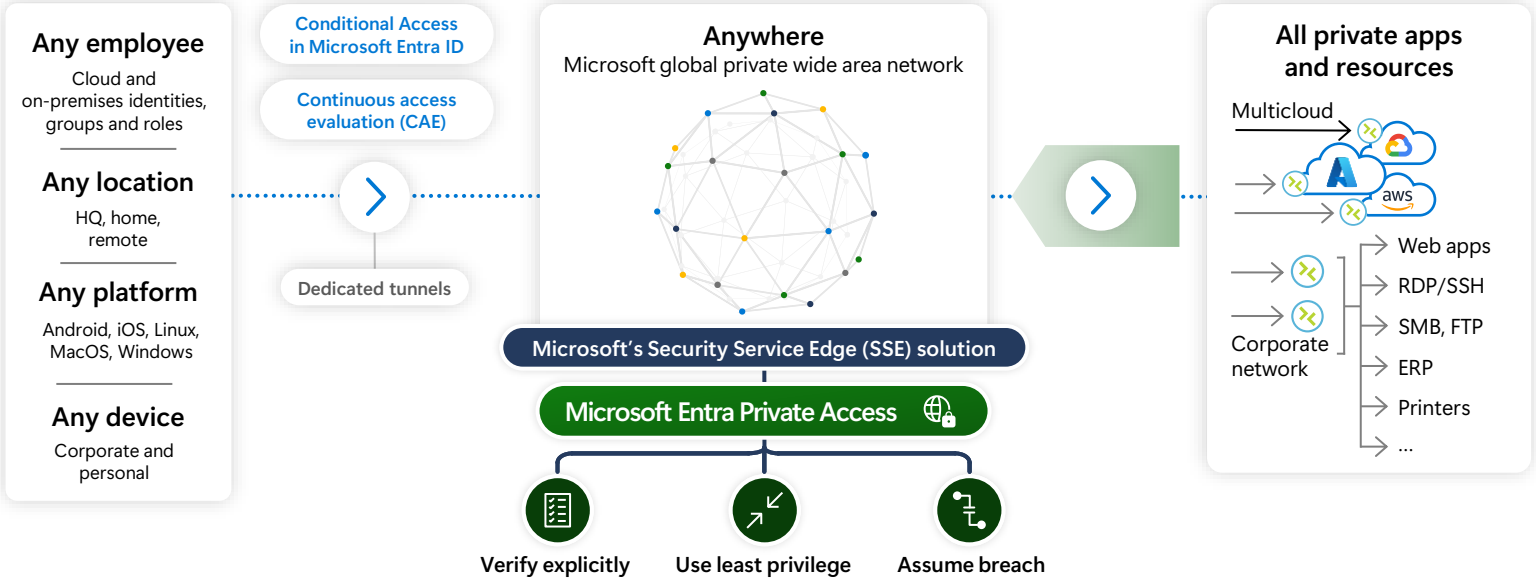
Replace legacy VPN with an identity-centric ZTNA

Secure access to all private apps and resources for users anywhere with an identity-centric Zero Trust Network Access (ZTNA) solution. Microsoft Entra Private Access allows you to replace your legacy VPN with ZTNA to securely connect users to any private resource and application without exposing full network access to all resources.



Your journey to ZTNA is simplified

Quick access
Easy migration from VPNs to ZTNA to all private apps with quick access policy

App discovery
Discover apps and onboard/ register them in Microsoft Entra ID

Segment access
Configure segmented access to private apps

Identity-centric access
Extend Conditional Access/enable single sign-on (SSO) to private apps

App groups and policies
Assign policies to individual apps or to app group(s)

Key benefits

Reduce risk by enforcing adaptive Conditional Access controls across all your private apps and resources

Enforce adaptive multifactor authentication (MFA) on on-premises private apps and resources including legacy and custom apps, command line access tools, file shares, databases, and more

Deliver fast and easy access at global scale and enable secure connectivity from different OS platforms (Windows, Android, iOS, MacOS)

Enable SSO support for non-https apps with SSO for legacy protocols like Kerberos

Frequently asked questions

How can Microsoft Entra Private Access help me to replace traditional VPN with ZTNA?

- Microsoft Entra Private Access, an identity-centric ZTNA solution, is built on Zero Trust principles to protect against cyberthreats and mitigate lateral movement while enabling advanced app segmentation and adaptive access.
- Without making any changes to your apps, you can extend Conditional Access policies to your network using identity-centric access controls and enable SSO and MFA across all private apps and resources.
- Through globally distributed points of presence, give your users a fast, seamless access experience that balances security with productivity.

I can't make an immediate switch from my VPN. How can I transition to Microsoft Entra Private Access in a more gradual manner?

Start your journey from legacy VPN to ZTNA with a pilot program by onboarding just a few private applications and users to Microsoft Entra Private Access. Then gradually increase onboarding additional applications and users to Private Access (ZTNA) as you phase out your existing legacy VPN solution. Here are the initial steps:

1. Deploy private network connectors (on the same network or DMZ as VPN servers).
2. Install client (use Intune/any SCCM for enterprise deployment) on Entra joined devices.
3. Configure QuickAccess with the IP address range(s) published over legacy VPN.
4. Turn on private traffic forwarding profile under Global Secure Access configuration.

What is the most effective strategy for integrating Microsoft Entra Private Access into our existing infrastructure?

Use Quick Access to provide broad access to your on-premises resources, enabling a seamless transition from VPN to Microsoft Entra Private Access. By starting with an initial, broad access setup, you can connect users to the applications and resources they need while enforcing identity-centric Zero Trust access controls. Over time, you can refine your deployment by utilizing app discovery to identify and onboard private applications to Microsoft Entra ID, allowing for further segmentation of access based on devices, users, and specific processes, thereby enhancing your security and control.

I currently have an SSE provider in place. How can I effectively integrate Microsoft Entra Private Access with my existing solution?

Microsoft's SSE solution offers flexible deployment options where it can coexist with other network security providers including Cisco, Palo Alto Networks, Zscaler, and Netskope. Coexistent deployment guides outline how you can implement Microsoft Entra Private Access alongside your existing SSE solution, where you can route specific traffic profiles through Microsoft's SSE solution. This approach allows for enhanced security and seamless connectivity, enabling you to transition gradually while maintaining your current infrastructure. Learn more: Coexistence with Cisco, Coexistence with Palo Alto Networks, Coexistence with Zscaler, Coexistence with Netskope

What are the key enhanced security capabilities compared to traditional VPN solutions?

With Microsoft Entra Private Access, you can implement Conditional Access policies, including MFA, and enable sign-sign on for private applications. Additionally, the solution provides Windows Authentication Manager (WAM) integration for seamless Windows-integrated SSO.

What are the costs associated with Microsoft Entra Private Access, and how do they compare to traditional VPN solutions?

- Microsoft Entra Private Access is available as a standalone offering for $5 user/month. Alternatively, you can purchase it as part of the Entra Suite for $12 user/month. The bundle includes a comprehensive set of solutions, combining network access, identity protection, governance, and identity verification for enhanced security and management.
- Microsoft Entra Private Access help reduce the total cost of ownership (TCO) compared to traditional VPNs, as it minimizes infrastructure and hardware dependencies, while streamlining management with a unified approach across identity and network access
- The solution also help reduce operational complexities and resources required to manage, configure, or support physical appliances, which often necessitates a dedicated engineering team.

Getting started with Microsoft Entra Private Access

Start a Microsoft Entra Suite trial today

You can experience the benefits of Microsoft Entra Private Access as part of the Microsoft Entra Suite, the industry's most comprehensive Zero Trust access solution for the workforce. Entra Suite unifies identity and network access controls to secure employee access to any cloud or on-premises application and resource from any location. It also consistently enforces least privilege access and improves the employee experience.

Get started with the Microsoft Entra Suite with a free 90-day trial today!

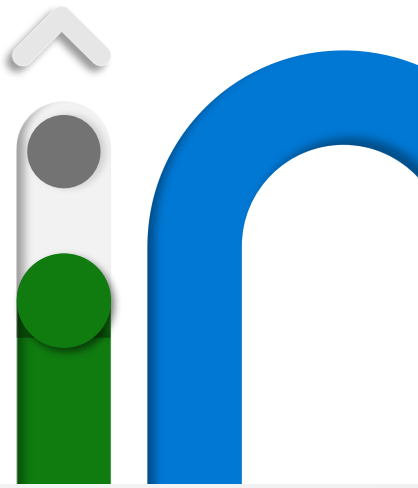
Start a Microsoft Entra Private Access trial today

Replace legacy VPN and level up to Zero Trust Network Access (ZTNA) with Microsoft Entra Private Access. Secure access to all private apps and resources for users anywhere while removing the risk and operational complexity of legacy VPNs. Boost user productivity by quickly and securely connecting remote users from any device and any global network to private apps—on-premises, across any cloud.

Get started with Microsoft Entra Private Access with a free 1-month trial today!

Prerequisites

- ✓ Requires a **Microsoft Entra tenant** onboarded to Microsoft Entra Private Access
- ✓ **Windows devices** must be managed devices joined to the onboarded tenant. The device must be either Microsoft Entra joined, or Microsoft Entra hybrid joined.
- ✓ The **Global Secure Access client** requires a 64-bit versions of Windows 10 or Windows 11
  - Microsoft Azure Virtual Desktop single-session is supported
  - Azure Virtual Desktop multi-session isn't supported
  - Windows 365 is supported
- ✓ **Android and MacOS devices** must be managed devices and Microsoft Entra registered



Resources

- Microsoft Entra Private Access
- Video: Microsoft Entra Private Access Overview
- Microsoft Entra plans and pricing
- Microsoft Entra Suite trial

Learn more

- It's time to move beyond traditional VPNs
- Blog: Microsoft Entra Private Access: An identity-centric solution Zero Trust Network Access Solution
- Blog: Microsoft Entra Private Access for on-premises users
- Microsoft Mechanics Video: Microsoft Entra Private Access: Replacing VPNs for on-premises resources