

ConfigureDefender Help (ver. 3.0.1.0)

ConfigureDefender works on Windows 10 - earlier versions are not supported. If the user upgraded the system from Windows 8 or 8.1 and it is still possible to downgrade while preserving user settings, then the application shows the alert and exits. This prevents transferring the settings (made by ConfigureDefender) from Windows 10 to previous versions, when the user forgot to restore Defender default settings before downgrading.

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 of 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 hides 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 a Protection Level 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 will log events and warn 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 the user an option to unblock the content. The user can then retry their action, and the operation completes. When a user unblocks content, the content remains unblocked for 24 hours, and then blocking resumes. Warn mode is not supported on devices running older versions of Windows. In those cases, ASR rules that are configured to run in Warn mode will run in block mode (the "ON" setting).

<Defender Security Log> button:

It can be used gather the last 300 entries from the Microsoft Defender Antivirus events. These entries are reformatted and displayed in the notepad.

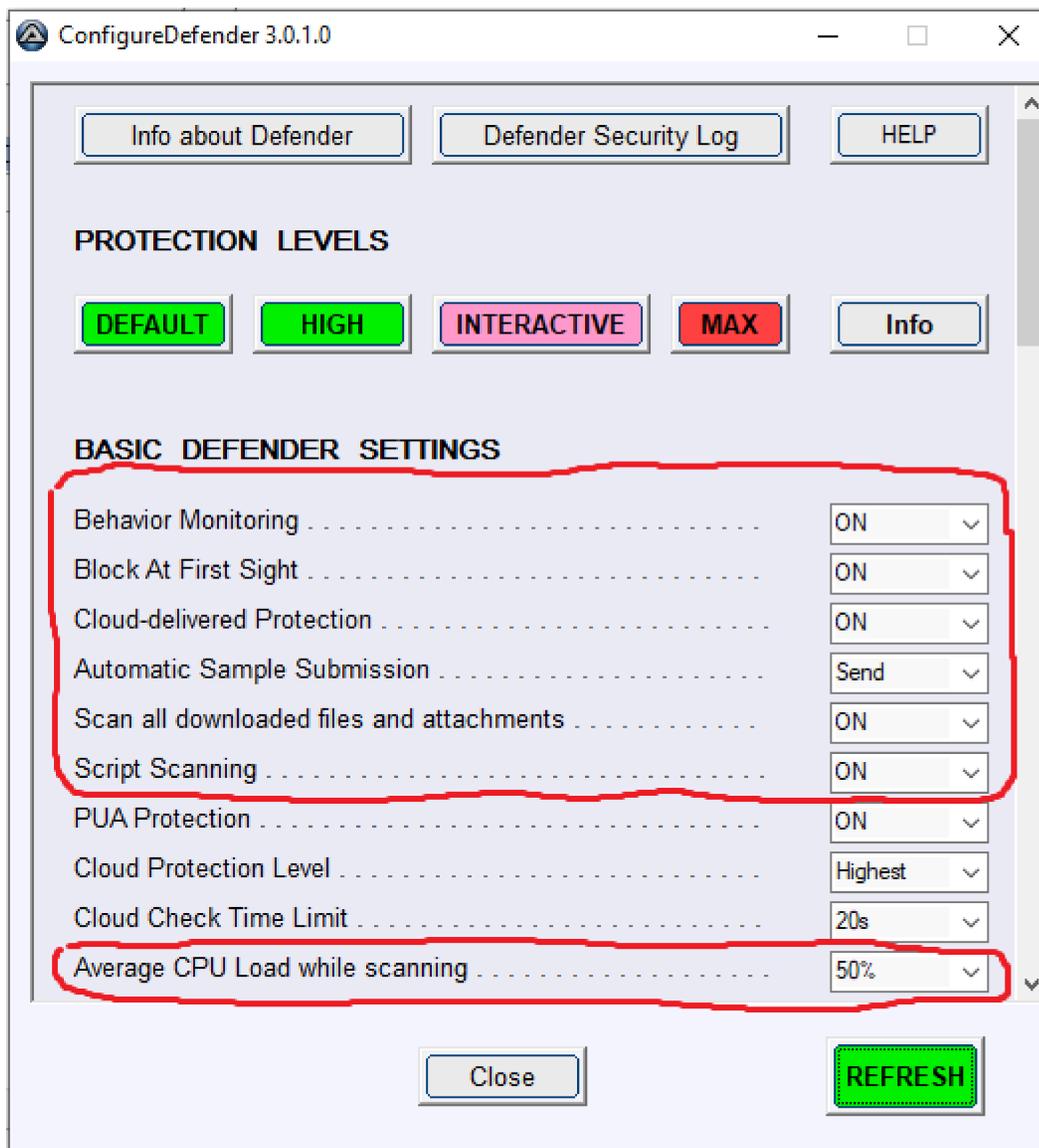
The following event IDs are included: 1006, 1008, 1015, 1116, 1118, 1119, 1121, 1122, 1123, 1124, 1125, 1126, 1127, 1128, 3002, 5001, 5004, 5008, 5010, and 5012. Inspecting the log can be useful when a process or file execution has been blocked by the Defender Exploit Guard.

III. Protection Levels

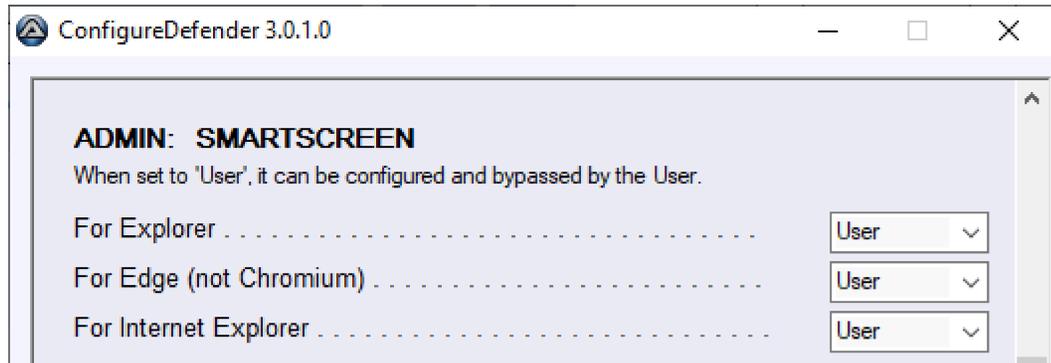
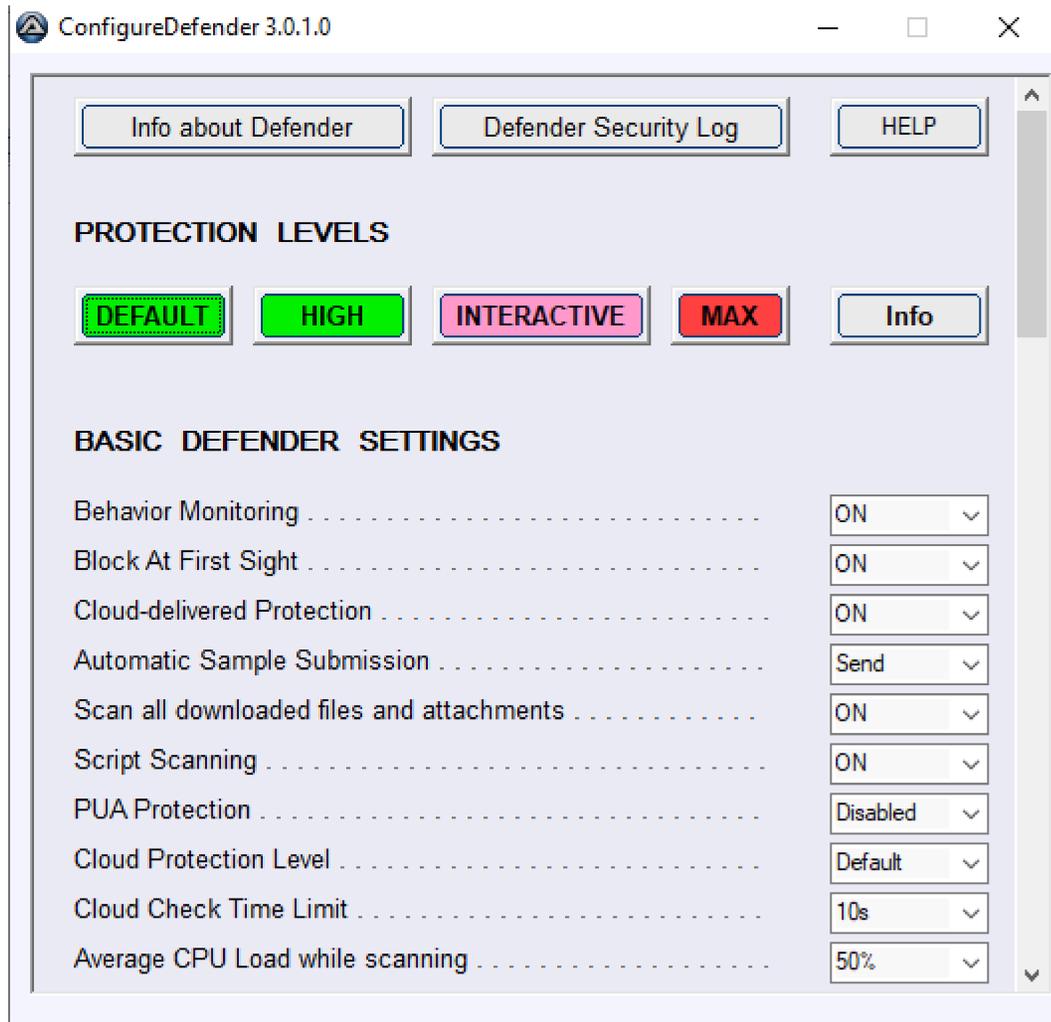
The below settings are the same for **DEFAULT, HIGH, INTERACTIVE, and MAX** Protection Levels:

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%



The **DEFAULT** Protection Level applies the other settings as follows:



EXPLOIT GUARD

ASR EXCLUSIONS: [Manage 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 Disabled ▾
creating child processes
- Block executable content from email client and webmail Disabled ▾

Other rules:

- Block executable files from running unless they meet Disabled ▾
a prevalence, age, or trusted list criteria
- Block credential stealing from the Windows local security . . . Disabled ▾
authority subsystem (lsass.exe)
- Block process creations originating from PSEXEC and Disabled ▾
WMI commands
- 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.

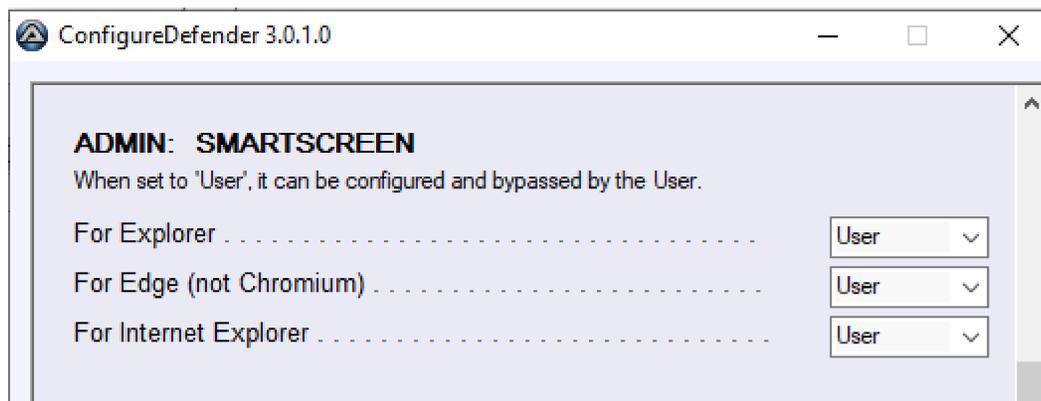
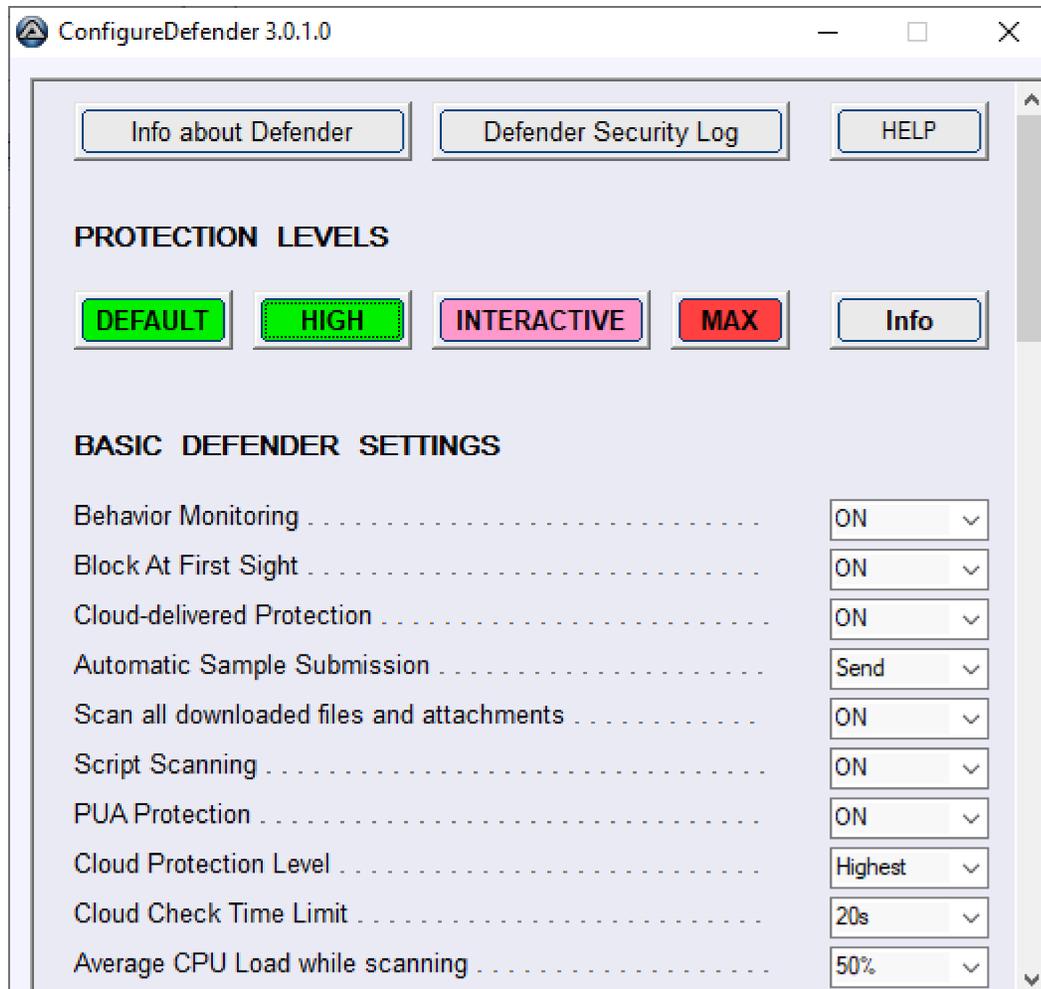
- Network Protection Disabled ▾
- Controlled Folder Access [Folders](#) [Exclusions](#) Disabled ▾

ADMIN: HIDE SECURITY CENTER Visible ▾

Close

REFRESH

The HIGH Protection Level applies the other settings as follows:



EXPLOIT GUARD

ASR EXCLUSIONS: [Manage 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 ON ▾
creating child processes
- Block executable content from email client and webmail . . . ON ▾

Other rules:

- Block executable files from running unless they meet Disabled ▾
a prevalence, age, or trusted list criteria
- Block credential stealing from the Windows local security . . Disabled ▾
authority subsystem (lsass.exe)
- Block process creations originating from PSEXec and Disabled ▾
WMI commands
- 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. Wam ▾

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

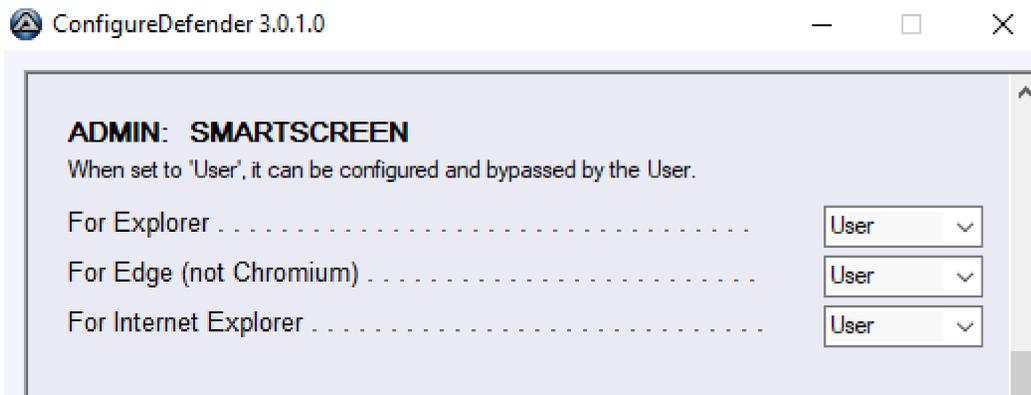
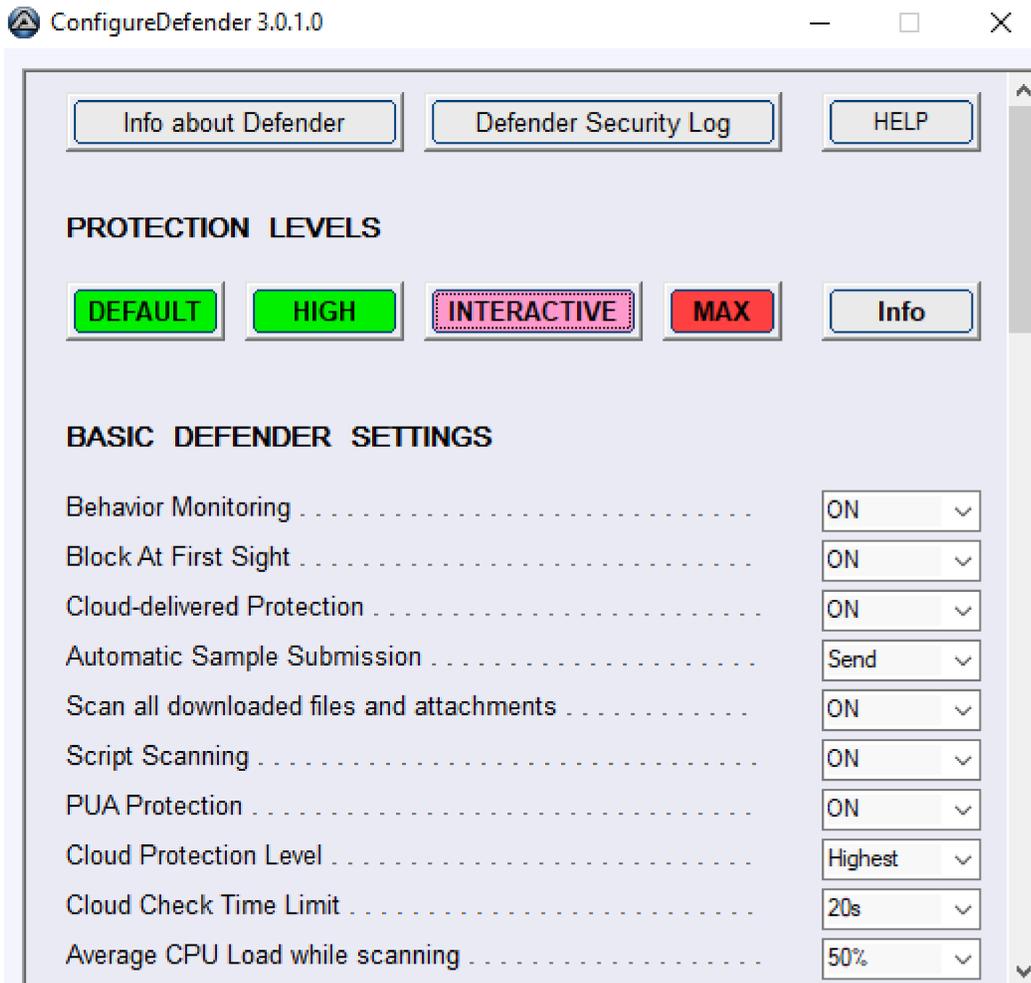
- Network Protection ON ▾
- Controlled Folder Access [Folders](#) [Exclusions](#) Disabled ▾

ADMIN: HIDE SECURITY CENTER Visible ▾

Close

REFRESH

The INTERACTIVE Protection Level applies the other settings as follows:



EXPLOIT GUARD

ASR EXCLUSIONS: [Manage ASR Exclusions](#)

Productivity apps rules:

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

Script rules:

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

Email rules:

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

Other rules:

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

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

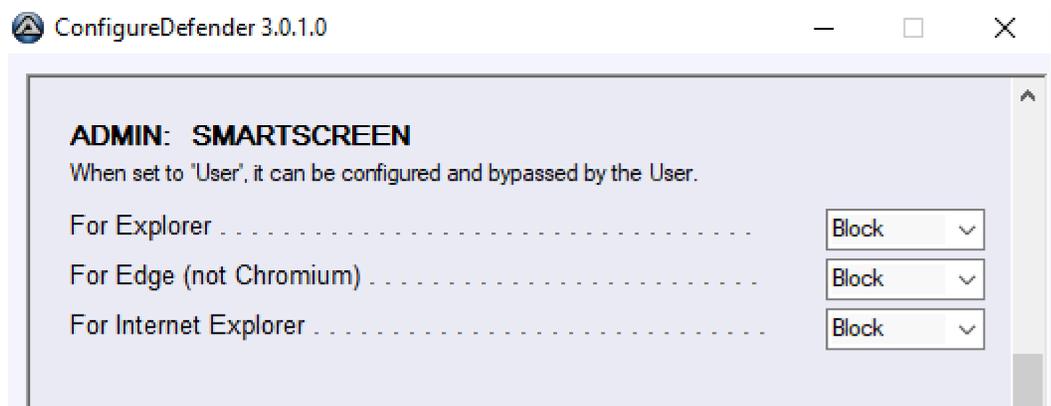
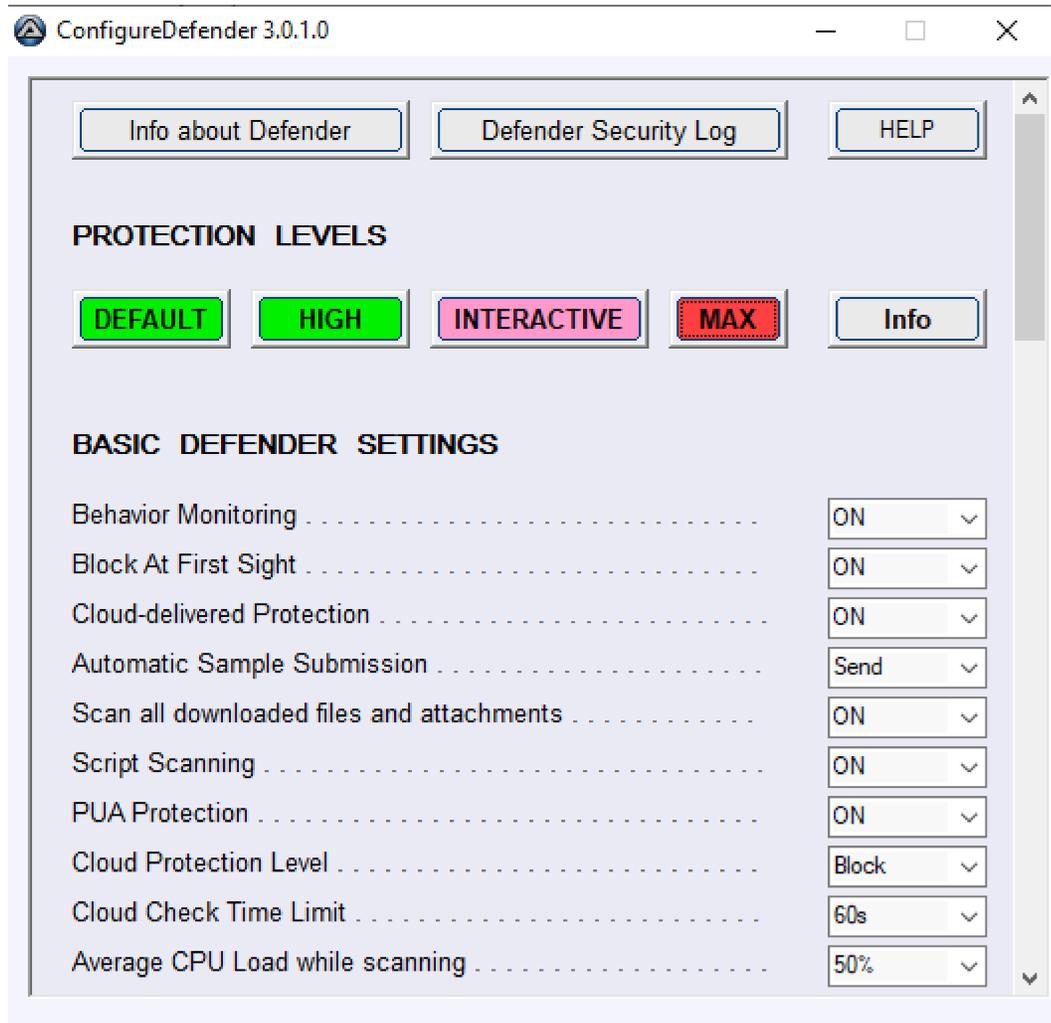
- Network Protection ▾
- Controlled Folder Access [Folders](#) [Exclusions](#) ▾

ADMIN: HIDE SECURITY CENTER ▾

Close

REFRESH

The MAX Protection Level applies the other settings as follows:



EXPLOIT GUARD

ASR EXCLUSIONS: [Manage 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 ON ▾
creating child processes
- Block executable content from email client and webmail ON ▾

Other rules:

- Block executable files from running unless they meet ON ▾
a prevalence, age, or trusted list criteria
- Block credential stealing from the Windows local security . . . ON ▾
authority subsystem (lsass.exe)
- Block process creations originating from PSEXEC and ON ▾
WMI commands
- 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 [Folders](#) [Exclusions](#) ON ▾

ADMIN: HIDE SECURITY CENTER Hidden ▾

Close

REFRESH

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 useless 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 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.

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 set initially this ASR rule to Audit.

Controlled Folder Access

It can be very useful, but only after excluding the applications that need to access protected folders and applications that need to access the protected disk areas. The second group can include backup applications, disk management applications, and disk optimization programs. 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. Changes made in different Windows versions.

Microsoft added new Defender features with successive Windows 10 feature updates. Below is the list of ConfigureDefender features available on **different versions of Windows 10**:

- *At least Windows 10*
Real-time Monitoring, Cloud-delivered Protection, Cloud Check Time Limit, Automatic Sample Submission, Behavior Monitoring, Scan all downloaded files and attachments, Average CPU Load while scanning, PUA Protection
- *At least Windows 10, version 1607 (Anniversary Update)*
Block At First Sight
- *At least Windows 10, version 1703 (Anniversary Update)*
Cloud Protection Level, Cloud Check Time Limit (Extended to 60s)
- *At least Windows 10, version 1709 (Creators Fall Update)*
Attack Surface Reduction, Cloud Protection Level (extended Levels: Highest, Block), Controlled Folder Access, Network Protection
- *At least Windows 10, version 1809*
Attack Surface Reduction Warn mode (Minimum platform release requirement: 4.18.2008.9 and Minimum engine release requirement: 1.1.17400.5)

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.

The ConfigureDefender utility 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.

The ConfigureDefender utility may be used on all Windows 10 versions. **But, on Windows Professional and Enterprise editions it will only work if your Administrator has 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 to configure the settings, 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.](#)

[Use attack surface reduction rules to prevent malware infection - Windows security | Microsoft Docs](#)

[Microsoft Defender for Endpoint - Microsoft Tech Community](#)

[Update - ConfigureDefender utility for Windows 10 | MalwareTips Community](#)

@Andy Ful