There are many ways to disable UAC on your computer. Here are a few...

Option A - Disable UAC Through User Account Control Settings

This is the method that should be used by most users wanting to disable UAC.

Go to User Account Control Settings.

Type in UAC, or go to the System and Security applet.

Click on the "Change User Account Control Settings" link.



BTW, you can also type in this command from the Run menu:

C:\Windows\System32\UserAccountControlSettings.exe

To turn off UAC, move the slider to the Never notify position, and then click OK. If you're prompted for an administrator password or confirmation, type the password or provide confirmation.



To turn UAC back on, move the slider to choose when you want to be notified, and then click OK. If you're prompted for an administrator password or confirmation, type the password or provide confirmation.

You will need to restart your computer for UAC to be turned off.

Option B - Disable UAC Through Group Policy

This is the method that should be used by administrators wanting to disable UAC across several computers at once.

This can be done via Local Group Policy or via Active Directory-based GPO, which is much more suited for large networks where one would like to disable UAC for many computers at once.

If using Local Group Policy you'll need to open the Group Policy Editor (Start > Run > gpedit.msc).

If using in AD-based GPO, open Group Policy Management Console (Start > Run > gpmc.msc) from a Windows Vista/7/2008 computer that is a member of the domain. In the GPMC window, browse to the required GPO that is linked to the OU or domain where the computers are located, then edit it, or, if needed, create a new GPO.

🧟 Group Policy Manag	gement					- 0	×
📓 File Action View	Window Help					_16	
🗢 🔿 🔁 📅 🗋	I 🖾 🙆 🖬						
Group Policy Manager	ment VII	rtual.lab nked Group Policy Ob	jects Group Policy Inheritanc	e Delegat	ion)		
E 🚔 virtua	Create a GPO in this domain, and	Link it here	GPO	Enforced	Link Enabled	GPO Status	N
	Link an Existing GPU Block Inheritance	Default Domain Policy		No	Yes	Enabled	N
	Group Policy Modeling Wizard New Organizational Unit						
	Search Change Domain Controller						
Group Pol	Remove Active Directory Users and Comp	outers					
C Group Poi	View New Window from Here	•					
	Refresh Properties Help						
-							
		•					
Dreate a GPO in this doma	in and link it to this container						-



📓 Group Policy Management					_ 🗆 🗵
File Action View Window Help	6				_8×
🗇 🤿 🖄 📅 🐹 🤉 👔 📷					
Group Policy Management Group Policy Management Forest: virtual.lab Domains Default Domain Policy Disable UAC G Disable UAC G Disable UAC G Edit. Enfor Users Componion Contro Component Contro Contro Component Contro Component Contro Contro Component Contro Component Contro Contro Component Contro Component Contro Contr	Disable Scope [Links Display lin ced % inabled Report	UAC GPO Details Settings Delegat nks in this location: ng sites, domains, and OL	ion) vitual Jab Js are linked to this GPO: Enforced No	I Link Enabled Yes	▼ Path virtual Jab
Eligi Starter GPOs Eligi Sites Coup Policy Modeling Rena Coup Policy Results Refre	e me sh	Filtering as in this GPO can only apply to the following groups, users, and computers:			
Help		inticated Users			
	A WMI Filt This GPC (cnone>	Add Rem tering O is linked to the following V	Nove Propert	es Open	
Open the GPO editor	,				

In the Group Policy Editor window, browse to Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options. Make the following changes:

- User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode Set its value to **Elevate without prompting**.
- User Account Control: Detect application installations and prompt for elevation Set its value to **Disabled**.
- User Account Control: Only elevate UIAccess applications that are installed in secure locations Set its value to **Disabled**.
- User Account Control: Run all administrators in Admin Approval Mode Set its value to **Disabled**.

le Action View Help			
• 🔿 🙍 🖬 🕞 😰 🗃			
Disable UAC GPO [KARENDC.VI	Policy A	Policy Setting	
👫 Computer Configuration	Network security: Restrict NTLM: Audit Incoming NTLM Traffic	Not Defined	
E Policies	Retwork security: Restrict NTLM: Audit NTLM authentication in this domain	Not Defined	
Software Settings	Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined	
E 🔛 Windows Settings	Network security: Restrict NTLM: NTLM authentication in this domain	Not Defined	
Name Resolutio	Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Not Defined	
Scripts (Startup	Recovery console: Allow automatic administrative logon	Not Defined	
E 🚡 Security Setting	Recovery console: Allow floppy copy and access to all drives and all folders	Not Defined	
Account Pol	Shutdown: Allow system to be shut down without having to log on	Not Defined	
E Cocal Policie	Shutdown: Clear virtual memory pagefile	Not Defined	
H Audit Pt	System gryptography: Force strong key protection for user keys stored on t	Not Defined	
	System gryptography: Use FIPS compliant algorithms for encryption, hashin	Not Defined	
T T Supplier	System objects: Require case insensitivity for non-Windows subsystems	Not Defined	
Destricted (System objects: Strengthen default permissions of internal system objects (Not Defined	
E Suctem Ser	System settings: Optional subsystems	Not Defined	
E Registry	System settings: Lise Certificate Rules on Windows Everytables for Softwar	Not Defined	
E Ble System	User Account Control: Admin Approval Mode for the Built-in Administrator ac-	Not Defined	
E In Wred Netw	Diser Account Control: Allow URAccess applications to promot for elevation w.	Not Defined	
🕀 🧮 Windows Fit	Dear Account Control: Bahavior of the alevation prompt for administratore i	Elevate without promotion	
Network Lis	Control Delayed of the develop prompt for etandard users	Not Defined	
🕀 📝 Wireless Ne	Control, beneficial patient and and a sent and a sent for all states	Disabled	
🗉 🦲 Public Key F	By Oser Account Control: Detect approaction installations and prompt for elevation	Nat Defined	
🗉 🧮 Software Ri	is user Account Control: Only elevate executables that are signed and validated	Not Denned	
🗉 🧮 Network Ac	and user Account Control: Only elevate OLAccess applications that are installed I	Disabled	
Application	all user Account Control: Run all administrators in Admin Approval Mode	Usabled	
🛨 🛃 IP Security	all user Account Control: Switch to the secure desktop when prompting for ele	Not Defined	
🕀 🧮 Advanced A 🚚	User Account Control: Virtualize file and registry write failures to per-user lo	Not Defined	
	d		11

Restart the computer when done.

Option C - Disable UAC Through the Registry

Another method to disable UAC is through the computer's Registry.

Warning!

This document contains instructions for editing the registry. If you make any error while editing the registry, you can potentially cause Windows to fail or be unable to boot, requiring you to reinstall Windows. Edit the registry at your own risk. Always back up the registry before making any changes. If you do not feel comfortable editing the

registry, do not attempt these instructions. Instead, seek the help of a trained computer specialist.

Click Start, click Run, type regedit, and then click Enter.

If prompted to enter your credentials by UAC, do so and/or press Yes to continue.

Navigate to the following registry subkey:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\S
ystem
```

In the details pane, locate the *EnableLUA* key (REG_DWORD type).

On the Edit menu, click Modify. In the Value data box, type 0 (zero), and then click OK.



Exit Registry Editor, and then reboot the computer.