



REPORT

Enforcing Operating System Patching Policy via Local GPO

v1.0.0

Author:

Eldon Gabriel

September 26, 2025



Cybersecurity Professional | IT Security Consultant

TABLE OF CONTENTS


REVISION HISTORY.....	2
SECTION 1.0: OPERATING SYSTEM PATCHING POLICY ENFORCEMENT.....	3
1.1 Project Description.....	3
1.2 Configuration Tasks.....	3
1.3 Implementation Steps.....	3
1.4 Key Observations.....	4
1.5 Supporting Work.....	4
SECTION 2.0: CONCLUSION.....	5
2.1 Key Takeaways.....	5
2.2 Security Implications and Recommendations.....	5





Cybersecurity Professional | IT Security Consultant

REVISION HISTORY

Version	Date	 Author	Description of Changes
v1.0.0	09/26/2025	Eldon G.	Initial draft.





Cybersecurity Professional | IT Security Consultant

SECTION 1.0 OPERATING SYSTEM PATCHING POLICY ENFORCEMENT

1.1 Project Description

This project demonstrates how to set up a Local Group Policy Object (GPO) on a standalone Windows computer. The main objective was to enforce a patching policy that balances security and system usability. By automating updates, the system remains protected from new threats while minimizing user disruptions.



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 Configuration Tasks

The following GPO settings were configured:

- Allow Automatic Updates, immediate installation → Enabled
 - Configure Automatic Updates → Enabled
 - Do not include drivers with Windows Updates → Disabled
 - No auto-restart with logged-on users for scheduled automatic updates installations → Enabled
 - Remove access to use all Windows Update features → Disabled
 - Turn on recommended updates via Automatic Updates → Enabled
-

1.3 Implementation Steps

1. The Local Group Policy Editor (`gpedit.msc`) was opened.
 2. Navigated to:
`Computer Configuration > Administrative Templates > Windows Components > Windows Update.`
 3. The configuration settings listed above were applied.
 4. The `gpupdate /force` command was run in an elevated Command Prompt to immediately enforce the new policies.
 5. Verified enforcement with `gpresult /r`, confirming the policies appeared in the Windows Update settings.
-



1.4 Key Observations

- Policies were enforced immediately after running the command `gpupdate /force`.
 - Automatic updates were installed without requiring any user input.
 - The “**No auto-restart**” setting prevented unexpected reboots during use.
 - *However, this also delays the installation of certain security patches until a restart is performed.*
 - To address this issue, organizations should schedule regular maintenance windows or enforce restart policies.
-

1.5 Supporting Work

- Video screen recordings were captured to validate the GPO application.
 - Policy compliance was verified using Windows Update logs.
-



SECTION 2.0 CONCLUSION

2.1 Key Takeaways

- Local GPOs can effectively enforce patching policies without an Active Directory.
 - Automating updates reduces system exposure to such vulnerabilities.
 - Balancing usability and security through the “**No auto-restart**” setting supports the user experience but requires supplemental administrative oversight.
-

2.2 Security Implications and Recommendations

- Regular patching is a fundamental defense against exploitation.
- Enforcing GPO settings ensures the timely installation of Microsoft security updates and reduces the risk of unpatched vulnerabilities.

Forward-Looking Recommendations: Local GPOs are the most suitable for standalone systems. In larger environments, the **Active Directory Group Policy (AD GPO)** should be used to manage patching across all endpoints. Combined with scheduled reboots, this ensures domain-wide compliance and reduces the delays in patch application.
