REPORT
Deploying Strict Password & Account Lockout GPO

v1.0.0

Author:

Eldon Gabriel

September 28, 2025

TABLE OF CONTENTS

REVISION HISTORY

Version	Date	Author	Description of Changes
v1.0.0	09/28/2025	Eldon G.	Initial draft.

SECTION 1.0 PASSWORD & 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.

Disclaimer: This report documents my personal work completing an MCSI lab exercise. It reflects my 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.

1.2 GPO Configuration Steps

The configuration was performed using the **Local Group Policy Editor** (gpedit.msc) under the following paths:

Logon Policy (Computer Configuration → Administrative Templates → System → Logon)

- Disabled convenience PIN sign-in.

Password Policy (Computer Configuration → Windows Settings → Security Settings → Account Policies → Password Policy)

- Limited password history to **five remembered passwords**.
- Password expiration is enforced every **90 days**.
- Password changes were restricted to occur only after **24 hours.**
- The minimum password length was set to **10 characters**.
- Enabled password complexity requirements:
- Disable reversible encryption for passwords.

Account Lockout Policy (Computer Configuration → Windows Settings → Security Settings → Account Policies → Account Lockout Policy)

- Set the account lockout threshold to **five failed logon attempts**.
- Configured account lockout duration to **15 minutes**.
- The configured lockout counter was reset after **15 minutes**.

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.

SECTION 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.
