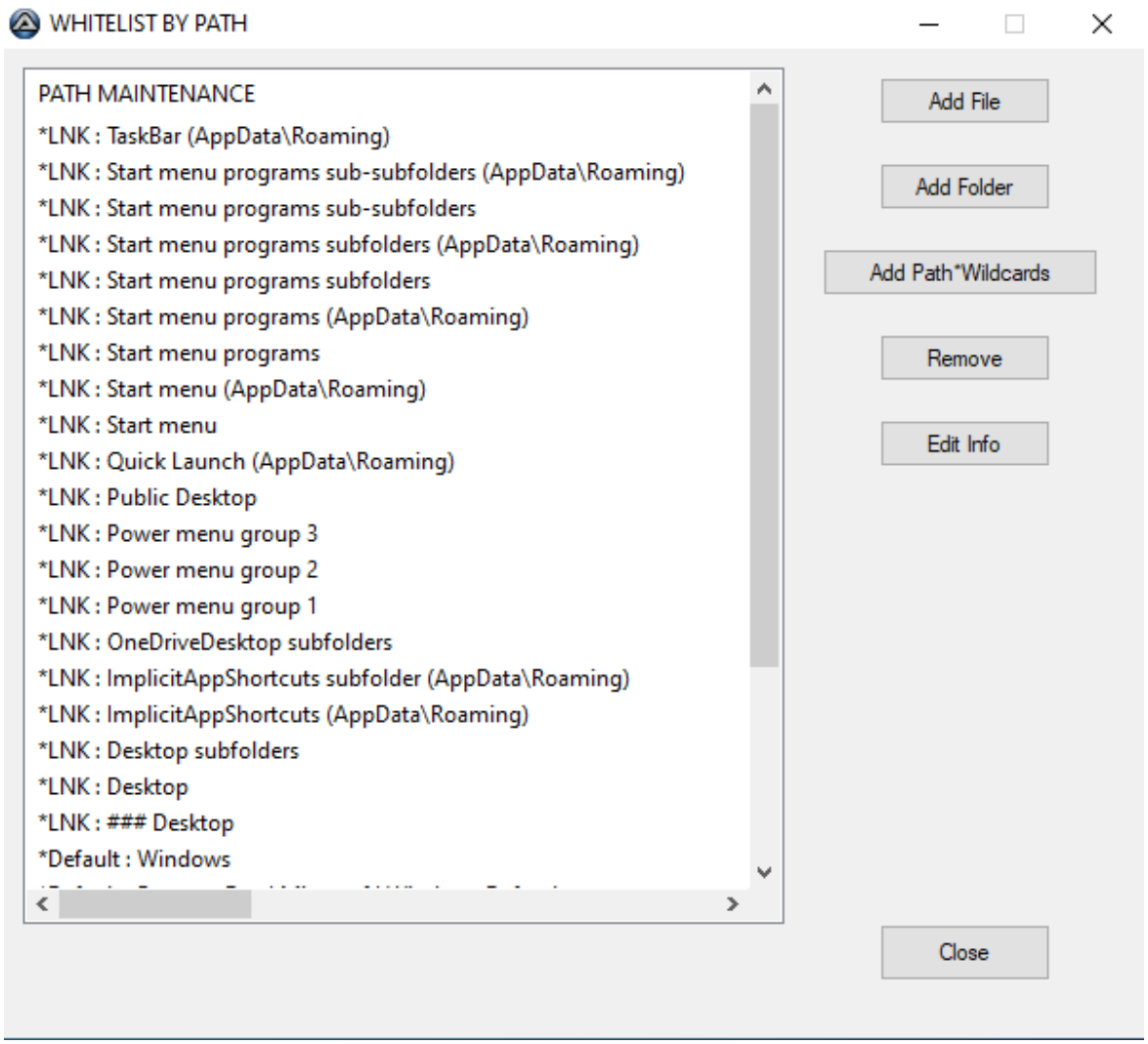
Whitelist by hash.



Sometimes files are wrapped and have to use the TEMP folder to execute (most frequently it is '%UserProfile%\AppData\Local\Temp').
If so, then the unwrapped/blocked file can be whitelisted by hash (in the TEMP folder this is safer than whitelisting by path).

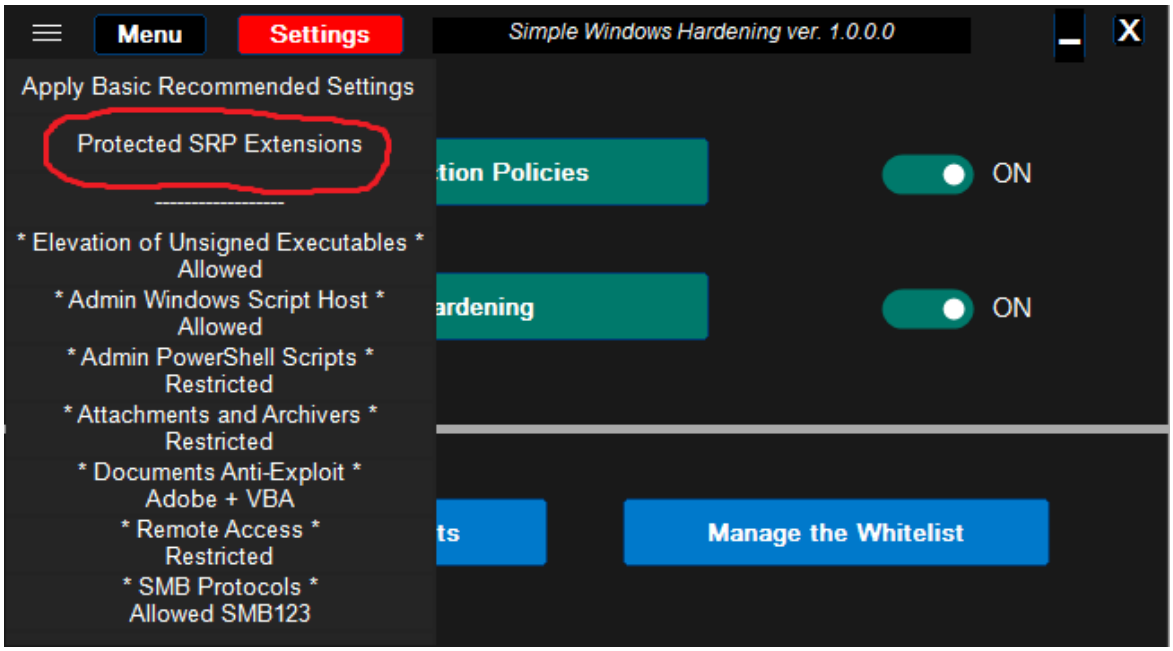
Whitelist by path.

It is very useful when running files located in UserSpace (outside of the system folders: 'Windows', 'Program Files ...'). Whitelisting has to be done with caution because SRP will not block the malware running from the whitelisted path.



Whitelisting by path a shortcut (LNK file) or a path with wildcards is only possible when using <Add Path*Wildcards> option. **This option does not support the paths with environment variables or quotation marks.**
It is forbidden to adopt environment variables when using <Add Path*Wildcards> option to whitelist the paths!

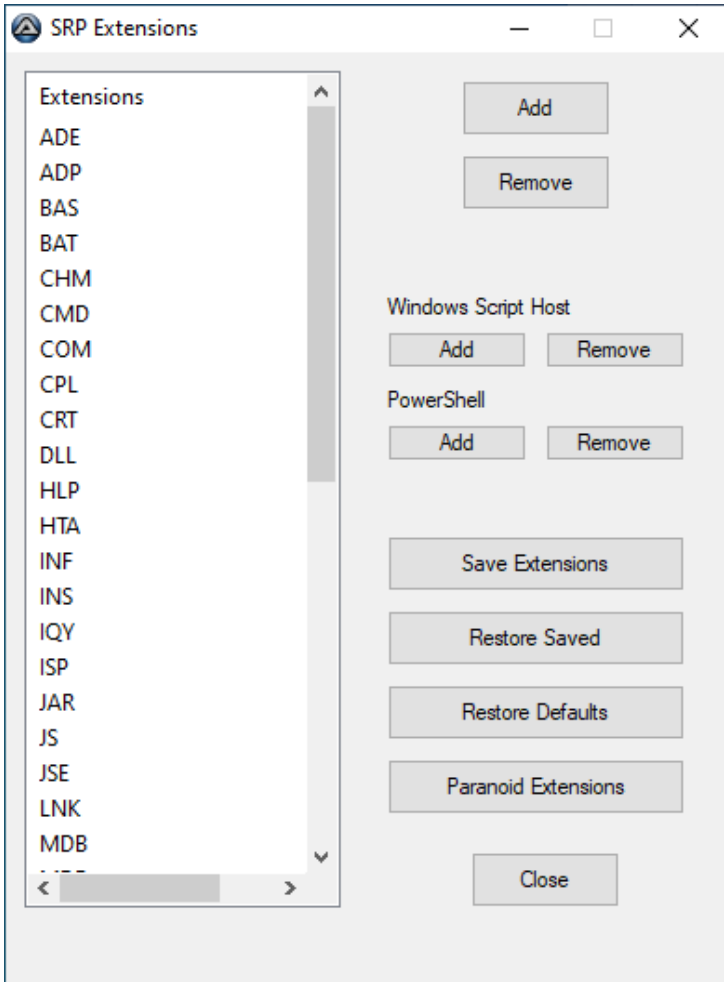
Protected SRP Extensions



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

The default extensions are as follows: ADE, ADP, BAS, BAT, CHM, CMD, COM, CPL, CRT, DLL, HLP, HTA, INF, INS, IQY, ISP, JAR, JS, JSE, LNK, MDB, MDE, MSC, MSP, MST, OCX, PCD, PIF, REG, SCR, SCT, SETTINGCONTENT-M, SHS, URL, VB, VBE, VBS, WS, WSC, WSF, WSH.

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 (over 250 entries), which were abused in the wild to exploit Windows or MS Office. It can be used to protect casual users.

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**.

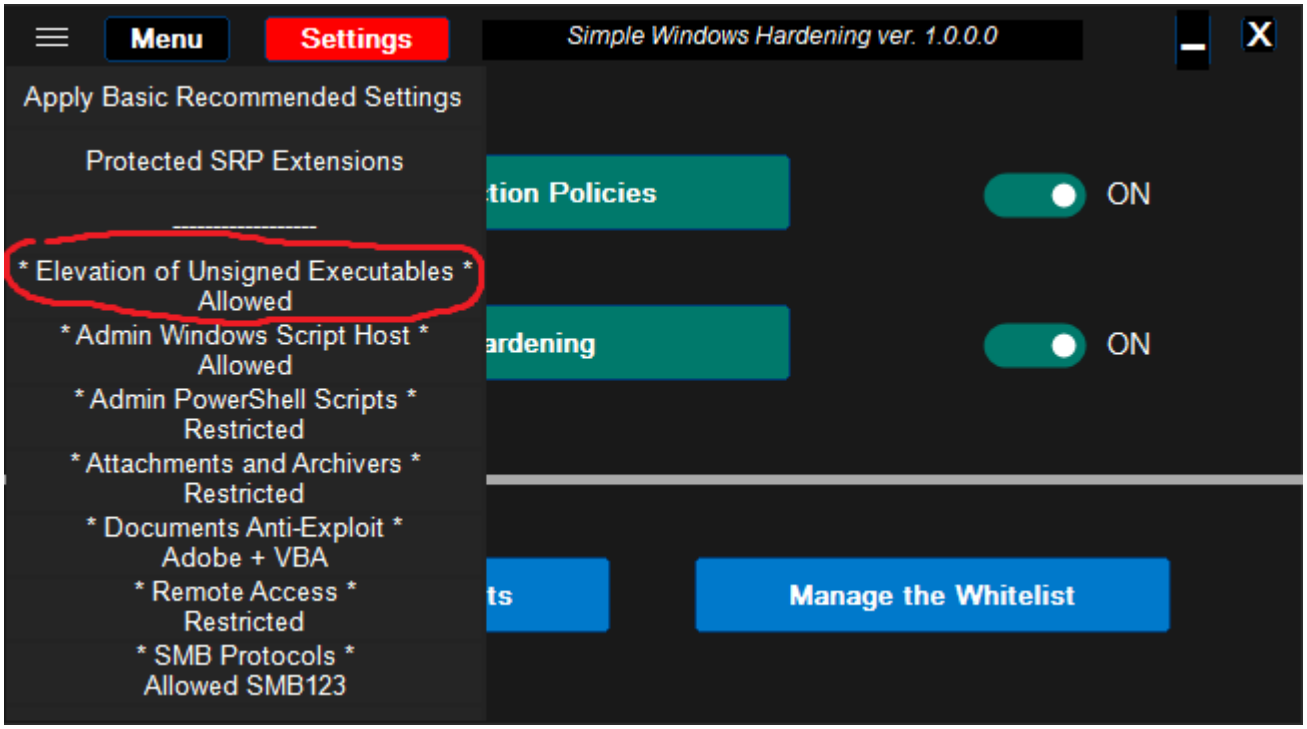
PROTECT SHORTCUTS

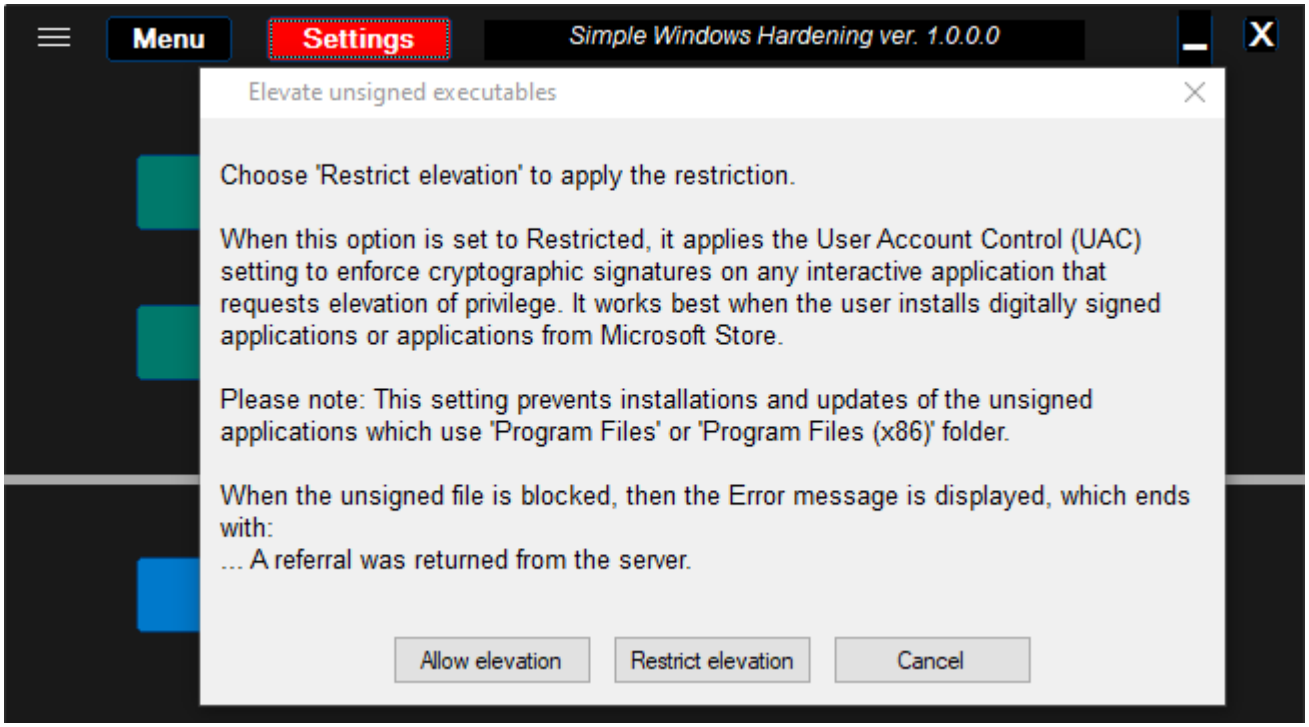
The SWH restrictions prevent the execution of shortcuts in UserSpace.
Shortcuts can be executed when:

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).

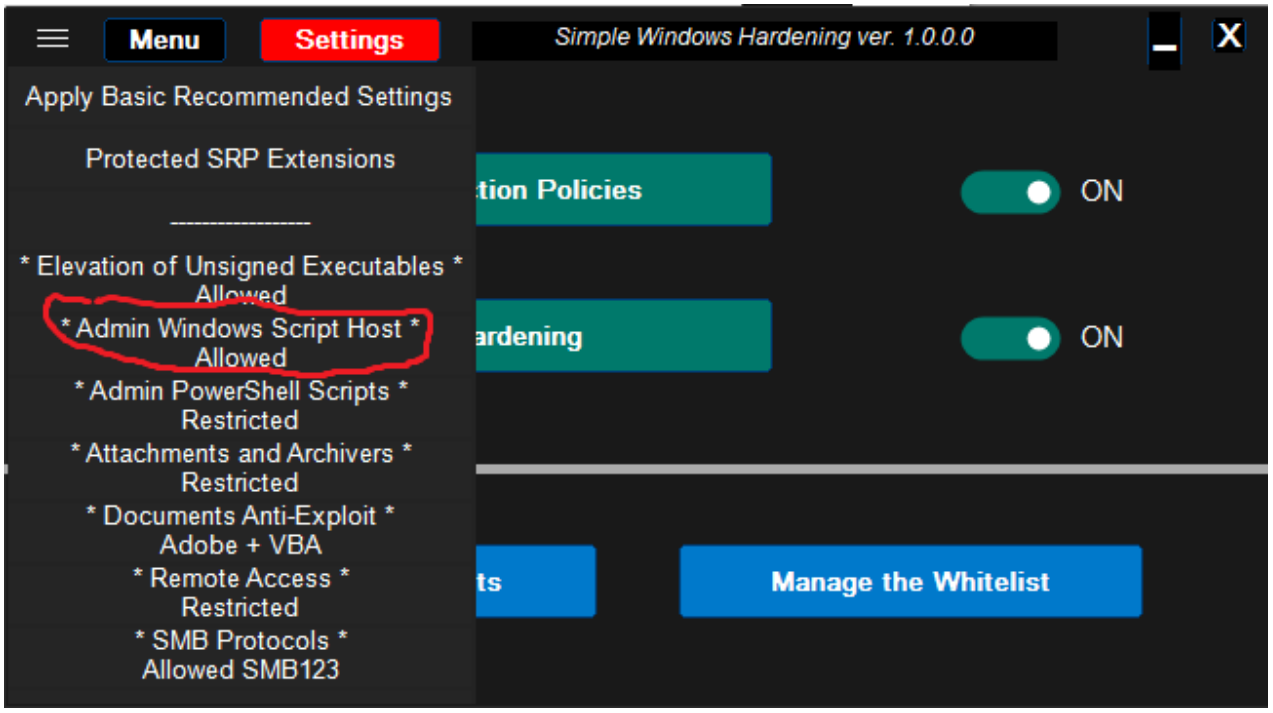
This restriction works best when the user installs digitally signed applications, or unsigned applications which do not require Administrative rights.

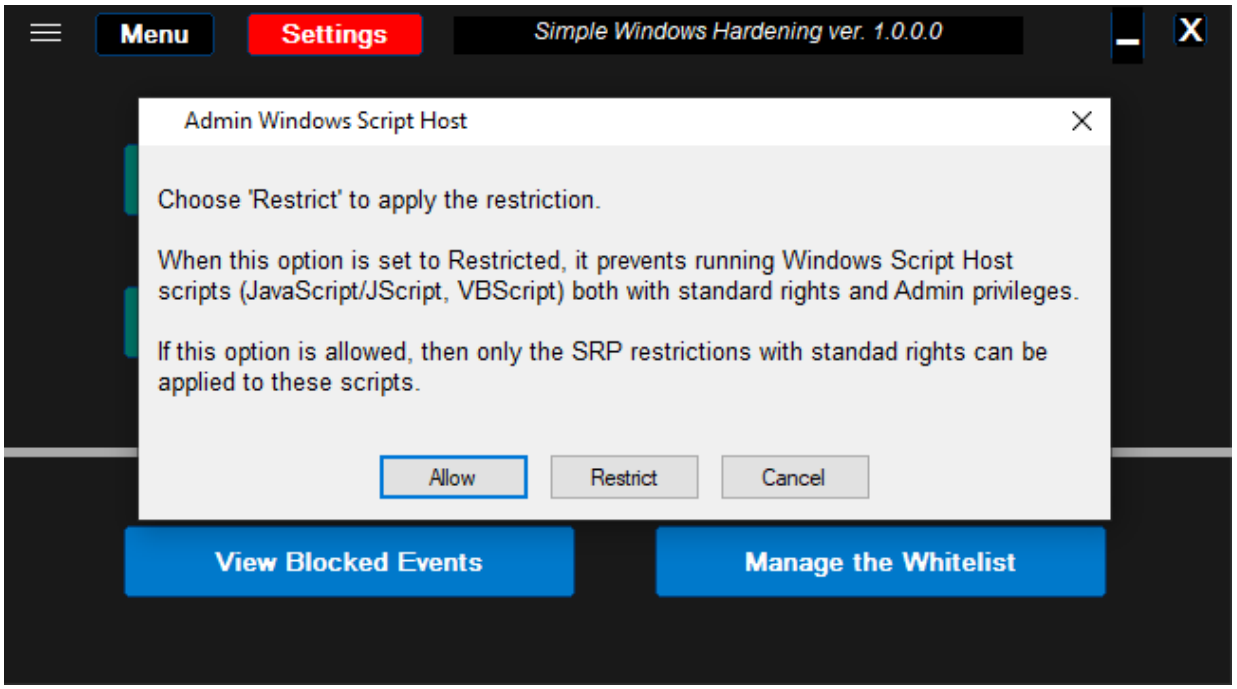
When the unsigned file is blocked, then the Error message is displayed, which ends with: ***"... A referral was returned from the server".***

* 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.

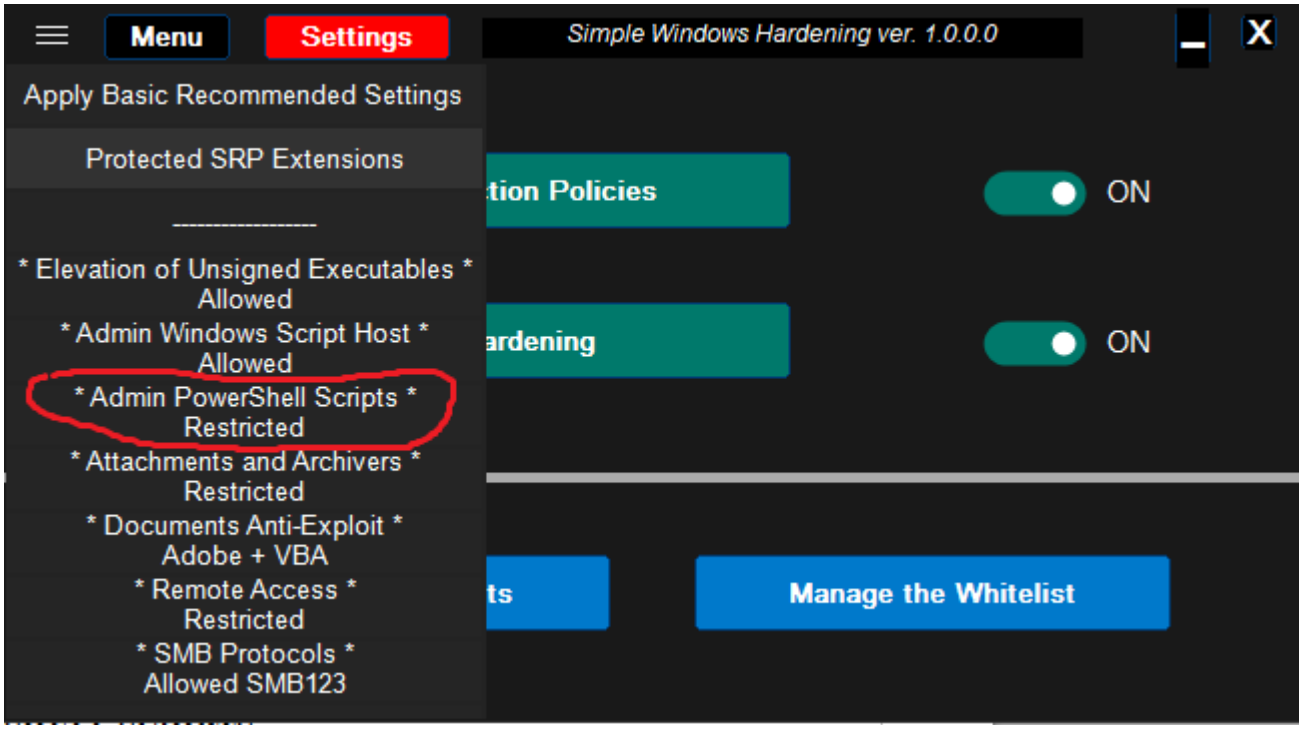
This option is not Restricted in the SWH default settings, because Windows Script Host is already restricted for standard processes by SRP (which allows whitelisting).

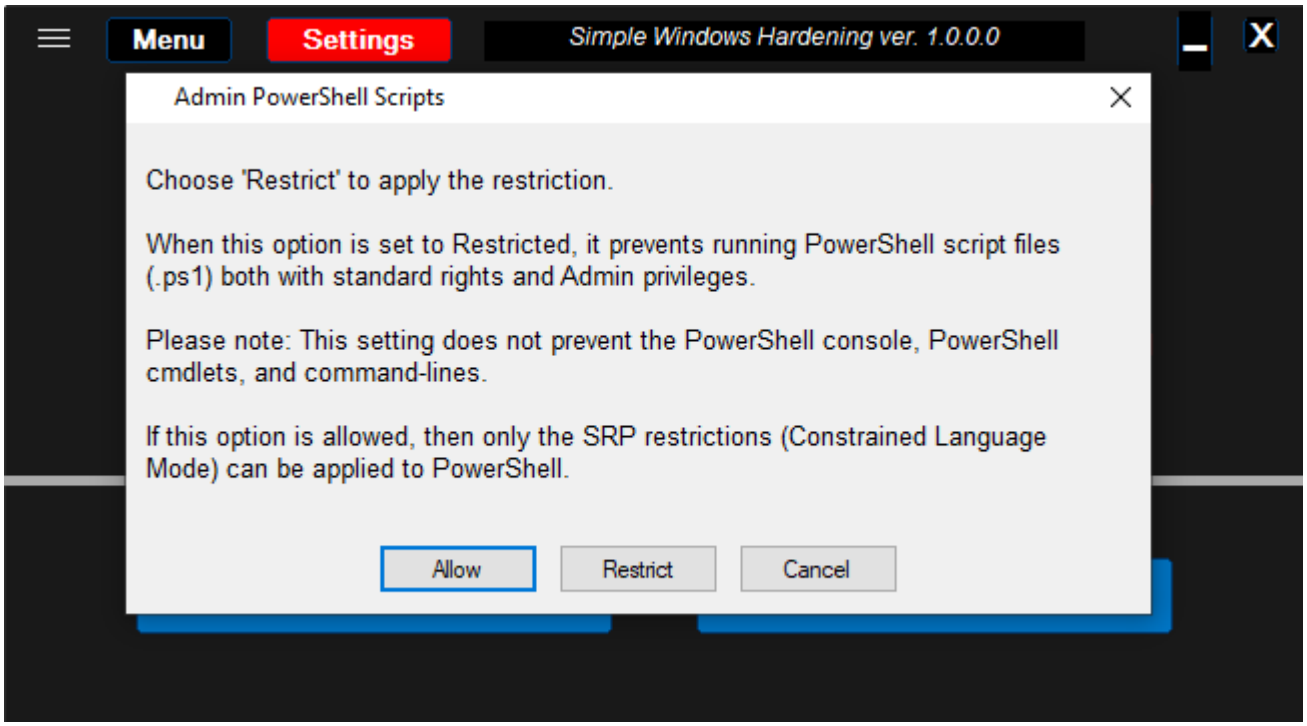




When it is Restricted, some scripts from the system folder: %SYSTEMROOT%\system32\ may be blocked at the boot time, for example: gathernetworkinfo.vbs, gathernetworkinfo.vbs, gatherwiredinfo.vbs, etc. The above scripts are not essential for the Windows system in the home environment, so they may be blocked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

* Admin PowerShell Scripts *

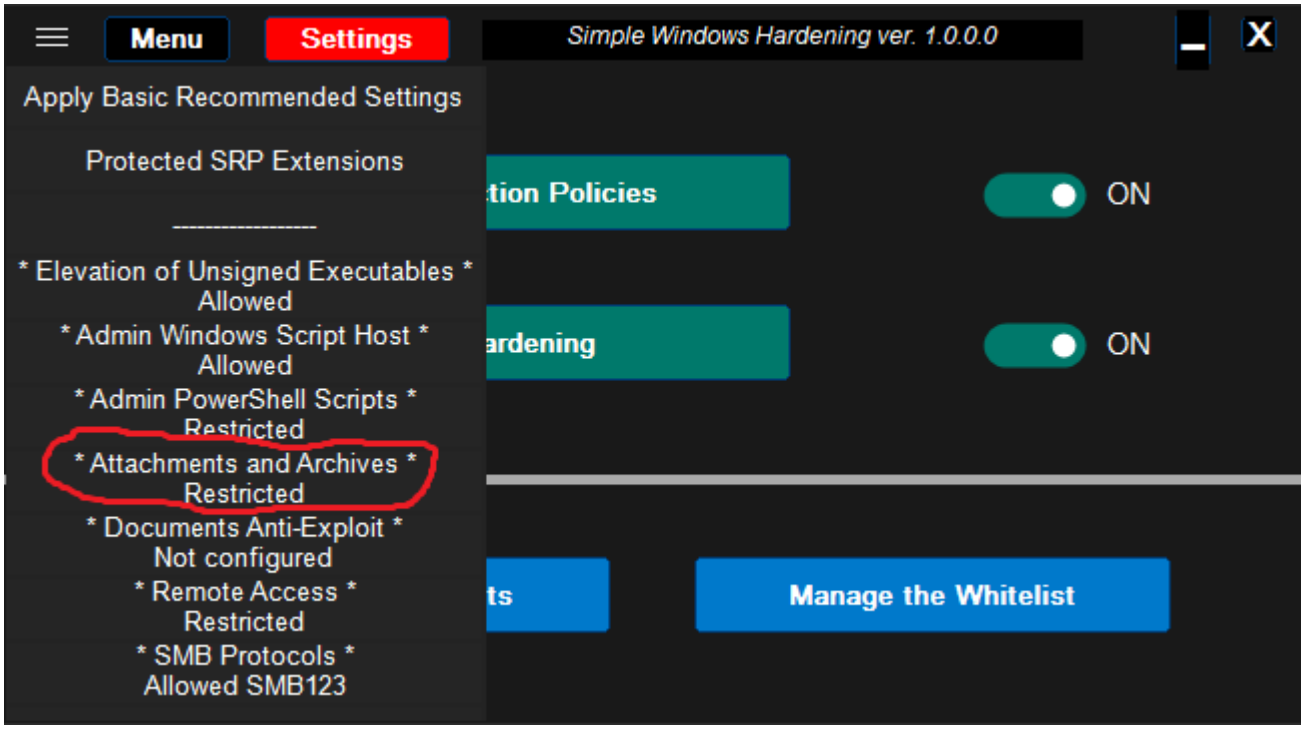




If this option is Restricted, then script file execution is blocked, but the user can still execute PowerShell **commands and cmdlets.** The cons are that PowerShell scripts cannot be whitelisted. Keep this option Restricted, because scripts are the weak point of most antimalware programs.

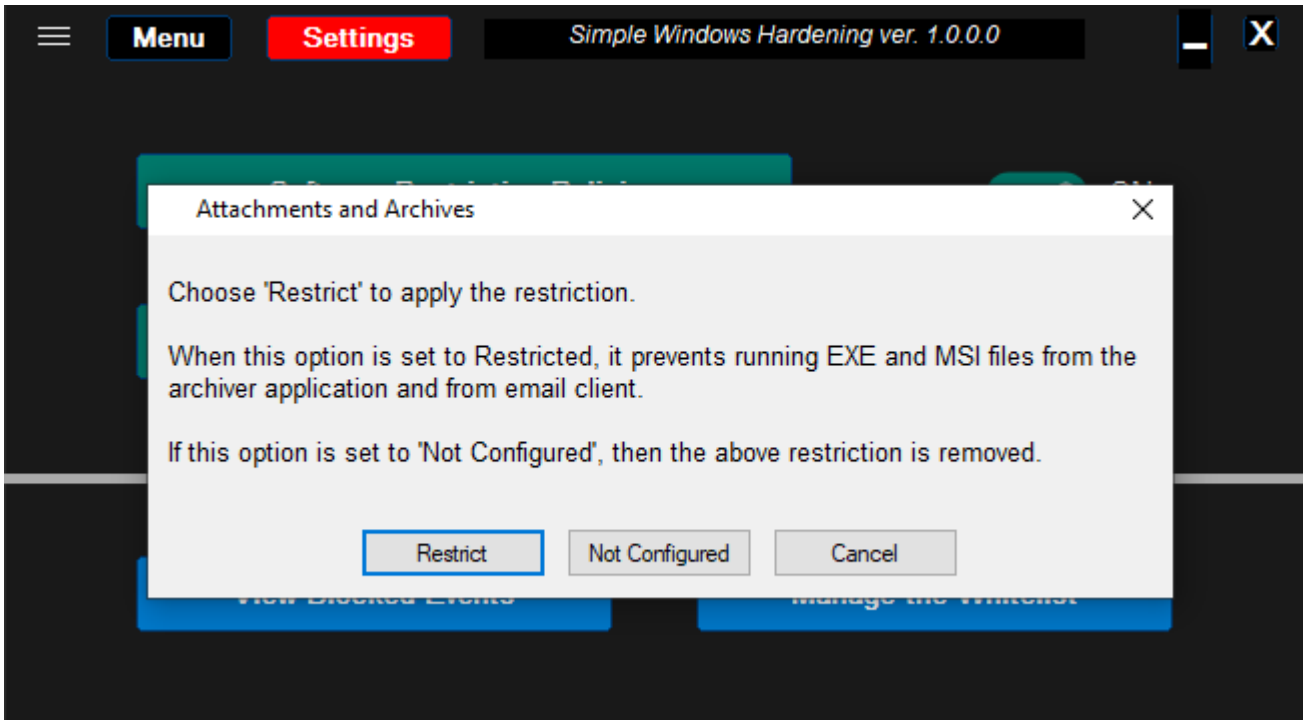
It is worth remembering that this option is stronger than Windows Execution Policy set to Restricted or adding .ps1 file extension to Protected SRP Extensions. These methods can be bypassed by using command-lines with PowerShell Sponsors (pwershell.exe or powershell_ise.exe), that will be blocked when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

* Attachments and Archives *



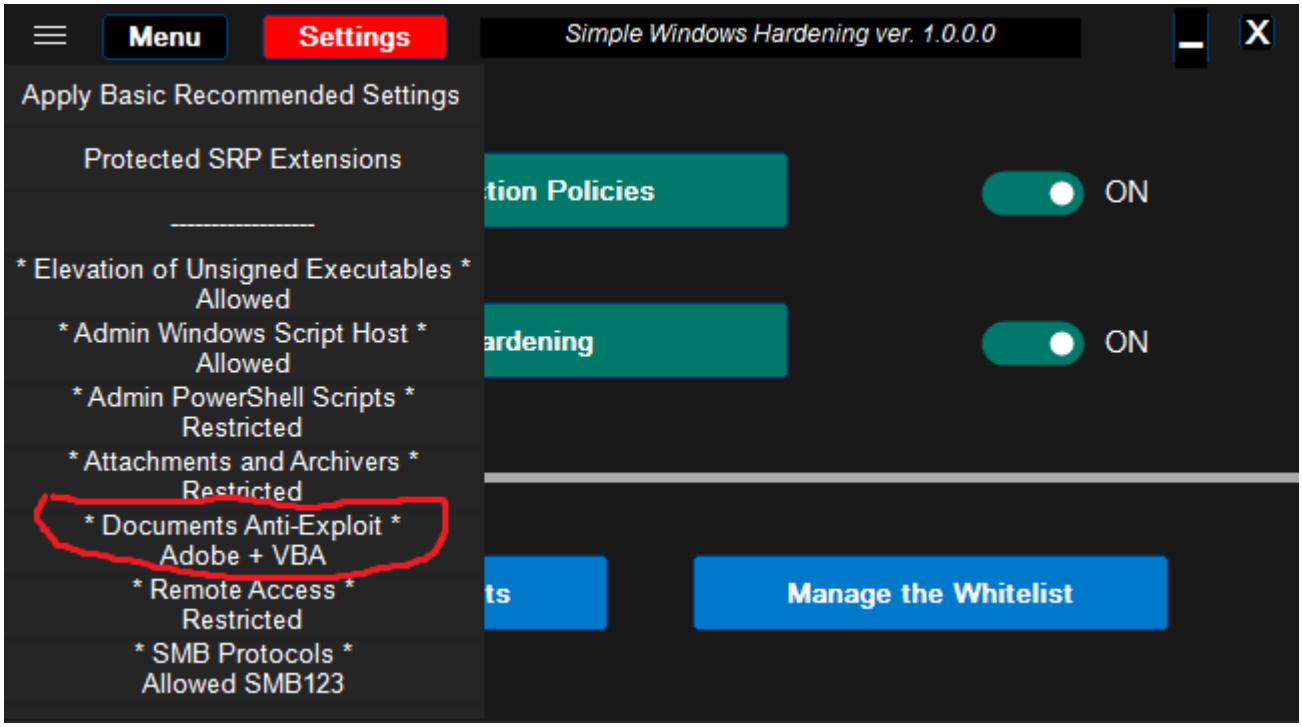
Supported archiver applications:
Windows built-in Zip, 7-Zip, ALZip, Bandizip, B1 Free Archiver, Explzh, ExpressZip, IZArc, PeaZip, PKZip, PowerArchiver, WinRar, WinZip.

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.

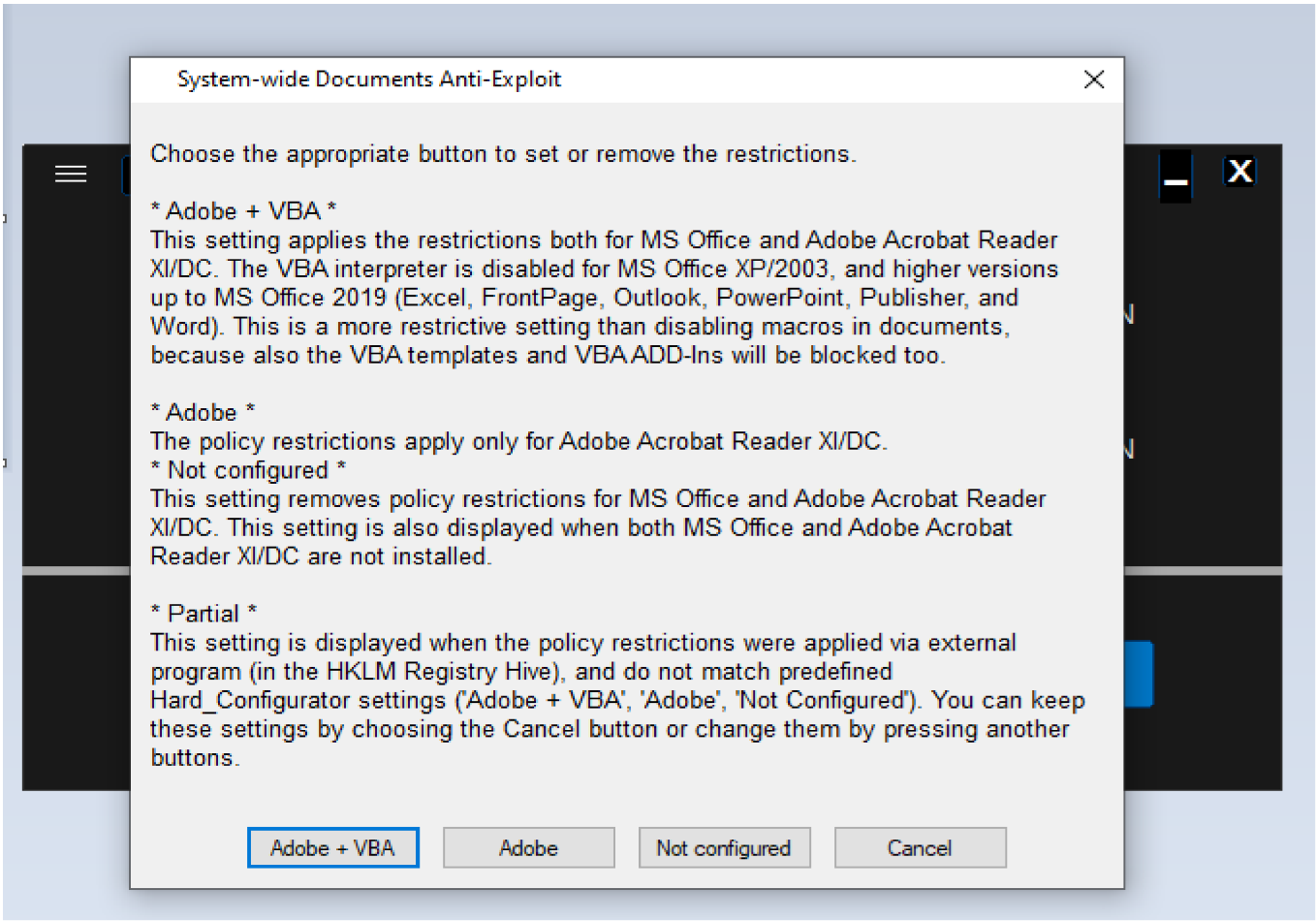
* Documents Anti-Exploit *



Important remarks.
The home users should avoid installing MS Office or Adobe Acrobat Reader, except when it is necessary. These applications have so many advanced features, that it is hardly possible to fully protect users against all vulnerabilities. They can be fully protected only in theory, because the more protection, the greater the chances to see some documents unreadable. Most home users do not use those advanced features at all, and on the contrary, the weaponized documents often use them to exploit/infect the system.

Generally, it is recommended to use online services or Universal Applications from Microsoft store (especially with **AppContainer**), for managing documents (Office Online, Google Drive, Word Mobile, Excel Mobile, PowerPoint Mobile, Adobe Reader Touch, Foxit MobilePDF, etc.).

Such popular desktop applications like Libre Office, WPS Office, SoftMaker Office are also a better choice, but they are not as safe as the above solutions. For compatibility reasons, some active content of the documents can be still functional.



Anyway, some users have no choice and are obliged to use Acrobat Reader or MS Office. So, what can they do to provide enhanced security?
MS Office 2007 and newer versions provide not so bad default protection against weaponized office documents, but the user has to avoid allowing the active content (macros, OLE, DDE, ActiveX, etc.). That is hardly possible for inexperienced users, who usually do not understand the security alerts.
The situation is even worse for Adobe Acrobat Reader, because in many cases, the active content embedded in PDF documents, is allowed by default without any alert. Furthermore, there is no possibility to silently block the active content, because Adobe Acrobat Reader shows the 'Yellow Message Bar' with an option to allow the blocked features.

What <Documents Anti-Exploit> can do:

- **This feature works well for the desktop versions of MS Office** - the versions based on the Universal Windows Platform can ignore this setting. In such a case it is possible to use DocumentsAntiExploit tool.
- The VBA interpreter in MS Office is disabled, so VBA Macros (in documents, templates, etc.), VBA Add-ins, and VBA UserForms are blocked. This may have sometimes a direct impact on the proper functioning of OLE Automation, Form/ActiveX/COM controls, etc.
- The dangerous features in Adobe Acrobat Reader DC (version from the year 2018 at least) on Windows 8.1/10 can be blocked with the 'Yellow Message Bar', and if allowed by the user, then silently mitigated in App-Container;
- The dangerous features of Adobe Acrobat Reader XI (all Windows versions) and Adobe Acrobat Reader DC (Windows 8 and prior versions) can be blocked with the 'Yellow Message Bar' (the user can allow them);
- The restrictions apply as policies for all accounts and override (but not overwrite) applications' native settings in MS Office and Adobe Acrobat Reader XI/DC;
- The restrictions cannot be modified by the user from within MS Office and Adobe Acrobat Reader XI/DC.

The available settings.

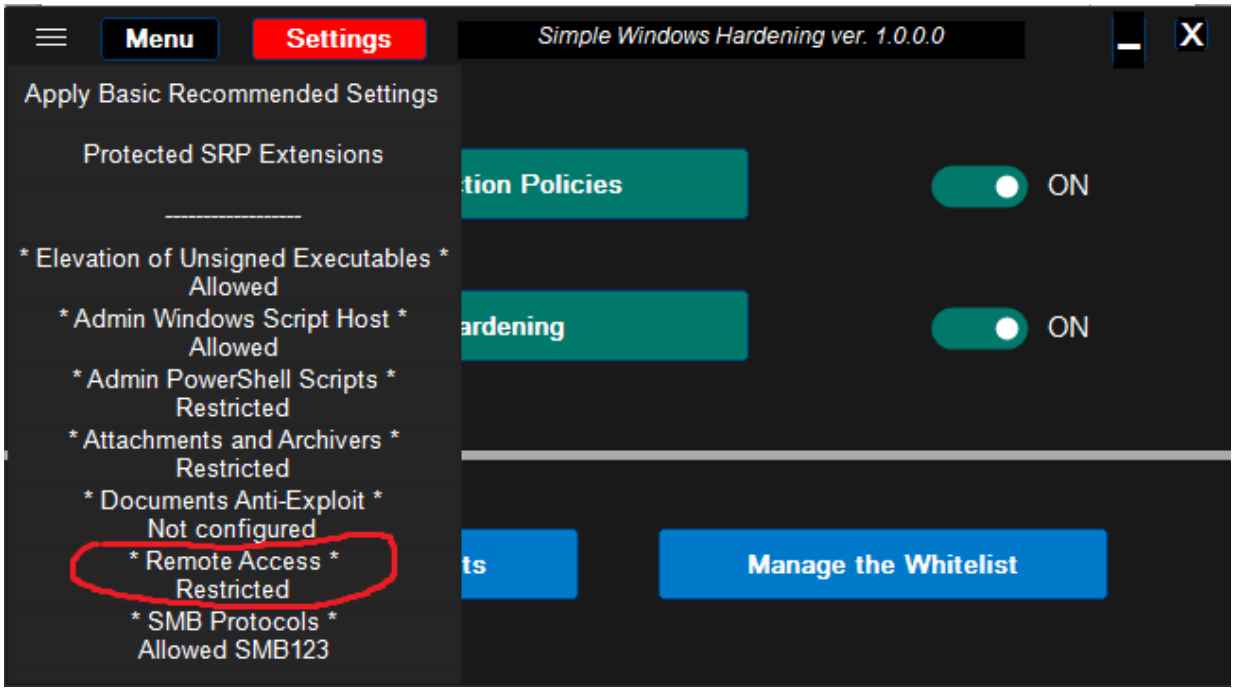
<Documents Anti-Exploit> = Not configured
Generally, the system-wide policies can override but do not overwrite non-system-wide restrictions. This setting removes policy restrictions for MS Office and Adobe Acrobat Reader XI/DC, so the non-system wide restrictions can apply (via DocumentsAntiExploit tool or from within MS Office or Adobe Acrobat Reader applications). This setting is also displayed when both MS Office and Adobe Acrobat Reader are not installed.

<Documents Anti-Exploit> = Adobe
The policy restrictions apply only for Adobe Acrobat Reader XI/DC.
This setting is recommended when MS Office is not installed and other applications are used for managing office documents.

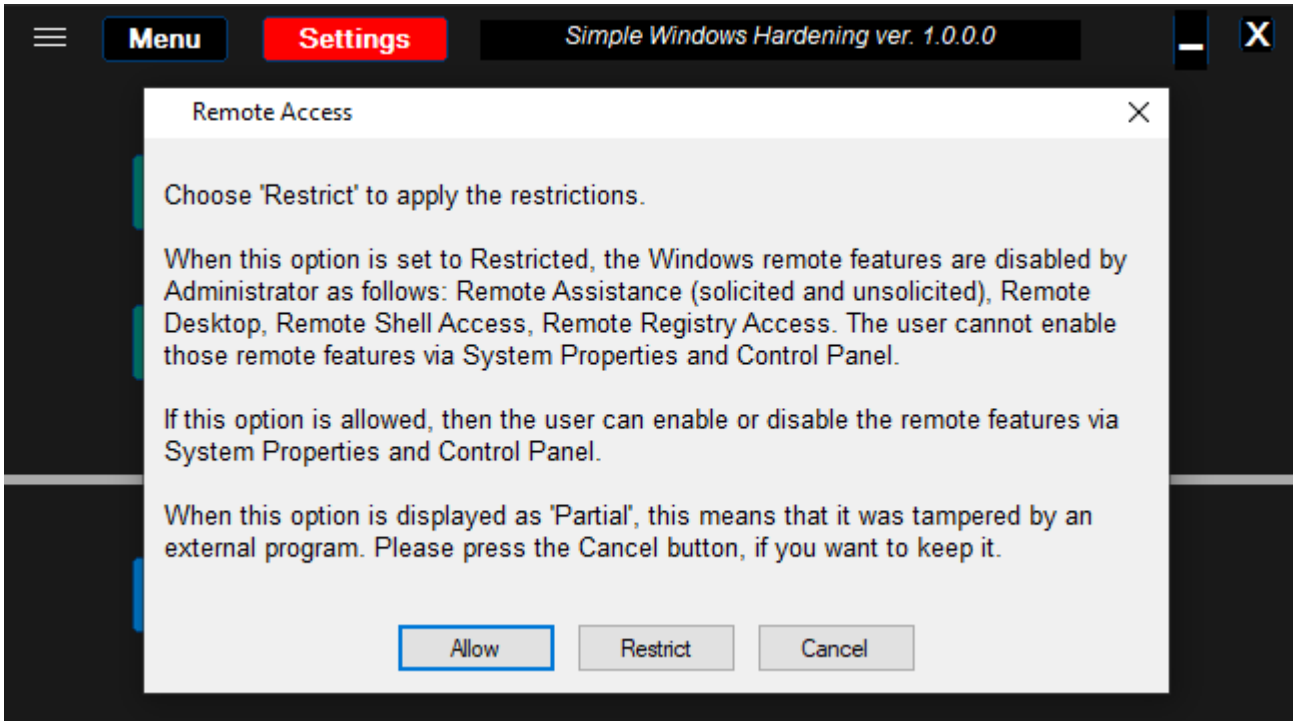
<Documents Anti-Exploit> = Adobe + VBA

This setting is recommended for anyone on Windows 10, who installed the desktop versions of MS Office and Adobe Acrobat Reader XI/DC. The VBA interpreter is disabled for MS Office XP/2003, and higher versions up to MS Office 2019 (Excel, FrontPage, Outlook, PowerPoint, Publisher, and Word). In Adobe Acrobat Reader XI/DC, the important & protective features are turned ON. The users, who require the protection against the 0-day sophisticated malware, may also consider activating Windows Defender ASR rules on Windows 10.

* Remote Access *



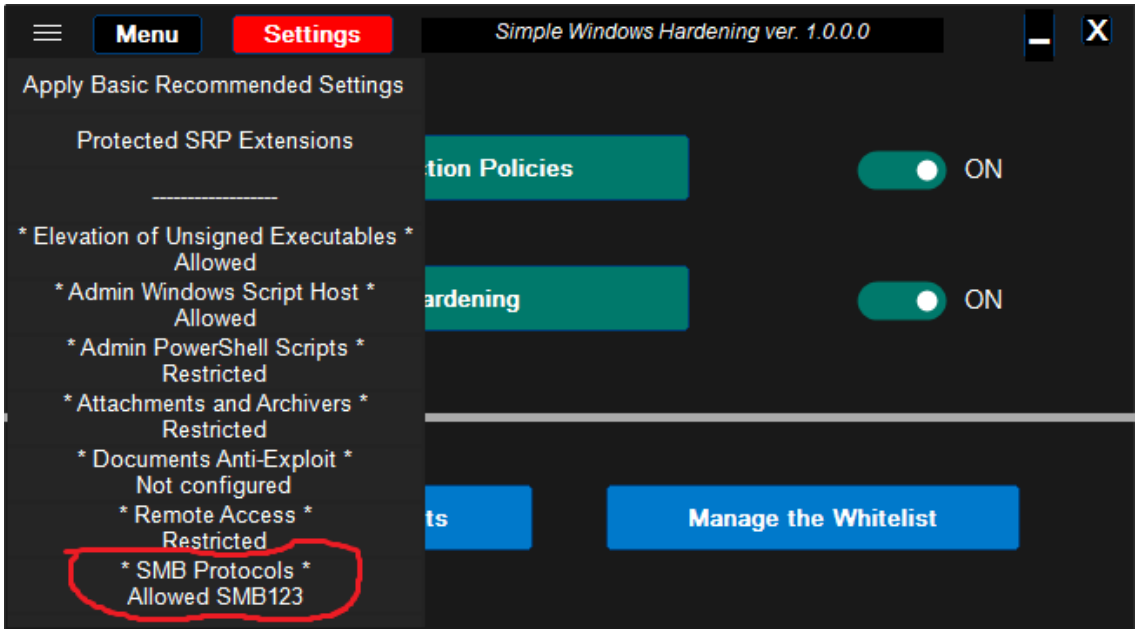
It is recommended for home users to keep <Remote Access> Restricted. The remote connections are frequently exploited by malware and hackers.
Changing this option always stops 'Remote Registry' service, if it was started.

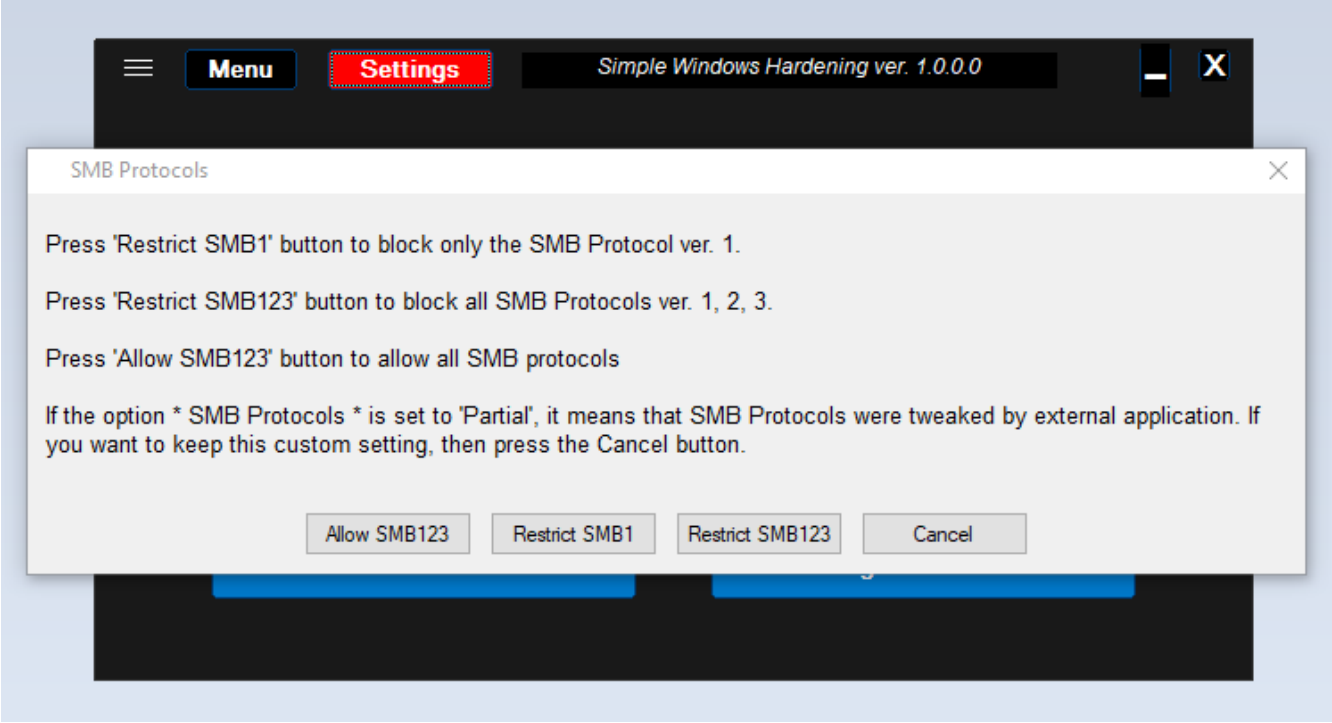


The potential problems may occur when disabling Remote Acess, for example:

“Note that print spooler and directory services replication require access through the remote registry service for certain functions to work properly. Other custom applications may also depend on remote registry access.“
http://www.blackviper.com/windows-services/remote-registry/

* SMB Protocols *





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 installations of Windows 10 do 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 networks, 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).

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 --> installation of MSI file is not permitted by SRP
- 1008 --> installation of MSI file is not permitted due to an error in SRP

★ **Non-SRP related**

Windows Script Host (provider: Windows Script Host)

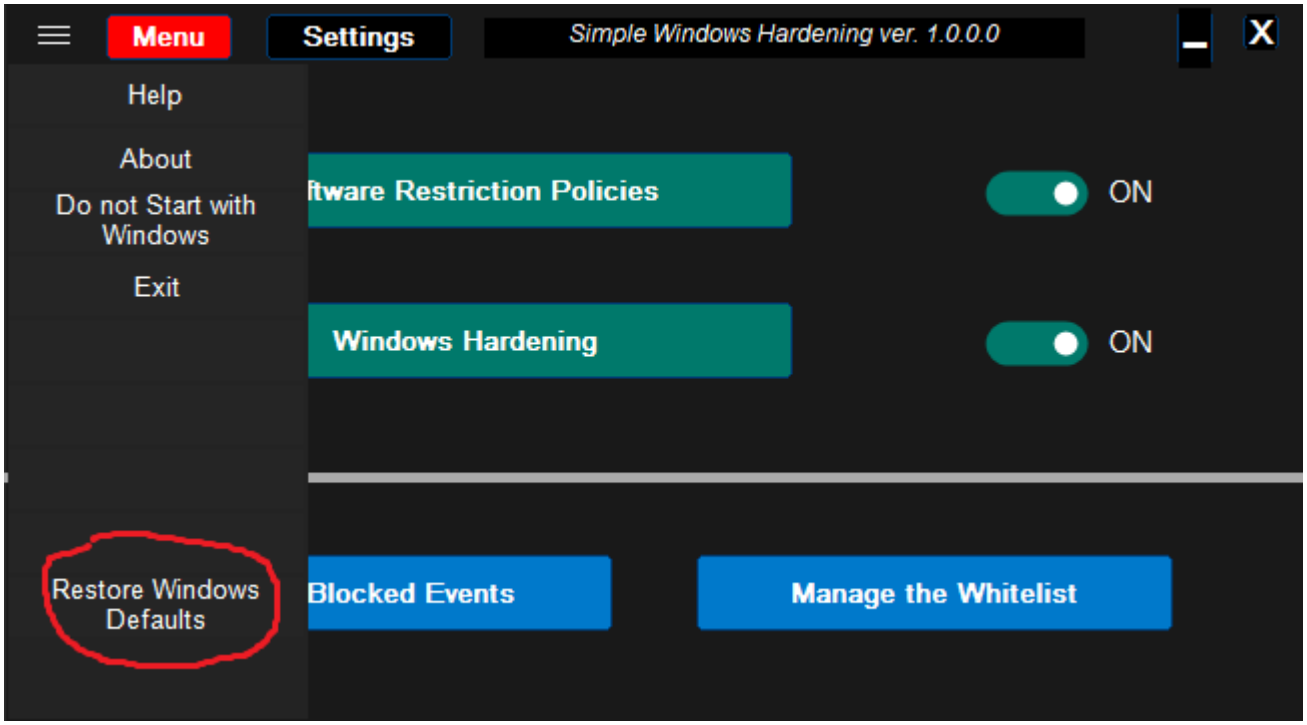
- 1000 --> Attempt to execute Windows Script Host with Administrative Rights while it is disabled

PowerShell (provider: Microsoft-Windows-PowerShell)

- 4100 --> PowerShell encounters an error (also when script execution is disabled via policy)

Only SRP events 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).