ConfigureDefender

ConfigureDefender utility is a GUI application to view and configure important Windows Defender settings on Windows 10. It mostly uses PowerShell cmdlets (with a few exceptions). Furthermore, the user can apply one of three predefined Protection Levels: Default, High, and Max. ConfigureDefender is integrated with Hard_Configurator GUI, but can be used as a standalone application, too.

Most settings available in ConfigureDefender are related to Windows Defender real-time protection and work only when Windows Defender real-time protection is set to "ON".

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"

ConfigureDefender Protection Levels (predefined settings):

"DEFAULT"
Microsoft Windows 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 Network Protection and most of Exploit Guard (ASR) features. Three Exploit Guard features and Controlled Folder Access ransomware protection are disabled to avoid false positives. This is the recommended configuration which is appropriate for most users and provides significantly increased security.

"MAX"
This is the most secure protection level which enables all advanced Windows 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 the "HIGH" settings and may require more user knowledge or skill.

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, Windows Defender will log events and warn the user about processes which 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.

Defender Security Log:
This option can gather the last 200 entries from the Windows Defender Antivirus events. These entries are reformatted and displayed in the notepad. The following event IDs are included: 1006, 1008, 1015, 1116, 1117, 1118, 1119, 1121, 1122, 1123, 1124, 1125, 1126, 1127, 1128, 3002, 5001, 5004, 5007, 5008, 5010, 5012. Inspecting the log can be useful when a process or file execution has been blocked by Windows Defender Exploit Guard.
ConfigureDefender works on Windows 10. Windows 8.1 and earlier versions are not supported. Microsoft has added new Windows 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 Protection Level (Default), 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
Cloud Protection Level (High level for Windows Pro & Enterprise), Cloud Check Time Limit (Extended to 60s)

At least Windows 10, version 1709 (Fall Creators Update)
Attack Surface Reduction, Cloud Protection Level (extended levels for Windows Pro & Enterprise), Controlled Folder Access, Network Protection.

Windows 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 policy settings for Windows Defender. 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 Windows 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 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 > Windows 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.