

Microsoft reopens Always On VPN bug it wrongly marked as fixed



Microsoft says the Always On VPN connection bug on Windows 11 was wrongly marked resolved after the October 2026 updates. A fix is planned in the coming weeks; a protocol workaround exists meanwhile.

- Microsoft returned the Always On VPN issue from Resolved to Mitigated after wrongly closing it on October 13, 2026.
- The bug affects Windows 11 24H2 and later after the September 2026 security updates, when the first connection attempt fails.
- Affected connections may stay in a Connecting state or show the error 'The specified port is already in use.'
- The workaround is to change the profile from automatic protocol selection to either SSTP only or

IKEv2 only.

- A permanent fix is planned in an update due in the coming weeks.

Microsoft has told IT administrators that it wrongly marked a known Always On VPN problem as resolved. The status was set to Resolved on October 13, 2026, following the October Patch Tuesday cumulative updates for Windows 11, and has now been returned to Mitigated.

What is affected

The issue was first acknowledged in late September. It appears on systems running Windows 11 24H2 and later after the September 2026 security updates, when the initial Always On VPN connection attempt fails, for example where automatic protocol selection with IKEv2 and SSTP is configured. Affected connections can remain stuck in a Connecting state or fail to connect, and later attempts may show the error that the specified port is already in use.

Always On VPN runs in the background and builds secure tunnels to the corporate network whenever a device is online. It supports domain-joined, non-domain-joined and Microsoft Entra ID-joined devices.

Workaround and outlook

Microsoft says a resolution will be included in an update planned for the coming weeks. Until then, administrators can change the Always On VPN profile from automatic protocol selection to a single protocol, either SSTP only or IKEv2 only. Microsoft advises choosing the protocol according to the organisation's environment, security and deployment requirements.

The September cumulative updates have also been linked to other problems, including Hyper-V, Remote Desktop Services and USB audio faults that prompted emergency out-of-band updates, a domain login issue with a temporary workaround, and a File History backup bug under investigation.

Institutions that rely on Always On VPN for remote staff should not assume the October updates have resolved the problem and should plan accordingly.

What to do now

1. Check whether Windows 11 24H2 or later devices with the September 2026 updates use automatic protocol selection in Always On VPN profiles.
2. If users report stuck or failed connections, test switching the profile to SSTP only or IKEv2 only, choosing the protocol that fits your security and deployment requirements.
3. Run any profile change through your change-management process and a pilot group before wide rollout.
4. Do not treat the October 2026 updates as the fix; track Microsoft's service alerts for the planned update.
5. Brief the help desk on the symptoms and the error message so remote-access tickets are triaged quickly.

6. Plan to revert workaround profiles once the permanent fix is released and validated.