Microsoft fixes Always On VPN failures caused by September Windows 11 updates



Microsoft has fixed an Always On VPN bug introduced by the September 2026 Windows 11 updates. The October cumulative updates KB5127648 and KB5127646 resolve it, and a protocol workaround exists for those who cannot patch yet.

- The bug affected Always On VPN on Windows 11 24H2 and later after the September 2026 security updates.
- Connections could stay stuck in a Connecting state or fail with the error 'The specified port is already in use'.
- The trigger was a failed first connection attempt, for example with automatic protocol selection using IKEv2 and SSTP.
- KB5127648 and KB5127646 were released on Tuesday and fix the issue on all affected systems.

> - Temporary mitigation: set the VPN profile to a single protocol, either SSTP only or IKEv2 only.

Microsoft has resolved a known issue that disrupted Always On VPN connections after the September 2026 Windows 11 security updates. Always On VPN is the remote access solution that replaced DirectAccess. It runs in the background and builds a secure tunnel to the corporate network whenever a device goes online.

What happened

Microsoft first acknowledged the problem in a service alert to IT administrators in late September. On fully updated Windows 11 24H2 and later systems, a failed first connection attempt could leave the VPN unable to recover. This was seen when automatic protocol selection or fallback was configured, for example between IKEv2 and SSTP. Affected connections could remain stuck in a Connecting state or fail, and later attempts could show the error 'The specified port is already in use'.

The fix and the workaround

On Tuesday, Microsoft released the cumulative updates KB5127648 and KB5127646, which address the issue on all affected systems. For organisations that cannot yet install the October 2026 Patch Tuesday update, Microsoft suggests changing the Always On VPN profile from automatic protocol selection to a single protocol, SSTP only or IKEv2 only. The choice should reflect the organisation's environment, security and deployment requirements.

Wider context

The September updates also caused other problems that Microsoft addressed with emergency updates, including Remote Desktop Services failures, Hyper-V issues and USB audio problems. Microsoft has also confirmed that non-admin users may fail to connect via Remote Desktop when the Administrator protection feature is enabled.

For teams that depend on remote access, the practical step is to test the October updates on a pilot group and keep the temporary profile change in reserve.

What to do now

1. Identify Windows 11 24H2 and later devices that use Always On VPN with automatic protocol selection or fallback.
2. Test KB5127648 or KB5127646 on a pilot group, then deploy through your normal change process.
3. If patching must wait, switch the affected Always On VPN profiles to SSTP only or IKEv2 only, choosing the protocol that fits your security and deployment requirements.
4. Record any temporary profile change as an approved exception and plan to revert it after patching.
5. Check Remote Desktop access for non-admin users if Administrator protection is enabled.