Simplify Application Access with Azure Active Directory
People use many apps and devices to get work done, which can mean multiple logins and complex technology such as VPN. Thankfully, there’s an easier and more secure way.

Connect and sync Microsoft Active Directory and other directory services to Azure Active Directory (Azure AD) in the cloud using Azure AD Connect, enabling seamless access with one unified identity across mobile, cloud, and on-premises apps.
SaaS applications give users instant access to apps they need to be productive, without the need for IT to build and manage them. However, without a unified identity, people may have to juggle individual accounts for every service, and IT won’t have visibility into who is using what.

**Thousands of apps**

**One identity for Software as a Service (SaaS) apps**

Azure AD integrates from day one with the SaaS apps people use every day, such as Office 365, Salesforce.com, Box, and Workday—giving users seamless access, with one-stop visibility and management for IT. It even enables mobile login without a password using Windows Hello and the Microsoft Authenticator app.
February 2018

Simplify Application Access with Azure Active Directory

Many companies use VPNs to authenticate users into on-premises resources, but this can cause management complexity and poor user productivity.

One identity for remote access to on-premises apps

Azure AD Application Proxy provides single sign-on access to on-premises apps with enterprise-grade security, reducing the need to use VPN or other legacy publishing solutions. There’s no need to modify applications, and you get the security benefits of Azure, including threat analytics, conditional access, and multifactor authentication.
03.
Mobile apps

Giving people flexibility to use the devices and platforms they prefer can boost productivity. However, rigid enrollment requirements can make it challenging to provide highly secure access through personal devices—especially for short-term workers or partners.

One identity for mobile apps

Microsoft Authenticator enables people to log in just once for access to all their Azure AD-connected mobile apps. It supports multifactor authentication to prevent unauthorized access. With easy end-to-end identity and access management, you can enable appropriate levels of access without requiring workers to enroll devices, and even support password-free login for ultimate convenience and security.
04. Migrating on-premises apps to the cloud

Migrating directory-aware apps to the cloud can seem daunting if you have to deploy and manage cloud-based domain controllers.

One identity for migrating on-premises apps to the cloud

Lift and shift apps to the cloud with no identity worries using Azure AD Domain Services. Join Azure virtual machines to a domain, without having to deploy domain controllers, and enable users to sign in using their Azure AD credentials for seamless access.
You can empower your users with seamless application access while improving security and control. Download the Crash Course in Azure Active Directory e-book.

→ Download the Crash Course