Report: Group Policy Management for Security Hardening

1. Introduction

Group Policy is a vital tool in Windows Active Directory environments, allowing administrators to centrally manage configuration settings and enforce security policies across users and computers. Through the use of Group Policy Objects (GPOs), organizations can standardize behavior, minimize human error, and ensure compliance with internal and external regulations. In this task, we leveraged GPOs to improve workstation security, mitigate legacy protocol risks, and enforce user awareness at login.

By applying targeted GPOs to the appropriate Organizational Units (OUs), we ensured that security configurations were uniformly deployed and managed. This centralized approach reduces administrative overhead and strengthens overall security posture by enforcing consistent rules across the domain.

2. Objective

The primary objective of this task was to implement essential Group Policy configurations that directly improve security, user accountability, and system compliance within a domain environment. Through the deployment of three specific GPOs—enforcing a 15-minute screen lock timeout, disabling the insecure SMBv1 protocol, and configuring a legal logon banner—we aimed to address both operational security gaps and regulatory requirements. These policies help reduce the risk of unauthorized access, protect systems from legacy protocol vulnerabilities, and ensure that users are clearly informed of acceptable use policies upon logging into the network.

Another key objective was to ensure that these GPOs were applied with precision—targeting only the relevant Organizational Units such as "Workstations" while maintaining system usability. Applying group policies in a structured and scalable manner demonstrates a proactive IT governance strategy. By aligning technical enforcement with administrative goals, the task also supports larger organizational initiatives like audit readiness, security policy enforcement, and risk management across the domain infrastructure.

Key goals include:

- **Enforce Automatic Screen Lock for Inactivity**
  Implementing a 15-minute screen lock timeout helps prevent unauthorized access when users leave their workstations unattended. This policy reduces the risk of insider threats and data leakage. It also aligns with common compliance frameworks like CIS and ISO 27001.

- **Disable Legacy and Vulnerable Protocols (SMBv1)**
  Disabling SMBv1 across the domain protects systems from exploitation via known vulnerabilities like EternalBlue. This goal enhances network security by eliminating outdated technologies. It ensures systems communicate using secure and supported protocols only.

- **Standardize Security Configuration Across Workstations**
  Applying GPOs to the Workstations OU ensures that all user devices follow the same security rules. This centralized control minimizes configuration drift and enforces consistent security practices. It also simplifies troubleshooting and policy audits.

- **Improve User Awareness with Legal Logon Banner**
  Deploying a legal notice through GPO educates users about acceptable use policies before login. This reinforces organizational rules and serves as a deterrent for unauthorized behavior. It's also a legal safeguard during security investigations or audits.

- **Demonstrate Proactive Policy-Based Security Management**
  This task showcases how Group Policy can be used as a strategic tool for security hardening. Implementing these policies highlights the importance of automation and standardization. It also supports long-term IT governance and regulatory compliance initiatives.

3. Methodology

This methodology outlines the structured execution of Group Policy enhancements aimed at strengthening domain-wide security. The task was divided into three key phases: screen lock enforcement, SMBv1 protocol disablement, and legal logon banner deployment.

3.1 Enforce 15-Minute Screen Lock on Workstations

This phase focuses on configuring a Group Policy that ensures workstations are automatically locked after 15 minutes of user inactivity. This prevents unauthorized access and protects sensitive information when users step away from their systems. The policy is applied specifically to the Workstations OU to ensure targeted enforcement.

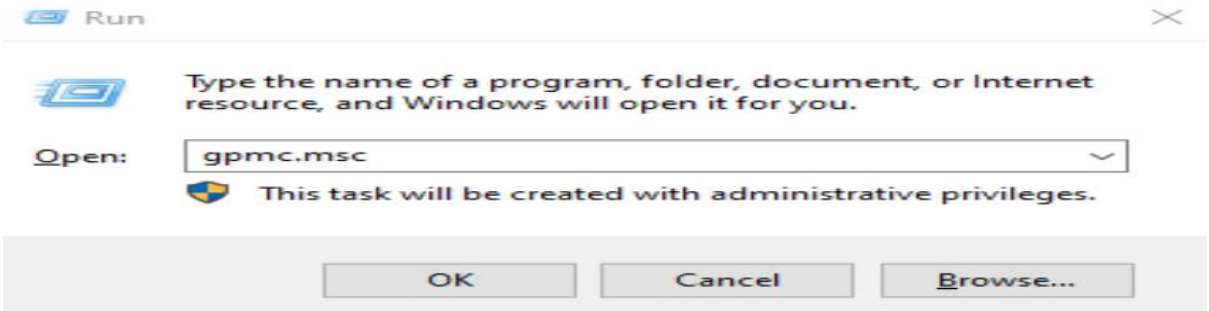
Navigation Path:

Group Policy Management Console (GPMC) → Right-click Group Policy Objects → New → Edit → User Configuration → Administrative Templates → Control Panel → Personalization

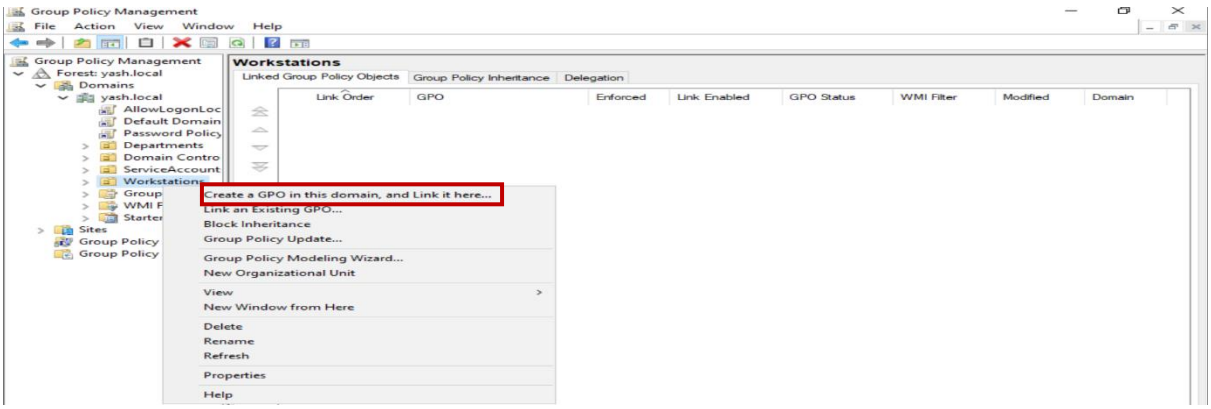
- **Create and Name the GPO**

  A new GPO was created under the Group Policy Objects container and named "ScreenLockPolicy" to reflect its purpose. This GPO is isolated initially so its settings can be configured without affecting live systems.

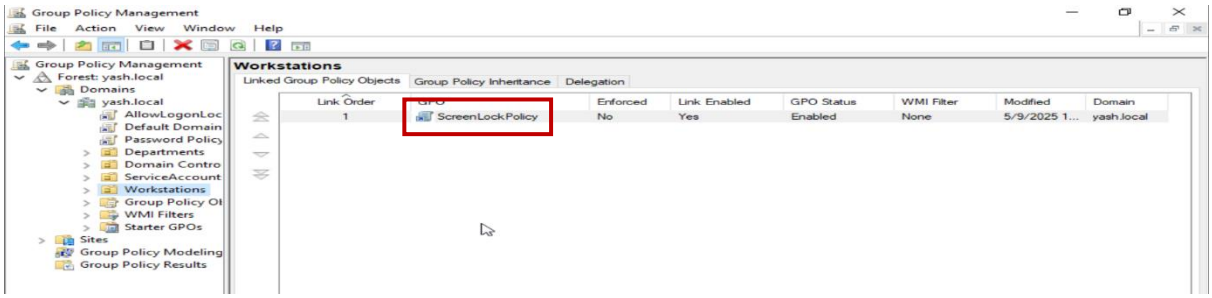
(Open Group Policy Management Console)



(GPO creation window)



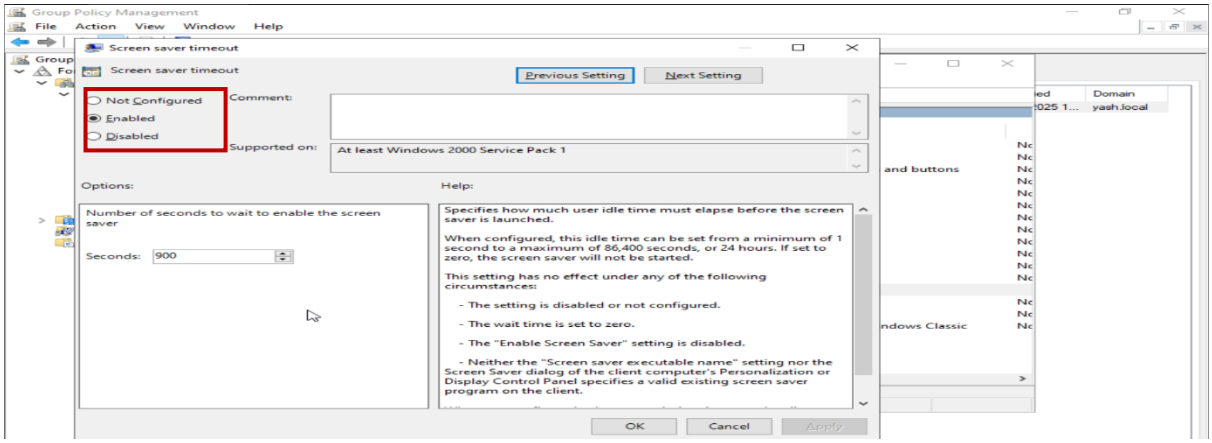
(GPO – ScreenLockPolicy created)



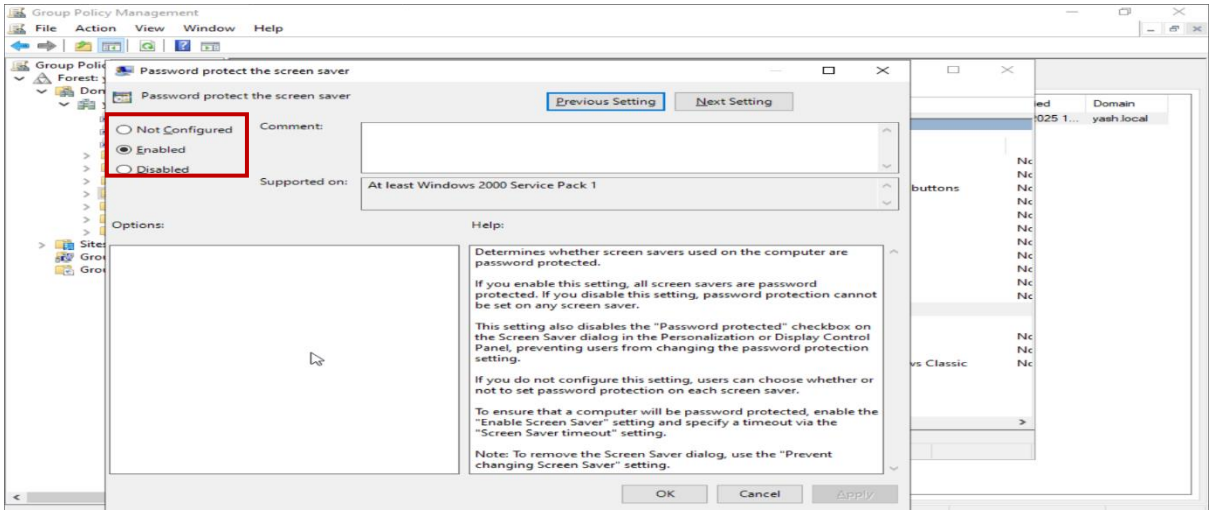
- **Configure Inactivity Timeout and Lock Settings**

  Inside the GPO editor, we navigated to Personalization settings and enabled "Password protect the screen saver" and set "Screen saver timeout" to 900 seconds (15 minutes). This ensures screens auto-lock after the set time of inactivity.

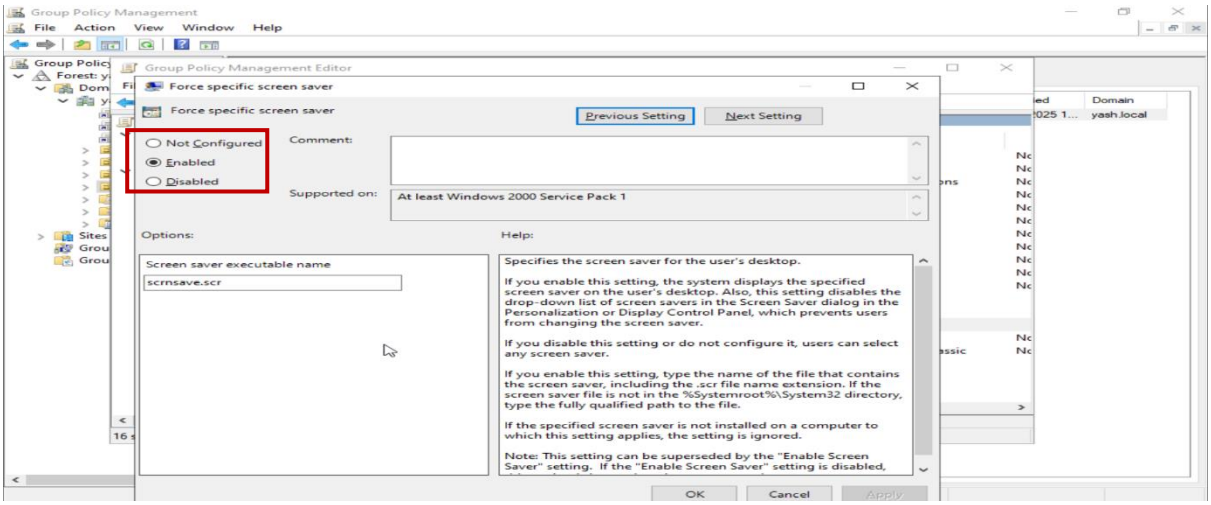
(Enable screen saver timeout)



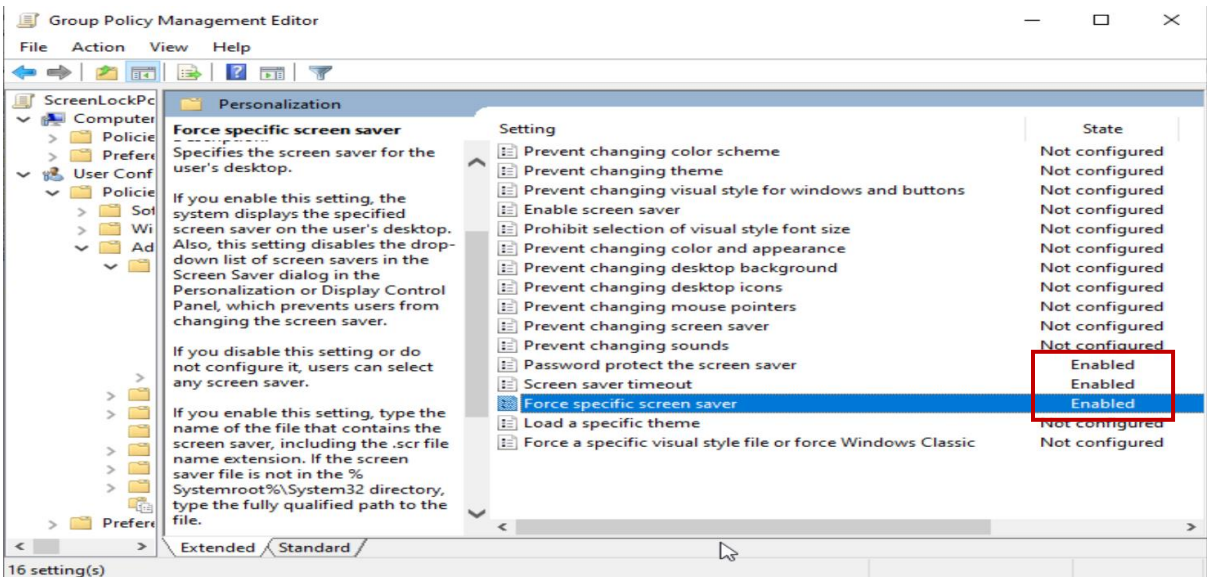
(Enable password protect the screen saver)



(Enable force specific screen saver)



(GPO editor showing timeout settings)



3.2 Disable SMBv1 Protocol Across the Domain

This phase eliminates the deprecated and vulnerable SMBv1 protocol, which is commonly exploited in ransomware and other attacks. Disabling SMBv1 helps secure the network by preventing legacy fallback and unauthorized access.

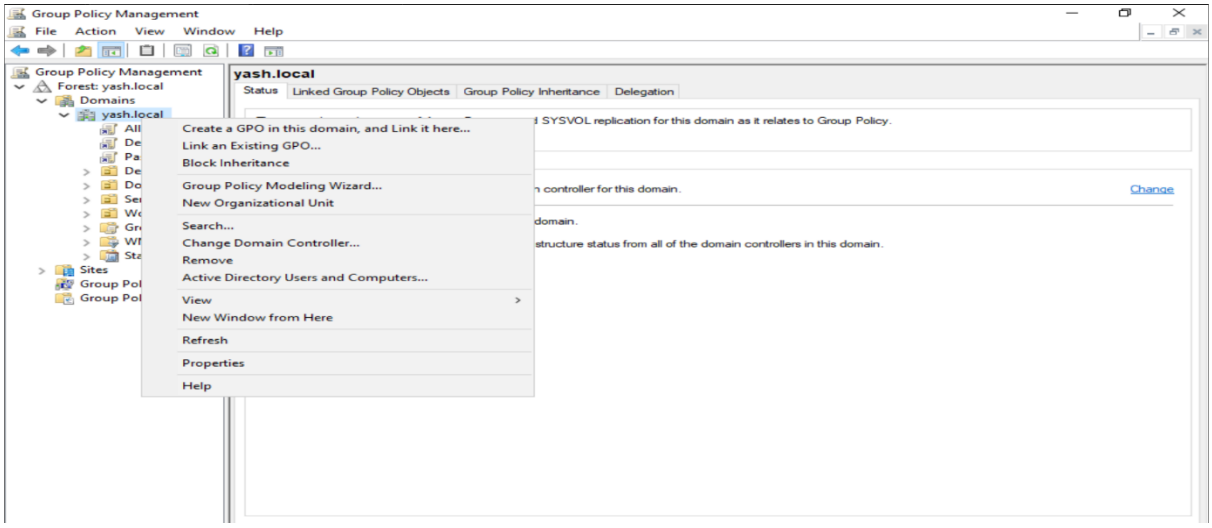
Navigation Path:

Group Policy Management Console (GPMC) → Group Policy Objects → New → Edit → Computer Configuration → Preferences → Windows Settings → Registry

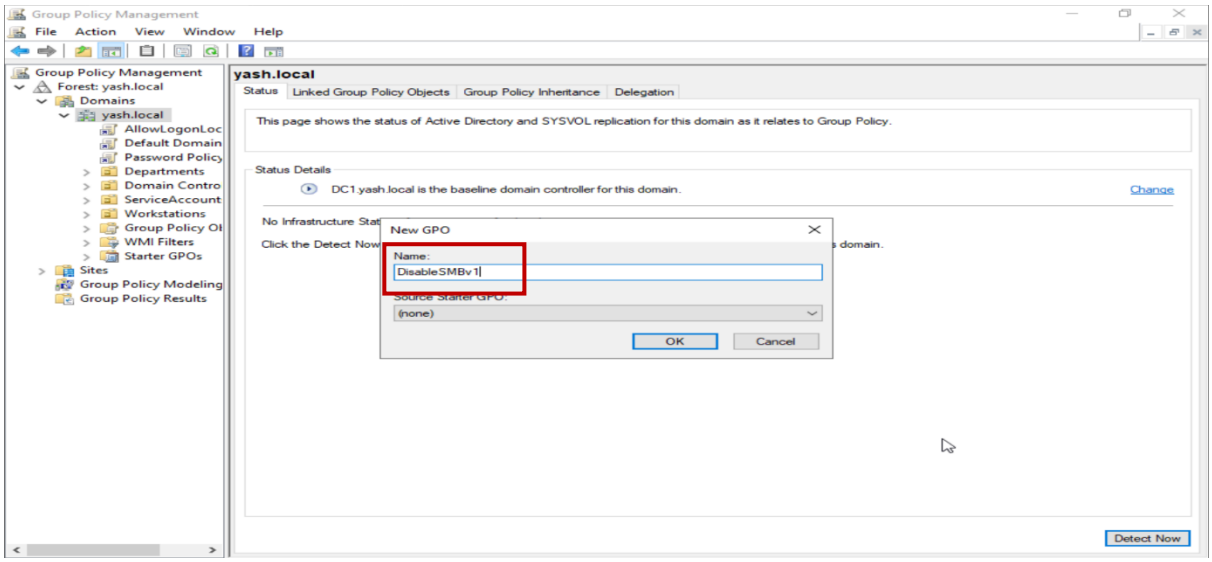
- **Create and Name the GPO**

  A GPO titled "DisableSMBv1" was created to handle the deactivation of SMBv1. This naming convention clearly indicates its function for auditing and maintenance purposes.

  (GPO Creation)



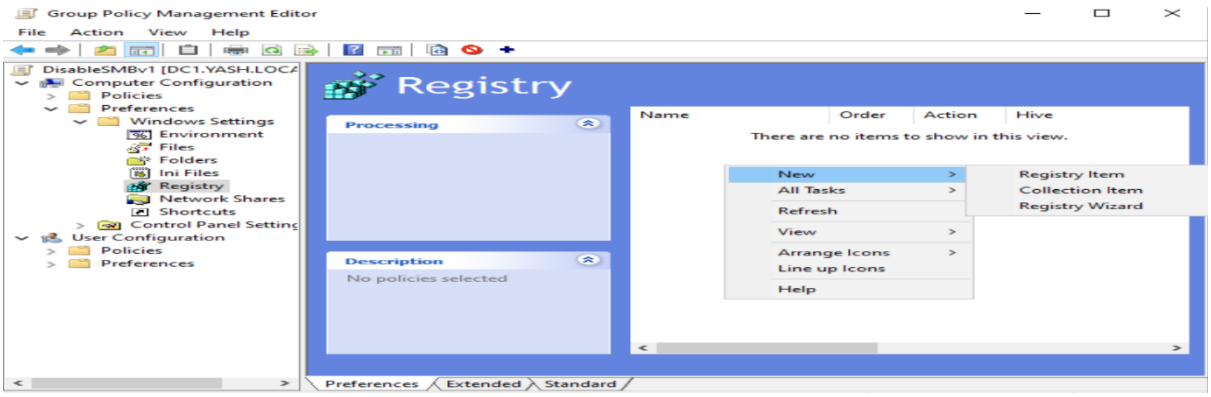
  (Created GPO-DisableSMBv1)



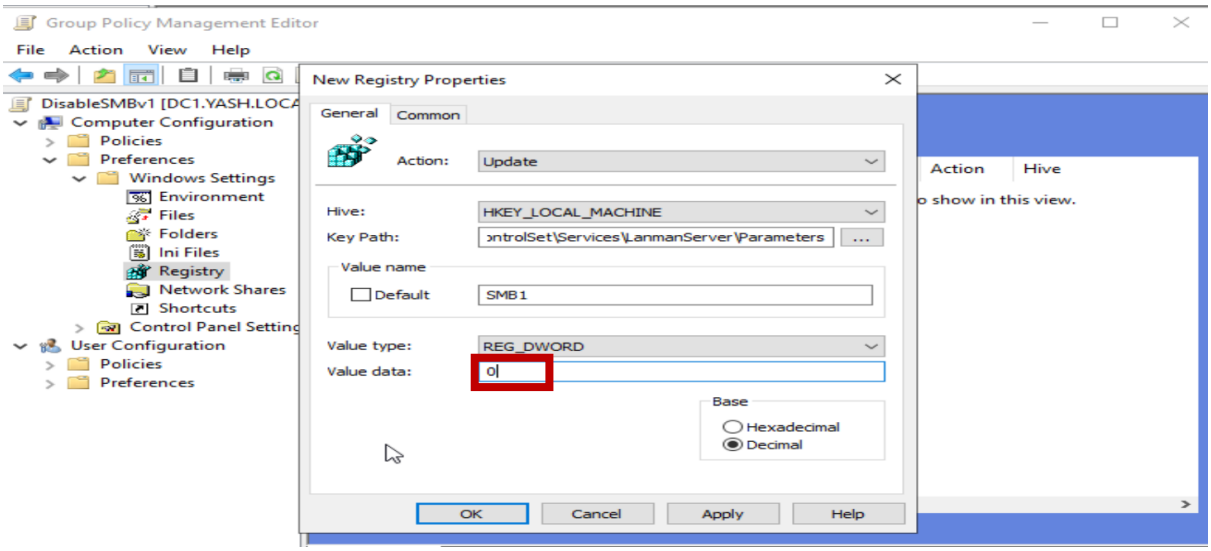
- **Add Registry Settings to Disable SMBv1**

  Created a DWORD value named SMB1 with value 0. This disables SMBv1 protocol support on all linked systems.

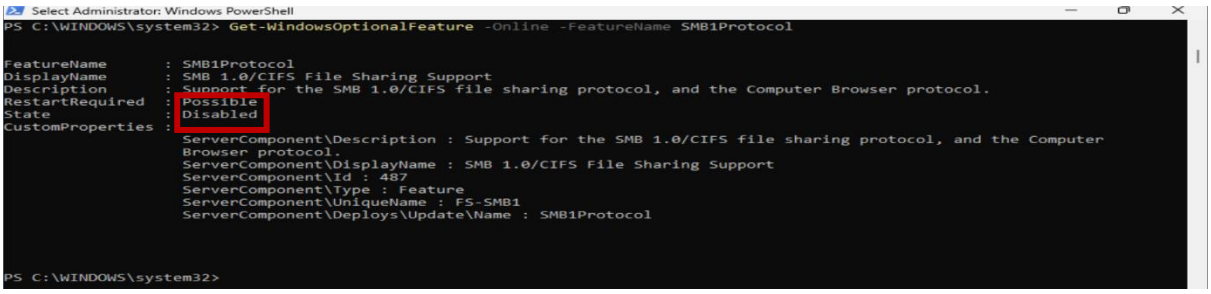
(Creating a new entry)



(Set value data to 0)



On a domain client, we ran Get-WindowsOptionalFeature -Online -FeatureName SMB1Protocol. It showed the protocol was disabled, confirming successful GPO implementation.



3.3 Deploy Legal Logon Banner via GPO

In this phase, a legal notice banner was deployed to inform users of acceptable use policies before login. This serves as both a deterrent for misuse and a legal safeguard for the organization, ensuring users acknowledge monitoring and company rules.

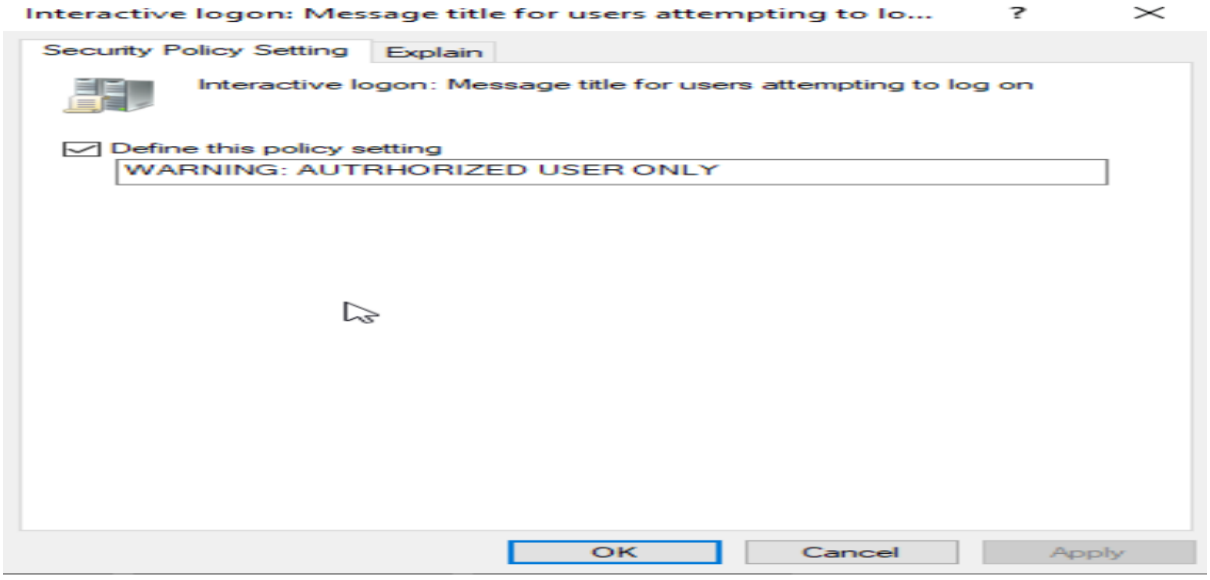
Navigation Path:

Group Policy Management Console (GPMC) → Group Policy Objects → New → Edit → Computer Configuration → Windows Settings → Security Settings → Local Policies → Security Options

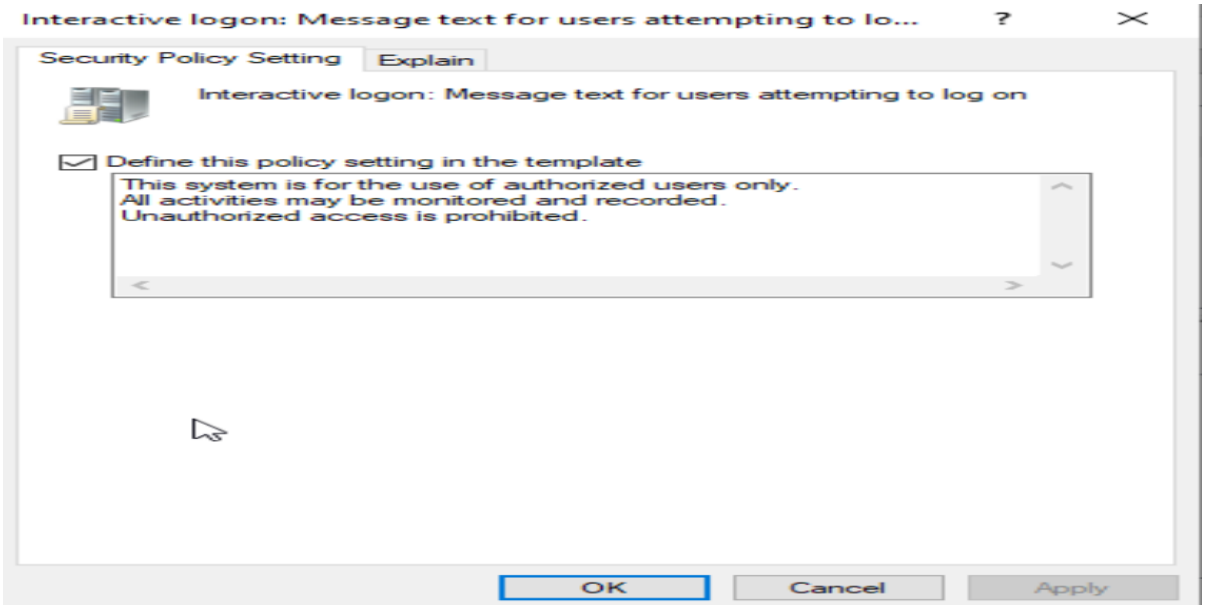
- **Configure Banner Message Settings**

  In Security Options, we set "Interactive logon: Message title" to "Authorized Use Only" and the message text to a standard legal disclaimer. This message appears before any user login.

(Message title entry in GPO editor)



(Message text entry in GPO editor)



On reboot, the legal banner appeared before the login screen. Users had to acknowledge the notice before proceeding, confirming successful deployment.

4. Results And Findings

The implementation of Group Policies in this task yielded successful security improvements across the domain. Each GPO functioned as intended, enforcing configurations and reducing security risks on domain-joined systems. Verification steps confirmed that the changes were active and effective. This phase validated the application of security policies through real-time tests such as gpresult reports, command-line verification, and user login experiences. Each objective was met, proving that Group Policy Management is a powerful tool for consistent, organization-wide security enforcement.

- **Screen Lock Policy Applied Successfully**
  After applying the Group Policy to the Workstations OU, all targeted systems locked automatically after 15 minutes of inactivity. This was verified through live testing and policy reports using gpresult /r. The enforced timeout effectively reduces the risk of unauthorized access during user absence.

- **SMBv1 Protocol Disabled on All Clients**
  Disabling SMBv1 was validated using PowerShell commands and registry inspection. Clients showed the SMBv1 feature as removed or disabled. This ensures protection against vulnerabilities associated with older SMB versions, such as the EternalBlue exploit used in WannaCry attacks.

- **Logon Banner Displayed on Login Screen**
  After linking the logon banner GPO, domain users were shown a custom legal notice before reaching the login screen. This was confirmed through system reboots and visual checks. The banner informs users of monitoring and legal accountability, helping enforce acceptable use policies.

- **GPOs Linked Correctly to Ous**
  Each GPO was precisely linked to its respective OU (e.g., Workstations OU for screen lock). gpresult /r confirmed that intended policies were applied, with no unintended inheritance or blocking. This demonstrates good scope management and policy targeting in GPMC.

- **No Conflicting GPOs Detected**
  Through RSOP and Resultant Set of Policy analysis, we verified that none of the new GPOs conflicted with existing policies. This helped maintain consistency across the domain and avoided misconfiguration issues such as settings being overridden or not applied.

5. Recommendation

While the current GPO configurations enhanced domain security, further steps can optimize the environment. Regular policy audits, layered policies, and education will strengthen long-term effectiveness. The following recommendations aim to ensure sustainability and continuous improvement.

- **Audit GPOs Quarterly**
  It is recommended to perform quarterly reviews of all GPOs to ensure they remain relevant and effective. This includes checking for outdated policies, unlinked GPOs, or configurations no longer needed. Regular audits help in minimizing security risks and maintaining a clean policy environment.

- **Extend Lock Policy to All Endpoints**
  Currently, the screen lock policy is applied only to workstations. It should be expanded to include all endpoints like laptops and remote-access devices. This ensures consistent security regardless of user location or device, especially important for hybrid or remote work environments.

- **Educate Users on Policy Changes**
  Users should be informed about newly implemented policies, such as the screen timeout and login banner. Providing a brief training or communication can reduce confusion, accidental lockouts, or user resistance. Awareness leads to smoother transitions and better compliance.

- **Implement Logging and Alerts for SMB Protocol Usage**
  Although SMBv1 is disabled, attempts to use it should still be logged using tools like Sysmon or Windows Event Logs. Alerts can help detect outdated software or unauthorized access attempts trying to rely on the deprecated protocol.

- **Document All GPOs with Justification**Each
  Group Policy should be documented with its name, purpose, linked OUs, and justification for implementation. This helps during audits, troubleshooting, and when onboarding new administrators. Proper documentation supports policy transparency and operational efficiency.

6. Conclusion

The Group Policy Management task demonstrated how centralized policy enforcement through Active Directory can significantly enhance organizational security and standardization. By implementing targeted Group Policy Objects (GPOs), we were able to enforce critical settings such as automatic screen lock after inactivity, disablement of insecure legacy protocols like SMBv1, and display of a legal logon banner to all users. Each of these configurations addresses a distinct area of risk and reflects best practices in enterprise IT security.

The testing and verification process confirmed that all applied GPOs functioned as intended and affected only the designated Organizational Units (OUs), showcasing proper scope control and GPO inheritance management. In particular, the disabling of SMBv1 closes the door to a range of exploits, while the screen lock policy reduces physical security risks related to unattended machines. The logon banner, meanwhile, fulfills both legal and ethical requirements by clearly communicating the acceptable use terms to all users.

Overall, this task reinforces the importance of using Group Policies not just for configuration but as a powerful security tool. Proper planning, execution, and verification ensure that these policies don’t interfere with user productivity while providing essential protections. Ongoing maintenance, documentation, and periodic policy reviews will ensure that these GPOs continue to align with the organization’s evolving security needs and compliance obligations.