SOP
System Hardening via Local GPO: Windows Defender

v1.0.1

Author:
Eldon Gabriel

March 21, 2025

Table of Contents

Table of Contents **1**
Revision History **2**
0.0 Executive Summary **3**
1.0 Windows Defender GPO Hardening **5**
1.1 Project Description 5
1.2 Configuration Summary 6
1.3 Validation and Testing 6
1.4 Supporting Work 7
2.0 Conclusion **8**
2.1 Key Takeaways 8
2.2 Security Implications and Recommendations 8

Disclaimer: This report documents my personal work completing an MCSI lab exercise. It reflects the author's understanding and configuration of Windows Defender settings in a controlled offline environment. No MCSI videos or lab materials have been posted, shared, or distributed, ensuring compliance with MCSI policies.

Revision History

Version	Date	Author	Description of Changes
v1.0.0	10/01/2025	Eldon G.	Initial draft.
v1.0.1	03/21/25	Eldon G.	Aligned endpoint hardening with CIS Benchmarks and NIST CSF (PR.PT); established an immutable security baseline and verified policy persistence via CLI diagnostics; added Executive Summary.

0.0 Executive Summary

0.1 Project Overview

System Hardening via Local GPO: Windows Defender This report documents the implementation of an immutable endpoint security baseline using **Local Group Policy Objects (GPOs)**. The project focuses on hardening **Windows Defender Antivirus** settings to ensure that critical protections remain active, persistent, and non-bypassable by standard users or malicious scripts.

Project Objective

The primary goal was to transition from a "default" to an "enforced" security posture. By configuring specific GPO Administrative Templates, the project aimed to prevent the unauthorized deactivation of antivirus services, which is a common pre-encryption step in ransomware attacks. This implementation ensures that real-time monitoring, cloud-based protection, and deep-scanning protocols are permanently enabled across the host system.

Technical Specifications

The hardening process utilizes the following core mechanisms:

Service Integrity: Applied policies to prevent users from disabling or avoiding antivirus software, ensuring that the "Security Center" remains the definitive authority on host health.

Advanced Scanning: Configured mandatory scanning of removable drives, archived files (ZIP/RAR), and email attachments to mitigate "Living off the Land" and phishing threats.

Policy Persistence: `gpupdate/force` and system restarts were utilized to verify that security controls were resistant to local tampering and remained active across user sessions.

Framework Alignment: Mapped the hardening steps to the **National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) Protect (PR.PT)** and **Center for Internet Security (CIS) Control 5**, establishing a defensible security baseline that meets enterprise compliance standards.

Validation and Quality Assurance To confirm the integrity of the hardened state, the following diagnostic protocols were executed:

Negative Testing: We attempted to manually disable Windows Defender services as a standard user to confirm the "Access Denied" prompts and GPO enforcement.

Persistence Verification: Confirms that the settings remained "greyed out " in the Windows Security GUI, indicating that policy-level control superseded local user preference.

CLI Diagnostics: Used command-line tools to verify the successful refresh of the Group Policy engine and the application of all 11 targeted security subpolicies.

1.0 Windows Defender GPO Hardening

1.1 Project Description

This project shows how we set up a Local Group Policy Object (GPO) on a Windows 10 computer. It aims to strengthen the **Windows Defender Antivirus**. The goal was to establish important defender options. These options include protection, scanning actions, and preventing users from turning off antivirus software.

1.2 Configuration Summary

Eleven policies were established using the Local Group Policy Editor (`gpedit.msc`) under **Windows Defender Antivirus**. This study was divided into three main areas.

1. **Core Antivirus Service Control**: Windows Defender remains on and cannot be turned off.
2. **Real-Time and Behavioral Monitoring**: Ensure that downloads, archives, and removable media are regularly scanned. In addition, it monitors behavior and processes to detect various types of threats.
3. **User Access Restrictions**: Restricting standard users from pausing, disabling, or bypassing antivirus protection.

This setup strengthens security in layers while maintaining ease of use.

1.3 Validation and Testing

After applying the Group Policy changes, the system was refreshed using the following command:

```cmd
gpupdate /force
```

The machine was then restarted to confirm the persistence of the fault. We logged in as a regular user and attempted to change the Windows Defender settings. The test showed that **Defender Antivirus could not be turned off or avoided**, and all scanning features remained active.

1.4 Supporting Work

1. Compared hardened settings with default Windows Defender behavior to confirm policy impact.
2. Documented configuration categories for portfolio presentation to prevent explicit solution disclosure.
3. Confirmed that the system behavior aligned with exercise expectations and novice-level learning objectives.
4. Confirmed persistence of settings after system restart and refresh with `gpupdate /force`.

2.0 Conclusion

2.1 Key Takeaways

- Successfully hardens Windows Defender through Local GPO.
- Three categories of configurations were applied: service control, advanced scanning, and user access restrictions.
- The protections were found to be persistent and non-removable by a standard user account.

2.2 Security Implications and Recommendations

Using group policies to enforce antiviral protection makes computers safer and more secure. This prevents users from turning off or avoiding antiviral software. This helps protect computers from viruses, phishing, and threats from USB drives.

Recommendation: Apply these settings to a domain-level GPO in business settings to protect all devices similarly.