Hard_Configurator - Manual

Version 2.0.1 (December 2016)

Copyright: Andy Ful
Developer Web Page: https://github.com/AndyFul/Hard_Configurator

Distribution

This software may be freely distributed as long as no modification is made to it.

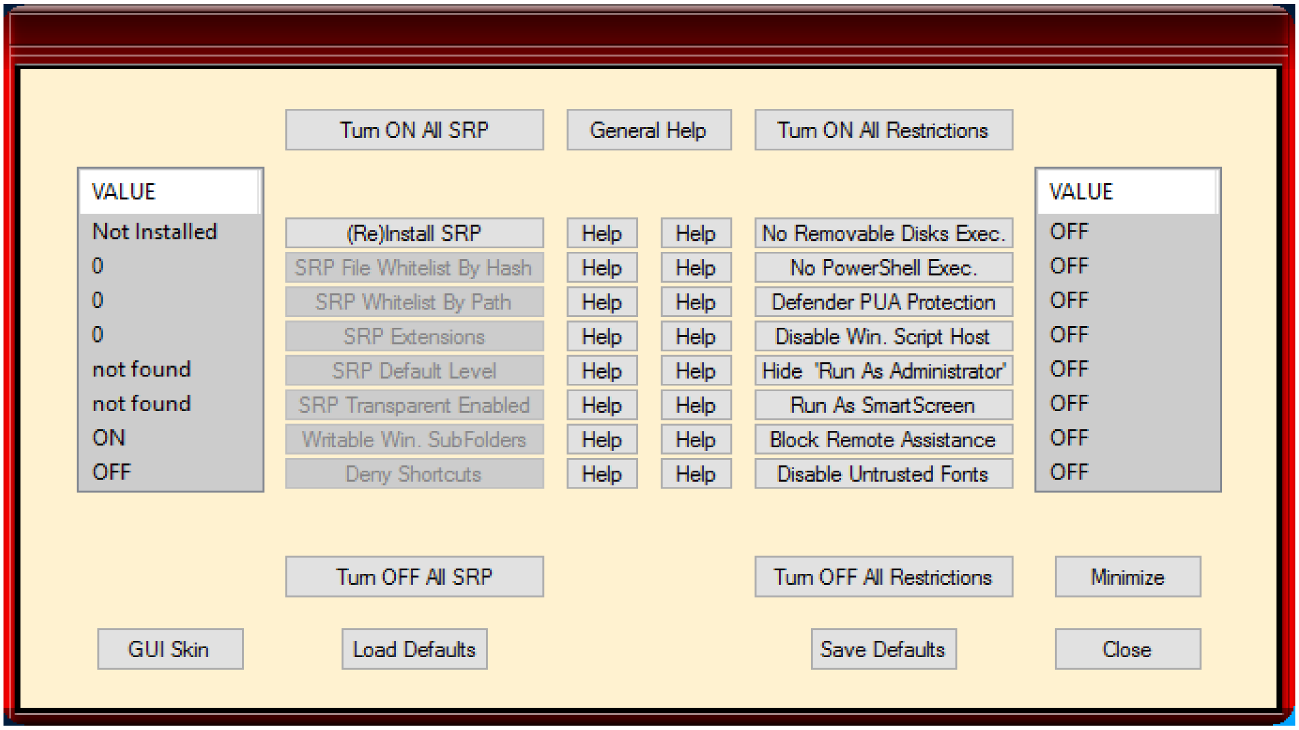
Disclaimer of Warranty

THIS SOFTWARE IS DISTRIBUTED "AS IS". NO WARRANTY OF ANY KIND IS EXPRESSED OR IMPLIED. YOU USE IT AT YOUR OWN RISK. THE AUTHOR WILL NOT BE LIABLE FOR DATA LOSS, DAMAGES, LOSS OF PROFITS OR ANY OTHER KIND OF LOSS WHILE USING THIS SOFTWARE.

TABLE OF CONTENTS

INTRODUCTION

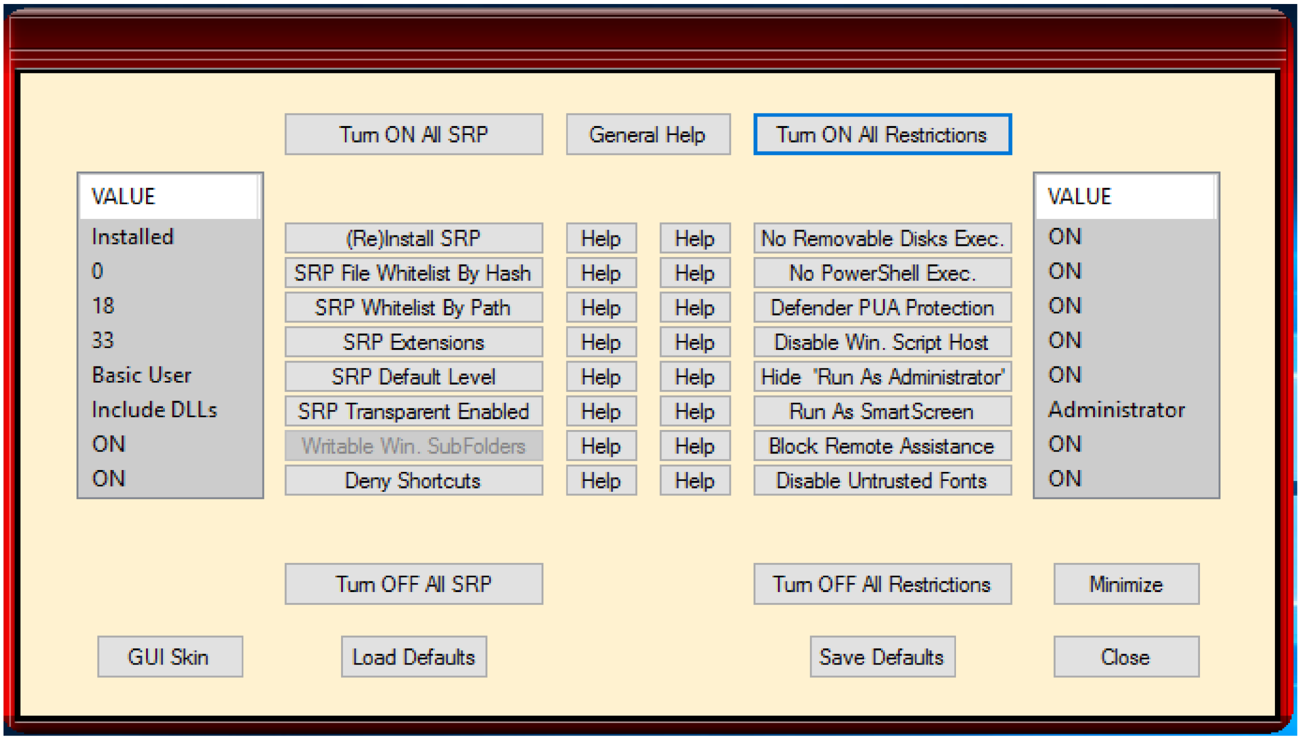
1. Hard_Configurator works with Windows Vista and higher versions. It is intended for users, who want to use Windows built-in security. This program can manage some well-known system restrictions to harden the Windows OS. Actually, they are directed to control code execution, so in the wide sense, Hard_Configurator can be seen as a kind of anti-exe protection.
   After starting the program, it is good to "Save Defaults", so the initial settings can be quickly retrieved by clicking "Load Defaults" button.



	VALUE
(Re)Install SRP	Not Installed
SRP File Whitelist By Hash	0
SRP Whitelist By Path	0
SRP Extensions	0
SRP Default Level	not found
SRP Transparent Enabled	not found
Writable Win. SubFolders	ON
Deny Shortcuts	OFF

	VALUE
No Removable Disks Exec.	OFF
No PowerShell Exec.	OFF
Defender PUA Protection	OFF
Disable Win. Script Host	OFF
Hide 'Run As Administrator'	OFF
Run As SmartScreen	OFF
Block Remote Assistance	OFF
Disable Untrusted Fonts	OFF

2. Turning on all options ("Turn ON All SRP" and "Turn ON All Restrictions") , gives users pretty good, set and forget security setup. Almost all programs can be run as usual by mouse click or pressing the ENTER key. Downloaded programs cannot be run from the Web Browser. They should be first saved, and next 'Run As Smartscreen' from DOWNLOAD folder using Windows Explorer context menu. Portable applications located outside 'Windows' and 'Program Files' folders can be whitelisted by hash (or by path), and then run as usual.



	VALUE
(Re)Install SRP	Installed
SRP File Whitelist By Hash	0
SRP Whitelist By Path	18
SRP Extensions	33
SRP Default Level	Basic User
SRP Transparent Enabled	Include DLLs
Writable Win. SubFolders	ON
Deny Shortcuts	ON

	VALUE
No Removable Disks Exec.	ON
No PowerShell Exec.	ON
Defender PUA Protection	ON
Disable Win. Script Host	ON
Hide 'Run As Administrator'	ON
Run As SmartScreen	Administrator
Block Remote Assistance	ON
Disable Untrusted Fonts	ON

3. There is no need to turn off the program options to install Windows Updates and perform system Scheduled Tasks.
4. Some precautions should be taken when turning on SRP. In some exotic hardware configurations, SRP can block something important in Hardware Manufacturer Folder (Intel, AMD, Lenovo, Asus, Toshiba, etc.), if it is not in the 'Windows', 'Program Files' or 'Program Files (x86)' folder. In that case, the system can hang after restarting. This very unpleasant situation can happen with any security program. But, with SRP there is a clear procedure to fully recover the system functionality (see TROUBLESHOOTING paragraph for more info).
5. Some options are not supported by earlier Windows versions:
   "Disable Untrusted Fonts" - Windows Vista, Windows 7, 8, 8.1
   "PUA Protection" - Windows Vista, Windows 7
   "Run As Smartscreen" - Windows Vista, Windows 7
   "No Removable Disk Exec." - Windows Vista
   "No PowerShell Exe." - Windows Vista
   Also, the option "Writable Win. SubFolders" is not available in Windows 10, because it is not thoroughly tested there.

INSTALLATION

0. Make the system restore point - it costs nothing, and can save you a lot of time when in trouble. Please do not use Hard_Configurator on laptops with the system installed on eMMC flash memory, because the program was not fully tested on this hardware.
1. Uninstall and delete the previous version of Hard_Configurator.
2. Unzip Hard_Configurator.zip .
3. Copy the unzipped folder 'Hard_Configurator' to 'C:\Windows' (Administrative Rights are needed).
4. If Windows is 64Bit, then run Hard_Configurator(x64).exe from 'C:\Windows\Hard_Configurator' folder.
5. If Windows is 32Bit, then run Hard_Configurator(x86).exe from 'C:\Windows\Hard_Configurator' folder.

* Do not change the path and the name of:
RunAsSmartscreen(x64).exe, RunAsSmartscreen(x86).exe,
RunBySmartscreen(x64).exe, RunBySmartscreen(x86).exe .
The path 'C:\Windows\Hard_Configurator' and above executable filenames are hard-coded.
* Do not run executables RunAsSmartscreen(x64).exe or RunAsSmartscreen(x86).exe, they are invoked by 'Run As Smartscreen' option in Explorer context menu.
* Do not run executables RunBySmartscreen(x64).exe or RunBySmartscreen(x86).exe, they are invoked by 'RunBy Smartscreen' option in Explorer context menu.

DEINSTALLATION

1. Run Hard_Configurator.
2. Press "Turn OFF All SRP", and next "Turn OFF All Restrictions".
3. Close Hard_Configurator.
4. Delete Hard_Configurator folder from C:\Windows.

To avoid collisions with other programs (SBGuard, CryptoPrevent), the deinstallation process does not delete all registry subkeys in:
‘HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\’ key.

SOFTWARE RESTRICTION POLICIES (SRP)

From the technet.microsoft.com :

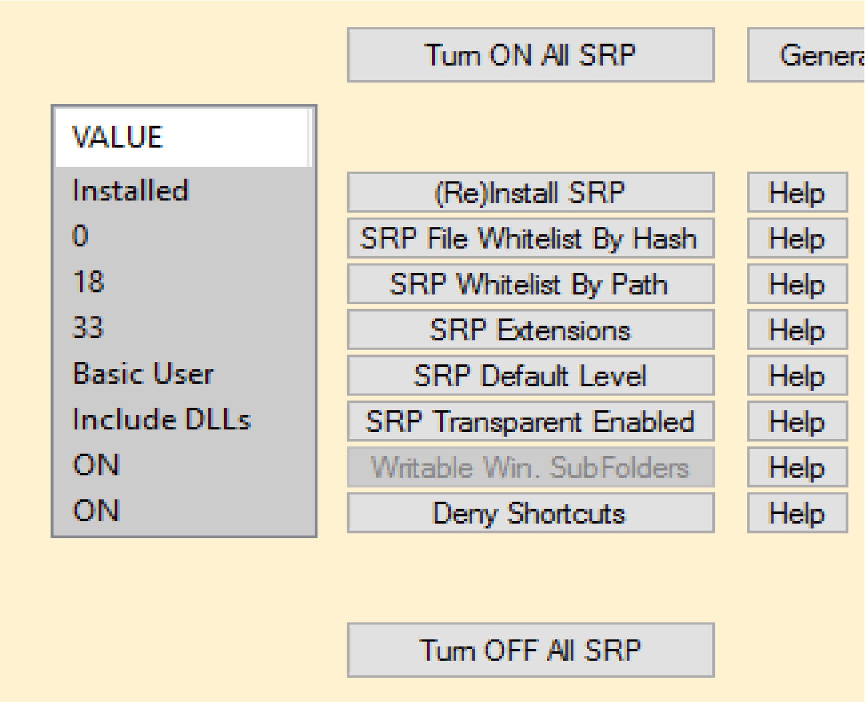
"Software Restriction Policies (SRP) is Group Policy-based feature that identifies software programs running on computers in a domain, and controls the ability of those programs to run. Software restriction policies are part of the Microsoft security and management strategy to assist enterprises in increasing the reliability, integrity, and manageability of their computers.

You can also use software restriction policies to create a highly restricted configuration for computers, in which you allow only specifically identified applications to run. Software restriction policies are integrated with Microsoft Active Directory and Group Policy. You can also create software restriction policies on stand-alone computers. Software restriction policies are trust policies, which are regulations set by an administrator to restrict scripts and other code that is not fully trusted from running."

https://technet.microsoft.com/en-us/library/hh831534(v=ws.11).aspx

Software Restriction Policies are available through Group Policy, for Windows Pro, Windows Enterprise, Windows Server, and Windows Education. Well configured SRP is known in enterprise case studies, as one of the best protections against virus infections.

Hard_Configurator program can apply several SRP settings in Windows Home, too. Some settings were skipped because they are not needed for home users.



VALUE		
Installed	(Re)Install SRP	Help
0	SRP File Whitelist By Hash	Help
18	SRP Whitelist By Path	Help
33	SRP Extensions	Help
Basic User	SRP Default Level	Help
Include DLLs	SRP Transparent Enabled	Help
ON	Writable Win. SubFolders	Help
ON	Deny Shortcuts	Help

"(Re)Install SRP" button makes changes in the Registry to install Windows SRP. The SRP parameters can be changed using the buttons: "SRP Whitelist By Hash", "SRP Whitelist By Path", "SRP Extensions", "SRP Default Level", "SRP Transparent Enabled". Two SRP options: "Ignore certificate rules" and "All users except local administrators" are hardcoded, and set to ON.

WARNING!
Before installing SRP, check if there is a Manufacturer Folder on the system disk (Intel, AMD, Lenovo, Asus, etc.). Sometimes files from this folder are loaded at the boot time, and should not be blocked by SRP. It is recommended to whitelist this folder, because in some special configurations, the system may hang after the restart. Please, use Sysinternals Autoruns to check for paths that **are not** in the safe SRP locations: C:\Windows, C:\Program Files, C:\Program Files (x86).

In this program, SRP is used as a simple anti-exe, that is based on Windows built-in security features. Executables can be run without SRP restrictions in the System Space, that contains UAC protected folders: 'Windows' and 'Program Files' (and 'Program Files (x86)' in 64Bit versions). Outside those folders (= User Space), executables will be blocked by default, when running by mouse click or pressing ENTER key.
The list of blocked executable extensions can be accessed by pressing "SRP Extensions" button. Some file extensions are blocked by default, even if they are not on this list (for example: COM, EXE, MSI).
There's a possibility to run the executable from User Space if it was whitelisted by hash or by path.

REMARKS
SRP restrictions can be bypassed using 'Run As Administrator' option from Explorer context menu, but this works only for some extensions (for example: BAT, CMD, EXE). Running new files with Administrative Rights can be dangerous for many users, so Hard_Configurator can replace 'Run As Administrator' option in Explorer context menu with safer 'Run As SmartScreen' (see "Run As Smartscreen" manual section).

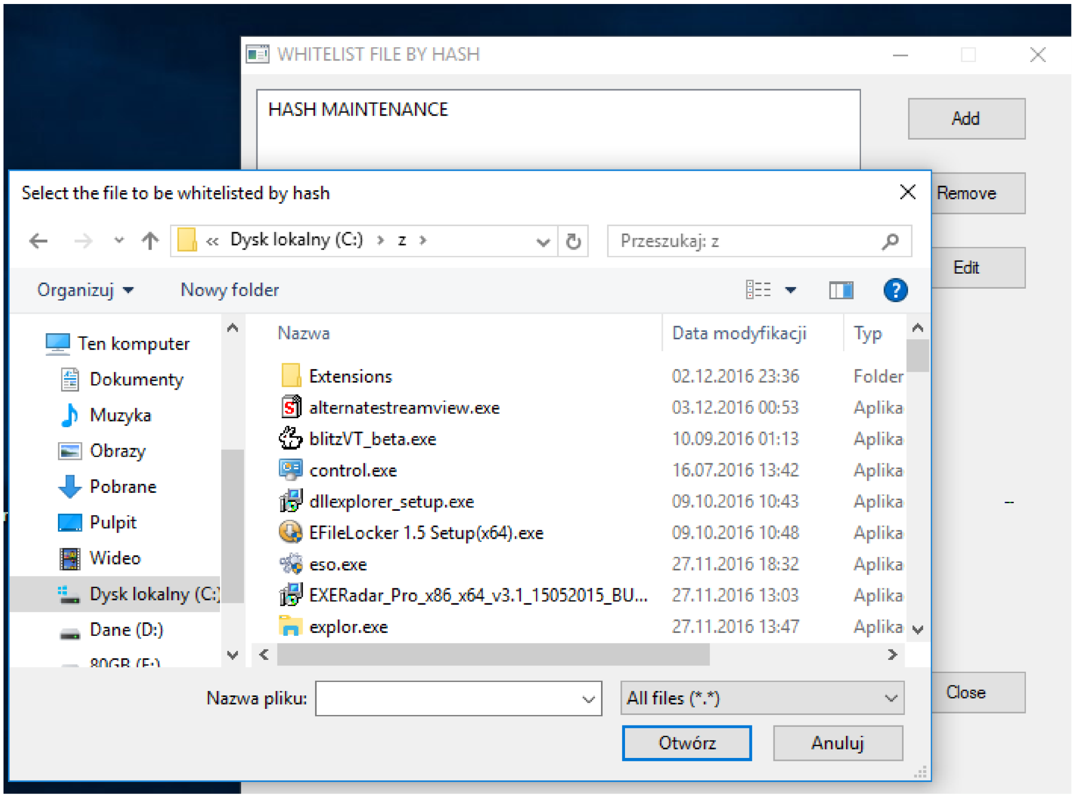
Known folder GUIDs were used for whitelisting folders: C:\Windows, C:\Program Files, and C:\Program Files (x86) . Additionally, the program uses GUIDs based on Simple Software Restriction Policies to handle file whitelisting by hash.

This program cannot uninstall SRP, but that is not really needed. SRP in Hard_Configurator can be completely deactivated by pressing "Turn OFF All SRP" button.

Useful links:
https://malwaretips.com/threads/windows-pro-owner-use-software-restriction-policies.61871/
http://www.wilderssecurity.com/threads/maximising-windows-7-security-with-srp-under-lua-whatever-the-win7-version.262686/
http://www.bleepingcomputer.com/tutorials/create-an-application-whitelist-policy-in-windows/

Registry changes:
HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers

WHITELISTING BY HASH



Select the file to be whitelisted by hash

Nazwa	Data modyfikacji	Typ
Extensions	02.12.2016 23:36	Folder
alternatestreamview.exe	03.12.2016 00:53	Aplika
blitzVT_beta.exe	10.09.2016 01:13	Aplika
control.exe	16.07.2016 13:42	Aplika
dllexplorer_setup.exe	09.10.2016 10:43	Aplika
EFileLocker 1.5 Setup(x64).exe	09.10.2016 10:48	Aplika
eso.exe	27.11.2016 18:32	Aplika
EXERadar_Pro_x86_x64_v3.1_15052015_BU...	27.11.2016 13:03	Aplika
explor.exe	27.11.2016 13:47	Aplika

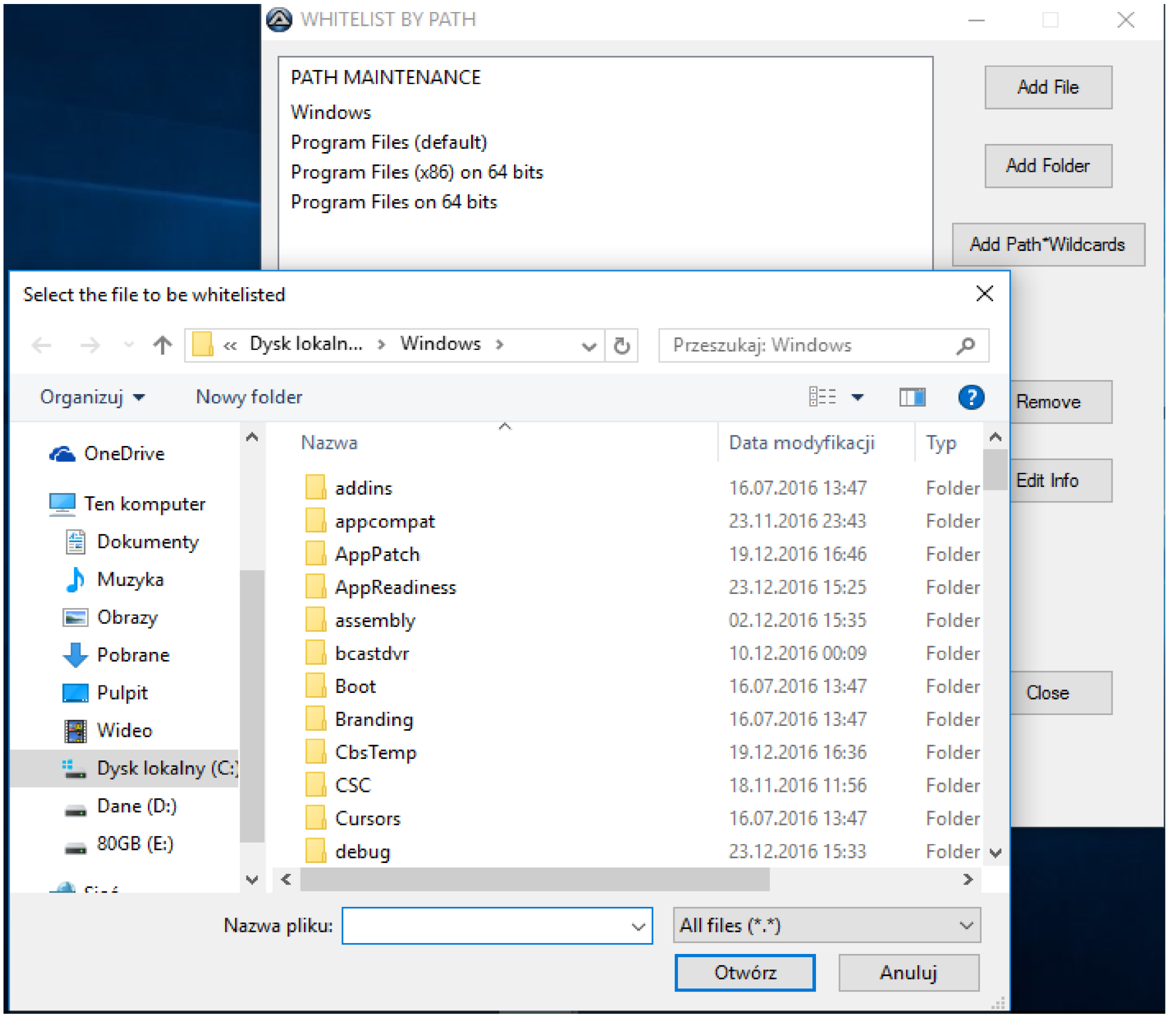
"SRP Whitelist By Hash" button opens ADD/REMOVE/EDIT window to manage file whitelisting by hash. It is very useful for running programs located in the User Space (outside the folders: Windows, Program Files, and Program Files (x86)).
User Space is not protected by UAC, so the file can be easily modified by virus infection. Yet, this also changes the file hash, and then SRP can block file execution.
Managing file hashes is not comfortable. Use this function only if you have to. The program tries to extract some info about the file to make hash entries more readable.

REMARKS

Sometimes programs are wrapped and have to use TEMP folder in the User Profile to execute (most frequently it is ...\AppData\Local\Temp).
Execution in the TEMP folder will be blocked by SRP, so the unwrapped file should be whitelisted by hash too. Usually, such files are quickly deleted, and then utilities similar to "Moo0 FileMonitor" may be needed to find out which files were temporary dropped to TEMP folder.

Registry changes:
HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\262144\Hashes

WHITELISTING BY PATH



PATH MAINTENANCE
Windows
Program Files (default)
Program Files (x86) on 64 bits
Program Files on 64 bits

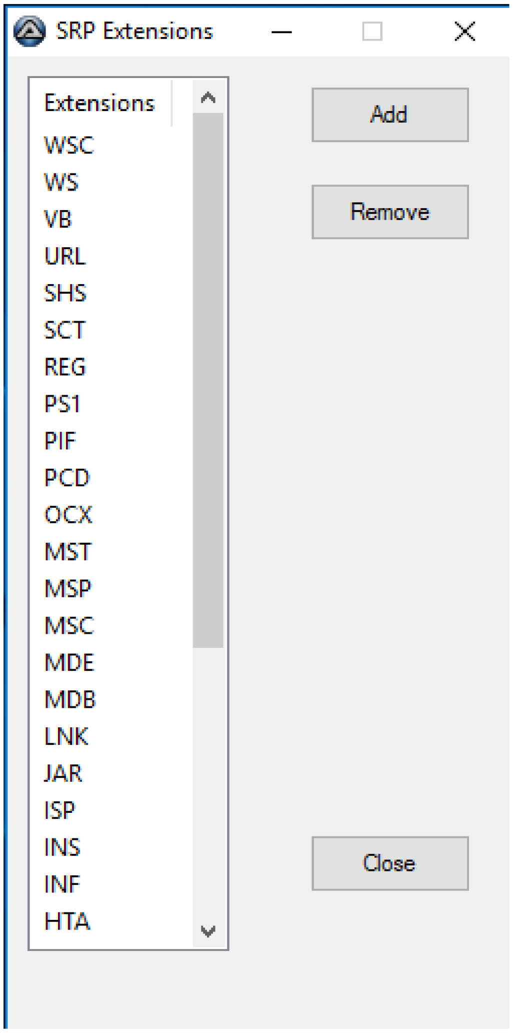
Nazwa	Data modyfikacji	Typ
addins	16.07.2016 13:47	Folder
appcompat	23.11.2016 23:43	Folder
AppPatch	19.12.2016 16:46	Folder
AppReadiness	23.12.2016 15:25	Folder
assembly	02.12.2016 15:35	Folder
bcastdvr	10.12.2016 00:09	Folder
Boot	16.07.2016 13:47	Folder
Branding	16.07.2016 13:47	Folder
CbsTemp	19.12.2016 16:36	Folder
CSC	18.11.2016 11:56	Folder
Cursors	16.07.2016 13:47	Folder
debug	23.12.2016 15:33	Folder

"SRP Whitelist By Path" button opens ADD/REMOVE/EDIT window to manage file/folder whitelisting by path. It is very useful, for running programs located in User Space (outside the folders: 'Windows', 'Program Files', and 'Program Files (x86)'). Yet, User Space is not protected by UAC, so in theory, the malware file can bypass SRP when running from the whitelisted path. Whitelisting well known locations in User Profile is especially dangerous, for example:
%USERPROFILE%\AppData\Local
%USERPROFILE%\AppData\Local\Temp
Music, Pictures, Videos, Documents, Desktop, Downloads, etc.

The safer method (but less convenient) is whitelisting the file by hash. Whitelisting the shortcuts and whitelisting paths with wildcards is only possible with the "Add Path*Wildcards" option.

Registry changes:
HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\262144\Paths

PROTECTED EXTENSIONS



Extensions
WSC
WS
VB
URL
SHS
SCT
REG
PS1
PIF
PCD
OCX
MST
MSP
MSC
MDE
MDB
LNK
JAR
ISP
INS
INF
HTA

"SRP Extensions" button opens ADD/REMOVE window with the list of actually protected extensions. Default extensions:
WSC, WS, VB, URL, SHS, SCT, REG, PS1, PIF, PCD, OCX, MST, MSP, MSC, MDE, MDB, LNK, JAR, ISP, INS, INF, HTA, HLP, EXE, CRT, CPL,

COM, CMD, CHM, BAT, BAS, ADP, ADE.
The above extensions differ from SRP defaults in Windows Pro. Windows Script Host extensions (JS, JSE, VBE, VBS, WSF, WSH) were removed, because Hard_Configurator has "Disable Win. Script Host" option to deal with them. Also, the MSI and SCR extensions were removed to work with "Run As SmartScreen" option (SRP can still protect them when they are not on the SRP extension list).

You can customize this list by adding or removing some extensions.

Warnings.
Do not add MSI and SCR extensions if "Run As Smartscreen" is set ON.
Do not add JS, JSE, VBE, VBS, WSF, and WSH extensions, if the option "Disable Win. Script Host" is set ON.

REMARKS

Some executable files are protected by SRP even when the list is empty.
In "Basic User" security level, the COM, EXE and MSI extensions are always protected.
In "White List" (Disallowed) security level, the protection covers:
BAT, CMD, COM, EXE, MSI, JS, JSE, VBE, VBS and WSF extensions.
However, there's the difference in the protection. If one of the above extensions is not on the list, then Windows is going to run sponsors (msiexec.exe, cmd.exe, wscript.exe, cscript.exe), and after that the file execution will be blocked. If the extensions are on the list, then sponsors does not even start.

Registry changes:
HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\ExecutableTypes

SECURITY LEVELS

"SRP Default Level" button changes the security levels between:
"Basic User" -> "Allow All" -> "White List"

"Basic User" corresponds to default deny (Disallowed) security level. All files with SRP protected extensions in the User Space (outside C:\Windows, C:\Program Files, and C:\Program Files (x86)), will not be allowed to execute in a standard way (by mouse click or pressing ENTER key).

"White List" is very similar to "Basic User", but it differently supports LNK, MSI extensions and also default extensions, that can be omitted from the SRP list (see help for "SRP Extensions" button).

"Allow All" turns off default deny SRP protection (but not the SRP Blacklist). It is worth mentioning that Windows SRP functionality is wider than this program can provide. The SRP Blacklist and some other options cannot be managed here (see also "Deny Shortcuts" help).

If you want to run executable file in the User Space with SRP set to "Basic User" or "White List", then it can be done with "Run As Administrator" option in Explorer context menu. But, bypassing SRP with Administrative Rights can be dangerous. Hard_Configurator provides the safer option by replacing 'Run As Administrator' with 'Run As Smartscreen'.
If you want to use frequently the application that is located in the User Space, then consider whitelisting it by hash.

REMARKS

The BAT, CMD and EXE files located in the User Space, can be run (bypassing SRP) using "Run As Administrator". If you want to run MSI files with "Run As Administrator", then you can adopt Symantec reg tweak.
Finally, if you want to run BAT, CMD, COM, EXE, JSE, MSI and VBE files, then activate "Run As SmartScreen" + SRP "White List". Another solution is to run Total Commander with "Run As Administrator", and then use it to execute files protected by SRP.

Registry changes:
HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers

DefaultLevel

Value (Dword)

0	"White List (Disallowed)"
131072	"Basic User" (131072 = 20000 hex)
262144	"Allow All" (262144 = 40000 hex)

ENFORCEMENT OPTIONS

"SRP Transparent Enabled" button changes the Enforcement options :
"Include DLLs" -> "No Enforcement" -> "Skip DLLs"

"Include DLLs" option is most restrictive, but DLL checking
may result in performance degradation. If so, consider changing the setup to "Skip DLLs".

Registry changes
HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers

TransparentEnabled

Value(Dword)

0	No Enforcement
1	skip DLLs
2	include DLLs

WRITABLE ‘C:\WINDOWS’ SUBFOLDERS

Setting **"Writable Win. SubFolders"** to 'ON' denies the execution from ‘C:\Windows’ subfolders, that are writable (no UAC protection). In Windows 10 this option is inactive, because it is not thoroughly tested there. For Windows 8.1 and prior versions some subfolders are added to SRP blacklist:
c:\windows\debug\WIA
c:\windows\Registration\CRMLog
c:\windows\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}
c:\windows\System32\com\dmp
c:\windows\System32\FxsTmp
c:\windows\System32\spool\drivers\color
c:\windows\System32\spool\PRINTERS
c:\windows\System32\Tasks
c:\windows\SysWOW64\com\dmp
c:\windows\SysWOW64\FxsTmp
c:\windows\SysWOW64\Tasks
c:\windows\Tasks
c:\windows\Temp
c:\windows\tracing

Registry changes:
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\safer\CodeIdentifiers\0\Paths\

WARNING
Using this option can in theory stop some Windows tasks from working properly. Please, look at Windows Event Log to check if SRP blocks something important (see TROUBLESHOOTING section).

EXECUTING SHORTCUTS

"Deny Shortcuts" button disables/enables shortcut execution restrictions.
If this option is set to 'ON', then shortcuts can be executed only in 'Windows', 'Program Files', 'Program Files (x86)', 'Desktop', 'Power Menu', and 'Start Menu' locations.
This restriction is applied, because specially crafted shortcuts can bypass Software Restriction Policies.

Registry changes:
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\safer\CodeIdentifiers\262144\Paths\

Added GUIDs:

{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}]
{625B53C3-AB48-4EC1-BA1F-A1EF4146FC20}]
{625B53C3-AB48-4EC1-BA1F-A1EF4146FC21}]
{625B53C3-AB48-4EC1-BA1F-A1EF4146FC22}]
{625B53C3-AB48-4EC1-BA1F-A1EF4146FC23}]
{625B53C3-AB48-4EC1-BA1F-A1EF4146FC24}]
{99a0fd77-ed0c-4e30-91ff-9d51428d2f21}]
{99a0fd77-ed0c-4e30-91ff-9d51428d2f22}]
{99a0fd77-ed0c-4e30-91ff-9d51428d2f23}]
{B4BFCC3A-DB2C-424C-B029-7FE99A87C641}]
{B4BFCC3A-DB2C-424C-B029-7FE99A87C642}]
{B4BFCC3A-DB2C-424C-B029-7FE99A87C643}]
{B4BFCC3A-DB2C-424C-B029-7FE99A87C644}]
{B4BFCC3A-DB2C-424C-B029-7FE99A87C645}]

EXECUTION FROM REMOVABLE DISKS

"No Removable Disk Exec." button disables/enables file execution from removable disks (Pendrives, USB disks, Memory Cards). The files cannot be executed by mouse click, pressing Enter key, or using 'Run As Administrator' from Explorer context menu. Yet, if the "Run As Smartscreen" is set to 'Administrator' or 'Standard User', then this restriction can be bypassed using Explorer context menu options: 'Run As Smartscreen' or 'Run by Smartscreen'. If additionally SRP is activated, only 'Run As Smartscreen' from Explorer context menu will work, because 'Run By Smartscreen' cannot automatically elevate file execution to bypass SRP.

Registry changes:
HKLM\SOFTWARE\Policies\Microsoft\Windows\RemovableStorageDevices\
{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}

Deny_Execute
Value (Dword)

1	block execution
0	allow execution

POWERSHELL SCRIPTS

"No PowerShell Exec." button disables/enables PowerShell script execution.
If this option is ON, then script execution is blocked, but you can still execute script commands in the Powershell window. Keep this option ON because scripts are the weak point of most antimalware programs. Alternatively, you can activate SRP to block script extensions.

Registry changes:
HKLM\Software\Policies\Microsoft\Windows\PowerShell

EnableScripts
Value (Dword)

0	script execution is disabled
1	script execution is enabled

PUA PROTECTION

"Defender PUA Protection" button activates/deactivates Windows Defender PUA protection.

"By default, PUA protection quarantines the file so they won’t run. PUA will be blocked only at download or install-time. A file will be included for blocking if it meets one of the following conditions:
* The file is being scanned from the browser
* The file has Mark of the Web set
* The file is in the %downloads% folder
* Or if the file in the %temp% folder "
https://blogs.technet.microsoft.com/mmpc/2015/11/25/shields-up-on-potentially-unwanted-applications-in-your-enterprise/

REMARKS
PUA = Potentially Unwanted Application ~ PUP ~ PUS
PUP = Potentially Unwanted Program
PUS = Potentially Unwanted Software

"A potentially unwanted program is bundled software which computer users are fooled into installing along with a wanted program.
Such software can compromise privacy or weaken the computer's security. Companies often bundle a wanted program download with a wrapper application. This may install an unwanted application, without providing a clear opt-out method.[1][2] Unwanted programs often include no sign that they are installed, and no uninstall or opt-out instructions.[3]
Antivirus companies define the software bundled as potentially unwanted programs (PUP)[3][4] which can include software that displays intrusive advertising, or tracks the user's Internet usage to sell information to advertisers, injects its own advertising into web pages that a user looks at, or uses premium SMS services to rack up charges for the user.[5][6] The practice is widely considered unethical because it violates the security interests of users without their informed consent.
Some unwanted software bundles install a root certificate on a user's device, which allows hackers to intercept private data such as banking details, without a browser giving security warnings."
https://en.wikipedia.org/wiki/Potentially_unwanted_program

Registry changes:
HKLM\Software\Policies\Microsoft\Windows Defender\MpEngine

MpEnablePus

Value (DWORD)	
0	Potentially Unwanted Application protection is disabled.
1	Potentially Unwanted Application protection is enabled.

WINDOWS SCRIPT HOST

"Disable Win. Script Host" button disables/enables Windows Script Host. If this option is ON, then execution of JS, JSE, VBS, VBE, and WSF scripts is blocked. Keep this option ON because scripts are the weak point of most antimalware programs.
Alternatively, you can activate SRP to block script extensions. But then JS, JSE, VBS, VBE, and WSF extensions have to be manually added to SRP extension list, because they are omitted in default settings.

Registry changes:
HKLM\SOFTWARE\Microsoft\Windows Script Host\Settings

Enabled

Value (Dword)	
0	script execution is disabled
1	script execution is enabled

RUN AS ADMINISTRATOR

"Hide 'Run As Administrator'" button hides/shows "Run As Administrator" option in Explorer context menu. It is useful when you choose to replace this option by "Run As SmartScreen".
Set "Hide 'Run As Administrator'" to "ON" if "Run As SmartScreen" is set to 'Administrator'.
Otherwise, it is better to turn "Hide 'Run As Administrator'" 'OFF'.

REMARKS

When "Hide 'Run As Administrator'" is set to 'ON', then 'Command Prompt (Administrator)' option in Windows Power Menu, and 'Run As Administrator' option in the Search context menu, are hidden too. Furthermore, files with extensions: BAT, CMD, CPL, and MSC will not run from the User Space (= outside 'Windows', 'Program Files', and 'Program Files (x86)' folders), when default SRP protection is active. 'Run As Smartscreen' cannot replace functionality of 'Run As Administrator' in this case, because access to BAT, CMD, CPL, and MSC extensions is blocked by SRP default settings. It should not be a problem, since files with above extensions are mostly run from System Space (= inside 'Windows', 'Program Files', and 'Program Files (x86)' folders), and their location in the User Space is very suspicious.

Registry changes:
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer

HideRunAsVerb

Value (Dword)

0	"Run As Administrator" is not hided
1	"Run As Administrator" is hided

RUN AS SMARTSCREEN

"Run As SmartScreen" button adds/removes 'Run As SmartScreen' or 'Run By SmartScreen' option in Explorer context menu. Those options force file execution with SmartScreen check for files located in the User Space. If the file is located in the System Space (inside 'Windows', 'Program Files', 'Program Files (x86)' folders), then Smartscreen check is skipped.
Pressing "Run As SmartScreen" button changes between values:
'Administrator' -> 'Standared User' -> 'OFF'

The value 'Administrator' corresponds to 'Run As SmartScreen' option in Explorer context menu.
The value 'Standard User' corresponds to 'Run By SmartScreen' option in Explorer context menu.
The value 'OFF' removes each of the above options from Explorer context menu.

Keep the value 'Administrator' when SRP is activated. If so, the users can safely:
1. Run programs (with mouse click or pressing ENTER button) already installed in the System Space.
2. Install new programs from the User Space using 'Run As SmartScreen' option in Explorer context menu.

If SRP is activated (with program defaults) and "Disable Win. Script Host" option is 'ON', then only DLL, EXE, MSI, and SCR files are allowed to 'Run As SmartScreen' in the User Space. Other files, located in the User Space, cannot be executed by 'Run As SmartScreen'.
Keep the value 'Standard User' when SRP is deactivated. If so, then set "Hide 'Run As Administrator" to 'OFF', because 'Run By SmartScreen' option in Explorer context menu is not the replacement for 'Run As Administrator' - it does not automatically elevate the Rights of executed program.

Warning!
Some extensions (for example: BAT, CMD, CPL) cannot be protected at the same time by SRP and "Run As SmartScreen". If SRP is activated, then by default "Run As SmartScreen" execution of those files, located in the User Space, will be blocked by SRP.

REMARKS

The SmartScreen Filter in Windows 8+ allows some vectors of infection listed below:
A) You have got the executable file (BAT, CMD, COM, CPL, DLL, EXE, JSE, MSI, OCX, PIF, SCR and VBE) using:
* the downloader or torrent application (EagleGet, utorrent etc.);
* container format file (zip, 7z, arj, rar, etc.);
* CD/DVD/Blue-ray disc;
* CD/DVD/Blue-ray disc image (iso, bin, etc.);
* non NTFS USB storage device (FAT32 pendrive, FAT32 usb disk);
* Memory Card;
so the file does not have the proper Alternate Data Stream attached.
B) You have run the executable file with runas.exe (Microsoft), AdvancedRun (Nirsoft), RunAsSystem.exe (AprelTech.com), etc.

"Run As SmartScreen" covers all vectors of infection listed in the A) point.

If you are executing executable files downloaded on NTFS hard drive by most popular Internet Browsers, Windows Store or from One Drive, then the SmartScreen Filter gives you very good protection against malware files (especially 0-day).
Alternatively to "Run As SmartScreen", you can simply upload the file to One Drive (or mailbox) , and download it again. This procedure also activates SmartScreen check automatically.
Registry changes:
HKEY_CLASSES_ROOT*\shell\Run As Smartscreen\

REMOTE ASSISTANCE

"Block Remote Assistance" button disables/enables remote desktop connections and remote requests from both the local user or remote user. For home users, it is recommended to keep this setting 'ON'.
Remote connections are frequently exploited by malware and hackers.

REMARKS
If this setting is 'ON', then local user cannot request remote assistance from a friend or a support professional. Also, Unsolicited Remote Assistance is blocked.

Registry changes:
HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services

If "Block Remote Assistance" is ON
fAllowUnsolicited = 0
fAllowToGetHelp = 0
fDenyTSConnections = 1

If "Block Remote Assistance" is OFF
fAllowUnsolicited = 1
fAllowToGetHelp = 1
fDenyTSConnections = 0

UNTRUSTED FONTS

"Disable Untrusted Fonts" button activates/deactivates the Blocking Untrusted Fonts feature in Windows 10.
Blocking untrusted fonts help prevent attacks that can happen during the font file-parsing process.

"This security feature provides a global setting to prevent programs from loading untrusted fonts. Untrusted fonts are any font installed outside of the %windir%\Fonts directory.

This feature can be configured to be in 3 modes: On Off and Audit. By default it is Off and no fonts are blocked. If you aren't quite ready to deploy this feature into your organization you can run it in Audit mode to see if blocking untrusted fonts causes any usability or compatibility issues."
http://winintro.com/Category=Windows_10_2016&Policy=Microsoft.Policies.GroupPolicy::FontMitigation&Language=en-en

REMARKS

"Potential reductions in functionality
After you turn this feature on, your employees might experience reduced functionality when:

Sending a print job to a remote printer server that uses this feature and where the spooler process hasn’t been specifically excluded. In this situation, any fonts that aren’t already available in the server’s %windir%/Fonts folder won’t be used.

Printing using fonts provided by the installed printer’s graphics .dll file, outside of the %windir%/Fonts folder. For more information, see Introduction to Printer Graphics DLLs.

Using first or third-party apps that use memory-based fonts.

Using Internet Explorer to look at websites that use embedded fonts. In this situation, the feature blocks the embedded font, causing the website to use a default font. However, not all fonts have all of the characters, so the website might render differently.

Using desktop Office to look at documents with embedded fonts. In this situation, content shows up using a default font picked by Office."
https://technet.microsoft.com/en-us/itpro/windows/keep-secure/block-untrusted-fonts-in-enterprise

Registry changes

HKLM\SOFTWARE\Policies\Microsoft\Windows NT\MitigationOpions

MitigationOptions_FontBocking

Value (REG_SZ)

1000000000000	Enable (block untrusted fonts)
2000000000000	Disable (do not block untrusted fonts)
3000000000000	Audit (log events without blocking untrusted fonts)

TROUBLESHOOTING

Please read this paragraph carefully, because it can be helpful when in trouble, after installing any security software.

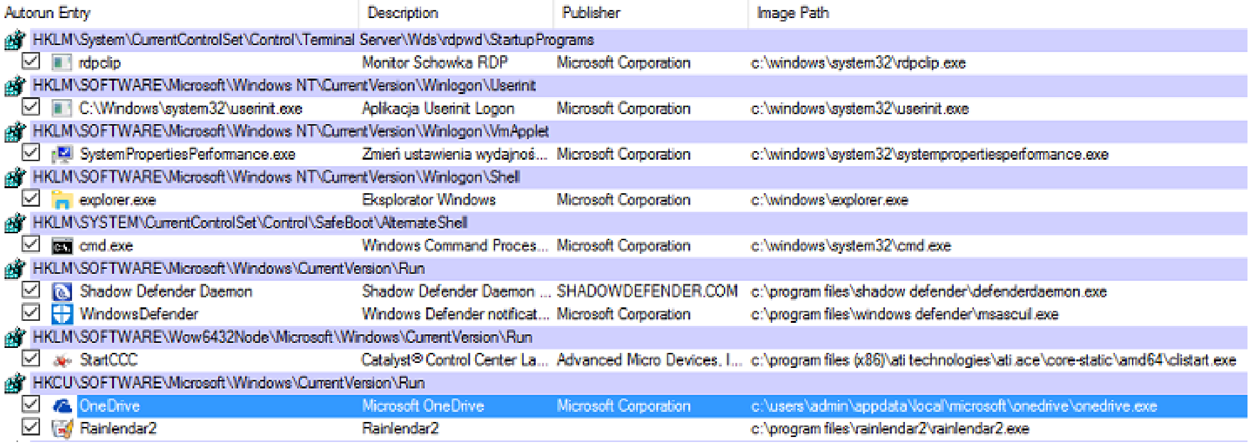
1. Check if you have operational bootable media to access a Command Prompt, in the case when the system hangs or is unbootable.
2. Some computers can have problems with a bootable media or recovery partition after upgrading the system (especially to Windows 10).
3. Before installing any security program, make the system restore point.
4. Sometimes system becomes unbootable from another cause. It is recommended to unplug all external devices (pendrives, USB disks, printers, headphones, USB DVD, etc.) and restart the system.
5. Having a bootable media, gives you access to Command Prompt. And then, using Regedit or Sysinternals Autoruns, the Registry can be loaded for offline editing. From Autoruns you can disable some autostart entries that may cause problems.

Hard_Configurator troubleshooting.

1. If the system hangs after reboot, then it can be a sign, that SRP or one of program restrictions has blocked something important from loading at the boot time.
2. The simplest method to solve this problem is using one of system restore points.
3. Another solution is using bootable media to access a Command Prompt, and then editing the Registry offline. In most cases the problem would be with SRP, so one must edit the key:
   HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers
   DefaultLevel
   change **hexagonal** value to **40000**
4. If the above did not help, then it is possible to edit or remove any registry changes made by Hard_Configurator. The Registry keys altered by the program are enumerated in this manual at the end of each paragraph.

Using Sysinternals Autoruns.

Some processes can be loaded at the boot time from the User Space (= outside 'Windows', 'Program Files', 'Program Files (x86)'). They should be whitelisted by path in SRP to load properly. Autoruns allows to find the paths of those processes. It is very important because stopping something important from loading at the boot time may hang the system.



Autorun Entry	Description	Publisher	Image Path
HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\StartupPrograms			
☑ rdpclip	Monitor Schowka RDP	Microsoft Corporation	c:\windows\system32\rdpclip.exe
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit			
☑ C:\Windows\system32\userinit.exe	Aplikacja Userinit Logon	Microsoft Corporation	c:\windows\system32\userinit.exe
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\VmApplet			
☑ SystemPropertiesPerformance.exe	Zmień ustawienia wydajnoś...	Microsoft Corporation	c:\windows\system32\systempropertiesperformance.exe
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell			
☑ explorer.exe	Eksplorator Windows	Microsoft Corporation	c:\windows\explorer.exe
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell			
☑ cmd.exe	Windows Command Proces...	Microsoft Corporation	c:\windows\system32\cmd.exe
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
☑ Shadow Defender Daemon	Shadow Defender Daemon ...	SHADOWDEFENDER.COM	c:\program files\shadow defender\defenderdaemon.exe
☑ WindowsDefender	Windows Defender notificat...	Microsoft Corporation	c:\program files\windows defender\msascuil.exe
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run			
☑ StartCCC	Catalyst® Control Center La...	Advanced Micro Devices, I...	c:\program files (x86)\ati technologies\ati.ace\core-static\amd64\clistart.exe
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run			
☑ OneDrive	Microsoft OneDrive	Microsoft Corporation	c:\users\admin\appdata\local\microsoft\onedrive\onedrive.exe
☑ Rainlendar2	Rainlendar2		c:\program files\rainlendar2\rainlendar2.exe

We can see that OneDrive is starting from the User Space at the boot time.

SRP Event Log.

When an SRP rule is applied, it can be seen in the application event log. The event ID between 865 and 868 shows the details of the process that triggered the SRP rule. It is good to look at it to see if the SRP restrictions block something important. The information about events are very short, but sufficient in most cases to identify the problem. There is also a nice NirSoft tool FullEventLogView, that can be used for quick event checking.

Verbose trace logging of SRP.

If someone would like enhanced logging of running processes, then the following registry setting must be added:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\safer\CodeIdentifiers]
"LogFileName"="c:\\Windows\\Hard_Configurator\\SRP_events.log"
```

LogFileName is a REG_SZ type. SRP will put more info about running processes to the file ‘SRP_events.log’. This can be used to identify the problems with blocked application, too. Simply, run the blocked application with "Run As Administrator" or "Run As SmartScreen", and then look at the last entry in the log.
For example, when ‘dllexplorer_setup.exe’ is run with "Run As SmartScreen", then the entries in the log will look like:

```
dllexplorer_setup.exe (PID = 5236) identified C:\Users\Admin\AppData\Local\Temp\is-PPQV9.tmp\dllexplorer_setup.tmp as Unrestricted using default rule, Guid = {11015445-d282-4f86-96a2-9e485f593302}"
```

So, we know that dllexplorer_setup.exe is using dllexplorer_setup.tmp to execute in temporary folder ‘C:\Users\USERNAME\AppData\Local\Temp\is-ASDAD.tmp\’.
Now, dllexplorer_setup.tmp can be whitelisted, and the problem is solved.