

# WDAC Lockdown 1.25



User Guide

June 2024

# Welcome to WDAC Lockdown

## **The Concept**

WDAC Lockdown simplifies Zero-Trust Endpoint Protection by enhancing and automating Microsoft WDAC to help you get to application control enforcement much quicker, while making the entire process as seamless and user-friendly as possible. In addition, WDAC Lockdown's Kernel Lockdown feature currently blocks 139 potentially dangerous file types, including scripts and other fileless malware.

WDAC Lockdown's WDAC Lockdown feature enhances and automates Microsoft's Windows Defender Application Control (WDAC) and enables you to quickly and effortlessly build WDAC policies customized to your system. End-users are prompted when WDAC blocks an event and are able to allow blocked events on the fly, all in real-time.

WDAC Lockdown also includes a training mode to make building the perfect WDAC policy for your system even easier. Simply place WDAC Lockdown in Training mode, and once you are finished training, select any of the other modes, and WDAC Lockdown will automatically build your new WDAC policy for you that will automatically allow all new events from the training period.

The Auto build policy feature is able to create entire customized policies with a single click. It can take anywhere from a few minutes to a couple of hours to automatically build the custom policies, depending on how extensive you want the policy to be.

Existing audit events can also be automatically allowed by utilizing WDAC Lockdown's "Whitelist all events from the last X days" feature. And the Reset User Policies feature will reset your WDAC policies to factory default, so you can start from scratch if you need to.

WDAC Lockdown also includes a customized version of the Microsoft WDAC Wizard that allows you to effortlessly create WDAC policies from scratch that are automatically deployed within WDAC Lockdown.

Windows Sandbox is also integrated into WDAC Lockdown. End-users can execute files in Windows Sandbox to test before executing on their local machine. Windows Sandbox must be activated on the system in order for this feature to function.

Warning: When enabled, Microsoft's Windows Defender Application Control (WDAC) might initially affect overall system performance until WDAC Lockdown finishes automatically building and refining the WDAC policies. Once the policies are customized to your system, overall system performance should return to normal.

## WDAC Lockdown Settings



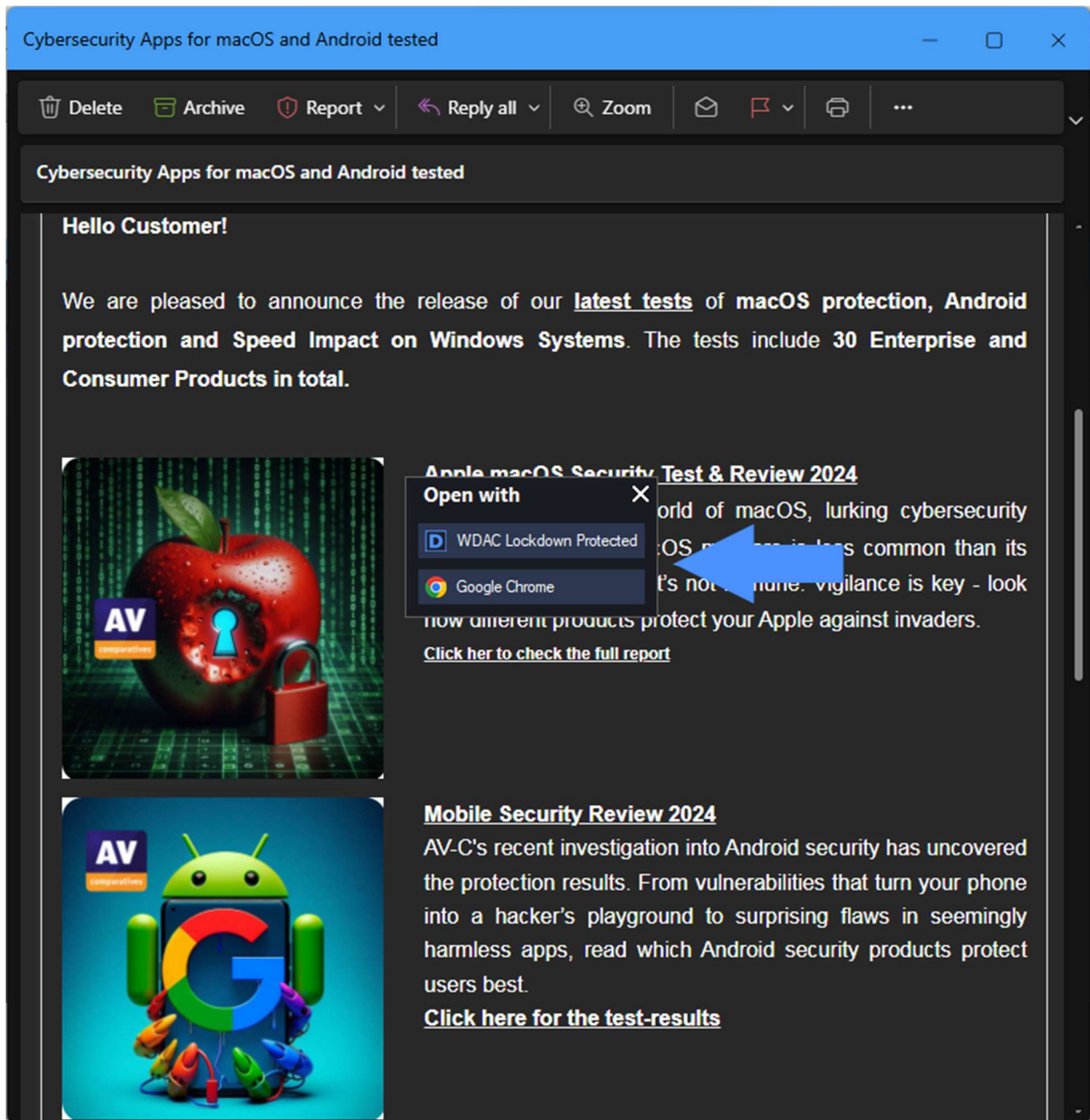
### Kernel Lockdown features

**Anti-Malware and Anti-Exploit Contextual Engine:** This feature is a collection of Zero-Trust Windows hardening rules that monitors the behaviors in an attack chain / process execution flow to detect potentially malicious activity. This feature also monitors and blocks scripts, exploits, LOLBins, and other suspicious or vulnerable processes.

**Scan non-whitelisted files before automatically allowing:** This feature scans non-whitelisted processes before they are allowed to automatically execute. Only files that the Contextual Engine determine to be potentially malicious or that are in potentially malicious locations are scanned. If this feature is disabled, files that comply with the Context Engine rules are not scanned and are automatically allowed.

**Dynamic Security Postures:** This feature utilizes VoodooSoft's patented automatic toggling computer lock feature to automatically lock the computer when the end-user is browsing the web, checking email, or is engaged in other potentially malicious activities. In other words, this feature dynamically adjusts WDAC Lockdown's security posture on the fly, based on the end-user's current activity and behavior.

**Email client links:** This is a new patent-pending feature that automatically presents a micro-prompt in email clients when a link is clicked, and allows you to open the selected link in either your default web browser or within Windows Sandbox. Windows Sandbox must be activated on the system in order for this feature to function.



Cybersecurity Apps for macOS and Android tested

Delete Archive Report Reply all Zoom

Cybersecurity Apps for macOS and Android tested

**Hello Customer!**

We are pleased to announce the release of our **latest tests** of **macOS protection, Android protection and Speed Impact on Windows Systems**. The tests include **30 Enterprise and Consumer Products in total**.

**Apple macOS Security Test & Review 2024**

World of macOS, lurking cybersecurity threats are more common than its reputation. It's not just a matter of time. Vigilance is key - look for how different products protect your Apple against invaders.

[Click her to check the full report](#)

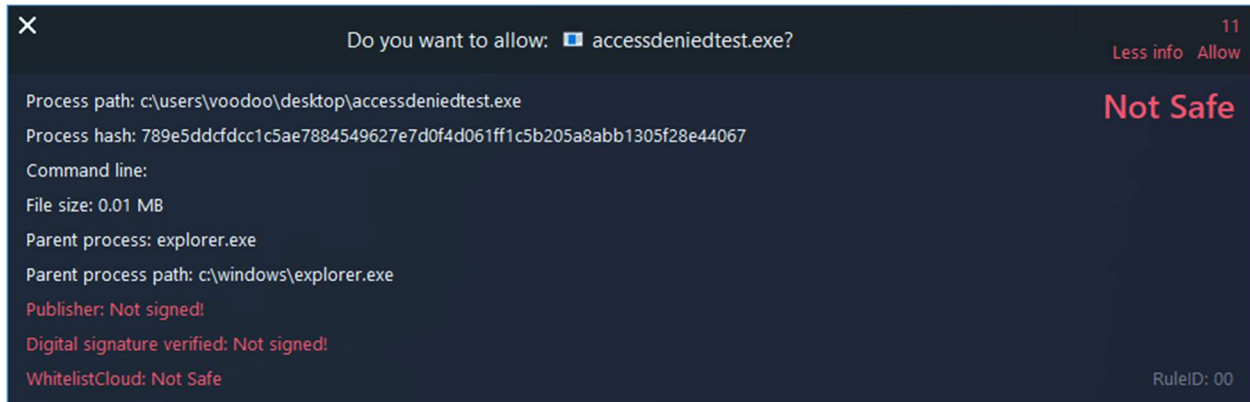
**Mobile Security Review 2024**

AV-C's recent investigation into Android security has uncovered the protection results. From vulnerabilities that turn your phone into a hacker's playground to surprising flaws in seemingly harmless apps, read which Android security products protect users best.

[Click here for the test-results](#)

## WDAC Lockdown features

**Enable WDAC User Prompts:** When enabled, WDAC Lockdown will display a user prompt when WDAC blocks a file, so the end-user is able to allow the file on the fly, in real-time. When disabled, users are not provided the option to manually allow a blocked WDAC file.



**WDAC Mode:** The following modes are available

- WDAC Lockdown: Disabled
- WDAC Lockdown: Training
- WDAC Lockdown: OFF (Audit)
- WDAC Lockdown: ON (Enforced)

**Prefer Rule Options:** You can choose to create signer rules with a path fallback, create only signer rules, or create only path rules. This feature works across all of the WDAC rule creation mechanisms in our software (e.g. WDAC user prompt, Training mode, Auto build, whitelist all events, etc.).

Prefer signer rules, path fallback: WDAC Lockdown will create a signer rule if the file is signed, otherwise it will create a path rule

Create signer rules only: WDAC Lockdown will create a signer rule if the file is signed, and will not create a path rule, whether the file is signed or not

Create path rules only: WDAC Lockdown will not create signer rules at all, and will create a path rule for every event

**Auto build policy:** The Auto build policy feature is able to create entire customized policies with a single click. It can take anywhere from a few minutes to a couple of hours to automatically build the custom policies, depending on which option you select.

- Auto build a folder or drive
- Auto build user space
- Auto build ProgramData
- Auto build Program Files

Auto build C: drive

Create golden image

**Whitelist all events from the last X days:** Existing audit events can also be automatically allowed by utilizing DefenderUI Pro's "Whitelist all events from the last X days" feature.

**Microsoft WDAC Wizard:** WDAC Lockdown also includes a customized version of the Microsoft WDAC Wizard that allows you to effortlessly create WDAC policies from scratch that are automatically deployed within WDAC Lockdown.

**Reset User Policies:** The Reset User Policies feature will reset your WDAC policies to factory default, so you can start from scratch if you need to.

**Set Password:** A password can be set to prevent unauthorized users from changing settings and policies.