



REPORT

GPO Hardening for Windows Application Control

v1.0.0

Author:

Eldon Gabriel

September 7, 2025



Cybersecurity Professional | IT Security Consultant

TABLE OF CONTENTS


REVISION HISTORY	2
1.0 GPO HARDENING AND LESSONS LEARNED	3
1.1 Overview of the Task.....	3
1.2 GPO Settings Applied in Lab.....	4
1.3 Extended GPO Research and Best Practices.....	4
1.4 Cloud Troubleshooting Findings.....	6
SECTION 2.0: CONCLUSION	7
2.1 Key Takeaways.....	7
2.2 Security Implications and Recommendations.....	7





Cybersecurity Professional | IT Security Consultant

REVISION HISTORY

Version	Date	 Author	Description of Changes
v1.0.0	09/07/2025	Eldon G.	Initial draft.





Cybersecurity Professional | IT Security Consultant

1.0 GPO HARDENING AND LESSONS LEARNED

1.1 Overview of the Task

This project was about hardening a Windows computer to be much more secure by using special rules called **Group Policy Objects (GPOs)**. My main goal was to prevent regular users from installing any programs they wanted. This is important because hackers often trick people into downloading harmful software to steal their data. Using these GPO rules, I was able to block the risks and make the system safer.



Disclaimer: This report is based on my independent practice and understanding of Windows access permissions and Group Policy. This is intended for portfolio demonstration purposes only.



1.2 GPO Settings Applied in Lab

In the Windows test environment, the following policies were applied:

- **Windows Defender SmartScreen:** Enabled to warn users and block risky files.
- **Windows Installer Restrictions:** Disabled user control over installations and blocked elevated privileges.

Validation: I tested this by attempting to install 7-Zip as a standard user. The installation was blocked, confirming that the GPOs were functioning.

1.3 Extended GPO Research and Best Practices

I researched additional GPO settings to understand how to strengthen Windows security beyond the laboratory. This includes controlling applications, storage, authentication, and user actions.

Application and Installer Controls

- **Prohibit User Installs** → Enabled: Hides user installation behavior.
- **Turn off Windows Installer** → Enabled: Disables the installer for all users.

Cloud and Storage Restrictions

- **Prevent OneDrive for file storage** → Enabled: Stops syncing and uploading data to the cloud.
- **Software Restriction Policies** → New rules for blocking access to the Windows Store app.
- **Removable Storage Access** → Deny all access, preventing USB-based attacks and data exfiltration.
- **Hide specified drives in File Explorer** → Restrict visibility and access to sensitive system drives.

Update and Availability Management

- **Turn off auto-restart during active hours** → Ensures that updates do not disrupt business hours.



Cybersecurity Professional | IT Security Consultant

- Configurable integration with **Windows Server Update Services (WSUS)** for controlled patch delivery.

Password and Authentication Policies

- **Password History** → Prevents the reuse of recent passwords.
- **Minimum Password Age** → 7–14 days to enforce disciplined credential rotation.
- **Minimum Password Length** → 10–14 characters to reduce the brute-force risk.
- **Guest Account Disabled** → Ensures that no weak default accounts remain active.
- **Do Not Store LAN Manager Hashes** → Reduces exposure to legacy hash attacks.

User Restrictions

- **Prohibit Control Panel and PC Settings** → Prevent unauthorized system changes.
- **Prevent Command Prompt** → Blocks cmd.exe to stop scripting abuse.
- **Prevent Registry Editing Tools** → Disables regedit.exe to limit tampering.

Business Impact Example: A common way for ransomware to spread is when a user is tricked into downloading fake invoice software. These policies block installations, reducing the likelihood of system breaches.

ELDON GABRIEL



1.4 Cloud Troubleshooting Findings

When testing the AWS and GCP virtual machines, the GPO did not work because of the restricted or stateless service profiles. Specifically:

- **Stateless or restricted service profiles** lock critical services, such as gpsvc.
- Group Policy Client freezing (Startup type: Automatic but greyed out).
- gpupdate failed, and gpresult showed no applied settings.

Effect: Group Policy restrictions fail in these environments. Standard users are free to install applications or execute scripts on the system. This highlights the need to confirm policy enforcement **in the context of deployment**.

Lesson Learned: It is critical to confirm GPO enforcement in the target environment. Cloud images may require special configurations or hardened baselines to ensure policy compliance.



SECTION 2.0: CONCLUSION

2.1 Key Takeaways

- GPOs provide a robust method for **controlling software installation and user privileges**.
- SmartScreen adds another layer of **defence against social engineering and malicious downloads**.
- Research on broader GPO settings has highlighted how organizations can achieve **defense-in-depth**. They use password policies, removable media restrictions, and cloud storage controls.
- Cloud VM images cause unique problems. This highlights the importance of validating **policy enforcement in various environments**.

2.2 Security Implications and Recommendations

These GPO controls strengthen the **CIA Triad**:

- **Confidentiality**: By restricting removable media and cloud synchronization.
- **Integrity**: By blocking unauthorized software that can corrupt the system state.
- **Availability**: Updates are configured to avoid unexpected reboots.

They also align with cybersecurity frameworks and compliance requirements.

- **NIST 800-53 / NIST CSF**: Application whitelisting, least privilege, and access control.
- **ISO 27001**: Annex A controls for access restriction and secure system configuration are discussed.
- **PCI-DSS**: Requirement 2 (secure configuration) and Requirement 6 (system hardening).

Recommendation: Organizations should use multiple layers of protection. They should enforce GPO, allow only approved applications, protect endpoints, and train users to be aware.