# Microsoft Windows User Account Control (UAC)

The goal of this document is to assist Qualys customers with a basic understanding of the UAC technology and how the use of UAC may affect Qualys scans of computers running Microsoft Windows operating systems.

## Contents

# 1. Summary

## 1.1 How does UAC impact Qualys scanning?

### Remote Registry Access

- Local Security Policy disables Remote Registry Service by default
- Alternative access to the registry requires installation of Qualys Dissolvable Agent (DA)
- Only domain users (members of local Administrators group) and built-in Administrator user can use Qualys DA by default
- Local users (members of Administrator group) cannot use Qualys DA and cannot access the registry

### File system access

- Only domain users (members of local Administrators group) and built-in Administrator can access C$ share remotely
- Local users (members of Administrator group) cannot access C$ share which prevents Qualys scans from reading version information of system and application files

## 1.2 How would I know if UAC changed the results from a Qualys scan?

- Normal and compliance scans return partial results
- DA installation fails with the insufficient privileges for local users (members of Administrators group)

## 1.3 What are the implications of scanning without adjusting the UAC settings?

- Local users (members of Administrator group) cannot install the Qualys DA because access to ADMIN$ share is disabled by default

# 2. Rationale

User Account Control (UAC) is a technology first introduced in Windows Vista that is currently supported by all modern versions of Microsoft Windows operating system.

For a detailed description of the UAC technology, please refer to the following articles published by Microsoft TechNet magazine and written by Sysinternals co-founder Mark Rossinovich.

Inside Windows Vista User Account Control:
http://technet.microsoft.com/en-us/magazine/2007.06.uac.aspx

Inside Windows 7 User Account Control:
http://technet.microsoft.com/en-us/magazine/2009.07.uac.aspx

## 3. UAC design

The UAC designers main goal was improved Microsoft Windows security which they achieved by making use of operating system by non-administrative users a standard. This means that any user, regardless whether it is a build-in Administrator, any other member of Administrators group, or any other group, always uses Windows as a standard user. This also means that administrative tasks that require elevated privileges can be performed only when needed or specifically requested by a user. UAC mode that elevates administrative privileges is called "Admin Approval Mode".

To illustrate how this works, let's look at some examples.

Example 1 – Alice is a member of Users group and would like to make changes to the system registry by running Registry Editor (regedit.exe) application. Alice can make any modifications to HKEY_CURRENT_USER hive but any modifications to HKEY_LOCAL_MACHINE will be denied. Alice can choose to run Registry Editor as administrator and UAC controls this process by either denying Alice this privilege completely or presenting Alice with a dialog box that requires a member of Administrators group approval.

Example 2 – Bob is a member of Administrators group and would like to make changes to the system registry by running Registry Editor (regedit.exe) application. UAC controls this process by allowing the program to run uninterrupted or by presenting Bob with a dialog box that request his approval to run the program with elevated privileges.

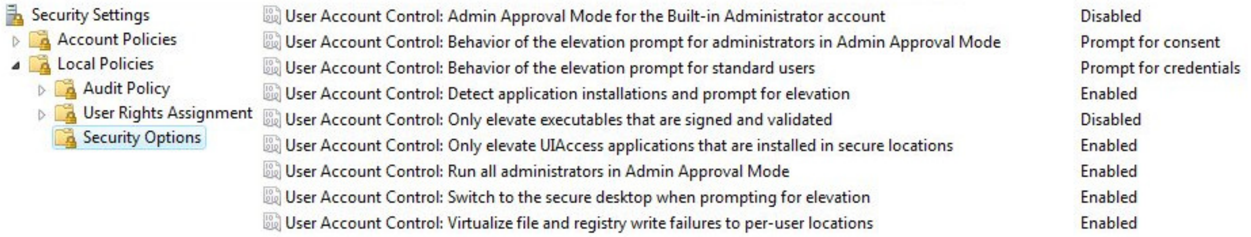
## 4. UAC policy – default settings

Local Security Policy defines a number of UAC settings that control the above behavior. For example, a UAC policy can be set up such that launching any unsigned Windows program is prohibited.

The UAC settings are defined in the Local Security Policy and use the prefix "User Account Control". The Local Security Policy editor can be launched directly by selecting Administrative Tools > Local Security Policy. It can be also launched by running Microsoft Management Console (mmc.exe) application and adding Local Policy Editor or Group Policy Object Editor snap-in for a Local Computer.

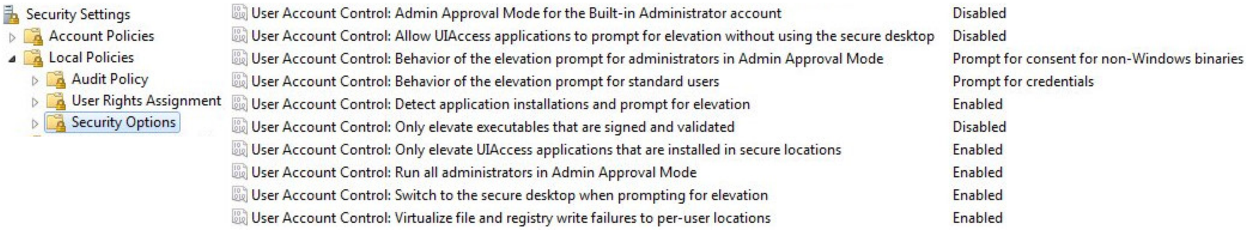
The following section shows UAC policy location in the Local Security Policy and UAC default values.

**Windows Vista**



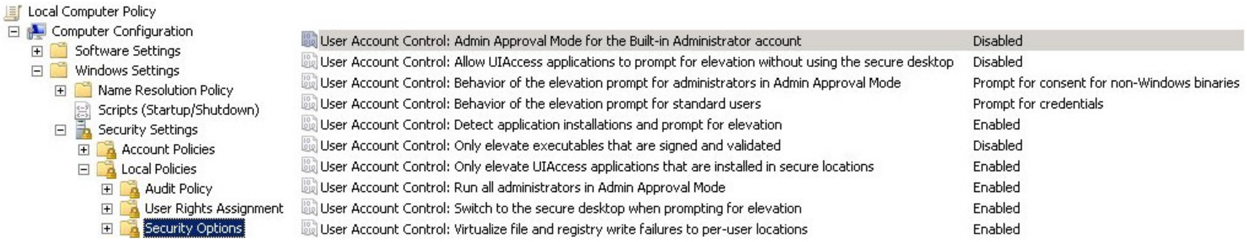
| | |
|---|---|
| User Account Control: Admin Approval Mode for the Built-in Administrator account | Disabled |
| User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode | Prompt for consent |
| User Account Control: Behavior of the elevation prompt for standard users | Prompt for credentials |
| User Account Control: Detect application installations and prompt for elevation | Enabled |
| User Account Control: Only elevate executables that are signed and validated | Disabled |
| User Account Control: Only elevate UIAccess applications that are installed in secure locations | Enabled |
| User Account Control: Run all administrators in Admin Approval Mode | Enabled |
| User Account Control: Switch to the secure desktop when prompting for elevation | Enabled |
| User Account Control: Virtualize file and registry write failures to per-user locations | Enabled |

### Windows 7



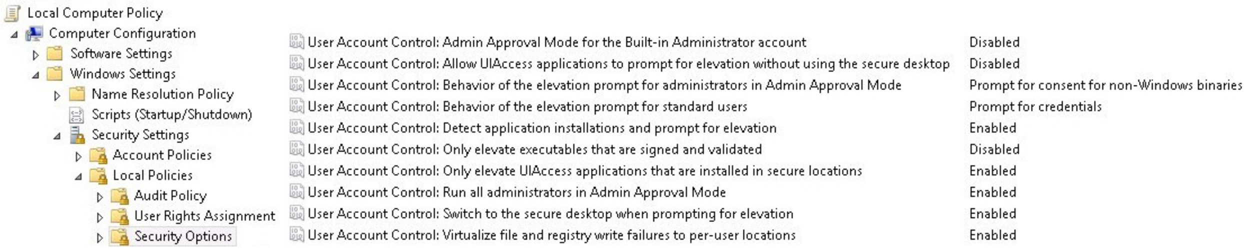
| | |
|---|---|
| User Account Control: Admin Approval Mode for the Built-in Administrator account | Disabled |
| User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop | Disabled |
| User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode | Prompt for consent for non-Windows binaries |
| User Account Control: Behavior of the elevation prompt for standard users | Prompt for credentials |
| User Account Control: Detect application installations and prompt for elevation | Enabled |
| User Account Control: Only elevate executables that are signed and validated | Disabled |
| User Account Control: Only elevate UIAccess applications that are installed in secure locations | Enabled |
| User Account Control: Run all administrators in Admin Approval Mode | Enabled |
| User Account Control: Switch to the secure desktop when prompting for elevation | Enabled |
| User Account Control: Virtualize file and registry write failures to per-user locations | Enabled |

### Windows 2008, Windows 2008 R2



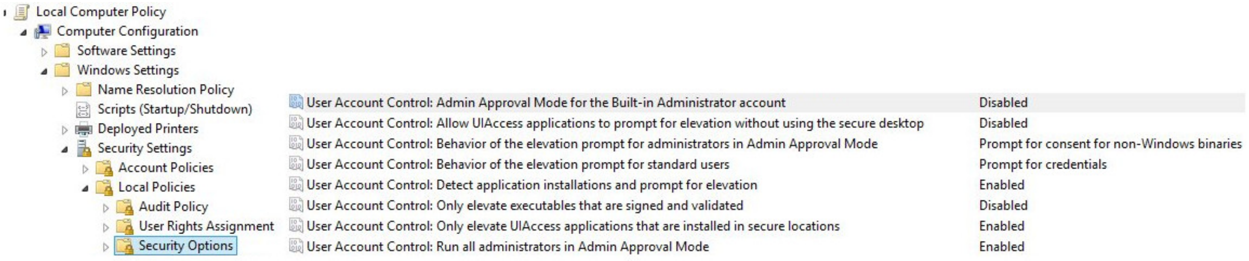
| | |
|---|---|
| User Account Control: Admin Approval Mode for the Built-in Administrator account | Disabled |
| User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop | Disabled |
| User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode | Prompt for consent for non-Windows binaries |
| User Account Control: Behavior of the elevation prompt for standard users | Prompt for credentials |
| User Account Control: Detect application installations and prompt for elevation | Enabled |
| User Account Control: Only elevate executables that are signed and validated | Disabled |
| User Account Control: Only elevate UIAccess applications that are installed in secure locations | Enabled |
| User Account Control: Run all administrators in Admin Approval Mode | Enabled |
| User Account Control: Switch to the secure desktop when prompting for elevation | Enabled |
| User Account Control: Virtualize file and registry write failures to per-user locations | Enabled |

### Windows 2012, Windows 2016, Windows 2019



| | |
|---|---|
| User Account Control: Admin Approval Mode for the Built-in Administrator account | Disabled |
| User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop | Disabled |
| User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode | Prompt for consent for non-Windows binaries |
| User Account Control: Behavior of the elevation prompt for standard users | Prompt for credentials |
| User Account Control: Detect application installations and prompt for elevation | Enabled |
| User Account Control: Only elevate executables that are signed and validated | Disabled |
| User Account Control: Only elevate UIAccess applications that are installed in secure locations | Enabled |
| User Account Control: Run all administrators in Admin Approval Mode | Enabled |
| User Account Control: Switch to the secure desktop when prompting for elevation | Enabled |
| User Account Control: Virtualize file and registry write failures to per-user locations | Enabled |

### Windows 8, Windows 8.1



| | |
|---|---|
| User Account Control: Admin Approval Mode for the Built-in Administrator account | Disabled |
| User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop | Disabled |
| User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode | Prompt for consent for non-Windows binaries |
| User Account Control: Behavior of the elevation prompt for standard users | Prompt for credentials |
| User Account Control: Detect application installations and prompt for elevation | Enabled |
| User Account Control: Only elevate executables that are signed and validated | Disabled |
| User Account Control: Only elevate UIAccess applications that are installed in secure locations | Enabled |
| User Account Control: Run all administrators in Admin Approval Mode | Enabled |

## 5. Admin Approval Mode

Admin Approval Mode can be entered on normal or secure desktops and certain UAC policy settings control this process. In a normal desktop case, a dialog box to approve elevation of the administrative privileges is shown on a desktop and use of other applications is not prohibited. In a secure desktop case, a new desktop is created specifically to display a dialog box to approve elevation of administrative privileges and until approval is either granted or denied, the use of other applications is prevented.

# 6. Local Policy UAC settings

There are 2 settings in the UAC policy that are common for all Windows versions that support UAC. Other UAC settings have no effect on Qualys authenticated scans of Windows systems.

## 6.1 User Account Control: Run All Administrators in Admin Approval Mode

This setting effectively controls whether UAC is enabled or disabled. The default is “enabled”. Changing this option to “disabled” turns UAC off and requires a system reboot.

## 6.2 User Account Control: Admin Approval Mode for the built-in Administrator accounts

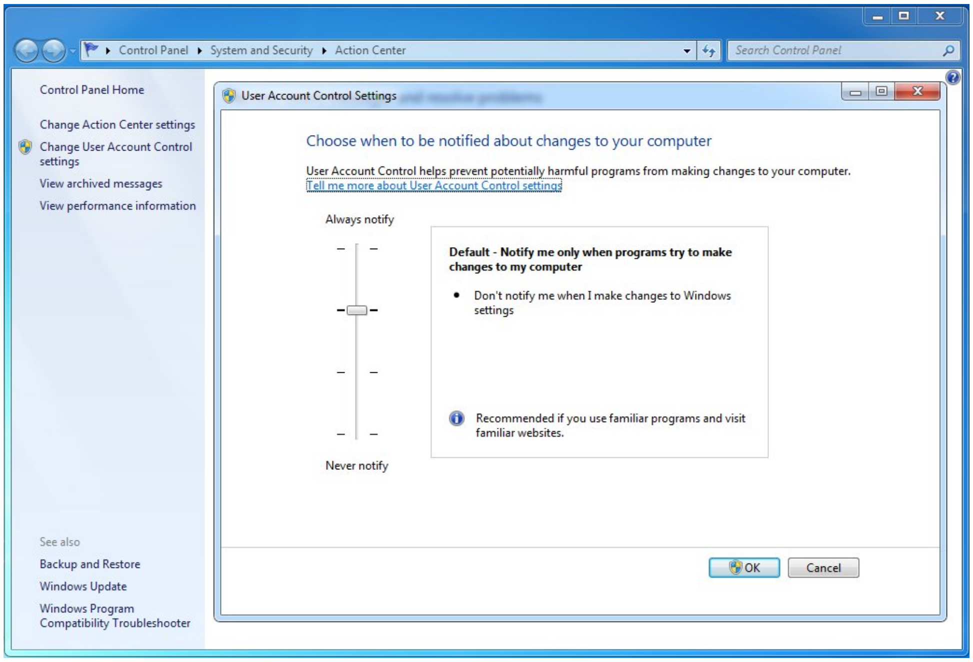
This setting only affects the built-in Administrator user. It has no effect on any other user accounts, regardless whether a user is members of Administrators group or not.

The default is “disabled”. This means that when a built-in Administrator user launches any application, the Admin Approval Mode is not required and the approval is automatically granted.

# 7. UAC settings – Alternative interface

There is an alternative interface with 4 different notification types that can be selected with a simple slider control. This interface is supported by Windows versions released after Windows Vista, including 2008 and 2012.

This interface can be accessed in the Control Panel > System and Security > Action Center > Change User Account Control settings (sample below). Setting the slider control to “Never notify” effectively disables UAC and requires a system reboot to take effect.


Control Panel ▸ System and Security ▸ Action Center
Search Control Panel
Control Panel Home
Change Action Center settings
Change User Account Control settings
View archived messages
View performance information
See also
Backup and Restore
Windows Update
Windows Program Compatibility Troubleshooter
User Account Control Settings
Always notify
Never notify
OK
Cancel

Choose when to be notified about changes to your computer

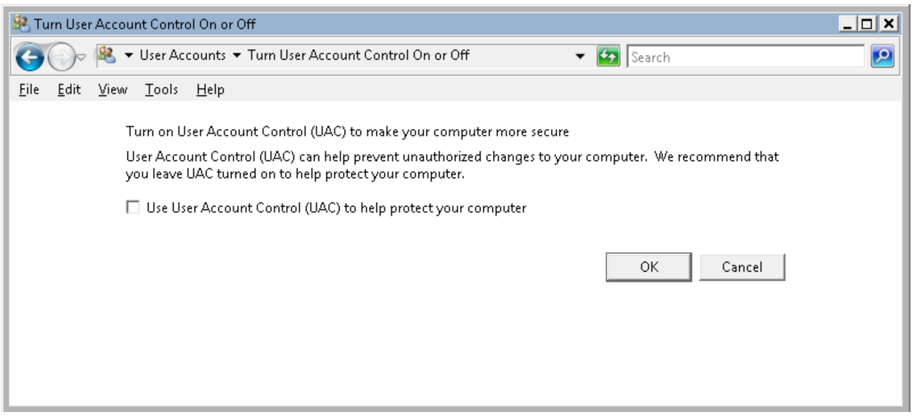
User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings

**Default - Notify me only when programs try to make changes to my computer**

- Don't notify me when I make changes to Windows settings

Recommended if you use familiar programs and visit familiar websites.

Starting with Windows 2016, you disable UAC by going to User Accounts > Turn User Account Control On or Off and clearing (unchecking) the option "Use User Account Control (UAC) to help protect your computer". Click OK to save your changes.


Turn User Account Control On or Off
User Accounts ▾ Turn User Account Control On or Off
Search
File Edit View Tools Help

Turn on User Account Control (UAC) to make your computer more secure

User Account Control (UAC) can help prevent unauthorized changes to your computer. We recommend that you leave UAC turned on to help protect your computer.

□ Use User Account Control (UAC) to help protect your computer

## 8. ADMIN$ share access

There are multiple reasons why Qualys scans require access to ADMIN$ share. This section discusses some of them.

### 8.1 Remote Registry service

Remote Registry service is disabled by default on Windows Vista and higher. Remote Registry service provides an API that supports remote access to the system registry. The API does not require access to ADMIN$ share and is accessed using RPC over SMB/TCP and access to the IPC$ share.

Qualys scans of Windows systems require access to the registry API which can be accomplished by one of the following methods:

- Enable Remote Registry service. This action may be in conflict with existing security policy set up on the customer Windows computers.
- Leave Remote Registry service disabled and enable Dissolvable Agent which provides alternative access the registry API. Installation and removal of Dissolvable Agent requires access to the ADMIN$ share.

### 8.2 Windows Firewall

Windows Firewall settings affect access to the ADMIN$ share and firewall rules take effect before UAC policy governing access to ADMIN$ is evaluated.

Access to Windows network shares requires a network transport (NetBIOS, SMB, etc.). One of the most commonly used transports of accessing Windows network shares is SMB over TCP. The SMB protocol is also known as CIFS.

Windows Firewall is enabled by default on Windows Vista and higher. Access to TCP port 445 is blocked by default.

A firewall rule is required to allow access to TCP port 445 from Qualys scanner IP addresses in order to access ADMIN$ share. This could be a new rule or a modification of an existing rule that is disabled by default.

## 9. Remote UAC

Access to ADMIN$ share is controlled by the Remote UAC part of the UAC policy. However, the Local Policy Editor does not define any settings that control Remote UAC. By default remote access to ADMIN$ share is disabled.

Enabling access to ADMIN$ share by modifying Remote UAC settings does not affect the Admin Approval Mode settings defined by the UAC policy. This allows UAC to remain in effect and function as designed for interactive users while enabling remote access to the ADMIN$ share. The setting that enables ADMIN$ share access needs to be defined in the system registry directly.

Note that enabling Remote UAC grants access not only to the ADMIN$ share but also makes it possible to manage a Windows system remotely from another Windows computer by selecting Computer Management > Action > Connect to another computer.

The proposed Remote UAC policy changes do not affect domain accounts which can access ADMIN$ by default. This means that Remote UAC policy only affects local user accounts that are members of the Administrators group.

### Use Cases

In these cases customers are required to make changes to the Remote UAC policy in order to run trusted scans and authenticate with a local user account which is a member of the Administrator's group.

1) Stand-alone Windows systems that don't have a domain membership (GPO won't work here because there's no domain to begin with. Changes to the registry need to be done with some other form of automation. A batch file, for example, that calls a REG command as described below.)

2) Domain-joined Windows systems which customers want to scan with the local account (GPO can be used to make changes to the registry.)

### What are the steps?

1) Launch Registry Editor (regedit.exe) in "Run as administrator" mode and grant Admin Approval, if requested

2) Navigate to HKEY_LOCAL_MACHINE hive

3) Open SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System key

4) Create a new DWORD (32-bit) value with the following properties:
Name: LocalAccountTokenFilterPolicy
Value: 1

5) Close Registry Editor

Warning: The value data types of DWORD (32-bit) and QWORD (64-bit) are located next to each other in the data type selection menu on 64-bit Windows versions. It may be easy to mistake one for another and select the incorrect data type. The required value data type must be DWORD (32-bit). Selecting QWORD (64-bit) and setting it to 1 will not enable Remote UAC.

The requirement to reboot system or restart Server service is questionable. Despite what some documents recommend, our tests have shown that disabling Remote UAC in the registry takes effect immediately and remote access to ADMIN$ is granted during the Qualys scan.

### An alternative method

To enable Remote UAC, you can also use a registry entry command (with elevated prompt) to remove the registry entry:

```
cmd /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system
/v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

### How to Disable Remote UAC

You can disable Remote UAC using the following methods.

1) Use registry edit command (with elevated prompt)

```
cmd /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system
/v LocalAccountTokenFilterPolicy /t REG_DWORD /d 0 /f
```

2) Use account control settings

Open Control Panel -> System and Security -> Change User Account Control settings. Or, run the following executable (use Start > Run or command prompt):

```
C:\Windows\System32\UserAccountControlSettings.exe
```

Then move the slider to Never Notify or clear (uncheck) the option "Use User Account Control (UAC) to help protect your computer", depending on your Windows version. Click OK and enter administrator password if prompted.

## 10. User access to ADMIN$ share

UAC controls access to ADMIN$ share and this permission depends on a user type. Windows systems can be accessed with domain or local credentials. This section describes what happens when different users access ADMIN$ share remotely.

### 10.1 Domain users

Domain users, who are members of the local Administrators group, are granted access to ADMIN$ share by default.

When a Qualys scan uses Windows domain credentials and the user is also a member of Administrators group, typically by inclusion of Domain Admins group or any other group, the ADMIN$ share can be accessed successfully without requiring any changes in the UAC policy.

## 10.2 Local users

UAC policy settings make a distinction between the following user types:

- built-in Administrator
- Administrators (members of Administrators group)
- standard local users

Permission to access ADMIN$ share by each of these users is controlled differently.

### 10.2.1 Built-in Administrator

The Built-in Administrator user can access ADMIN$ share by default. This is controlled by the UAC policy setting documented in section 6.2.
When Windows Vista or higher is installed on a new computer, the built-in Administrator account is disabled. During the installation a new user is created and automatically added to the Administrators group. This user can later add other users and elevate priorities of administrative tasks for system management by entering Admin Approval Mode.

Since the built-in Administrator user is disabled by default, the account needs to be enabled and its password set in order to use it. Qualys scans that use the built-in Administrator account can access the ADMIN$ share without requiring any changes to the **default** UAC policy.

### 10.2.2 Administrators (members of Administrators group)

Members of the Administrators group can access ADMIN$ share when Remote UAC is enabled (see section 8) or UAC policy is completely disabled.

Enabling Remote UAC while maintaining existing UAC policy is more secure than disabling UAC policy completely in order to access ADMIN$ share remotely.

### 10.2.3 Standard users

Standard users can access ADMIN$ share by default but the access is granted in a read-only mode which is not enough to install or remove Dissolvable Agent.

This permission does not depend on the UAC policy and is controlled by the NTFS permissions set up on the Windows installation directory that is shared as ADMIN$ when the Windows operating system is installed.