SOP
Deploying Strict Password & Account Lockout GPO

v1.0.1

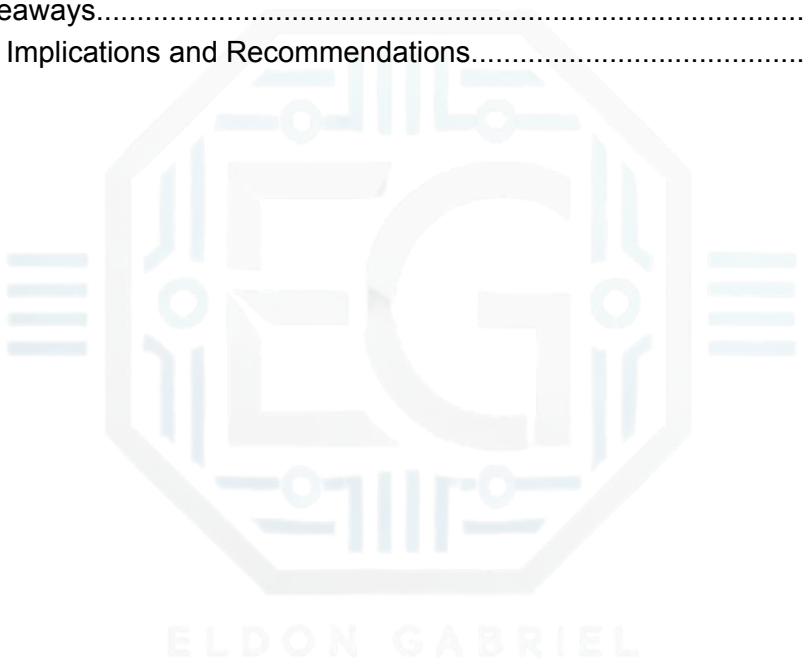
Author:

Eldon Gabriel

March 21, 2026

Security Systems Specialist

Table of Contents



Disclaimer: This report documents my personal work completing an MCSI lab exercise. It reflects the author's understanding and configuration of Windows 10 Local Group Policy settings for operating system patching in a controlled, offline environment. No MCSI instructional videos, lab guides, or proprietary materials have been posted, shared, or distributed. The content has been written independently to demonstrate my skills while remaining fully compliant with MCSI's academic pledge and policies.

Revision History

Version	Date	Author	Description of Changes
v1.0.0	09/28/2025	Eldon G.	Initial draft.
1.0.1	03/21/2026	Eldon G.	Aligned authentication baselines with NIST 800-53 (IA Family) and CIS Benchmarks; implemented account lockout and credential encryption restrictions; added Executive Summary.

0.0 Executive Summary

0.1 Project Overview

Password Policy & Account Lockout Hardening

This project focused on improving system security by strengthening password policies and account lockout settings using Local Group Policy (GPO). The goal was to protect user accounts by enforcing strong passwords and limiting repeated login attempts.

Project Objective

The main goal was to reduce the risk of unauthorized access from attacks, such as brute-force and password guessing. This was achieved by replacing the default Windows settings with stricter security rules.

All local accounts were configured as follows:

- Use strong and complex passwords
- Follow modern security standards
- Automatically lock after too many failed login attempts

Technical Implementation

The system was secured using the following controls:

Password Complexity: Set minimum length and complexity rules to make passwords harder to crack

Account Lockout: Limited failed login attempts and added a lockout timer to stop repeated attacks

Legacy Protection: Disabled weak features like reversible encryption and restricted PIN-based login methods

Framework Alignment: Aligned settings with NIST 800-53 (IA controls) and CIS Benchmarks

Validation and Testing

To confirm that the system was secure, the following tests were performed:

Password Testing: Tried to create weak passwords and confirmed they were rejected

Lockout Testing: Entered multiple wrong passwords to confirm the account was locked

System Verification: Used system tools to confirm all settings were active and remained applied after updates

1.0 Password and Account Lockout Policy Deployment

1.1 Project Description

The project used a **Group Policy Object (GPO)** on a Windows 10 virtual machine (VM) to enforce strict rules for passwords and for account lockouts. This setup helps prevent **password guessing** and **brute-force attacks** by following security standards. These standards match the best industry practices.

1.2 GPO Configuration Steps

The Local Group Policy Editor (`gpedit.msc`) was used to apply system hardening configurations across three main categories:

Password Policies: Enforced stronger complexity rules and rotation requirements to reduce the risk of password reuse and credential stuffing attacks.

Account Lockout Policies: Implemented limits on repeated failed logon attempts to defend against brute-force attacks.

Sign-in & Credential Controls: Disabled weaker convenience login methods and required secure authentication handling.

This approach aligns with recognized security best practices and ensures that system accounts are both resilient against guessing attempts and properly monitored for misuse.

1.3 Verification

- Logged into the test Windows machine.
- GPO settings were applied through the **Local Group Policy Editor**.
- The command `gpupdate /target:computer /force` was used to enforce the changes.
- Validated settings using `secpol.msc` under
    - **Account Policies** → **Password Policy** and **Account Lockout Policy**.

1.4 Security Impact

- Enforcing password complexity prevents users from creating weak credentials.
- Account lockout limits the effectiveness of brute-force attacks.
- Password expiration ensures periodic refreshment of credentials, reducing the risk of credential compromise.
- Disabling the PIN and reversible encryption eliminates weaker authentication fallbacks.

1.5 Security Impact

No additional policies were added beyond the laboratory scope. In the future, **fine-grained password policies** and **centralized audit logging** can be used to track logs for business purposes.

2.0 Conclusion

2.1 Key Takeaways

- Set up and checked **logon, password, and account lockout policies** using the Local Group Policy.
- Reinforced understanding of how Windows security baselines are applied at the OS level.
- Showed skill in setting up rules using the **Local Group Policy Editor** and checking if they worked.

2.2 Security Implications and Recommendations

From Lab to Enterprise

The same setup can be used across a company with **Active Directory domain-level GPOs**, even though it was tested on a single PC. This ensures consistent rule generation.

Compliance Alignment

These policies align with **CIS Benchmarks, NIST 800-53 (IA family), and ISO 27001 Annex A**, enabling organizations to meet legal requirements.

Operational Impact

Strong passwords and lockout controls help prevent the misuse of login details. They lower the chance of hackers moving through systems and make it harder for automated attacks to be successful.