



# **REPORT**

# **Harden UAC via Local Group Policy**

*v1.0.0*

Author:

**Eldon Gabriel**

September 24, 2025



Cybersecurity Professional | IT Security Consultant

## TABLE OF CONTENTS


<b>REVISION HISTORY</b> .....	<b>2</b>
<b>SECTION 1.0: HARDENING USER ACCOUNT CONTROL (UAC)</b> .....	<b>3</b>
1.1 Project Overview.....	3
1.2 Technical Configuration Steps.....	4
1.3 Validation Steps.....	4
1.4 Observations / Troubleshooting.....	4
1.5 Supporting Work.....	5
<b>SECTION 2.0: CONCLUSION</b> .....	<b>6</b>
2.1 Key Takeaways.....	6
2.2 Security Implications and Recommendations.....	6





Cybersecurity Professional | IT Security Consultant

## REVISION HISTORY

Version	Date	 Author	Description of Changes
v1.0.0	09/22/2025	Eldon G.	Initial draft.





Cybersecurity Professional | IT Security Consultant

## SECTION 1.0: HARDENING USER ACCOUNT CONTROL (UAC)

### 1.1 Project Overview

The objective of this project was to harden User Account Control (UAC) settings on a Windows 10 machine to mitigate risks such as unauthorized privilege escalation, credential spoofing, and malware installation without user approval. By enforcing explicit credential prompts and secure desktop elevation, the machine's security posture was significantly improved.



**Disclaimer:** This report documents my personal work completing an MCSI lab exercise. It reflects my understanding and configuration of Windows 10 UAC settings in a controlled, offline environment. No MCSI video or lab materials have been posted, shared, or distributed, ensuring compliance with MCSI's policies.



## 1.2 Technical Configuration Steps

- Open the **Local Group Policy Editor** (*gpedit.msc*).
  - Enabled **Admin Approval Mode** for the built-in administrator account.
  - Disabled **UIAccess application elevation without a secure desktop** to ensure that all prompts were securely executed.
  - Configured elevation prompts:
    - Administrators → Prompt for credentials on the secure desktop
    - Standard users → Prompt for credentials on the secure desktop
  - Enabled **Detect application installations and prompted for elevation**.
  - All administrators in Admin Approval Mode were enabled.
  - Enabled **Switch to the secure desktop when prompted for elevation**.
- 

## 1.3 Validation Steps

- Launched an application requiring administrative privileges.
  - A verified credential prompt appeared on the **secure desktop**, confirming that the hardened UAC policies were active.
-



## 1.4 Observations / Troubleshooting

- After enabling Admin Approval Mode, elevation prompts were consistently credential-based instead of a simple “Yes/No” confirmation.
  - No compatibility issues arose with applications tested; for example, **Microsoft Edge** and **Notepad++** ran without interruption under the hardened UAC settings.
- 

## 1.5 Supporting Work

- Conducted test runs with both standard and administrative accounts.
  - Documented policy paths for repeatability, e.g.:
    - Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options > User Account Control: Admin Approval Mode for the Built-in Administrator account
    - Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options > User Account Control: Switch to the secure desktop when prompting for elevation
-



## SECTION 2.0: CONCLUSION

### 2.1 Key Takeaways

- The hardening of UAC enforces credential-based authentication for sensitive actions.
- Secure desktop elevation reduces the risks of spoofing and phishing attacks.
- Group Policy provides a repeatable and centralized method for enforcing user access control.

### 2.2 Security Implications and Recommendations

- Hardened UAC reduces the opportunities for attackers to escalate privileges.
  - Credential-based prompts ensure the accountability and traceability of sensitive actions.
  - In business settings, these rules should be used with other measures such as logging, monitoring, and providing the least access needed for full protection.
-