Some Programs Cannot Access Network Locations When UAC Is Enabled

Symptom

After you turn on User Account Control (UAC) in Windows Vista or Windows 7, programs may not be able to access some network locations. This problem may also occur when you use the command prompt to access a network location.

Cause

This problem occurs because UAC treats members of the Administrators group as standard users. Therefore, network shares that are mapped by logon scripts are shared with the standard user access token instead of with the full administrator access token.

When a member of the Administrators group logs on to a computer running Windows Vista or Windows 7 that has UAC enabled, the user runs as a standard user. Standard users are members of the Users group. If you are a member of the Administrators group and you want to perform a task that requires a full administrator access token, UAC prompts you for approval. For example, if you try to edit security policies on the computer, you are prompted. If you approve the action in the **User Account Control** dialog box, you can then complete the administrative task by using the full administrator access token.

When an administrator logs on to a computer running Windows Vista or Windows 7, the Local Security Authority (LSA) creates two access tokens. If LSA is notified that the user is a member of the Administrators group, LSA creates the second logon that has the administrator rights removed (filtered). This filtered access token is used to start the user's desktop. Applications can use the full administrator access token if the administrator user provides approval in a **User Account Control** dialog box.

If a user is logged on to a computer running Windows Vista or Windows 7 and if UAC is enabled, a program that uses the user's filtered access token and a program that uses the user's full administrator access token can run at the same time. Because LSA created the access tokens during two separate logon sessions, the access tokens contain separate logon IDs.

When network shares are mapped, they are linked to the current logon session for the current process access token. This means that if a user uses the command prompt (cmd.exe) together with the filtered access token to map a network share, the network share is not mapped for processes that run with the full administrator access token.

Resolution

To configure the EnableLinkedConnections registry value
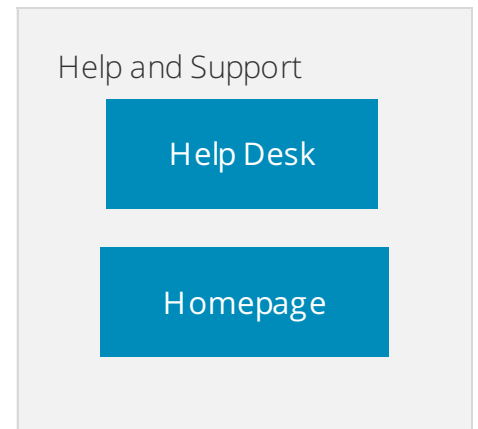
1. Click **Start**, type **regedit** in the **Start programs and files** box, and then press ENTER.
2. Locate and then right-click the registry subkey **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**.
3. Point to **New**, and then click **DWORD Value**.
4. Type **EnableLinkedConnections**, and then press ENTER.
5. Right-click **EnableLinkedConnections**, and then click **Modify**.
6. In the **Value data** box, type **1**, and then click **OK**.
7. Exit Registry Editor, and then restart the computer.