

[Home](#) / [Windows OS Hub](#) / [Windows 10](#) / Mapped Network Drive Not Showing in the Elevated Apps

July 19, 2018 | [Windows 10](#) [Windows 8](#)

Mapped Network Drive Not Showing in the Elevated Apps

One of the significant security improvements of Windows OSs (since Vista) is **User Account Control (UAC)** feature. User Account Control prompts the user for approval each time when the app tries to make any changes to the system. One of the side effects of UAC is the inability to access the mapped network drives (over `net use`) from the applications running in elevated (privileged) mode (Run As Administrator). This means that when you run the command prompt or a file manager (like Total Commander) with elevated privileges, they won't display the drive letters of the mounted shared folder.

In this article we'll show how to allow access to mapped network drives from the apps running in the elevated mode in Windows 10, Windows 8 and Windows 7. This problem occurs both for shared folders that are connected through Group Policy and for the folders connected by users.

Important. It is strongly not recommended to completely disable UAC, even for a [specific program](#).

Indeed, when UAC is enabled you cannot access a mapped network drive connected in the normal mode from an elevated app. Let's see what the problem looks like. For example, let's make sure you can access the contents of the connected network drive Z:\ in the command prompt run without privileges.

If you oper

```

C:\Users\root>net use
New connections will be remembered.

Status          Local        Remote              Network
-----
OK              Z:          \\.\.\.\.\shared   Microsoft Windows Network
                \\TSCLIENT\C Microsoft Terminal Services
                \\TSCLIENT\D Microsoft Terminal Services
                \\TSCLIENT\E Microsoft Terminal Services
OK              \\.\.\.\IPC$     Microsoft Windows Network
The command completed successfully.

C:\Users\root>dir z:
Volume in drive Z is shared
Volume Serial Number is AE6D-F66B

Directory of Z:\
08/26/2014  07:14 AM    <DIR>          .
08/26/2014  07:14 AM    <DIR>          ..
03/06/2008  12:08 PM    <DIR>          appl
03/02/2015  11:02 AM    <DIR>          db
03/07/2008  08:17 AM    <JUNCTION>    drivers [\\?\g:\<  ll\drivers]

```

the command prompt as administrator under this user, and try to access the same drive – you'll receive the message that the path to the drive has not been found:

The system cannot find the path specified.

```

Administrator: Command Prompt

Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Windows\system32>dir z:
The system cannot find the path specified.

C:\Windows\system32>_

```

This behavior of the system can cause some inconveniences when running applications frequently in elevated mode.

Why does it happen? This peculiarity is related to UAC mechanism for a user with the local administrator privileges. The matter is that when this user log in, two access tokens are created: the first token provides access with disabled administrator privileges (the filtered access token, with which most of the apps are running) and the second is the administrator token with full privileges in the system (all apps approved elevated in UAC are running in this context).

You can use whoami /all command in two cmd.exe sessions (normal and elevated) of the same user and compare the current privileges, you can see that they are very different. The following table lists the differences in the security groups and current privileges in each session.

	Normal user session	Elevated user session
Security group	Mandatory Label\Medium Mandatory Level S-1-16-8192	Mandatory Label\High Mandatory Level S-1-16-12288
Privileges	<ul style="list-style-type: none"> SeLockMemoryPrivilege SeMachineAccountPrivilege SeShutdownPrivilege SeChangeNotifyPrivilege SeUndockPrivilege SeIncreaseWorkingSetPrivilege SeTimeZonePrivilege 	<ul style="list-style-type: none"> SeLockMemoryPrivilege SeIncreaseQuotaPrivilege SeMachineAccountPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeSystemProfilePrivilege SeSystemtimePrivilege SeProfileSingleProcessPrivilege SeIncreaseBasePriorityPrivilege SeCreatePagefilePrivilege SeBackupPrivilege SeRestorePrivilege SeShutdownPrivilege SeSystemEnvironmentPrivilege SeChangeNotifyPrivilege SeRemoteShutdownPrivilege

SeUndockPrivilege

SeManageVolumePrivilege

SeImpersonatePrivilege

SeCreateGlobalPrivilege

SeIncreaseWorkingSetPrivilege

SeTimeZonePrivilege

SeCreateSymbolicLinkPrivilege

SeDelegateSessionUserImpersonatePrivilege

The image shows two overlapping Command Prompt windows. The background window displays a list of system groups with their SIDs and states. The foreground window displays a list of system privileges with their names, descriptions, and states.

Background Window: Group Information

Group Name	SID	State
NT AUTHORITY\INTERACTIVE	S-1-5-4	Mandatory group, Enabled by default
NT AUTHORITY\Authenticated Users	S-1-5-11	Mandatory group, Enabled by default
NT AUTHORITY\This Organization	S-1-5-15	Mandatory group, Enabled by default
NT AUTHORITY\Local account	S-1-5-113	Mandatory group, Enabled by default
LOCAL	S-1-2-0	Mandatory group, Enabled by default
NT AUTHORITY\NTLM Authentication	S-1-5-64-10	Mandatory group, Enabled by default
Mandatory Label\Medium Mandatory Level	S-1-16-8192	Label

Foreground Window: Privileges Information

Privilege Name	Description	State
SeShutdownPrivilege	Shut down the system	Disabled
SeChangeNotifyPrivilege	Bypass traverse checking	Enabled
SeUndockPrivilege	Remove computer from docking station	Disabled
SeIncreaseWorkingSetPrivilege	Increase scheduling priority	Disabled
SeTimeZonePrivilege	Change the system time	Disabled
SeIncreaseQuotaPrivilege	Adjust memory quotas for a process	Disabled
SeSecurityPrivilege	Manage auditing and security log	Disabled
SeTakeOwnershipPrivilege	Take ownership of files or other objects	Disabled
SeLoadDriverPrivilege	Load and unload device drivers	Disabled
SeSystemProfilePrivilege	Profile system performance	Disabled
SeSystemtimePrivilege	Change the system time	Disabled
SeProfileSingleProcessPrivilege	Profile single process	Disabled
SeIncreaseBasePriorityPrivilege	Increase scheduling priority	Disabled
SeCreatePagefilePrivilege	Create a pagefile	Disabled
SeBackupPrivilege	Back up files and directories	Disabled
SeRestorePrivilege	Restore files and directories	Disabled
SeShutdownPrivilege	Shut down the system	Disabled
SeDebugPrivilege	Debug programs	Disabled
SeSystemEnvironmentPrivilege	Modify firmware environment values	Disabled
SeChangeNotifyPrivilege	Bypass traverse checking	Enabled
SeRemoteShutdownPrivilege	Force shutdown from a remote system	Disabled
SeUndockPrivilege	Remove computer from docking station	Disabled
SeManageVolumePrivilege	Perform volume maintenance tasks	Disabled

Applications under the same user may be run in two contexts when UAC enabled (privileged and unprivileged). When you connect shared network folders, the system creates symbolic links (DosDevices) that store the drive letter mapping to the UNC paths. These links are associated with the current process access token and are not available with another token.

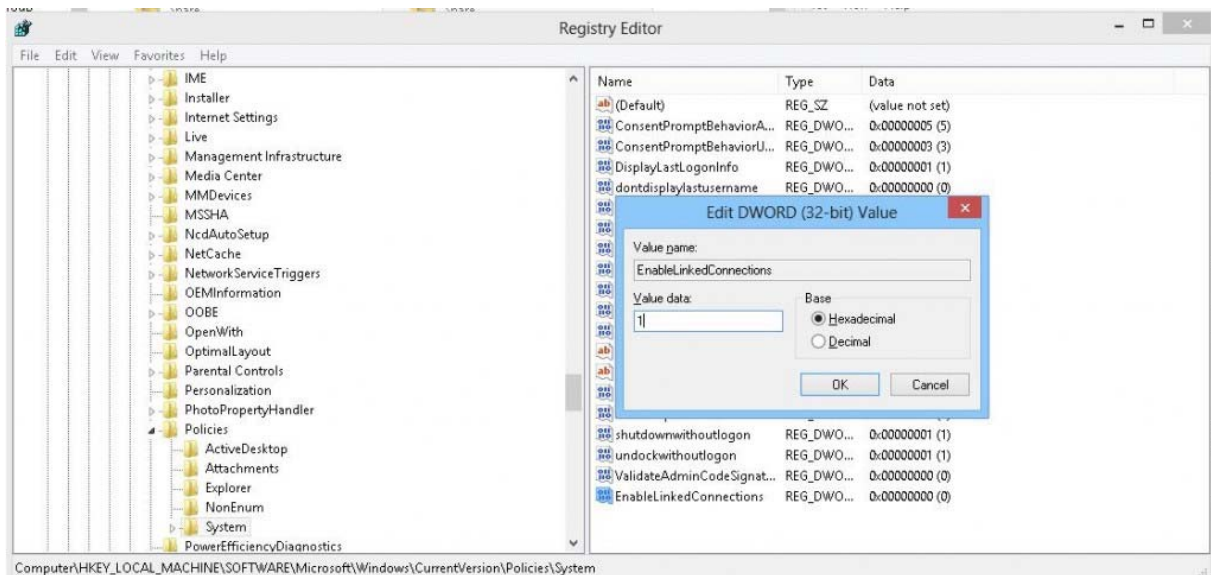
The reverse problem may also occur: when the user with administrator permissions on the computer is connecting network drives using the group policy logon scripts, schedule the tasks or SCCM jobs (which are running with elevated privileges), these drives are not visible to the user in File Explorer (unprivileged process).

Tip. In Windows Server you can [run File Explorer as administrator \(elevated privileges\)](#).

As a workaround, you can mount network drives from the elevated command prompt using the commands: `net use` or `rundll32 SHELL32.dll,SHHelpShortcuts_RunDLL Connect`.

There is an easier solution. To implement it, you have to make some changes to the registry:

- Open the registry editor (**regedit.exe**);
- Go to the registry key **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**;
- Create a new parameter (DWORD type) with the name **EnableLinkedConnections** and the value **1**;



Tip. The same change can be done with a single command: `reg add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v "EnableLinkedConnections" /t REG_DWORD /d 0x00000001 /f`

- Restart your computer (or restart the LanmanWorkstation service).

After the computer has been restarted, make sure that the user sees mapped network drives in the programs that are running with admin rights. The reverse statement is true: all network drives mapped in the elevated mode will also be available in the unprivileged session.



```
C:\Windows\system32>dir z:
Volume in drive Z is shared
Volume Serial Number is AE6D-F66B

Directory of Z:\

08/26/2014  07:14 AM    <DIR>          .
08/26/2014  07:14 AM    <DIR>          ..
03/06/2008  12:08 PM    <DIR>          appl
03/02/2015  11:02 AM    <DIR>          db
03/07/2008  08:17 AM    <JUNCTION>     drivers [\\??\g:\s  ll\drivers]
06/20/2014  04:26 PM    <DIR>          PUSL...
```

Note. Unfortunately, it is not possible to enable the `EnableLinkedConnections` parameter using the GPO. To deploy this setting on the domain computers, you need [to distribute registry parameter to the computers using GPP](#).

How it works? After you enabled `EnableLinkedConnections` parameter of the registry, LanmanWorkstation and LSA will check if there is the second access token associated to the session of the current user. If this token is found, the list of the mounted network drives will be copied from one token to another. Thus, the network drives mounted in the elevated mode will be visible in the normal mode, and vice versa.

Tip. As an alternative solution, you can create a symbolic link to the target shared folder. For example, as follows:

```
mklink /D c:\docs \\dublin-fs1\docs
```

The access to this drive is possible both in the standard and in the elevated mode. It should be noted that one of the drawbacks of this method is that you access the shared folder as a current user. It is impossible to use the account of another user as in the case of net use.

1 comment

0

f t G+ p

[previous post](#)
[RDP Scaling Issue on High-DPI Displays in Windows 10](#)

[next post](#)
[Windows Defender Threat Service has stopped. Restart](#)

RELATED READING

[it now](#)

[Resetting Windows Update Agent Settings](#)

May 31, 2019

[Fix: "Signature" Button Not Working in Outlook 2013/2016](#)

May 15, 2019

[How to Automatically Turn Off Wi-Fi When an...](#)

May 14, 2019



1 COMMENT



VANDREY TRINDADE

Rep

🕒 July 19, 2018 - 6:23 pm

Great! Well explained!

I remember having a hard work to understand why my mapped drives were not appearing in the elevated prompts... Until I found a technet post that saved my life lol

LEAVE A COMMENT

Your Comment

Name*

Email*

Website