

Group Policy Testing Results

Test Date: December 28, 2025

Tester: Dhelcy Mensah

Environment: gpo.local domain

Project Repository: [Insert GitHub Link Here]

Summary

Total GPOs Tested: 15

Passed: 15

Failed: 0

Success Rate: 100%

Detailed Test Results

1. Password Policy

Status:  PASS

Test: Attempted to set 8-character password.

Result: Rejected - minimum 14 characters enforced.

2. Account Lockout

Status:  PASS

Test: 6 failed login attempts on test account.

Result: Account locked after 5 attempts, requires admin unlock.

Note: Modified to require admin unlock (duration = 0) for enhanced security.

3. Audit Policy

Status:  PASS

Test: Generated logon event, checked Security log.

Result: Event ID 4624 captured with full details.

4. Command Prompt Restriction

Status:  PASS

Test: Attempted to open cmd.exe as standard user.

Result: Access denied with GPO message.

5. Registry Editor Restriction

Status:  PASS

Test: Attempted to open regedit.exe.

Result: Access denied with GPO message.

6. Run Menu Removal

Status:  PASS

Test: Checked Start menu context menu.

Result: Run option not present.

7. Screen Lock Policy

Status:  PASS

Test: Verified registry setting for timeout.

Result: ScreenSaveTimeOut = 600 seconds (10 min).

8. Windows Firewall

Status:  PASS

Test: Checked firewall status, tested ping.

Result: Firewall enabled on Domain profile, exceptions working.

9. User Rights Assignment

Status:  PASS

Test: Attempted to change system time as standard user.

Result: Access denied - only Administrators can modify time.

10. Security Options

Status:  PASS

Test: Verified administrator rename, CTRL+ALT+DEL requirement.

Result: Admin renamed to SysAdmin, secure login required.

11. Removable Media Control

Status:  PASS

Test: Checked Deny_All registry value.

Result: All removable storage classes denied.

12. Windows Update

Status:  PASS

Test: Checked automatic update configuration.

Result: Auto-download and install at 3 AM daily.

13. Remote Desktop Hardening

Status:  PASS

Test: Verified NLA requirement in registry.

Result: UserAuthentication = 1 (NLA enforced).

14. Software Restriction Policies

Status:  PASS

Test: Attempted execution from %TEMP% and Downloads.

Result: Both locations blocked by policy.









15. Event Log Configuration

Status:  PASS

Test: Checked Security log maximum size.

Result: Increased to 102400 KB (100 MB).

Before vs After Comparison

Security Control	Before (Baseline)	After (Hardened)	Improvement
Min Password Length	7 characters	14 characters	+100% Strength
Account Lockout	Disabled	5 attempts, admin unlock	 Enabled
Audit Logging	None	6 categories (S&F)	 Enabled
CMD Access	Allowed	Blocked	 Restricted
Registry Access	Allowed	Blocked	 Restricted
USB Storage	Allowed	Blocked	 Restricted
Windows Firewall	Disabled	Enabled with rules	 Protected
Software Execution	Unrestricted	Temp/Downloads blocked	 Controlled
Event Log Size	20 MB	100 MB	+400% Retention
RDP Security	Basic	NLA + High Encryption	 Hardened

Conclusion

All 15 Group Policy Objects were successfully applied and tested. The environment security posture improved significantly:

Attack Surface Reduction:

- Restricted administrative tools access.
- Blocked malware execution paths.
- Enforced strong authentication.

Compliance:

- Password complexity meets standards.
- Audit logging enabled for incident response.
- Account lockout prevents brute force.

Detection & Response:

- Comprehensive logging enabled.
- Increased log retention.
- Attack indicators captured.

Overall Security Rating:

- Before: POOR (High Risk)
- After: GOOD (Significantly Hardened)