Configure Defender

Improve your system’s defences

Who

is Configure Defender for?

- For kids/elderly/casual for maximum safety
- For ordinary users
- For the savvy nerd

For kids/elderly/casual

- Enables all advanced (hidden) Microsoft Defender features
- More false positive alerts

For ordinary users

- Enhances default protections
- Some protections disabled to avoid false positives

For savvy users

- Highest protection
- More false positives/alerts
- Needs more judgement

- Max for kids/elderly/casual users
- Interactive for savvy users
- High for the rest of us

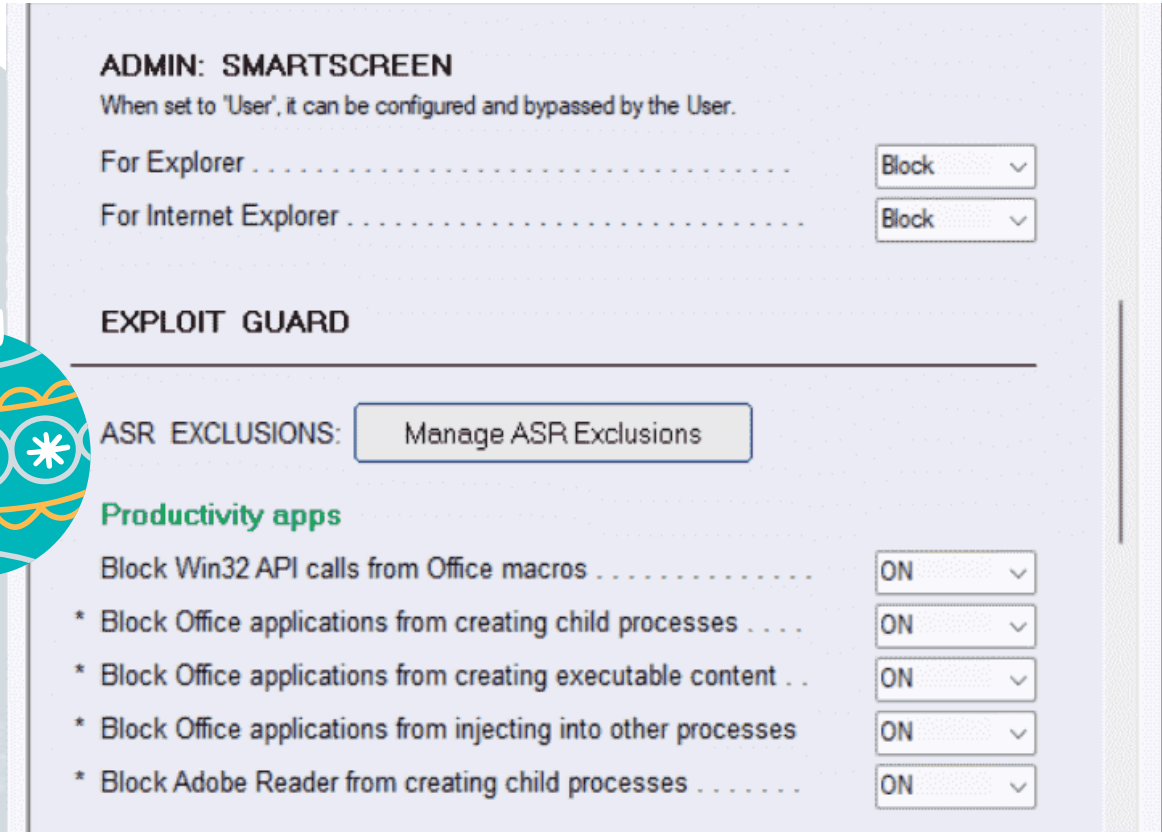
Refresh after High/Interactive/max shows updated settings

Log button shows last 300 entries

Circled items are the same for all initial configurations

SmartScreen uses web to check suspicions

Attack Surface Reduction (ASR) reduces possible vulnerabilities



More **ASR** rules

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 (no ASR exclusions).	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
Block rebooting machine in Safe Mode	Disabled
* Block use of copied or impersonated system tools	Disabled

Network protection

CFA - Controlled Folder Access

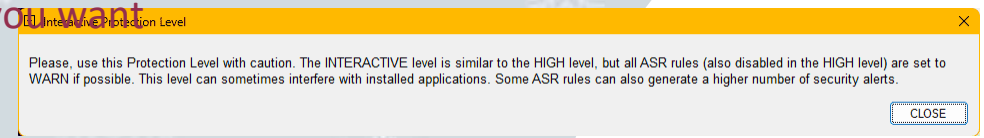
- ON - malicious/suspicious apps not allowed changes in protected folders or disk sectors
- BDMO = Block Disk Modifications Only - only protect disk sectors
- Audit - Changes will be allowed but logged
- Disabled - CFA protection & logging disabled

Settings

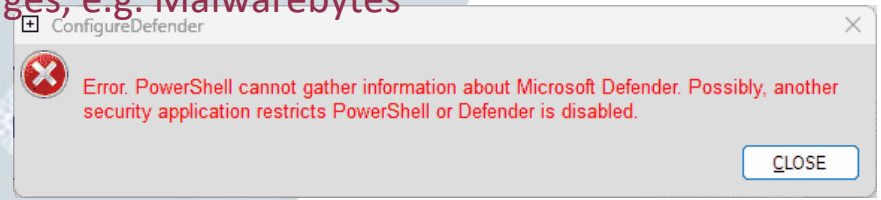
- ON - protection on
- WARN – User gets choice to enforce or bypass
  - Is unblocked (no warning) for 24 hours
- Audit – allow, but log
- Disabled – no protection, no logging

Caveats

- Fine-grained changes may frustrate you
- Interactive mode gives you control – perhaps more than you want



- May have to pause other real-time protection to allow changes, e.g. Malwarebytes



- Only Windows 10 & 11
- Group Policy Management, other enterprise security packages interfere. DO NOT USE TOGETHER
- Uses Powershell & registry edits

ConfigureDefender provides more protection to a variety of users

https://github.com/AndyFul/ConfigureDefender

https://github.com/AndyFul/ConfigureDefender/blob/master/ConfigureDefenderHelp.pdf


slidesgo