REPORT
Secure Credential Entry via Group Policy Objective (GPO)

v1.0.0

Author:

Eldon Gabriel

September 9, 2025

TABLE OF CONTENTS

REVISION HISTORY

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

SECTION 1.0: PROJECT OVERVIEW

1.1 Project Description

This exercise focuses on securing the Windows workstations. I configured the Local Group Policy to enforce secure credential entry. The goal is to reduce the risk of credential theft by malicious software such as keyloggers. I used "Secure Desktop" and other logon restrictions to do this.

Disclaimer: This report is based on my independent execution of the MCSI exercise *“Deploy a GPO on a single machine to ensure credentials are entered in a secure manner.”* The GPO settings and procedures are applied and documented by me for portfolio demonstration purposes and reflect my personal understanding and testing of secure credential entry

1.2 Technical Task: GPO Configuration

Configured Local Group Policy Settings

Policy Path	Policy Setting	Configured Value
Computer Configuration → Policies → Administrative Templates → System → Logon → Do not display network selection UI	Enabled	Enabled
Computer Configuration → Policies → Administrative Templates → System → Logon → Enumerate local users on domain-joined computers	Disabled	Disabled
Computer Configuration → Policies → Administrative Templates → Windows Components → Credential User Interface → Do not display the password reveal button	Enabled	Enabled
Computer Configuration → Policies → Administrative Templates → Windows Components → Credential User Interface → Enumerate administrator accounts on elevation	Disabled	Disabled
Computer Configuration → Policies → Administrative Templates → Windows Components → Credential User Interface → Require trusted path for credential entry	Enabled	Enabled
Computer Configuration → Policies → Administrative Templates → Windows Components → Windows Logon Options → Disable or enable software Secure Attention Sequence	Disabled	Disabled
Computer Configuration → Policies → Administrative Templates → Windows Components → Windows Logon Options → Sign-in last interactive user automatically after a system-initiated restart	Disabled	Disabled
Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Security Options → Interactive logon: Do not require CTRL+ALT+DEL	Disabled	Disabled
Computer Configuration → Policies → Windows Settings → Security Settings → Local Policies → Security Options → Interactive logon: Don't display username at sign-in	Enabled	Enabled

1.3 Verification & Testing

- The GPO setting was confirmed by logging into both standard and administrative accounts.
- I tested the policy and observed that the Secure Desktop prompt was working during login.
- In addition, I ensured that the password reveal and automatic logon options are disabled.

1.4 Lessons Learned

- Group Policy Objects can effectively secure endpoint logon and prevent local attacks from capturing credentials.
- Understanding Windows security settings is essential to mitigate common attack vectors like keylogging and credential theft.
- Testing on a single machine ensures safe validation before broader deployment.

1.5 Practical Applications

- Improves endpoint security in enterprise environments.
- Reduces the risk of credential-based attacks and lateral movement by attackers.
- Supports compliance with internal security policies and cybersecurity best practices.

SECTION 2.0: CONCLUSION

2.1 Key Takeaways

- Using secure logon practices via GPOs is an effective way to protect sensitive credentials.
- Applying these rules shows the importance of system administration skills in real-world security scenarios.

2.2 Security Implications and Recommendations

Risk

These GPO settings protect workstations from becoming easy targets. Attackers can steal credentials via keyloggers and gain unauthorized access.

Remediation Steps

Enforce Secure Desktop logon for standard users. Automatic logon should be disabled, password revelation should be restricted, and a trusted path for login entry should be required.

Technical Recommendations

Regularly check your GPO settings to ensure they are accurate—track who attempts to log in and keep all your devices up to date with the latest security patches.

Procedural Recommendations

Users should be trained to recognize phishing and social engineering attacks. Show them how to spot these tactics and set policies for secure password management.

Compliance Relevance

These practices align with the NIST and ISO 27001 guidelines for access control and endpoint security.
