

[Home](#) [Library](#) [Wiki](#) [Learn](#) [Gallery](#) [Downloads](#) [Support](#) [Forums](#) [Blogs](#)[Ask a question](#)[Search related threads](#)

Quick access

Answered by:

KB3161949 June 2016 Update Causes Network File Shares to Become Unavailable

[Windows 7 IT Pro](#) > [Windows 7 Networking](#)

Question

After installing KB3161949 on Windows 7 and 8.1 Professional, mapped network file shares become unavailable (red x). This seems to be an issue when the systems reside on separate networks (like Public/Private) Shares are only accessible via IP or FQDN. Uninstalling the update restores access. Microsoft needs to pull this update!

2

[Sign in to vote](#)Edited by [NightRyder1](#) Wednesday, June 15, 2016 10:19 PM

Wednesday, June 15, 2016 9:56 PM

[Reply](#) | [Quote](#)

Answers

We to had this issue but after following the information in <https://support.microsoft.com/en-us/kb/3161949> and applying the correct registry change the issue was resolved.

7
[Sign in](#)
[to vote](#)

After you install this security update, the following changes are applied:

- NETBIOS communication outside of the local subnet is hardened. Therefore, by default, some features that depend on NETBIOS (such as SMB over NETBIOS) will not work outside the local subnet. To change this new default behavior, create the following registry entry:
SUBKEY:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters
Value Name: AllowNBToInternet
Type: Dword
Value: 1
Default value of the flag: 0

Edited by [RLC1234](#) Thursday, June 16, 2016 8:28 PM

Proposed as answer by [G McCune](#) Thursday, June 16, 2016 9:11 PM

Marked as answer by [Teemo Tang](#) Microsoft contingent staff, Moderator
Friday, July 1, 2016 9:00 AM

Thursday, June 16, 2016 8:27 PM

[Reply](#) | [Quote](#)

All replies

Hi,

0
Sign in
to vote

Based on your description, I want to confirm that have you made any changes before the issue occurred? Have you got any error messages?

I noticed the KB, since the KB is related to WPAD, it will not affect your network file shares.

<https://support.microsoft.com/en-sg/kb/3161949>

I suggest that you could try to uninstall the KB and download it from official website then reinstall it and check the result.

Security Update for Windows 7 for x64-based Systems (KB3161949)

https://www.microsoft.com/en-us/download/details.aspx?id=52912&WT.mc_id=rss_windows_7

We could also try to check if it's related to incompatible issue with updated system files.

In addition, rebuild network file share may be a good idea, please try it.

Best Regards,

Tao

Please **mark the reply as an answer** if you find it is helpful. 😊

If you have feedback for TechNet Support, contact tnmff@microsoft.com

Thursday, June 16, 2016 11:32 AM

Moderator

[Reply](#) | [Quote](#)

Hi,

0
Sign in
to vote

Thanks for the response. I spent most of yesterday running down this issue and there is no doubt that KB3161949 is the cause. I've confirmed it across multiple systems, Win7 Pro, Win 8.1 Pro, Server 2008R2, Enterprise and Standard. Install KB3161949 and the problem appears, uninstall it and the problem goes away. Ran into the same type of thing on our print server with shared printers. KB3161949 was downloaded directly through Windows update on each machine. No changes to systems or our network have been made other than installing this month's updates.

I noticed that this update hardened NETBIOS, our servers with the file shares are all fixed IP on our public network and our workstations are all DHCP on the private side. The network settings all allow the use of NETBIOS over TCP/IP if necessary. Currently our Domain level is 2003, we are in the process of updating this. Obviously I can't allow any of our workstations to apply this update until the issue is resolved. Thanks for your assistance.

Edited by [NightRyder1](#) Thursday, June 16, 2016 3:27 PM

Thursday, June 16, 2016 2:32 PM

[Reply](#) | [Quote](#)

We also have the same issue and had to remove KB3161949 from our servers and computers that had access to servers on another network. This issue did affect server 2012 as well as Windows 7.

0
Sign in
to vote

Thursday, June 16, 2016 3:16 PM

[Reply](#) | [Quote](#)

We had this issue but after following the information in <https://support.microsoft.com/en-us/kb/3161949> and applying the correct registry change the issue was resolved.

7
Sign in
to vote

After you install this security update, the following changes are applied:

- NETBIOS communication outside of the local subnet is hardened. Therefore, by default, some features that depend on NETBIOS (such as SMB over NETBIOS) will not work outside the local subnet. To change this new default behavior, create the following registry entry:
SUBKEY:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters
Value Name: AllowNBToInternet
Type: Dword
Value: 1
Default value of the flag: 0

Edited by [RLC1234](#) Thursday, June 16, 2016 8:28 PM

Proposed as answer by [G McCune](#) Thursday, June 16, 2016 9:11 PM

Marked as answer by [Teemo Tang](#) Microsoft contingent staff, Moderator
Friday, July 1, 2016 9:00 AM

Thursday, June 16, 2016 8:27 PM

[Reply](#) | [Quote](#)

We just went through this yesterday and the registry edit fixed it as well, but only on Win 7 and not on Win 10. I'm researching the Win 10 fix now.

Here's the text you need to have in your .reg file, if it helps anyone.

0

[Sign in](#)
[to vote](#)

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\NetBT\Parameters]

"AllowNBToInternet"=dword:00000001

Thursday, June 16, 2016 9:13 PM

[Reply](#) | [Quote](#)

This is expected behavior with KB3161949 due to NETBIOS hardening. The following KB article explains the behavior changes.

<https://support.microsoft.com/en-us/kb/3161949>. Adding the following registry key will restore the previous behavior.

1

[Sign in](#)
[to vote](#)

SUBKEY: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters

Value Name: AllowNBToInternet

Type: Dword

Value: 1

Proposed as answer by [Mary Branscombe](#) Friday, June 17, 2016 5:05 PM

Thursday, June 16, 2016 11:41 PM

[Reply](#) | [Quote](#)

Does this require a reboot after changing the registry key?

Friday, June 17, 2016 5:14 PM

0

[Sign in](#)
[to vote](#)[Reply](#) | [Quote](#)

Yes, a reboot is required.

Friday, June 17, 2016 5:20 PM

0

[Sign in](#)
[to vote](#)[Reply](#) | [Quote](#)

Yes, tried starting TCP/IP NetBIOS Helper service and no luck. Full reboot allowed for register fix to kick in

0

[Sign in](#)
[to vote](#)

Monday, June 20, 2016 5:11 PM

[Reply](#) | [Quote](#)

Based on your description, Microsoft intentionally hosed all shares on domains where more than one subnet is used. This seems like a very, very poorly thought out patch.

1
[Sign in to vote](#)

Our network has departments separated into individual class C subnets. If I understand your description, shares between computers or printers which cross subnets will no longer work. Computers in most of our departments need to be able to send print jobs through an Oracle server. Currently, we find we have to uninstall this patch for this to function.

I understand the instructions for reverting this behavior. However, I don't like having to partially undo a security update. What is the best practice in this case for having security up to date while still being able to print to non Microsoft print shares on a different subnet?

Wednesday, June 22, 2016 8:51 PM

[Reply](#) | [Quote](#)

For those who do not want to edit the registry for all workstations:

I noticed that the file shares only stopped to work to servers using only Netbios over TCP/IP, if using IP or short name (`\\server\share`). Using FQDN (`\\server.domain.com\share`) worked fine.

1
[Sign in to vote](#)

Shares on Windows server using Direct hosting work normally, with IP, shortname or FQDN.

<https://support.microsoft.com/fi-fi/kb/204279>

The problem was that our old firewall rules were built to allow only those NBT ports and not direct hosting (tcp 445), so the solution was to open TCP 445 to the file server or to use UPN for mapping

Proposed as answer by [MichaelJMcNally](#) Thursday, June 23, 2016 3:17 PM

Thursday, June 23, 2016 8:42 AM

[Reply](#) | [Quote](#)

Thanks Mikko, that is great information. Does this mean that the simplest fix is to disable Netbios over TCP/IP on the server hosting the share? Or does this need to be done on both ends?

0
[Sign in to vote](#)

Thursday, June 23, 2016 3:16 PM

[Reply](#) | [Quote](#)

The link states "If both the direct hosted and NBT interfaces are enabled, both methods are tried at the same time and the first to respond is used".

1

[Sign in](#)
[to vote](#)

So disabling Netbios over TCP/IP should not be necessary (at least we did not have to do it). As long as SMB can traverse over TCP, everything should be fine. Security-wise however, disabling Netbios over TCP/IP might be recommended, unless there are some legacy applications / hosts depending on it.

So if you are having problems with "modern" Windows hosted file shares and Windows clients after applying this update, make sure that clients can access the server on TCP / UDP 445.

If you are having problems with non Windows / legacy clients (like Network scanners) accessing file shares, you need to either add the registry modification described earlier to the hosting server:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\NetBT\Parameters]
"AllowNBToInternet"=dword:00000001
```

Or you can try to map the shared folder to the device using FQDN ([\\server.domain.com\share](#)), assuming the device is DNS capable (FQDN seemed to work on Windows client, but have not actually tested this on anything else)

Edited by [Mikko Haapasaari](#) Saturday, June 25, 2016 7:49 AM

Thursday, June 23, 2016 5:02 PM

[Reply](#) | [Quote](#)

Anyone find a solution for this with Server 2012 R2?

The registry key doesn't seem to help and I've even gone as far as uninstalling the update and my scanner on another network still can't send to the folder it could a week ago. GAH!

0

[Sign in](#)
[to vote](#)

Friday, June 24, 2016 1:13 AM

[Reply](#) | [Quote](#)

I applied the registry key to our 2012R2 servers and they are now able to connect to the shares that they could not connect to before the key was applied.

0

[Sign in](#)
[to vote](#)

Friday, June 24, 2016 2:54 AM

[Reply](#) | [Quote](#)

We had this issue with Xerox scanners suddenly not liking logons without the DomainName\username format being used instead of username alone. The registry key fixed it for us as well after applying it to domain controllers that the printers were using for ldap.

0

[Sign in](#)
[to vote](#)

Friday, June 24, 2016 4:34 AM

[Reply](#) | [Quote](#)

Hi,

Sorry to hijack the post. I was wondering if you had to apply this to both the servers and the clients?

0

[Sign in to vote](#)

Many thanks

Friday, June 24, 2016 2:11 PM

[Reply](#) | [Quote](#)

This ended up being the resolution in our case as well. Canon iR3225 – sending the scans to a DFS folder on a 2012 R2 Server. Had to update the DCs (2008 R2) with the registry key before this would work.

0

[Sign in to vote](#)

Friday, June 24, 2016 2:15 PM

[Reply](#) | [Quote](#)

Thank you! I had a Kyocera scanning to my 2012 R2 server via SMB from a remote subnet and the registry change done on the server fixed it after a reboot.

0

[Sign in to vote](#)

Friday, June 24, 2016 3:27 PM

[Reply](#) | [Quote](#)

Hey MT_itsupport,

It worked for me just applying it to the server and rebooting.

0

[Sign in to vote](#)

Friday, June 24, 2016 3:28 PM

[Reply](#) | [Quote](#)

Our organization also experienced application failures on systems that were using URLs with a NETBIOS shortname (not a FQDN URL) to access CIFS shares. In particular, shares that are hosted on a Unix server unable to access the share. After uninstalling KB3161949 on domain controllers this fixed the issue. I am continuing to investigate, it appears some systems received the update but only the domain controllers caused an outage. We have Active Directory domain DFS namespace, perhaps that is the exposure felt?

0

[Sign in to vote](#)

George Perkins

Tuesday, June 28, 2016 4:48 PM

[Reply](#) | [Quote](#)

It appears to have partially worked for me. The only problem I have now are the drive mappings with item level targeting. I cant get those to map!!!

0

[Sign in to vote](#)

Wednesday, June 29, 2016 9:38 AM

[Reply](#) | [Quote](#)

I'm using DFS also and it's completely screwed everything up. I've even applied the Registry fix above and rebooted all servers but it's even worse. Although have you read some of the fixes with this rollout update? <https://support.microsoft.com/en-gb/kb/3161606>

0

[Sign in to vote](#)

Friday, July 1, 2016 9:17 AM

[Reply](#) | [Quote](#)

Any update on your issue.

We have DFS name spaces hosted on our servers and want to follow your progress here.

However we didnt have any issue we have 50% of our DC with the patch.

0

[Sign in to vote](#)

Thank you Vijay

Tuesday, July 5, 2016 3:09 PM

[Reply](#) | [Quote](#)

To clarify, we uninstalled KB3161949 and removed this update from the approved list of security updates in WSUS and SCCM. This 'resolved' our issues. At this time our organization cannot take this update because it will break production systems.

0

[Sign in to vote](#)

(With no publicity and little notice, Microsoft has removed backward-compatibility via a security update and this approach is not acceptable. To allow our organization to apply KB3161949 it will be a large project to identify all of the dependencies and remove them, something that should be done certainly, but not easy to do.)

George Perkins

Wednesday, July 6, 2016 1:43 PM

[Reply](#) | [Quote](#)

I have some Computer same issue. KB3161949 update deleted but doesn't help me. Only one thing helps, this is Clean install computer. Know anyone how i can to do completely reset network settings without clean install?

0

[Sign in to vote](#)

Wednesday, August 31, 2016 8:05 AM

[Reply](#) | [Quote](#)

What is it remote subnet and local subnet!

This problem for my is (scan/printer) from local subnet 10.94.1.0/24 and not problem from 10.1.54.0/24.

0

[Sign in](#)
[to vote](#)

After MS 10.94.1.0 subnets is remote?!

What kind of mushrooms used in MS!

cenubit

Friday, October 7, 2016 12:39 PM

[Reply](#) | [Quote](#)

I just recently ran into this problem. What I found out was very interesting and thought you might appreciate it as well.

0
[Sign in
to vote](#)

This applies to all Windows OSes 2000/XP and newer.

Per: <https://support.microsoft.com/en-us/help/204279/direct-hosting-of-smb-over-tcp-ip>

If your network adapter is set to allow NetBIOS over TCP (NBT), Windows uses either NetBIOS over TCP (NBT) or Direct hosting (SMB on TCP) to connect to SMB shares. NetBIOS over TCP uses ports 137-139 and Direct hosting uses port 445. So if you establish a connection to a share you can run `netstat -an` (run this quickly after opening the share) from the connecting PC and locate the IP of the hosted share and see if port 445 or 137-139 are in use. This will tell you what connection protocol is established.

Post Patch KB3161949

If your PC lost share connectivity via short name (`\\servername\share`) you have one of two issues.

1.) A DNS suffix for your PC is not specified so the domain is not being appended to your shortname search. Open System Properties, click the Computer Name tab, click the Change... button. This will open the Computer Name/Domain Changes window. Click the More... button and verify if the proper domain name is in the Primary suffix of this computer field. Now when you type "`\\servername`" the DNS suffix is appended and the connection is able to be established via the short name. If you need to work with multiple domain names you will need to add the list of domains to the "Append these DNS suffixes (in order)" section of DNS tab under TCP/IP Settings for the network adapter that you are using. Any unqualified short name will have each domain name in the list, in order from top to bottom, appended until it resolves in DNS or fails.

2.) Since patch KB3161949 has hardened NetBIOS over TCP it will only work for short names via the local subnet. If you specify the FQDN (`\\servername.domain.com\share`) it allows NetBIOS to look beyond your local subnet. So, if the proper domain name is in the Primary Suffix of the PC and specifying the FQDN works then you have something (firewall, antivirus, etc.) blocking port 445 between the PC and the share on another subnet. You can verify this by running `netstat -an` from a command prompt (do it quickly after establishing the share connection). You will see a connection from your machine to the IP of the share host with port "139 ESTABLISHED" and close to that you will see, (if you acted quickly enough) the same host IP with port 445 and a State of SYN_SENT. SYN_SENT indicates that your client has performed the first step of the three-way TCP handshake. Since something (firewall, antivirus, etc.) is blocking port 445 traffic this allows NetBIOS over TCP to win and the connection is established over port 139.

If you can clear what's blocking port 445, then using the short name (`\\servername\share`) will establish via Direct hosting (SMB on TCP). However, if the far end share is an older NAS, MFP, copier, etc that can only use SMB via NetBIOS over TCP (NBT) then you will have to use either the FQDN, the registry key, or remove the patch.

Friday, January 27, 2017 10:07 PM

[Reply](#) | [Quote](#)

As with some Win OS services, they get disabled with Win updater..To resolve the problem(s), in run or cmd, type:

0

[Sign in](#)
[to vote](#)

services.msc in msc, locate the service, double click, reset its run properties, set to auto run, or manual, exit

when thru. This being that the Win software is enabled in Win components, + chk your firewall/exceptions, &

edit internet options, set all to "default"...

Saturday, January 28, 2017 12:59 AM

[Reply](#) | [Quote](#)