REPORT
Applying a Local GPO for Session Lock Enforcement

v1.0.0

Author:

Eldon Gabriel

October 16, 2025

TABLE OF CONTENTS

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.

REVISION HISTORY

Version	Date	Author	Description of Changes
v1.0.0	10/16/2025	Eldon G.	Initial draft.

1.0 GPO SESSION LOCK CONFIGURATION

1.1 Project Description

This project aims to improve Windows computer security. It sets up a rule that locks the computer if no one uses it for a while. This lock prevents unauthorized access to computers when they are unattended. This aligns with fundamental system hardening practices and the principle of **least privilege** during non-use.

1.2 Configure Local Group Policy

The **Local Group Policy Editor (`gpedit.msc`)** was used on a Windows Virtual Machine to set the policy **Interactive logon: Machine inactivity limit to 15 seconds**. This setup ensured that the session was locked automatically after 15 seconds of no activity, as required by the exercise.

1.3 Validation and Testing

Following the policy application, the system was allowed to remain idle. The lock mechanism was engaged after 15 s, validating the inactivity timeout. This confirmed that the session lock policy was set up correctly.

1.4 Technical Notes

Parameter	Value
Tool Used	`gpedit.msc`
Policy Path	Computer Configuration \ Windows Settings \ Security Settings \ Local Policies \ Security Options
Policy Name	Interactive logon: Machine inactivity limit
Value Configured	15 seconds

1.5 Additional or Supporting Work

A Windows virtual machine was used to create a space for testing Local Group Policy without impacting the main network. The resulting configuration was saved and documented as part of the machine's local policy baseline.

2.0 CONCLUSION

2.1 Key Takeaways

- Inactivity-based lock policies reduce the window for **unauthorized system** access.
- Targeted endpoint policies improve physical and session security, supporting **defense-in-depth**.
- Local Group Policy gives administrators control over system security settings.

2.2 Security Implications and Recommendations

Mandatory session lock policies are important for maintaining the **endpoint security baseline**. They directly support the principle of **confidentiality** by restricting unauthorized access. Organizations should manage these settings using a central system via an **Active Directory Group Policy Object (GPO)**.

This ensures uniform and non-repudiable compliance across all devices. Setting short time limits for inactivity is a simple and effective way to prevent **"shoulder surfing"** and unattended system compromise.
