## How to Manage User Account Control (UAC) in Windows Server 2012

Microsoft has modified some of its processes for managing User Account Control (UAC) in Windows Server 2012. By default, UAC will now be enabled in Windows Server 2012. This article will walk you through the steps needed to disable User Account Control as necessary, based on user requirements.

There is a two-step process needed to enable/disable User Account Control in Windows Server 2012.

## Step One: Change UAC settings

- Click **Settings** on the right of the desktop to open the Control Panel.
- Click on User Accounts to change User Account Settings.
- The default User Control setting is pictured below:

Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to you <u>Tell me more about User Account Control settings</u>



Never notify

• You will need to change your notification settings to turn off the security level:

## Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your comp <u>Tell me more about User Account Control settings</u>



## Step Two: Disable User Account Control policy

• To see your current UAC status, go to the Action Center:



• To change the UAC policy in Server Manager, you need to first go into Server Manager and select Local Security Policy in the Tools menu:

| Se   | erver Manager        |   |   |
|--|----------------------|---|---|
| oard   | 🕶 🧭   🚩 Manage       | Tools   | View Help   |
| Server Manager         Coard       Cols       Vie         WELCOME TO SERVER MANAGER       Compared       Compared         QUICK START       1       Configure this loot       Defrage         QUICK START       2       Add roles and feat       Internet         3       Add other servers       Local S         WHAT'S NEW       4       Create a server gr       ODBC         ODBC       ODBC       ODBC       ODBC         ODBC       ODBC       ODBC       ODBC |                      | Component Services<br>Computer Management<br>Defragment and Optimize Drives |   |
|  | 1 Configure this lo  | (   | Event Viewer<br>Health Registration Authority<br>Hyper-V Manager<br>Internet Information Services (IIS) 6.0 Manager |
| QUICK START  | 2 Add roles and fea  | Ī   | Internet Information Services (IIS) Manager<br>iSCSI Initiator  |
|  | 3 Add other servers  |   | Local Security Policy<br>Network Policy Server  |
| WHAT'S NEW   | 4 Create a server gr |   | ODBC Data Sources (32-bit)  |
|  |                      |   | ODBC Data Sources (64-bit)<br>Performance Monitor   |
| LEARN MORE   |                      |   | Resource Monitor<br>Security Configuration Wizard   |

• To change the policy, right-click User Account Controls: Run all administrators in Admin Approve Mode:

| 24  | Local Security Policy  | Security Setting ^<br>in th Not Defined<br>c to Not Defined<br>n Disabled<br>rives Disabled<br>ug to Disabled<br>Disabled<br>ser k Not Defined  |   |  |
|---|--|---|---|--|
| File Action View Help   | Policy   | Security Setting<br>Not Defined   | ^ |  |
| <ul> <li>Local Policies</li> <li>Audit Policy</li> <li>Audit Policy</li> <li>User Rights Assignment</li> <li>Security Options</li> <li>Windows Firewall with Advanced Seci</li> <li>Network List Manager Policies</li> <li>Public Key Policies</li> <li>Software Restriction Policies</li> <li>Software Restriction Policies</li> <li>Application Control Policies</li> <li>IP Security Policies on Local Compute</li> <li>Advanced Audit Policy Configuration</li> </ul> | <ul> <li>Network security: Restrict NTLM: Outgoing NTLM traffic to</li> <li>Recovery console: Allow automatic administrative logon</li> <li>Recovery console: Allow floppy copy and access to all drives</li> <li>Shutdown: Allow system to be shut down without having to</li> <li>Shutdown: Clear virtual memory pagefile</li> <li>System cryptography: Force strong key protection for user k</li> <li>System cryptography: Use FIPS compliant algorithms for en</li> <li>System objects: Require case insensitivity for non-Windows</li> <li>System objects: Strengthen default permissions of internal s</li> <li>System settings: Optional subsystems</li> <li>System settings: Use Certificate Rules on Windows Executabl</li> <li>User Account Control: Admin Approval Mode for the Built-i</li> <li>User Account Control: Behavior of the elevation prompt for</li> <li>User Account Control: Behavior of the elevation prompt for</li> <li>User Account Control: Detect application installations and p</li> </ul> | Not Defined<br>Disabled<br>Disabled<br>Disabled<br>Disabled<br>Not Defined<br>Disabled<br>Enabled<br>Enabled<br>Posix<br>Disabled<br>Disabled<br>Disabled<br>Elevate without prompti<br>Prompt for credentials<br>Enabled |   |  |
|   | <ul> <li>User Account Control: Only elevate executables that are sign</li> <li>User Account Control: Only elevate UIAccess applications th</li> <li>User Account Control: Run all administrators in Admin Appr</li> <li>User Account Control: Switch to the secure desktop when pr</li> </ul>  | Disabled<br>Enabled<br>Enabled<br>Disabled  | Ш |  |
| < III >   | User Account Control: Virtualize file and registry write failure   | Enabled   | ~ |  |

- Your default setting will have "Run all administrators in Admin Approval Mode" enabled.
- To change this setting, click **Disable** as pictured below:



- Click **Apply**, then **OK**, and then restart the server to finish changing your settings.
- To verify that the changes were correctly applied, go to the Action Center and check the status of your User Account Control policy:

| p   |   | Action Center   |            | x   |
|---|---|---|------------|-----|
| ۲   | ) 🍥 🔹 🏌 🚩 🕨 Control Pane                | System and Security      Action Center     Search Control Pan | el         | ٩,  |
| Control Panel Home  |   | Review recent messages and resolve problems                   |            | • • |
|   | Change Action Center settings           | No issues have been detected by Action Center.                |            |     |
| 9   | Change User Account Control<br>settings | Security  | $\bigcirc$ |     |
| 9   | Change Windows SmartScreen<br>settings  | User Account Control Off                                      | 0          |     |
| View archived messages UAC will never notify you when apps try to make changes to the computer. |   |   |            |     |
|   |   | 😗 Choose your UAC level                                       |            |     |
|   |   |   |            |     |