



# Description of User Account Control and remote restrictions in Windows Vista

09/08/2020 • 2 minutes to read •  

## In this article

Introduction

How UAC remote restrictions work

How to disable UAC remote restrictions

UAC remote settings

This article describes User Account Control (UAC) and remote restrictions.

*Original product version:* Windows Vista

*Original KB number:* 951016

## Introduction

User Account Control (UAC) is a new security component of Windows Vista. UAC enables users to perform common day-to-day tasks as non-administrators. These users are called *standard users* in Windows Vista. User accounts that are members of the local Administrators group will run most applications by using the principle of *least privilege*. In this scenario, least-privileged users have rights that resemble the rights of a standard user account. However, when a member of the local Administrators group has to perform a task that requires administrator rights, Windows Vista automatically prompts the user for approval.

## How UAC remote restrictions work

To better protect those users who are members of the local Administrators group, we implement UAC restrictions on the network. This mechanism helps prevent against *loopback* attacks. This mechanism also helps prevent local malicious software from running remotely with administrative rights.

## Local user accounts (Security Account Manager user account)

When a user who is a member of the local administrators group on the target remote computer establishes a remote administrative connection by using the net use `*\\remotecomputer\Share$` command, for example, they will not connect as a full administrator. The user has no elevation potential on the remote computer, and the user cannot perform administrative tasks. If the user wants to administer the workstation with a Security Account Manager (SAM) account, the user must interactively log on to the computer that is to be administered with Remote Assistance or Remote Desktop, if these services are available.

## Domain user accounts (Active Directory user account)

A user who has a domain user account logs on remotely to a Windows Vista computer. And, the domain user is a member of the Administrators group. In this case, the domain user will run with a full administrator access token on the remote computer, and UAC won't be in effect.

### ⓘ Note

This behavior is not different from the behavior in Windows XP.

## How to disable UAC remote restrictions

### ⓘ Important

This section, method, or task contains steps that tell you how to modify the registry. However, serious problems might occur if you modify the registry incorrectly. Therefore, make sure that you follow these steps carefully. For added protection, back up the registry before you modify it. Then, you can restore the registry if a problem occurs. For more information about how to back up and restore the registry, see [How to back up and restore the registry in Windows](#).

To disable UAC remote restrictions, follow these steps:

1. Click **Start**, click **Run**, type `regedit`, and then press ENTER.
2. Locate and then click the following registry subkey:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
```

3. If the **LocalAccountTokenFilterPolicy** registry entry doesn't exist, follow these steps:
  - a. On the **Edit** menu, point to **New**, and then click **DWORD Value**.
  - b. Type *LocalAccountTokenFilterPolicy*, and then press ENTER.
4. Right-click **LocalAccountTokenFilterPolicy**, and then click **Modify**.
5. In the **Value data** box, type *1*, and then click **OK**.
6. Exit Registry Editor.

## Did this fix the problem

Check whether the problem is fixed. If the problem is fixed, you are finished with this article. If the problem is not fixed, you can contact support.

## UAC remote settings

The **LocalAccountTokenFilterPolicy** registry entry in the registry can have a value of 0 or of 1. These values change the behavior of the registry entry to the behavior that is described in the following table.

Value	Description
0	This value builds a filtered token. This is the default value. The administrator credentials are removed.
1	This value builds an elevated token.

Is this page helpful?

 Yes  No