

# Azure's Linux VPN Client Is Retiring — Here's What to Do

*A 10-minute guide for anyone running Azure Point-to-Site VPN on Linux*

**Deadline:** Microsoft retires the Azure VPN Client for Linux on **August 31, 2026**. After that date, it will not receive updates or security patches, and will be pulled from Microsoft's Linux package repo.

## What's actually happening

Microsoft is retiring one specific app — the Azure VPN Client for Linux preview (the `microsoft-azurevpnclient` package, Ubuntu 20.04/22.04 only). It is not retiring Azure VPN Gateway, and it is not retiring the OpenVPN protocol tunnel type your gateway already supports.

- **Affected:** the Azure VPN Client for Linux app itself. No more bug fixes, security patches, or downloads after Aug 31, 2026.
- **Not affected:** Azure VPN Gateway, the OpenVPN and IKEv2 tunnel types, and the Windows/macOS Azure VPN Client.
- **Who this hits:** any team with Linux laptops, VMs, or servers connecting to Azure over Point-to-Site (P2S) VPN using that client.

## Do this now (takes under an hour per fix) (this is the short-term band-aid solution)

Microsoft's own guidance points Linux users to one of two replacement clients. If your P2S gateway already offers the OpenVPN tunnel type — most do — this is the lower-friction path:

1. Confirm your Azure P2S gateway has the OpenVPN tunnel type enabled (Azure Portal → Virtual network gateway → Point-to-site configuration).
2. Download a fresh client profile (the `.ovpn` / VPN profile package) from the gateway.
3. Install a Linux OpenVPN client — either the open-source “`openvpn`” package with the `NetworkManager-openvpn` plugin (`sudo apt-get install openvpn network-manager-openvpn`), or the official OpenVPN 3 Linux client (`openvpn3`), available for Ubuntu, Debian, RHEL, and Fedora.
4. Import the profile and connect (`sudo openvpn --config profile.ovpn`, or `openvpn3 config-import + openvpn3 session-start`).
5. Uninstall the old Azure VPN Client for Linux app once the new connection is confirmed working.

**Fix it for good, not just for the deadline (this ensures your company is secure now and in the future)**

If you're already touching every Linux endpoint to swap VPN clients, it's an ideal moment to ask whether you want to keep hand-managing a native Azure gateway at all.

**Two OpenVPN products remove that maintenance burden entirely — and both use the same Linux-native OpenVPN 3 client end users already just installed.**

|            | Access Server                                             | CloudConnexa                                            |
|------------|-----------------------------------------------------------|---------------------------------------------------------|
| Model      | Self-hosted, in your own Azure VNet — full control        | Fully managed — no gateway to size, patch, or run       |
| Deployment | Azure Marketplace, BYOL or pay-as-you-go, live in minutes | Azure Marketplace Connector, or IPsec to your VNet      |
| Auth       | Microsoft Entra ID, SAML, RADIUS, LDAP, PAM               | SAML/Entra ID, plus device posture & location policy    |
| Scale      | No fixed connection ceiling — scales with your instance   | Multi-site, multi-cloud by default (AWS, GCP, branches) |
| Best fit   | Teams who want to keep infrastructure control             | Teams who'd rather not run VPN infrastructure at all    |

Both are already documented for Azure: [Access Server has a native Azure Marketplace listing](#) (BYOL and PAYG) and an ARM quickstart template; [CloudConnexa connects to an Azure VNet via a Marketplace Connector](#) or straight IPsec. Linux clients connect to either one using the same open-source or OpenVPN 3 client from the immediate fix above.

We are offering those affected by this a 20% discount - use the code **AZURE20** when signing up for a free trial for a discount on either a monthly or annual subscription (Access Server BYOL or CloudConnexa only).

## Full retirement timeline (for context)

| Date         | What happens                                                                  |
|--------------|-------------------------------------------------------------------------------|
| Mar 31, 2026 | New Azure VPN gateways can no longer enable SSTP. (Already passed.)           |
| Aug 31, 2026 | Azure VPN Client for Linux (preview) retires. This guide.                     |
| Mar 31, 2027 | Existing SSTP-enabled gateways stop accepting SSTP connections — hard cutoff. |
| Mar 31, 2028 | Manually registered Azure VPN Clients for Entra ID retire (public cloud).     |

## Quick FAQ

### Do I have to move off Azure VPN Gateway entirely?

No. Switching your Linux endpoints to the OpenVPN tunnel type keeps you on Azure VPN Gateway. Access Server and CloudConnexa are the recommended next step if you also want to shed the gateway's connection ceiling and management overhead — not a requirement to fix the Linux client issue.

### Does this affect my Windows or macOS users?

No — the Azure VPN Client for Windows and macOS is unaffected. This retirement is Linux-only.

### Is this the same as the SSTP retirement?

Related but different. SSTP (a separate, Windows-only protocol) has its own, later cutoff of March 31, 2027. The Linux client retirement is the more urgent, near-term item.

## Resources

[OpenVPN + Microsoft Azure overview](#)

[Access Server on Azure \(pay-as-you-go docs\)](#)

[Connect an Azure VNet to CloudConnexa via Connector](#)

[Connect Azure to CloudConnexa with IPsec](#)

[Microsoft: Azure VPN Client for Linux retirement overview](#)