Hard_Configurator FAQ

Abbreviations used in this FAQ:

H_C - Hard_Configurator
AV - Antivirus application
SRP - Software Restriction Policies (Windows built-in security feature)
UAC - User Account Control
SUA - Standard User Account
AA - Administrator Account; not to be confused with 'Built-in Administrator Account' (disabled by default), that can be used to boot Windows to 'Audit mode'.

Basic concepts:

Standard rights (standard user rights, Medium Integrity Level)
These are standard (default) rights granted by the Windows system to processes initiated by the user on AA or SUA. Access to higher rights is controlled by User Account Control (UAC). This feature was introduced with Windows Vista.
An Administrator Account (AA) created during a fresh installation of Windows, or any account created manually by the user (AA or SUA), is limited to standard rights by UAC.

Administrator rights (Administrative rights)
A process initiated by the user on AA or SUA may be elevated to Administrator rights and access important, high privileges. Process elevation is controlled by User Account Control (UAC).
Process elevation cannot be done on SUA. If the process is initiated by the user logged on SUA, then process elevation is redirected to AA (**account change SUA ---> AA, admin password required**). The elevated process runs in fact on AA (not on SUA).

H_C smart default-deny setup
Selected Windows built-in security features can restrict Windows, archiver applications, email client applications, MS Office, and Adobe Acrobat Reader with smart default-deny protection. These features are normally disabled in Windows. H_C allows the user to enable them, make configuration changes, and displays the user's chosen settings. After configuration, real-time protection comes *only* from Windows' built-in security features.

SystemSpace
The following file locations (system folders and subfolders) are defined as SystemSpace and are whitelisted by default in H_C:
'Windows'
'Program Files'
'Program Files (x86)' - only on Windows 64-bit
'ProgramData\Microsoft\Windows Defender'.

UserSpace
All locations on the *user's local* drives (also USB external drives) which are not included in SystemSpace, are defined as UserSpace. *Network locations* are excluded either from UserSpace or SystemSpace. UserSpace locations are usually writable by processes running with standard rights. All executables in UserSpace are blocked by default with H_C's default-deny setup, except when whitelisted or initiated by the user via "Run as administrator" (see also the Elevated Shell).

PLEASE NOTE: *The terms SystemSpace and UserSpace are specific to H_C settings. They should not be confused with the terms 'System Space' and 'User Space', which can have a more general meaning.*

Elevated Shell
Normally, the user on AA or SUA may initiate applications *only with standard rights*. However, this can be changed by accessing an elevated shell: PowerShell (Administrator), Command Prompt (Administrator), etc. An alternative solution is to run Total Commander via "Run as administrator". The user who wants to access the elevated shell must first accept the UAC prompt. As long as the applications are initiated from the elevated shell, SRP (configured

by H_C) and UAC will ignore them (i.e., no UAC alerts or SRP restrictions). This can be useful when doing administrative tasks on the computer.

Questions and answers:

What is conventional default-deny protection?
It allows all installed applications and system processes but blocks by default all new executables, except those which are whitelisted. Some executables may be whitelisted automatically. Others must first be whitelisted by the user, in order to run. It is the user's responsibility to whitelist clean files.

What are the advantages of H_C's smart default-deny vs conventional default-deny protection?
Smart default-deny makes the security setup more usable, while maintaining a high level of protection in the home environment. Hard_Configurator includes the below smart features:

- Forced SmartScreen, which allows safely to pass by SRP restrictions. Forced SmartScreen is supported on Windows 8, 8.1, and 10.
- SRP set to allow executables initiated with Administrator rights.
- SystemSpace folders/subfolders whitelisted by default.
- <Update Mode> feature which can whitelist the ProgramData and user AppData (hidden) folders for EXE (TMP) and MSI files.
- Some files in system 'Windows' folder may be blacklisted by the user when using <Block Sponsors> settings. Some folders may be blacklisted by options: <Harden Archivers> and <Harden Email Clients>.

These features allow installing most applications without much whitelisting or turning OFF the protection. Furthermore, Windows Updates, software updates, and scheduled tasks can automatically bypass SRP restrictions.
It is worth mentioning that Forced SmartScreen significantly extends the SmartScreen protection.

Are H_C's smart features safe?
They can be considered as safe in the home environment. Smart features can be bypassed in Enterprises because of targeted attacks and exploits. Also, certain H_C restrictions, e.g. "Block remote access", are not practical in enterprises

Will H_C smart default-deny setup block system processes, Windows Updates, or system scheduled tasks?
No. System processes, Windows Updates, and system scheduled tasks are not started directly by the user. These are initiated with higher than standard rights and automatically bypass SRP restrictions configured with H_C.

Will H_C smart default-deny block updates of user applications?
Not on Windows 8+ in the Recommended Settings with <Update Mode> feature. But, on Windows 7 (Vista) many application updates will be blocked, except when the H_C profile Windows_7_Basic_Recommended_Settings or the profiles for Avast AV are applied.

How to update applications with the H_C Recommended Settings.
On Windows 8+ the applications usually can auto-update without problems. The manual updates with standalone EXE or MSI installers can be done via "Install By SmartScreen" entry in the right-click Explorer context menu.
If the Recommended Settings are applied on Windows 7 (Vista), then the H_C protection should be temporarily turned off to allow software updates. The user should be very cautious to run only safe executables.

How to update applications with H_C's custom default-deny settings.
1. Use the SwitchDefaultDeny tool to switch OFF the Default Deny Protection temporarily.
2. Run & update the application normally.
3. Switch ON the Default Deny Protection.

Is it safe to whitelist SystemSpace?
Generally, it is safe in the smart default-deny setup. SystemSpace locations are usually not writable with standard rights. There are known exceptions, but they are covered by H_C's <Protect Windows Folder> setting.

The exploit or malware cannot silently drop payloads to SystemSpace when running with standard rights.

Are all applications installed in SystemSpace?
Usually they are, and this is recommended by Microsoft. However, some legal applications still install in UserSpace. Most of them are installed in AppData or ProgramData folders, which are whitelisted by default on Windows 8+ with H_C's Recommended Settings, and on any Windows version with Windows_*_Basic_Recommended_Settings profile or with profiles prepared for Avast AV.
If the user applied H_C's Recommended Settings on Windows 7 (Vista), then applications installed in UserSpacehave have to be whitelisted manually.

What is the difference between an AA and SUA?
Processes initiated by the user cannot run with Administrator rights on SUA. If a process running on SUA requires Administrator rights, then the UAC prompt appears, and the user must provide an Administrator password to log on to the AA. After accepting the UAC, the process is no longer running on SUA, but on AA (*user account is switched for that process only:* SUA ---> AA).
This behavior is quite different when a process is initiated on AA, because the user is not obliged to provide the Administrator password. Instead, the UAC prompt asks for a simple "Yes" or "No". After accepting the UAC prompt, the process continues running on the same AA (*user account is not switched for that process*).

Is SUA more secure than AA?
Yes, most definitely. On SUA, any unelevated processes (running with standard rights or lower) do not share the same user account as elevated processes. Malware or exploits cannot run with Administrator rights on SUA - they must first escape to the Administrator account. This is hardly possible, because Microsoft usually patches any system vulnerabilities which might allow malware to escape from SUA. H_C's smart default-deny setup relies on blocking unelevated programs, so SUA is an ideal companion to H_C.

When should SUA be used instead of AA?
SUA should be considered a vital part of any security solution when *using a vulnerable* system, or popular & vulnerable software. However, it is not necessary to use SUA with H_C's smart default-deny *when Windows 10 and all installed software are updated regularly.* A well maintained system that includes H_C is a dead-end for malware/exploits in the home environment.

How to install applications on Windows 8+ with the H_C Recommended Settings.
Forced SmartScreen feature is available only on Windows 8+.
In the Recommended Settings, the Forced SmartScreen feature is integrated with <Update Mode> = ON. So, the "Install By SmartScreen" entry in the right-click Explorer context menu can be used to install applications. This works well for EXE and MSI standalone installers. When <Update Mode> is set to ON, the installation process does not force high privileges and the application always installs in the right user profile.
The "Install By SmartScreen" entry will not work for non-standalone installers, for example when the installation must be done from CD/DVD drives, CD/DVD images, archives containing the installation files copied from CD/DVD, etc. In such cases, the user must disable default-deny protection temporarily with SwitchDefaultDeny tool like for Windows 7 (see below).

How to install applications on Windows 7 (Vista) with the H_C Recommended Settings.
1. Use the SwitchDefaultDeny tool to turn OFF the protection temporarily.
2. Install the application normally (by using left mouse-click or pressing the Enter key).
3. Whitelist the application if necessary.
4. Use the SwitchDefaultDeny tool again to turn ON the protection.

Why Recommended H_C settings are best as a starting default-deny setup?
New users of default-deny protection should be aware that it requires more skill than using an AV alone. Please use *only* the Recommended H_C settings along with your AV, until you are comfortable and familiar with H_C. Prematurely adding advanced H_C settings or more security software to this confi-

guration, may lead to complications and user discouragement with default-deny protection.

Who should consider applying advanced H_C settings?
Recommended H_C settings provide strong preventive protection against running malware/exploits in the system. Advanced H_C settings can mitigate the malware or an exploit that is already running in the system (post-exploitation prevention).
When using well-patched software on updated Windows 10, advanced settings are not required.

Can advanced settings spoil the system?
On most computers, even maximum H_C settings cannot break anything important in the system, but some applications may be not fully functional. Enabling advanced settings will usually require more whitelisting, more researching of logs, etc., and may be annoying for most users. If so, then the user should restore Recommended Settings.

How to restore Recommended Settings.
1. Press <Recommended Settings> green button,
2. Press <APPLY CHANGES> button.

Restoring the Recommended Settings preserves the user's whitelisted entries and blocked file extensions.

How to apply advanced H_C settings.
Advanced settings can be activated by turning ON additional individual H_C options, or by loading the setting profile (<Load Profile> button).
It is advisable to begin with the Recommended_Enhanced profile. This may be done by loading the file: Windows_*_Recommended_Enhanced.hdc, where the asterisk replaces the Windows version (7, 8, or 10).
Recommended_Enhanced profile will enable the Recommended Settings, and some well known Sponsors/LOLBins will be blocked (including Script Interpreters).

PLEASE NOTE: *It is not advisable to apply multiple advanced settings at once. When using advanced settings, the user should occasionally check for*

blocked entries (<Tools><Blocked Events / Security Logs>). This is because sometimes there is no alert when a process is blocked by Windows policies.

What is a Sponsor?

A Sponsor is an executable from SystemSpace (usually from system 'Windows' folder), that can run another file. For example, the executable **powershell.exe** can run PowerShell script files *.ps1. Sponsors can be used by an attacker to bypass default-deny protection (see also LOLBins). They are frequently used in targeted attacks on organizations and businesses, especially via exploits. Blocking some Sponsors in the home environment can be important for people who use a vulnerable system or software.

In the Recommended Settings, Windows Script Host Sponsors (wscript.exe and cscript.exe) are blocked by SRP. Furthermore, PowerShell Sponsors (powershell.exe and powershell_ise.exe) are restricted by Constrained Language mode in Windows 10 and blocked by SRP in Windows Vista, 7, 8, 8.1. These Sponsors are the most popular Script Interpreters. Some other Interpreters (mshta.exe, hh.exe, wmic.exe, etc.) can be blocked in H_C by using <Block Sponsors> option. Unfortunately, a few of them can be used occasionally by older software, usually those related to peripherals. Applications and web browser plugins may also use Interpreters for some actions, though most applications and plugins do not use them at all.

In H_C, Sponsors are blocked for processes running with standard rights, but allowed for administrative processes running with higher rights.

Can wildcards be used for whitelisting files and folders?

Yes, they can. Here are some examples, where the random characters are replaced by wildcards to whitelist the particular EXE file:

- C:\Users\Alice\Fly2theMoon\App.**1928-0928**\setup_**101989873**.exe
- C:\Users\Alice\Fly2theMoon\App.**????-????**\setup_**?????????**.exe
- C:\Users\Alice\Fly2theMoon\App.*****\setup_**?????????**.exe
- C:\Users\Alice\Fly2theMoon\App.*****\setup_*****.exe
- C:\Users\Alice\Fly2theMoon\App.**********

These rules (except the first) are correct, and the EXE file will be whitelisted even when the random numbers will change after some time. The last rule is

most general because it will whitelist many other files and folders, for example: C:\Users\Alice\Fly2theMoon\App.malware\virus.js