UAC Group Policy Settings and Registry Key Settings

TN technet.microsoft.com/en-us/library/dd835564(v=ws.10).aspx

There are 10 Group Policy settings that can be configured for User Account Control (UAC). The table lists the default for each of the policy settings, and the following sections explain the different UAC policy settings and provide recommendations. These policy settings are located in **Security Settings\Local Policies\Security Options** in the Local Security Policy snap-in. For more information about each of the Group Policy settings, see the Group Policy description. For information about the registry key settings, see Registry key settings.

Group Policy setting	Registry key	Default
User Account Control: Admin Approval Mode for the built-in Administrator account	FilterAdministratorToken	Disabled
User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop	EnableUIADesktopToggle	Disabled
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	ConsentPromptBehaviorAdmin	Prompt for consent for non-Windows binaries
User Account Control: Behavior of the elevation prompt for standard users	ConsentPromptBehaviorUser	Prompt for credentials on the secure desktop
User Account Control: Detect application installations and prompt for elevation	EnableInstallerDetection	Enabled (default for home) Disabled (default for enterprise)
User Account Control: Only elevate executables that are signed and validated	ValidateAdminCodeSignatures	Disabled
User Account Control: Only elevate UIAccess applications that are installed in secure locations	EnableSecureUIAPaths	Enabled
User Account Control: Run all administrators in Admin Approval Mode	EnableLUA	Enabled

User Account Control: Switch to the secure desktop when prompting for elevation	PromptOnSecureDesktop	Enabled
User Account Control: Virtualize file and registry write failures to per-user locations	EnableVirtualization	Enabled

User Account Control: Admin Approval Mode for the built-in Administrator account

The **User Account Control: Admin Approval Mode for the built-in Administrator account** policy setting controls the behavior of Admin Approval Mode for the built-in Administrator account.

The options are:

- **Enabled.** The built-in Administrator account uses Admin Approval Mode. By default, any operation that requires elevation of privilege will prompt the user to approve the operation.
- **Disabled.** (Default) The built-in Administrator account runs all applications with full administrative privilege.

User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop

The **User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop** policy setting controls whether User Interface Accessibility (UIAccess or UIA) programs can automatically disable the secure desktop for elevation prompts used by a standard user.

The options are:

- **Enabled.** UIA programs, including Windows Remote Assistance, automatically disable the secure desktop for elevation prompts. If you do not disable the **User Account Control: Switch to the secure desktop when prompting for elevation** policy setting, the prompts appear on the interactive user's desktop instead of the secure desktop.
- **Disabled.** (Default) The secure desktop can be disabled only by the user of the interactive desktop or by disabling the **User Account Control: Switch to the secure desktop when prompting for elevation** policy setting.

UIA programs are designed to interact with Windows and application programs on behalf of a user. This policy setting allows UIA programs to bypass the secure desktop to increase usability in certain cases; however, allowing elevation requests to appear on the interactive desktop instead of the secure desktop can increase your security risk.

UIA programs must be digitally signed because they must be able to respond to prompts regarding security issues, such as the UAC elevation prompt. By default, UIA programs are run only from the following protected paths:

- …\Program Files, including subfolders
- …\Program Files (x86), including subfolders for 64-bit versions of Windows
- …\Windows\System32

The **User Account Control: Only elevate UIAccess applications that are installed in secure locations** policy setting disables the requirement to be run from a protected path.

While this policy setting applies to any UIA program, it is primarily used in certain remote assistance scenarios, including the Windows Remote Assistance program in Windows 7.

If a user requests remote assistance from an administrator and the remote assistance session is established, any elevation prompts appear on the interactive user's secure desktop and the administrator's remote session is paused. To avoid pausing the remote administrator's session during elevation requests, the user may select the **Allow IT Expert to respond to User Account Control prompts** check box when setting up the remote assistance session. However, selecting this check box requires that the interactive user respond to an elevation prompt on the secure desktop. If the interactive user is a standard user, the user does not have the required credentials to allow elevation.

If you enable this policy setting, requests for elevation are automatically sent to the interactive desktop (not the secure desktop) and also appear on the remote administrator's view of the desktop during a remote assistance session. This allows the remote administrator to provide the appropriate credentials for elevation.

This policy setting does not change the behavior of the UAC elevation prompt for administrators.

If you plan to enable this policy setting, you should also review the effect of the **User Account Control: Behavior of the elevation prompt for standard users** policy setting. If it is configured as **Automatically deny elevation requests**, elevation requests are not presented to the user.

User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode

---

The **User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode** policy setting controls the behavior of the elevation prompt for administrators.

The options are:

- **Elevate without prompting.** Allows privileged accounts to perform an operation that requires elevation without requiring consent or credentials.

Note
Use this option only in the most constrained environments.

- **Prompt for credentials on the secure desktop.** When an operation requires elevation of privilege, the user is prompted on the secure desktop to enter a privileged user name and password. If the user enters valid credentials, the operation continues with the user's highest available privilege.
- **Prompt for consent on the secure desktop.** When an operation requires elevation of privilege, the user is prompted on the secure desktop to select either **Permit** or **Deny**. If the user selects **Permit**, the operation continues with the user's highest available privilege.
- **Prompt for credentials.** When an operation requires elevation of privilege, the user is prompted to enter an administrative user name and password. If the user enters valid credentials, the operation continues with the applicable privilege.

- **Prompt for consent.** When an operation requires elevation of privilege, the user is prompted to select either **Permit** or **Deny**. If the user selects **Permit**, the operation continues with the user's highest available privilege.
- **Prompt for consent for non-Windows binaries.** (Default) When an operation for a non-Microsoft application requires elevation of privilege, the user is prompted on the secure desktop to select either **Permit** or **Deny**. If the user selects **Permit**, the operation continues with the user's highest available privilege.

User Account Control: Behavior of the elevation prompt for standard users

---

The **User Account Control: Behavior of the elevation prompt for standard users** policy setting controls the behavior of the elevation prompt for standard users.

The options are:

- **Automatically deny elevation requests.** When an operation requires elevation of privilege, a configurable access denied error message is displayed. An enterprise that is running desktops as standard user may choose this setting to reduce help desk calls.
- **Prompt for credentials on the secure desktop.** (Default) When an operation requires elevation of privilege, the user is prompted on the secure desktop to enter a different user name and password. If the user enters valid credentials, the operation continues with the applicable privilege.
- **Prompt for credentials.** When an operation requires elevation of privilege, the user is prompted to enter an administrative user name and password. If the user enters valid credentials, the operation continues with the applicable privilege.

User Account Control: Detect application installations and prompt for elevation

---

The **User Account Control: Detect application installations and prompt for elevation** policy setting controls the behavior of application installation detection for the computer.

The options are:

- **Enabled.** (Default for home) When an application installation package is detected that requires elevation of privilege, the user is prompted to enter an administrative user name and password. If the user enters valid credentials, the operation continues with the applicable privilege.
- **Disabled.** (Default for enterprise) Application installation packages are not detected and prompted for elevation. Enterprises that are running standard user desktops and use delegated installation technologies such as Group Policy Software Installation or Systems Management Server (SMS) should disable this policy setting. In this case, installer detection is unnecessary.

User Account Control: Only elevate executables that are signed and validated

---

The **User Account Control: Only elevate executables that are signed and validated** policy setting enforces public key infrastructure (PKI) signature checks for any interactive applications that request elevation of privilege. Enterprise administrators can control which applications are allowed to run by adding certificates to the Trusted Publishers certificate store on local computers.

The options are:

- **Enabled.** Enforces the PKI certification path validation for a given executable file before it is permitted to run.
- **Disabled.** (Default) Does not enforce PKI certification path validation before a given executable file is permitted to run.

User Account Control: Only elevate UIAccess applications that are installed in secure locations

The **User Account Control: Only elevate UIAccess applications that are installed in secure locations** policy setting controls whether applications that request to run with a User Interface Accessibility (UIAccess) integrity level must reside in a secure location in the file system. Secure locations are limited to the following:

- …\Program Files, including subfolders
- …\Windows\system32
- …\Program Files (x86), including subfolders for 64-bit versions of Windows

Note

Windows enforces a PKI signature check on any interactive application that requests to run with a UIAccess integrity level regardless of the state of this security setting.

The options are:

- **Enabled.** (Default) If an application resides in a secure location in the file system, it runs only with UIAccess integrity.
- **Disabled.** An application runs with UIAccess integrity even if it does not reside in a secure location in the file system.

User Account Control: Run all administrators in Admin Approval Mode

The **User Account Control: Run all administrators Admin Approval Mode** policy setting controls the behavior of all UAC policy settings for the computer. If you change this policy setting, you must restart your computer.

The options are:

- **Enabled.** (Default) Admin Approval Mode is enabled. This policy must be enabled and related UAC policy settings must also be set appropriately to allow the built-in Administrator account and all other users who are members of the **Administrators** group to run in Admin Approval Mode.
- **Disabled.** Admin Approval Mode and all related UAC policy settings are disabled.

Note

If this policy setting is disabled, the Security Center notifies you that the overall security of the operating system has been reduced.

User Account Control: Switch to the secure desktop when prompting for elevation

The **User Account Control: Switch to the secure desktop when prompting for elevation** policy setting controls whether the elevation request prompt is displayed on the interactive user's desktop or the secure desktop.

The options are:

- **Enabled.** (Default) All elevation requests go to the secure desktop regardless of prompt behavior policy settings for administrators and standard users.
- **Disabled.** All elevation requests go to the interactive user's desktop. Prompt behavior policy settings for administrators and standard users are used.

When this policy setting is enabled, it overrides the **User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode** policy setting. The following table describes the behavior of the elevation prompt for each of the administrator policy settings when the **User Account Control: Switch to the secure desktop when prompting for elevation** policy setting is enabled or disabled.

Administrator policy setting	Enabled	Disabled
Prompt for credentials on the secure desktop	The prompt appears on the secure desktop.	The prompt appears on the secure desktop.
Prompt for consent on the secure desktop	The prompt appears on the secure desktop.	The prompt appears on the secure desktop.
Prompt for credentials	The prompt appears on the secure desktop.	The prompt appears on the interactive user's desktop.
Prompt for consent	The prompt appears on the secure desktop.	The prompt appears on the interactive user's desktop.
Prompt for consent for non-Windows binaries	The prompt appears on the secure desktop.	The prompt appears on the interactive user's desktop.

When this policy setting is enabled, it overrides the **User Account Control: Behavior of the elevation prompt for standard users** policy setting. The following table describes the behavior of the elevation prompt for each of the standard user policy settings when the **User Account Control: Switch to the secure desktop when prompting for elevation** policy setting is enabled or disabled.

Standard user policy setting	Enabled	Disabled
Automatically deny elevation requests	No prompt. The request is automatically denied.	No prompt. The request is automatically denied.
Prompt for credentials on the secure desktop	The prompt appears on the secure desktop.	The prompt appears on the secure desktop.
Prompt for credentials	The prompt appears on the secure desktop.	The prompt appears on the interactive user's desktop.

User Account Control: Virtualize file and registry write failures to per-user locations

The **User Account Control: Virtualize file and registry write failures to per-user locations** policy setting controls whether application write failures are redirected to defined registry and file system locations. This policy setting mitigates applications that run as administrator and write run-time application data to %ProgramFiles%, %Windir%, %Windir%\system32, or HKLM\Software.

The options are:

- **Enabled.** (Default) Application write failures are redirected at run time to defined user locations for both the file system and registry.
- **Disabled.** Applications that write data to protected locations fail.