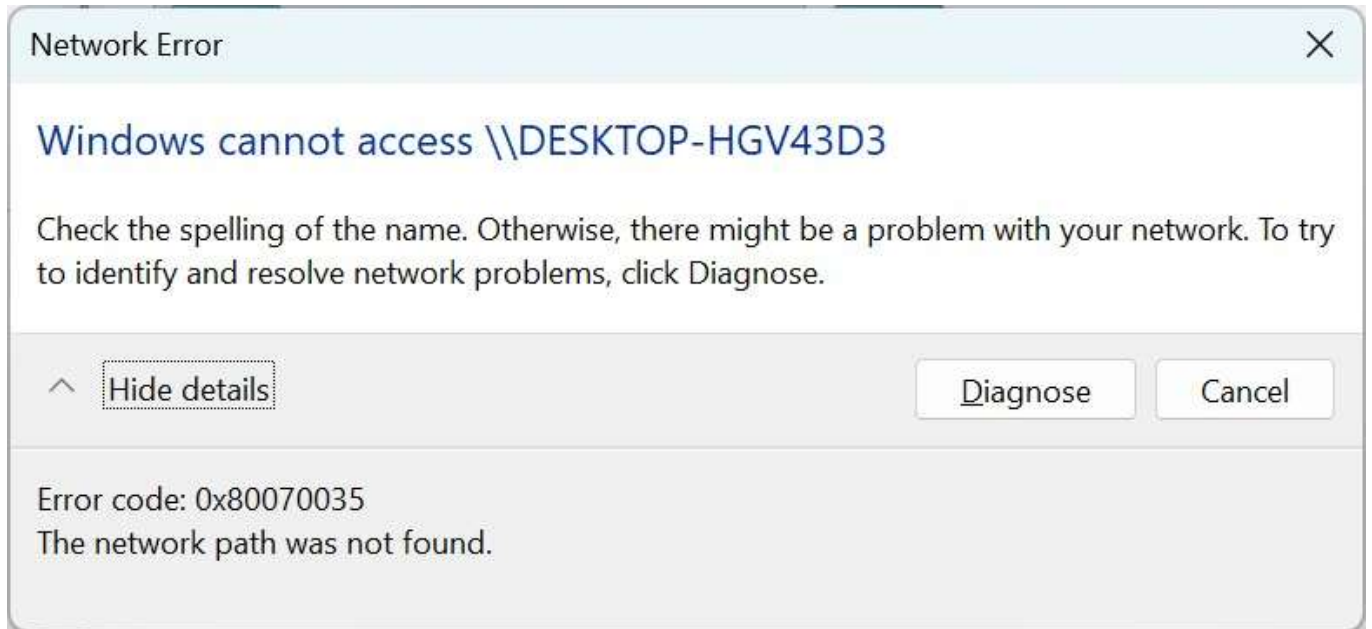


Error code 0x80070035 | Windows cannot access | The Network path was not found

Error code 0x80070035 ("The network path was not found") occurs when your Windows PC cannot locate or connect to a shared computer, server, or NAS drive on your local network. It is typically caused by incorrect network sharing profiles, disabled network discovery, or strict security and SMB configuration settings.



Follow this structured troubleshooting guide to resolve the error. Start with the easiest network settings first.

Step 1: Verify Network Profile is Set to Private

Windows blocks network sharing by default on Public networks to protect your security.

Click the Network/Wi-Fi icon in your taskbar and open Network & Internet settings.

Click on Wi-Fi or Ethernet (depending on your active connection).

Change the network profile type from Public to Private.

Step 2: Enable Network Discovery and File Sharing

Open the Control Panel and navigate to Network and Sharing Center.

Click Change advanced sharing settings on the left menu.

Under the Private dropdown, turn ON both Network discovery and File and printer sharing.

Expand the All Networks section at the bottom, and turn OFF Password-protected sharing (if you want to bypass credential errors temporarily). Click Save changes.

Step 3: Enable Insecure Guest Logins (For Windows 11/10 Pro & Home)

Recent Windows security updates block insecure guest logons to network devices like NAS drives by default.

For Windows Pro / Enterprise editions:

Press Windows Key + R, type gpedit.msc, and press Enter to open the Group Policy Editor.

Navigate to: Computer Configuration > Administrative Templates > Network > Lanman Workstation.

Double-click Enable insecure guest logons and set it to Enabled. Click Apply and OK.

For Windows Home editions (via PowerShell):

Right-click the Start menu and choose Terminal (Admin) or PowerShell (Admin).

Copy, paste, and run the following command to allow guest logins:

```
powershell
```

```
Set-SmbClientConfiguration -EnableInsecureGuestLogons $true -Force
```

Use code with caution.

Run this command next to remove the digital signing block:

```
powershell
```

```
Set-SmbClientConfiguration -RequireSecuritySignature $false -Force
```

Use code with caution.

Step 4: Access Using the IP Address Instead of Name

Sometimes Windows fails to resolve the computer name (NetBIOS) over the local network.

Press Windows Key + R to open the Run box.

Type two backslashes followed by the target device's IP address (e.g., \\192.168.1.50) and press Enter.

If this successfully opens the share, the problem is a local DNS or NetBIOS name resolution failure rather than a connectivity issue.

Step 5: Enable NetBIOS Over TCP/IP

If accessing via the IP address worked in Step 4, explicitly force Windows to resolve names using NetBIOS:

Press Windows Key + R, type `ncpa.cpl`, and hit Enter to view network adapters.

Right-click your active connection (Wi-Fi or Ethernet) and select Properties.

Double-click Internet Protocol Version 4 (TCP/IPv4).

Click the Advanced button at the bottom, then click the WINS tab.

Select Enable NetBIOS over TCP/IP, then click OK on all windows.

Step 6: Enable SMB 1.0 Support (For Older Network Storage/PC Links)

If you are trying to connect to an older NAS enclosure, Linux server, or legacy Windows machine, they may rely on the legacy SMBv1 protocol, which modern Windows disables by default.

Open the search bar, type `optionalfeatures`, and press Enter to open Turn Windows features on or off.

Scroll down to locate SMB 1.0/CIFS File Sharing Support.

Check the box next to SMB 1.0/CIFS Client.

Click OK and let Windows install the package. Restart your computer when prompted.

Method 2: Disable Microsoft Network Client Digitally Signed Communications

This adjustment fixes a strict security requirement in the Local Group Policy Editor.

Press the Windows Key, type `group policy`, and select Edit group policy to open the interface.

Navigate to: Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options.

Scroll down to locate Microsoft network client: Digitally sign communications (always).

Double-click it, change its status to Disabled, click Apply, and click OK.

Method 3: Enable Insecure Guest Logons

Windows 11 24H2 blocks unauthenticated guest access by default. This step re-enables it for local network devices.

Open the Edit group policy window again.

Navigate to: Computer Configuration > Administrative Templates > Network > Lanman Workstation.

Locate the setting named Enable insecure guest logons.

Double-click it, change the toggle from Not Configured to Enabled, click Apply, and click OK.

Once completed, close out of all windows and attempt to reconnect to your shared network folder.

Are you using Windows 11 Home or Windows 11 Pro? (Method 2 and 3 require Pro unless you use alternate PowerShell workarounds)