ConfigureDefender Help (ver. 3.1.0.0)

ConfigureDefender works on Windows 10 build 1809 or Windows Server 2019, and higher versions (including Windows 11).

Most settings available in ConfigureDefender are related to Microsoft Defender real-time protection and work only when real-time protection is enabled. After changing the settings via ConfigureDefender, the Windows restart is required.

Important: *These two settings (below) should* ***never*** *be changed because important features like "Block at First Sight" and "Cloud Protection Level" will not work properly:*
- "Cloud-delivered Protection" = "ON"
- "Automatic Sample Submission" = "Send"

TAMPER PROTECTION

The below settings cannot be disabled while Defender Tamper Protection is enabled:
- Behavior Monitoring = ON
- Scan all downloaded files and attachments = ON
- Script Scanning = ON

I. ConfigureDefender Protection Levels (pre-defined settings):

"DEFAULT"
Microsoft Defender default configuration, which is applied automatically when installing the Windows system. It provides basic antivirus protection and can be used to quickly revert any configuration to Windows defaults.

"HIGH"
Enhanced configuration, which enables many Exploit Guard features like Network Protection and most ASR rules. Three ASR rules and Controlled Folder Access (Ransomware protection) are disabled to avoid false positives. This is the recommended configuration that is appropriate for most users and provides significantly increased security.

"INTERACTIVE"
The configuration, which is similar to the HIGH Protection Level, but all ASR rules are activated and set to "Warn" if possible. Some rules that are disabled in the HIGH Protection Level are now activated, so the protection is stronger, but it can generate more false positive alarms. This setup is not recommended for children or casual users, because the "Warn" setting allows the user to unblock the suspicious file easily, and then it can be executed, anyway.

"MAX"
The most secure protection level, which enables all advanced Microsoft Defender features and can hide Windows Security Center. Configuration changes can be made *only* with the ConfigureDefender user

interface. The "MAX" settings are intended to protect children and casual users but can be also used (with some modifications) to maximize the protection. This protection level usually generates more false positives compared to other settings and may require more user knowledge or skill.

II. ConfigureDefender custom settings:

You may customize your configuration by choosing any of the three protection levels and then change individual features.

How to apply the settings:
Select one of the Protection Levels or custom configuration, press the "Refresh" green button and let ConfigureDefender confirm the changes. ConfigureDefender will alert if any of your changes have been blocked. **Reboot to apply chosen protection.**

Audit mode:
Many ConfigureDefender options can be set to "Audit". In this setting, Microsoft Defender does not use the option to block processes. Anyway, Defender still logs events and warns the user about processes that would otherwise be blocked with this setting "ON". This feature is available for users to check for software incompatibilities with applied Defender settings. The user can avoid incompatibilities by adding software exclusions for ASR rules and Controlled Folder Access.

Warn mode:
It is similar to the "ON" setting but additionally, users see a dialog box that also offers an option to unblock the content. The user should **retry the action** to complete the operation. When a user unblocks content, the content remains unblocked for 24 hours, and then blocking resumes.

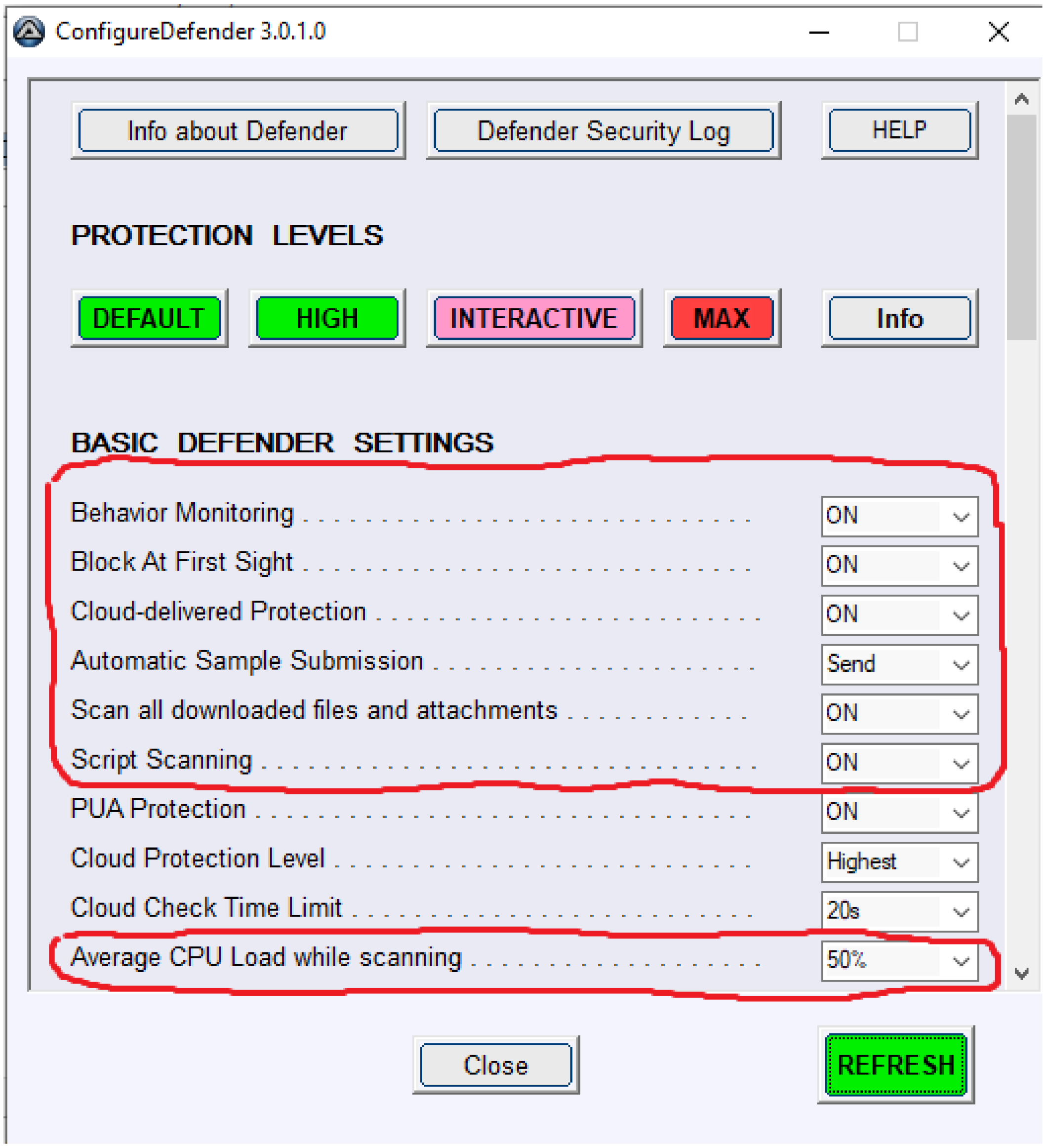
<Defender Security Log> button:
It can be used gather the last 300 entries from the Microsoft Defender Antivirus events. These entries are reformated and displayed in the notepad.
The following event IDs are included: 1006, 1008, 1015, 1116, 1118, 1119, 1120, 1121, 1122, 1123, 1124, 1125, 1126, 1127, 1128, 3002, 5001, 5004, 5008, 5010, and 5012. Inspecting the log can be useful when a process or file execution has been blocked by the Defender Exploit Guard.

III. Settings related to different Protection Levels

The below settings are the same for DEFAULT, HIGH, INTERACTIVE, and MAX Protection Levels:

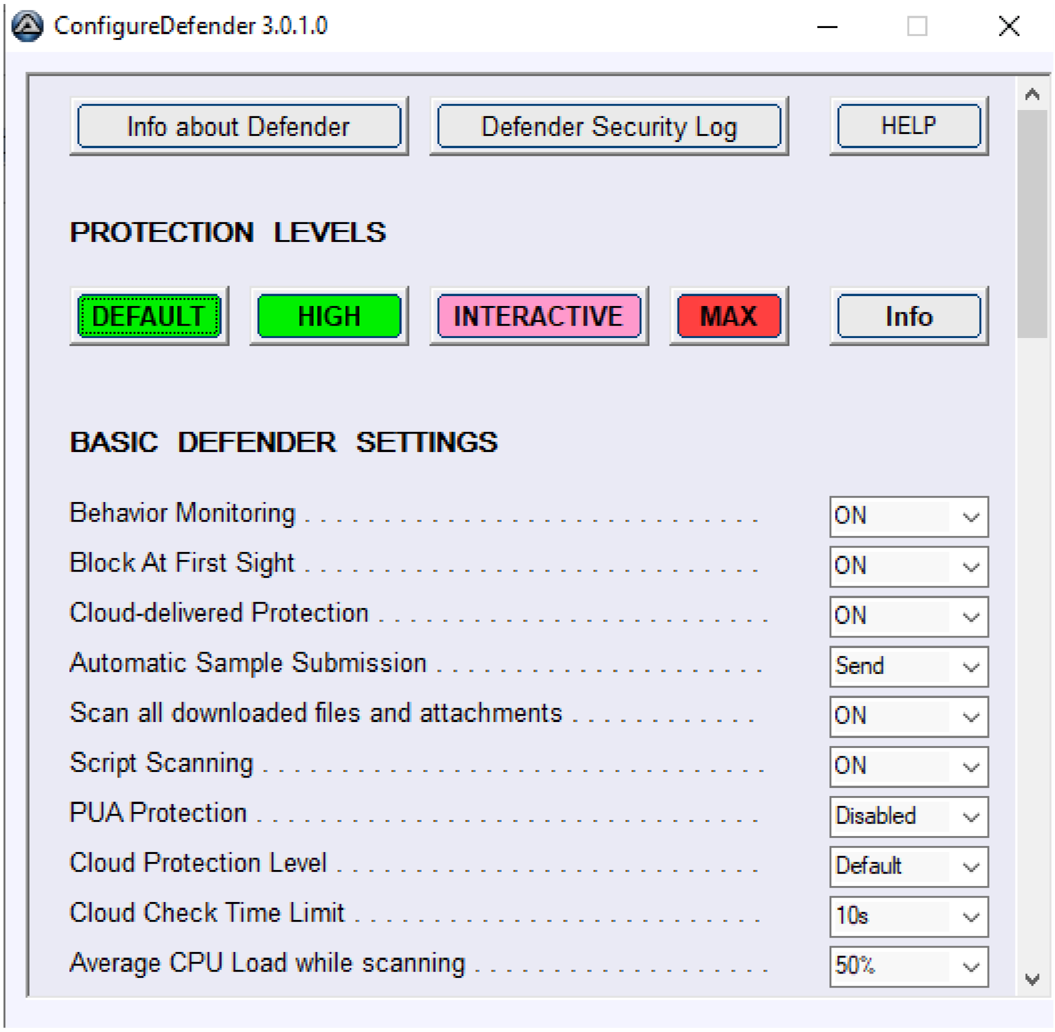
BASIC DEFENDER SETTINGS

- Behavior Monitoring = ON
- Block At First Sight = ON
- Cloud-delivered Protection = ON
- Automatic Sample Submission = Send
- Scan all downloaded files and attachments = ON
- Script Scanning = ON
- Average CPU load while scanning = 50%



Behavior Monitoring	ON
Block At First Sight	ON
Cloud-delivered Protection	ON
Automatic Sample Submission	Send
Scan all downloaded files and attachments	ON
Script Scanning	ON
PUA Protection	ON
Cloud Protection Level	Highest
Cloud Check Time Limit	20s
Average CPU Load while scanning	50%

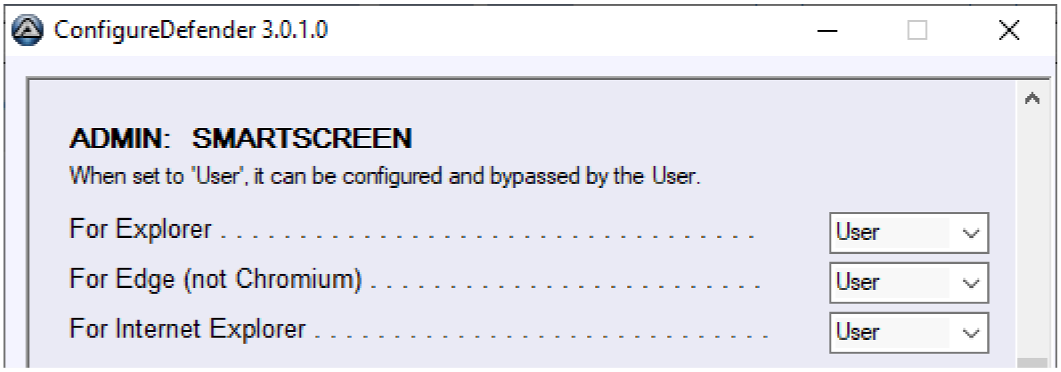
The DEFAULT Protection Level applies the other settings as follows:



PROTECTION LEVELS

BASIC DEFENDER SETTINGS

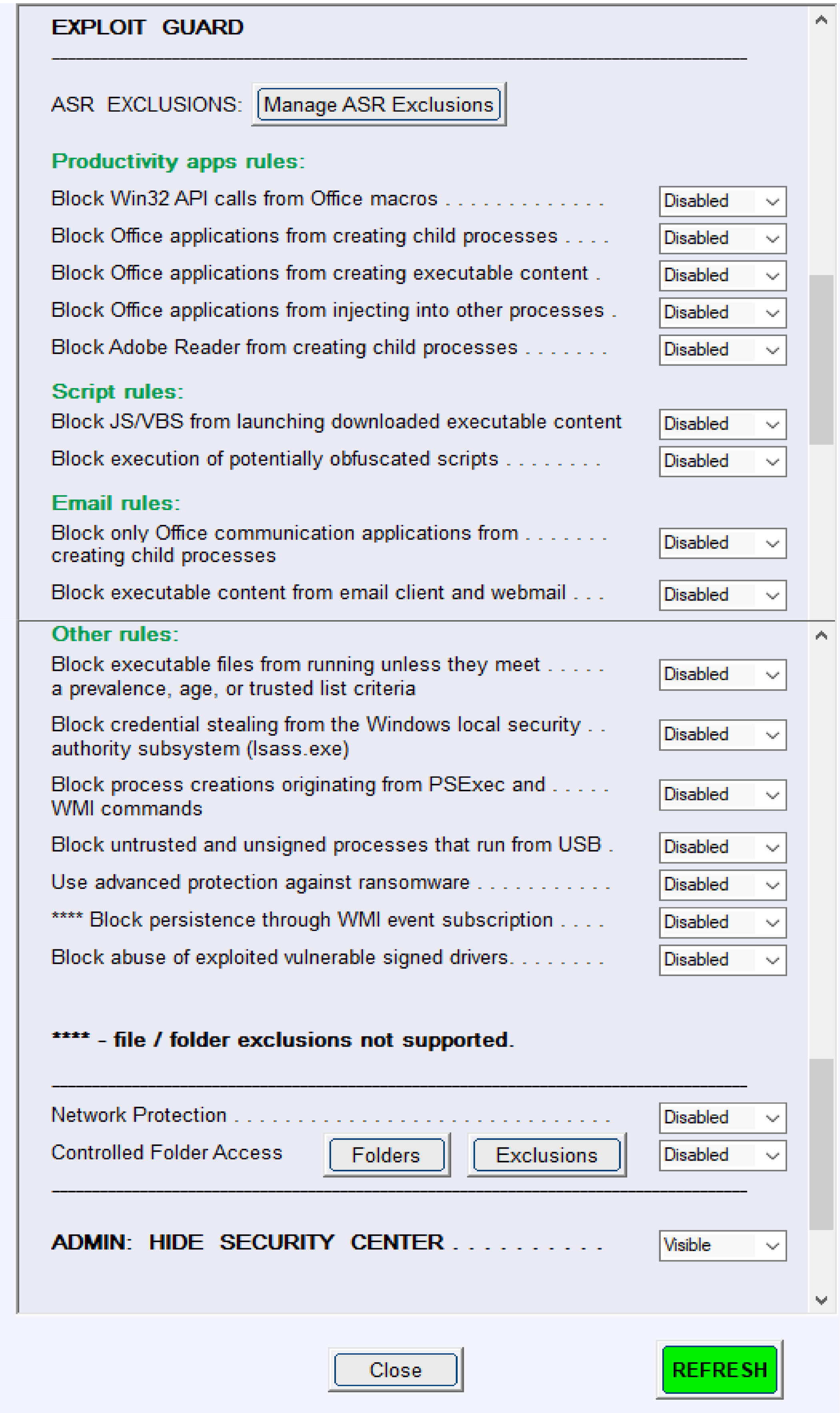
Behavior Monitoring	ON
Block At First Sight	ON
Cloud-delivered Protection	ON
Automatic Sample Submission	Send
Scan all downloaded files and attachments	ON
Script Scanning	ON
PUA Protection	Disabled
Cloud Protection Level	Default
Cloud Check Time Limit	10s
Average CPU Load while scanning	50%



ADMIN: SMARTSCREEN

When set to 'User', it can be configured and bypassed by the User.

For Explorer	User
For Edge (not Chromium)	User
For Internet Explorer	User



EXPLOIT GUARD

ASR EXCLUSIONS:

Productivity apps rules:

Block Win32 API calls from Office macros . . . . Disabled
Block Office applications from creating child processes . . . . Disabled
Block Office applications from creating executable content . Disabled
Block Office applications from injecting into other processes . Disabled
Block Adobe Reader from creating child processes . . . . Disabled

Script rules:

Block JS/VBS from launching downloaded executable content Disabled
Block execution of potentially obfuscated scripts . . . . Disabled

Email rules:

Block only Office communication applications from . . . . creating child processes Disabled
Block executable content from email client and webmail . . . Disabled

Other rules:

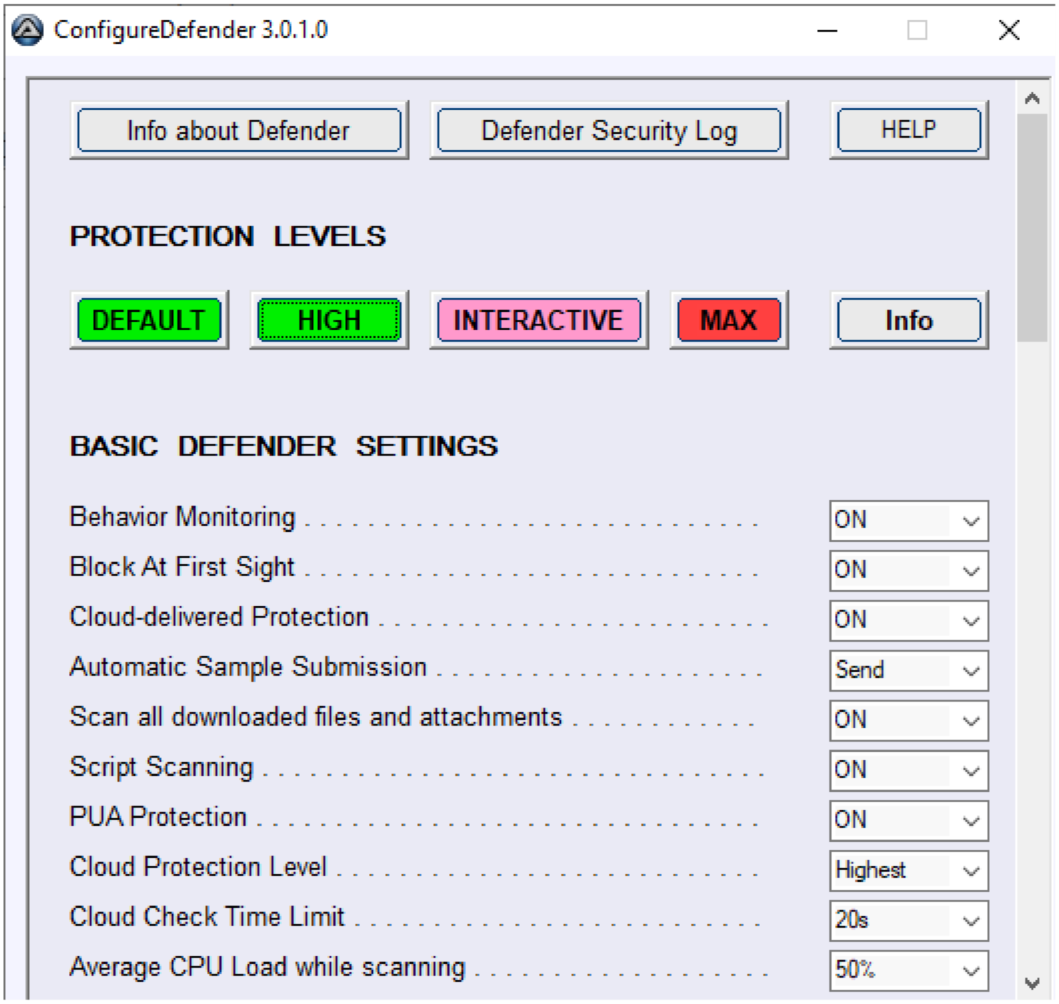
Block executable files from running unless they meet . . . . . a prevalence, age, or trusted list criteria Disabled
Block credential stealing from the Windows local security . . authority subsystem (lsass.exe) Disabled
Block process creations originating from PSExec and . . . . . WMI commands Disabled
Block untrusted and unsigned processes that run from USB . Disabled
Use advanced protection against ransomware . . . . Disabled
**** Block persistence through WMI event subscription . . . . Disabled
Block abuse of exploited vulnerable signed drivers. . . . . Disabled

****** - file / folder exclusions not supported.**

Network Protection . . . . Disabled
Controlled Folder Access Disabled

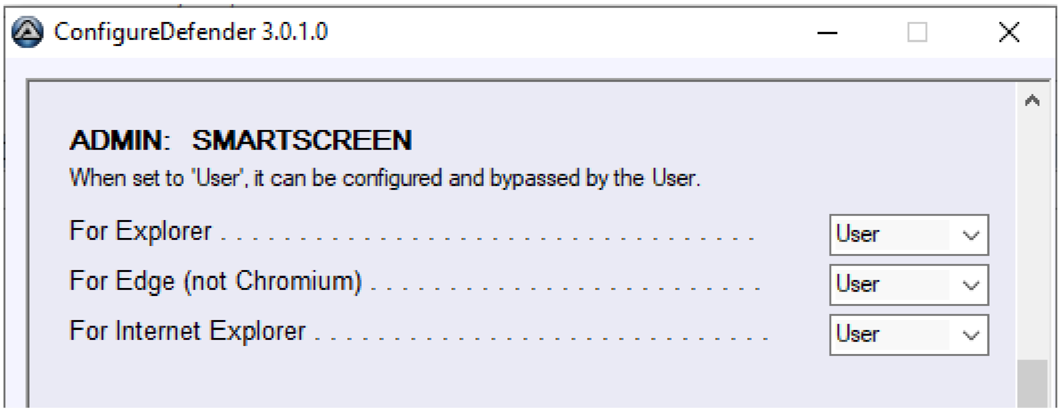
ADMIN: HIDE SECURITY CENTER . . . . Visible

The HIGH Protection Level applies the other settings as follows:



BASIC DEFENDER SETTINGS

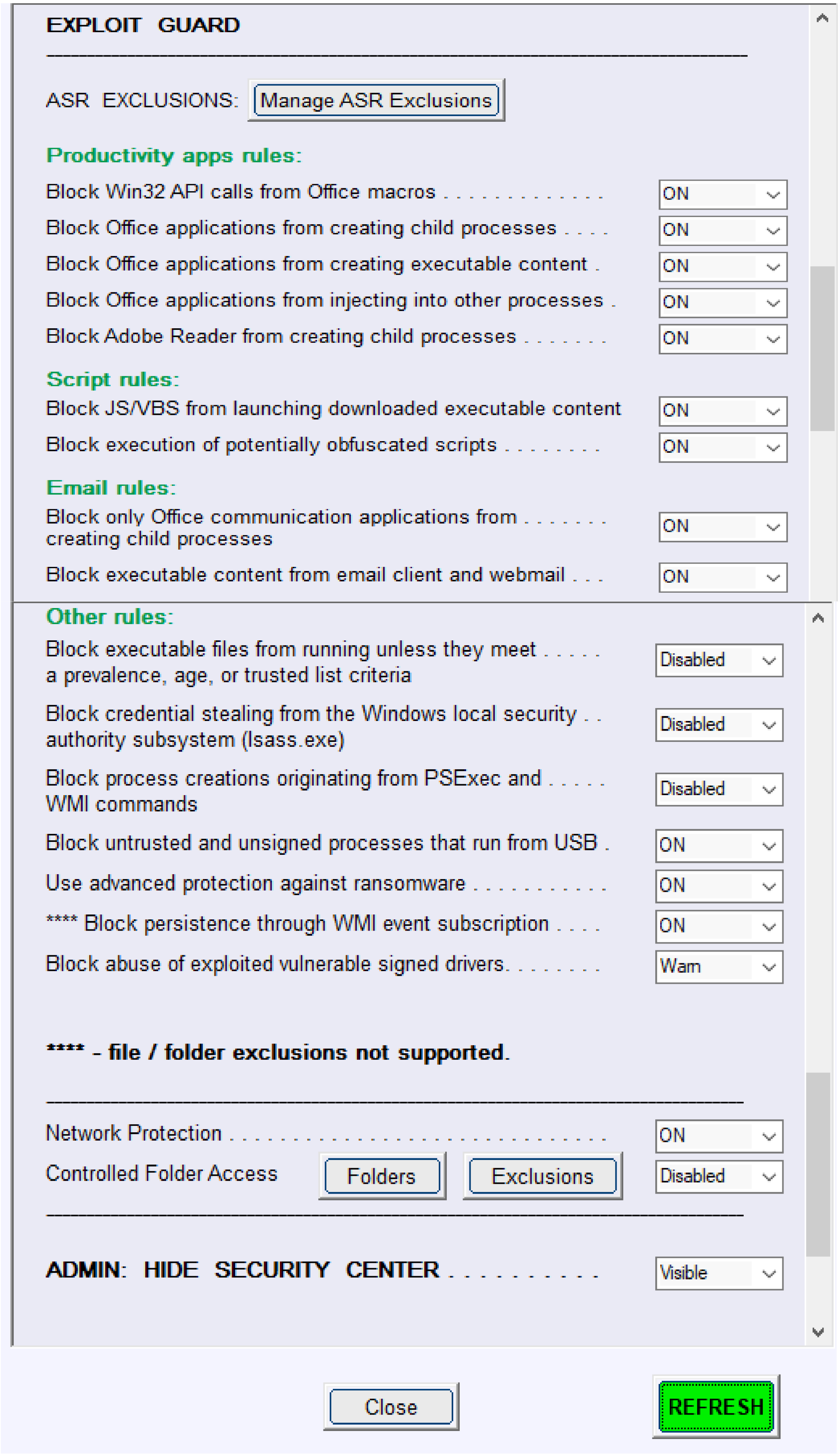
Behavior Monitoring	ON
Block At First Sight	ON
Cloud-delivered Protection	ON
Automatic Sample Submission	Send
Scan all downloaded files and attachments	ON
Script Scanning	ON
PUA Protection	ON
Cloud Protection Level	Highest
Cloud Check Time Limit	20s
Average CPU Load while scanning	50%



ADMIN: SMARTSCREEN

When set to 'User', it can be configured and bypassed by the User.

For Explorer	User
For Edge (not Chromium)	User
For Internet Explorer	User



EXPLOIT GUARD

ASR EXCLUSIONS:

Productivity apps rules:

Block Win32 API calls from Office macros . . . . ON
Block Office applications from creating child processes . . . . ON
Block Office applications from creating executable content . ON
Block Office applications from injecting into other processes . ON
Block Adobe Reader from creating child processes . . . . ON

Script rules:

Block JS/VBS from launching downloaded executable content ON
Block execution of potentially obfuscated scripts . . . . ON

Email rules:

Block only Office communication applications from creating child processes . . . . ON
Block executable content from email client and webmail . . . ON

Other rules:

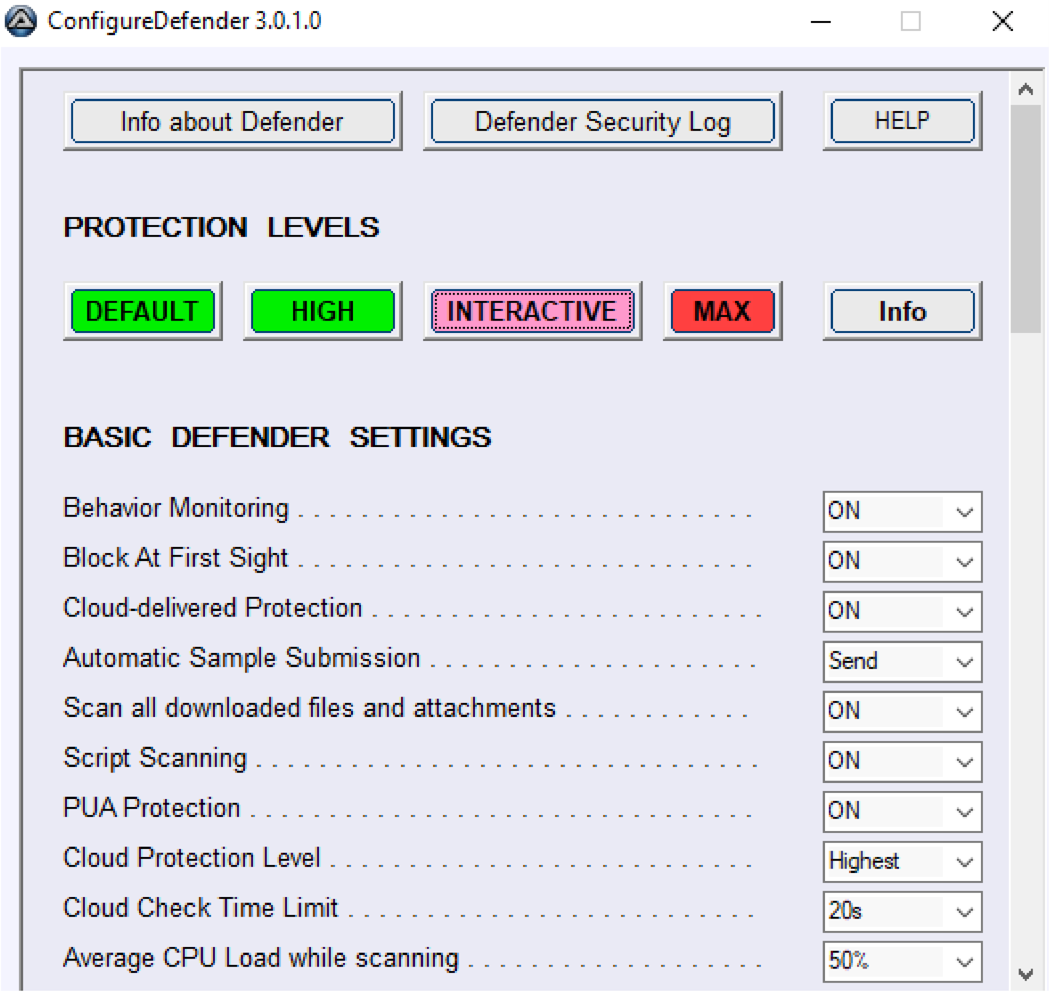
Block executable files from running unless they meet a prevalence, age, or trusted list criteria . . . . . Disabled
Block credential stealing from the Windows local security authority subsystem (lsass.exe) . . Disabled
Block process creations originating from PSExec and WMI commands . . . . . Disabled
Block untrusted and unsigned processes that run from USB . ON
Use advanced protection against ransomware . . . . ON
**** Block persistence through WMI event subscription . . . . ON
Block abuse of exploited vulnerable signed drivers. . . . . Warn

****** - file / folder exclusions not supported.**

Network Protection . . . . ON
Controlled Folder Access Disabled

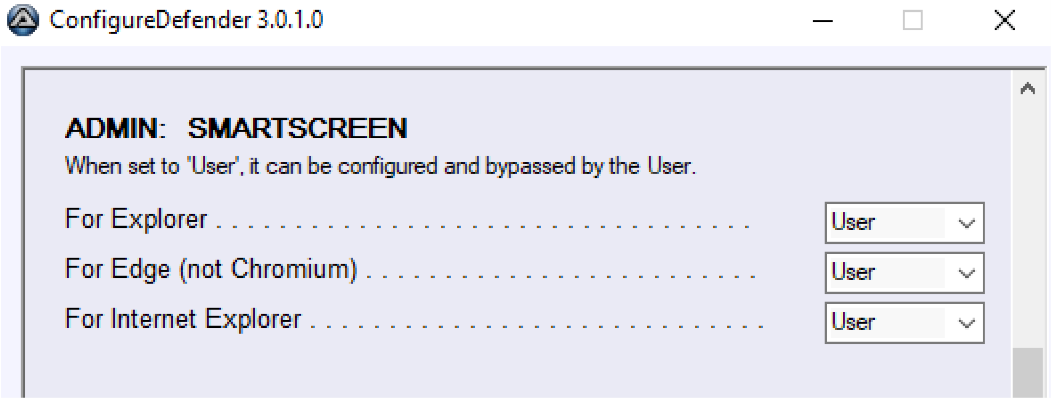
ADMIN: HIDE SECURITY CENTER . . . . Visible

The INTERACTIVE Protection Level applies the other settings as follows:



BASIC DEFENDER SETTINGS

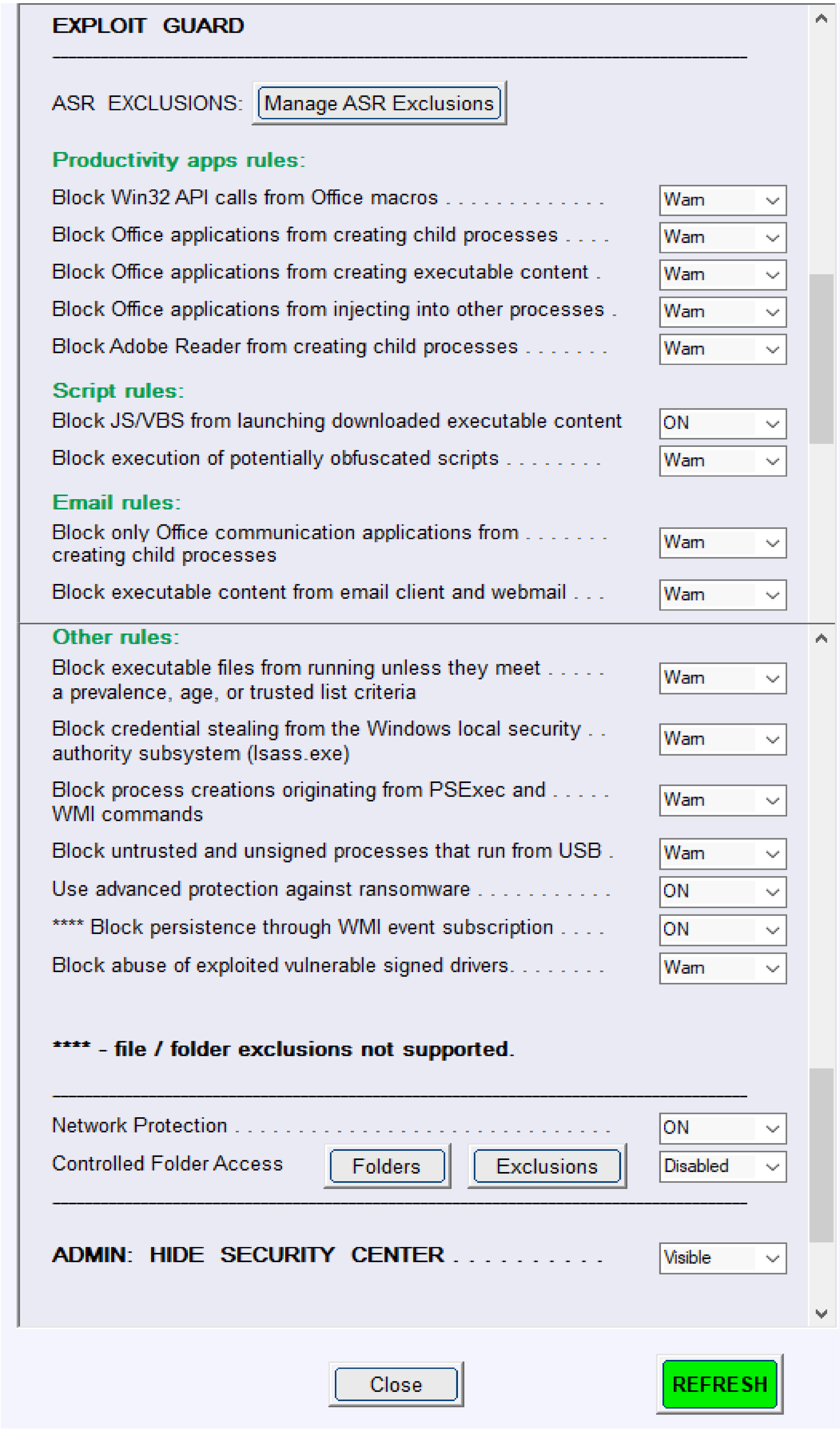
Behavior Monitoring	ON
Block At First Sight	ON
Cloud-delivered Protection	ON
Automatic Sample Submission	Send
Scan all downloaded files and attachments	ON
Script Scanning	ON
PUA Protection	ON
Cloud Protection Level	Highest
Cloud Check Time Limit	20s
Average CPU Load while scanning	50%



ADMIN: SMARTSCREEN

When set to 'User', it can be configured and bypassed by the User.

For Explorer	User
For Edge (not Chromium)	User
For Internet Explorer	User



EXPLOIT GUARD

ASR EXCLUSIONS:

Productivity apps rules:

Block Win32 API calls from Office macros	Warn
Block Office applications from creating child processes	Warn
Block Office applications from creating executable content .	Warn
Block Office applications from injecting into other processes .	Warn
Block Adobe Reader from creating child processes	Warn

Script rules:

Block JS/VBS from launching downloaded executable content	ON
Block execution of potentially obfuscated scripts	Warn

Email rules:

Block only Office communication applications from . . . . creating child processes	Warn
Block executable content from email client and webmail . . .	Warn

Other rules:

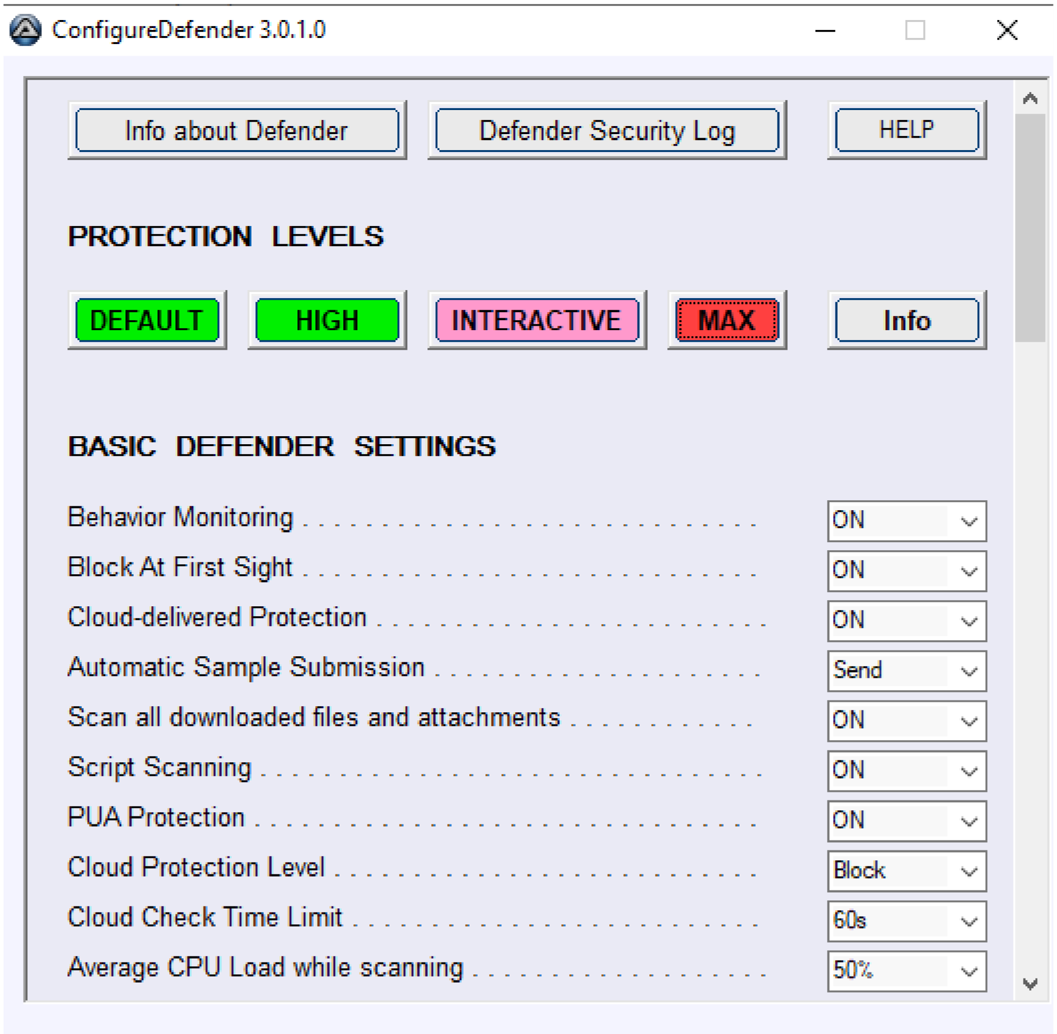
Block executable files from running unless they meet . . . . . a prevalence, age, or trusted list criteria	Warn
Block credential stealing from the Windows local security . . authority subsystem (lsass.exe)	Warn
Block process creations originating from PSExec and . . . . . WMI commands	Warn
Block untrusted and unsigned processes that run from USB .	Warn
Use advanced protection against ransomware	ON
**** Block persistence through WMI event subscription	ON
Block abuse of exploited vulnerable signed drivers.	Warn

****** - file / folder exclusions not supported.**

Network Protection	ON
Controlled Folder Access	Disabled

ADMIN: HIDE SECURITY CENTER	Visible

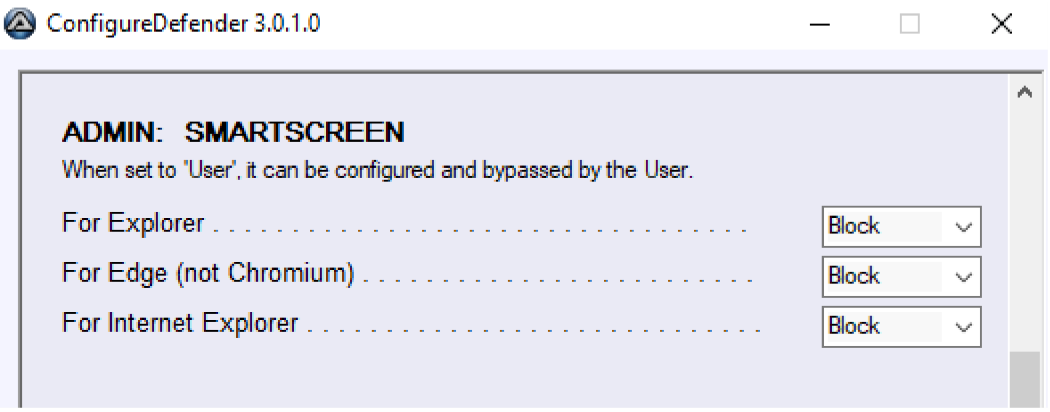
The MAX Protection Level applies the other settings as follows:



PROTECTION LEVELS

BASIC DEFENDER SETTINGS

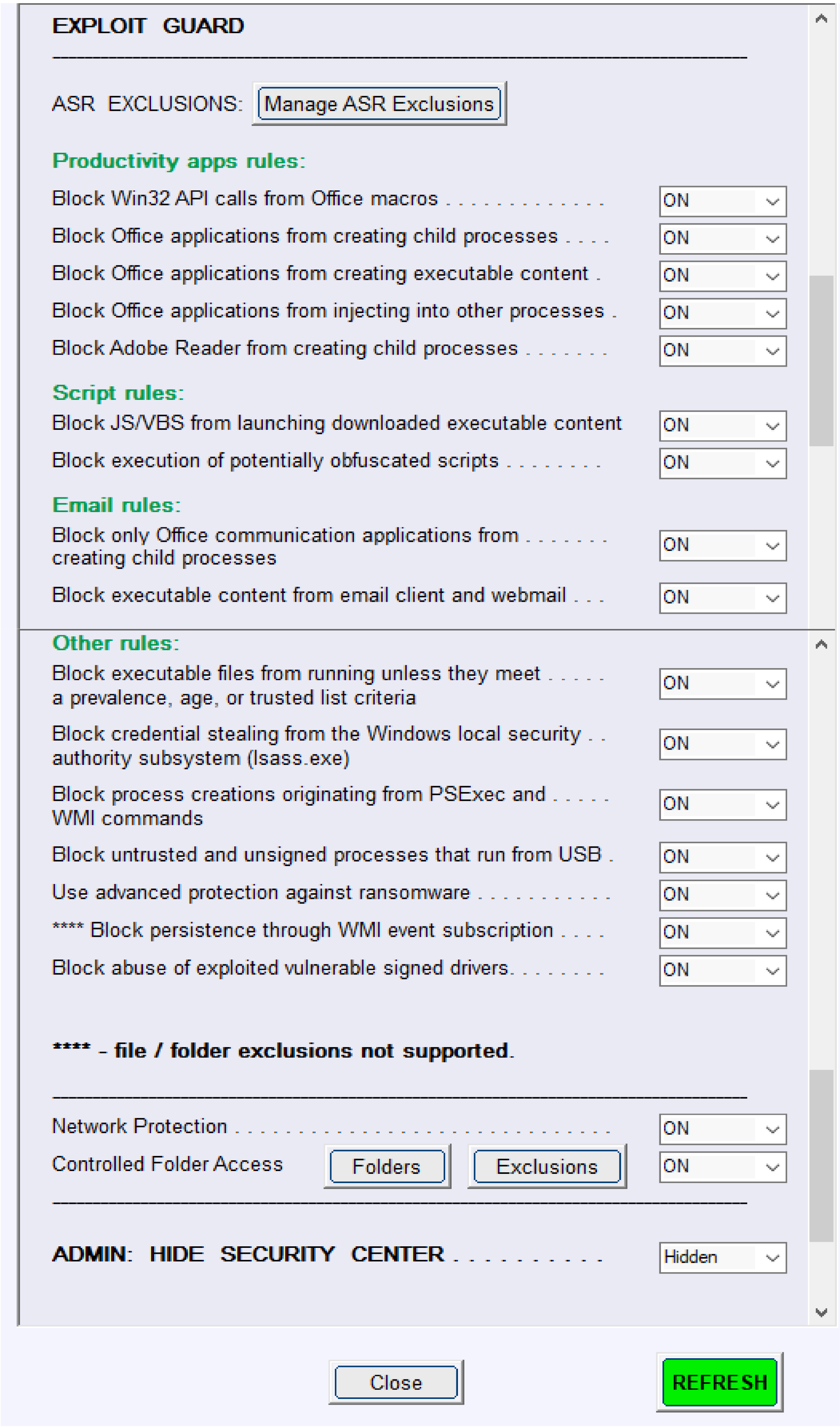
Behavior Monitoring . . . . ON
Block At First Sight . . . . ON
Cloud-delivered Protection . . . . ON
Automatic Sample Submission . . . . Send
Scan all downloaded files and attachments . . . . ON
Script Scanning . . . . ON
PUA Protection . . . . ON
Cloud Protection Level . . . . Block
Cloud Check Time Limit 60s
Average CPU Load while scanning 50%



ADMIN: SMARTSCREEN

When set to 'User', it can be configured and bypassed by the User.

For Explorer . . . . Block
For Edge (not Chromium) . . . . Block
For Internet Explorer . . . . Block



EXPLOIT GUARD

ASR EXCLUSIONS:

Productivity apps rules:

Block Win32 API calls from Office macros	ON
Block Office applications from creating child processes	ON
Block Office applications from creating executable content	ON
Block Office applications from injecting into other processes	ON
Block Adobe Reader from creating child processes	ON

Script rules:

Block JS/VBS from launching downloaded executable content	ON
Block execution of potentially obfuscated scripts	ON

Email rules:

Block only Office communication applications from creating child processes	ON
Block executable content from email client and webmail	ON

Other rules:

Block executable files from running unless they meet a prevalence, age, or trusted list criteria	ON
Block credential stealing from the Windows local security authority subsystem (lsass.exe)	ON
Block process creations originating from PSExec and WMI commands	ON
Block untrusted and unsigned processes that run from USB	ON
Use advanced protection against ransomware	ON
**** Block persistence through WMI event subscription	ON
Block abuse of exploited vulnerable signed drivers.	ON

****** - file / folder exclusions not supported.**

Network Protection	ON
Controlled Folder Access	ON

ADMIN: HIDE SECURITY CENTER	Hidden

IV. NOTES ABOUT ASR RULES AND CFA

Block credential stealing from the Windows local security
This ASR rule can make a lot of noise in the Defender Security Log. Most of the blocked events are usually false positives when the legal application tries to enumerate running processes and attempts to open them with exhaustive permissions. These applications can be excluded by using <Manage ASR Exclusions>.

Block executable files from running unless they meet a prevalence, age, or trusted list criteria
This rule is strong prevention against Polymorphic malware (EXE, DLL, etc.), but one has to accept the higher rate of false positives for application installers/updaters.
The prevalence is related to 1000 machines and age to 24 hours. The trusted list criteria are managed by Microsoft. The rule can recognize executables as suspicious only when Defender can connect to the Microsoft cloud. From my experience, most executable files blocked by this rule (application installers/updaters) are allowed after 48 hours. Anyway, some applications with a very low prevalence can be blocked for several days, and the users usually do not know how to unblock them.
Please note: It is not necessary to add exclusions for this rule. When it is used with the "ON" setting, the proper procedure to unblock files is as follows:

1. Set the rule temporarily to Audit - for simple installations, one can also use the Warn setting instead of Audit.
2. Run the installer/updater >> install/update the application.
3. Set the rule to Warn >> run the application >> use Unblock option in Defender's prompt (a few times times if required).

Block process creations originating from PSExec and WMI commands
This rule is important because malware can try to bypass the parent-child checking by using WMI. So, other ASR rules based on checking child processes will fail. On some computers, the WMI can be used by the computer's firmware so it is better to initially set this ASR rule to Audit.

Block abuse of exploited vulnerable signed drivers
This rule is important for protecting Windows kernel against exploits related to legal but vulnerable drivers. Such drivers can be used to perform dangerous attacks. The drivers already installed on the computer are not blocked. It is recommended to initially set this rule to Audit or Warn.

Controlled Folder Access (CFA)
ConfigureDefender can set CFA via four settings:

- ON - malicious and suspicious apps won't be allowed to make changes to files in protected **folders** (Id = 1123) and to write to protected **disk sectors** (Id = 1127),
- BDMO = Block Disk Modifications Only - malicious and suspicious apps won't be allowed to write only to protected **disk sectors** (Id = 1127),
- Disabled - CFA protection is disabled,
- Audit - Changes will be allowed, but they will be recorded in the Windows event log (Id = 1124 and Id = 1128).

When CFA is set to ON, BDMO, or Audit, the events are logged in the Window Event Log (Ids = 1123, 1124, 1127, 1128). These events can be also seen by using the button <Defender Security Log> in ConfigureDefender. When events 1127 or 1128 are logged, the Defender alerts about **memory modifications,** but these are disk memory modifications (disk sector writes) - not related to RAM.
CFA can be very useful as anti-ransomware protection, but only after excluding the applications that

need to access protected **folders** and applications that need to access protected **disk sectors**. The second group can include backup applications, disk management applications, disk optimization programs, etc. It is recommended to set initially this rule to Audit.

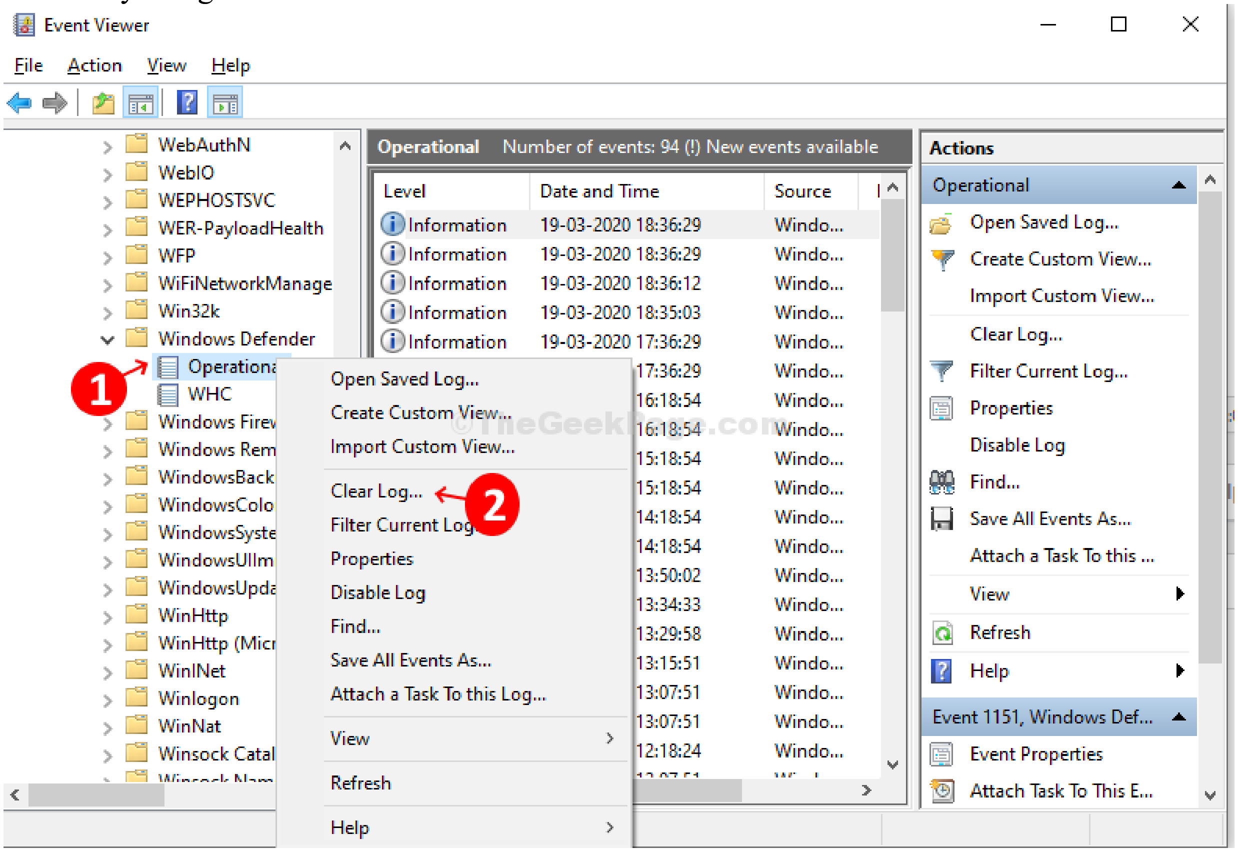
Making ASR exclusions for Universal Windows Platform (UWP) apps.

These apps are installed in the **Program Files\WindowsApps** folder, which is not directly accessible via Exclusions File Explorer. This issue can be avoided as follows:

1. Copy the full path of the blocked UWP app executable.
2. Use <Manage ASR Exclusions> in ConfigureDefender and choose <Add File> to open Exclusions File Explorer.
3. Paste this path to the Exclusions File Explorer in the place of File name.
4. Press the <Open> button.

V. Clearing the <Defender Security Log>

ConfigureDefender uses Windows Event Log to show events related to Defender. So, the log can be cleared by using Event Viewer:



Operational Number of events: 94 (!) New events available

Level	Date and Time	Source
Information	19-03-2020 18:36:29	Windo...
Information	19-03-2020 18:36:29	Windo...
Information	19-03-2020 18:36:12	Windo...
Information	19-03-2020 18:35:03	Windo...
Information	19-03-2020 17:36:29	Windo...
	17:36:29	Windo...
	16:18:54	Windo...
	16:18:54	Windo...
	15:18:54	Windo...
	15:18:54	Windo...
	14:18:54	Windo...
	14:18:54	Windo...
	13:50:02	Windo...
	13:34:33	Windo...
	13:29:58	Windo...
	13:15:51	Windo...
	13:07:51	Windo...
	13:07:51	Windo...
	12:18:24	Windo...

Instead of using Event Viewer to delete the Defender Operational events, one can run Wevtutil tool from the Administrator PowerShell console or Administrator CMD console with command-line:

```
wevtutil cl "Microsoft-Windows-Windows Defender/Operational"
```

VI. Info for Administrators.

Defender stores its native settings under the registry key (owned by SYSTEM):
HKLM\SOFTWARE\Microsoft\Windows Defender
These can be changed when using PowerShell cmdlets. A few settings can be also changed from Windows Security Center.

Administrators can use Group Policy Management Console to apply the Defender policy settings. They are stored under another registry key (policy key owned by ADMINISTRATORS):
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender
Group Policy settings can override but do not change native Defender settings. The native settings **are automatically recovered when removing** Group Policy settings.

ConfigureDefender removes the settings made via direct registry editing under the policy key:
HKLM\SOFTWARE\Policies\Microsoft\Windows Defender
This is required because those settings would override ConfigureDefender settings.

ConfigureDefender works on all Windows editions (including Windows Home). On Windows Server and Windows Professional/Enterprise editions, ConfigureDefender can work properly only if the Administrator did not applied Defender policies by using another management tool, for example, Group Policy Management Console. These policies are set to "Not configured" by default. **If they have been changed by the Administrator, then they should be reset to "Not configured".**
Group Policy settings may be found in Group Policy Management Console:
Computer Configuration > Policies > Administrative Templates > Windows Components > Microsoft Defender Antivirus
The settings under the tabs: MAPS, MpEngine, Real-time Protection, Reporting Scan, Spynet, and Windows Defender Exploit Guard should be examined.

Please note: Group Policy Refresh feature will override ConfigureDefender settings if Defender Group Policy settings are not reset to "Not configured"!
ConfigureDefender should not be used alongside other management tools deployed in Enterprises, like Intune or MDM CSPs.

Useful links:

GitHub - AndyFul/ConfigureDefender: Utility for configuring Windows 10 built-in Defender antivirus settings.

Attack surface reduction rules reference | Microsoft Docs

Microsoft Defender Attack Surface Reduction recommendations | Palantir Blog

Use attack surface reduction rules to prevent malware infection - Windows security | Microsoft Docs

Attack surface reduction frequently asked questions (FAQ) | Microsoft Docs

Microsoft Defender for Endpoint - Microsoft Tech Community

Update - ConfigureDefender utility for Windows 10 | MalwareTips Community

@Andy Ful