



REPORT

Deploy Local GPO for Windows Security Policies

v1.0.0

Author:

Eldon Gabriel

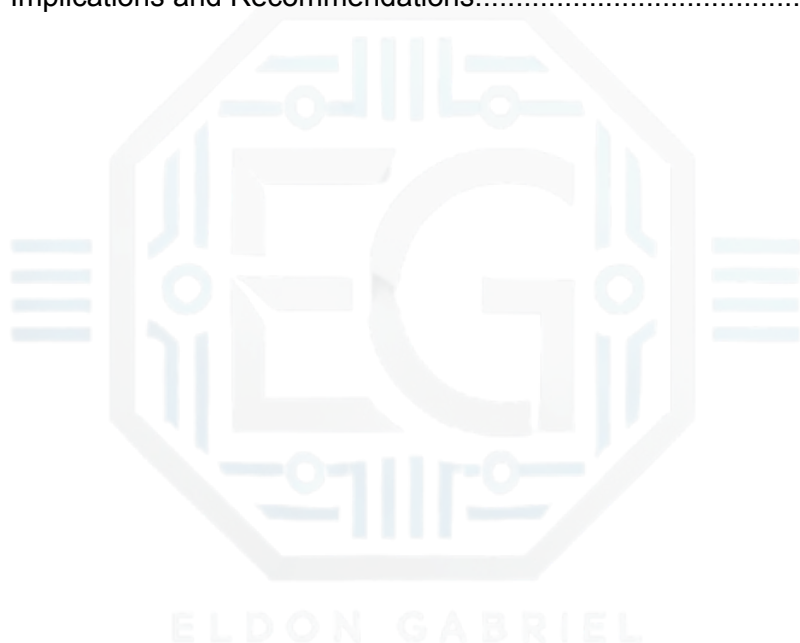
October 12, 2025



Cybersecurity Professional | IT Security Consultant

TABLE OF CONTENTS

REVISION HISTORY	2
1.0 DEPLOYING LOCAL GROUP POLICY	3
1.1 Project Description	3
1.2 Technical Task	4
1.3 Detailed Policy Actions	4
1.4 Next Task or Investigation Step	5
1.5 Optional Deep Dive / Special Case	5
1.6 Additional or Supporting Work	5
SECTION 2.0: CONCLUSION	6
2.1 Key Takeaways	6
2.2 Security Implications and Recommendations	6




Disclaimer: This report documents my personal work completing an MCSI lab exercise. It reflects my independent understanding and configuration of Windows 10 Local Group Policy settings in a controlled environment. No MCSI video content, lab materials, or proprietary instructions have been shared or distributed. All information presented follows MCSI's disclosure and academic integrity policies.



Cybersecurity Professional | IT Security Consultant

REVISION HISTORY

Version	Date	 Author	Description of Changes
v1.0.0	10/12/2025	Eldon G.	Initial draft.





Cybersecurity Professional | IT Security Consultant

1.0 DEPLOYING LOCAL GROUP POLICY

1.1 Project Description

This task involved setting up and using a Local Group Policy Object (GPO) on a Windows computer. The goal was to improve the security of computers by applying important security settings. These settings help protect against attacks, make protocols safer, and control access according to the security rules.





1.2 Technical Task

Using the **Local Group Policy Editor** (`gpedit.msc`), I navigated through the **Computer Configuration** node, specifically targeting policies within the **Administrative Templates** and **Windows Settings Security Settings** paths. I located and modified six distinct policies designed to enforce baseline security controls.

This implementation requires the accurate identification of the hierarchical path for each policy and setting its value to the institution's security standard (e.g., enabled, disabled, or a specific value). These changes were implemented in accordance with the best practices for workstation-level security management.

1.3 Detailed Policy Actions

A total of **six (6) security policies** were located and configured across two main policy categories: **Administrative Templates** and **Security Settings**.

Policy Category	Policies Configured	Resulting Action
Administrative Templates	Two (2) policies spanning Network and Windows Components configurations.	Mitigated a critical credential harvesting vulnerability (LLMNR/NBT-NS) and enhanced system integrity against memory exploits.
Windows Settings	Four (4) policies within Security Settings, Local Policies, and Security Options .	Strengthened domain member security, access control, and fundamental system object permissions.

Following the configuration, the changes were immediately enforced by executing the command, `gpupdate /force`. After configuration, all six policies were successfully applied and verified using the Group Policy Management Console to confirm enforcement.



1.4 Next Task or Investigation Step

After applying the policies, the configuration was validated to confirm the persistence of the new settings. The logical next step involves centralizing these configurations through a **Domain Group Policy Object (GPO)** in an Active Directory environment. This transition would enable consistent domain-wide enforcement and scalable security auditing.

1.5 Optional Deep Dive / Special Case

Execute a security assessment tool (such as a vulnerability scanner) before and after policy application. Documenting the audit results provides **measurable evidence** of improved baseline hardening, particularly concerning network-based exploits and system object security.

1.6 Additional or Supporting Work

Additional research was conducted to learn how GPOs work in the following order: Local, Site, Domain, and Organizational Unit. Knowing this order helps avoid problems and ensures that policies work well when moving from a local setup to a larger managed system.



2.0 CONCLUSION

2.1 Key Takeaways

- Using local GPOs allows direct management of a system's security. This is important for securing systems or for isolated setups.
- The exercise showed that knowing how to use Group Policy categories (such as Administrative Templates and Windows Settings) is important for setting things up correctly.
- Checking and recording the settings used is important to ensure that they work well and match the basic rules.

2.2 Security Implications and Recommendations

If security rules are not set and followed, systems can be at risk of known attacks. The steps taken here help reduce risks such as stealing login details (by fixing weak protocols) and unauthorized access (by strengthening system permissions).

Recommendation: Organizations should establish basic security rules using Group Policy. These rules must be followed by all. These rules should be regularly checked and updated. Automated systems should be used to apply them to all devices to keep everything secure and consistent.
