

Unlock the power of the cloud with enterprise-level identity services for all your apps.

AZURE ACTIVE DIRECTORY

Azure Active Directory is a cloud identity and access management solution that combines easy single sign-on to any cloud and on-premises application with advanced protection. It gives your people, partners, and customers a single identity to access the applications they want and collaborate from any platform and device. And because it's based on scalable management capabilities and risk-based access rules, Azure Active Directory protects your identities and streamlines IT processes.

THOUSANDS OF APPS, ONE IDENTITY

- Azure AD is the key for a productive modern workforce. Get easy and secure access to all your apps.
- Integrate your on-premises Active Directory and other directories with Azure AD through Azure AD Connect and use one identity to access any app.
- Azure AD already works with thousands of pre-integrated apps like Office 365, Salesforce.com, Box, and Workday.
- Add your own SaaS or custom apps
- Secure remote access to on-premises web application, eliminating the need to use VPN or other legacy publishing solutions.

BUSINESS WITHOUT BORDERS

- Azure AD puts application access and cross-organization collaboration at the tips of your fingers
- MyApps, is a single screen that gives your people a simple way to view and launch all their apps and manage their accounts.
- Users can securely manage their own services, like application requests, changing passwords and join or create groups.
- Vendors, contractors, and partners can get risk-free access to in-house resources with Azure AD B2B collaboration.
- Although available to all platforms, Azure AD is built in to Windows 10—which means your Windows 10 devices are connected and protected the moment you join them to Azure AD.

MANAGE ACCESS AT SCALE

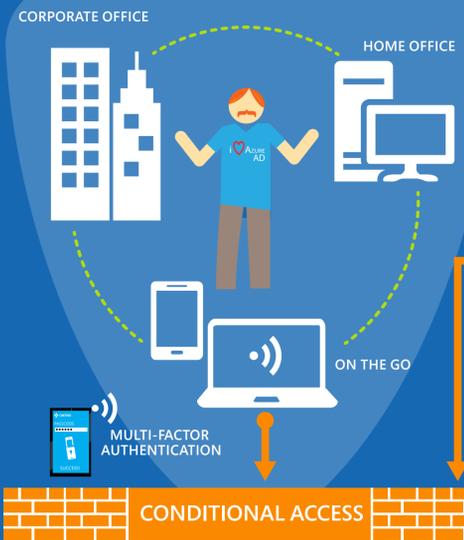
- Scale to manage all employee, partner, and customer identities without any degradation of service
- Get control of the user lifecycle and better management over work loads via integration with HR applications, dynamic groups and customizable provisioning.
- Keep IT overhead low with self-service capabilities, including password resets, group and application management.
- Azure AD Connect Health monitors your hybrid identity infrastructure, so you can keep an eye on the health of your Azure AD Connect sync engine, ADFS infrastructure and on-premises Active Directory Domain Services.

CLOUD-POWERED PROTECTION FOR A CLOUD-POWERED WORLD

- Azure AD takes secure identity and access management to the next level.
- Conditional access policies based on location, application sensitivity, device state, and user or sign-in risk
- Built in multifactor authentication gives you an additional layer of authentication protection.
- Identity protection insights for user, sign-in and configuration risk
- Privileged identity management helps you discover, restrict, and monitor administrators
- Provide just-in-time administration for eligible users.

EMPOWER AND PROTECT YOUR USERS

Enable users to work from any location and any device. Give them access to all their resources using a secure single set of credentials. Protect their identities with multi-factor authentication and conditional access policies based on location, device, user, app and risk.



IDENTITY PROTECTION

- Possibly bot-infected devices
- Anonymous sign-in
- Suspicious sign-in activity
- Impossible travel
- Leaked credentials



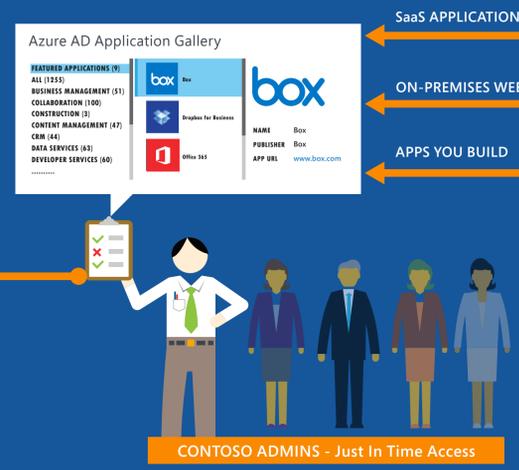
B2B COLLABORATION

Collaborate with external users and provide secure access to resources. Invite collaborators with any email address. Protect guest access with conditional access policies and multi-factor authentication.



PROVIDE SSO TO APPLICATIONS

Add pre-configured SaaS apps by using the Azure AD application gallery or your own via build-in templates. Add on-premises apps via the Application proxy. Users can get secure SSO to all these apps from their access panel or within Office 365. Set up provisioning and assign apps to users and groups.



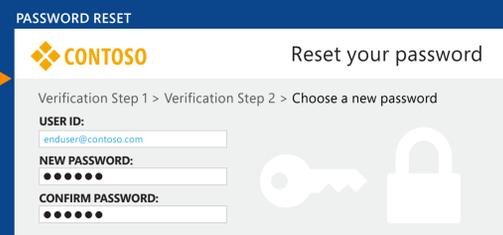
INTEGRATE YOUR LOB AND SAAS APPS

Build line-of-business (LOB) or SaaS applications for enterprise users or your customers/citizens and use Azure AD or Azure AD B2C for identity and access management. Integrated applications leverage Azure AD for single sign-on, identity and access management, querying the directory/Graph, conditional access and more. Publish your app to the Azure AD Application Gallery.



SELF-SERVICE CAPABILITIES

Azure AD helps keep IT overhead low with self-service capabilities, including password resets, group management, application requests, and application management. Also provides a single screen to access all your apps from any device.



USERS CHANGE AND RESET THEIR OWN PASSWORDS

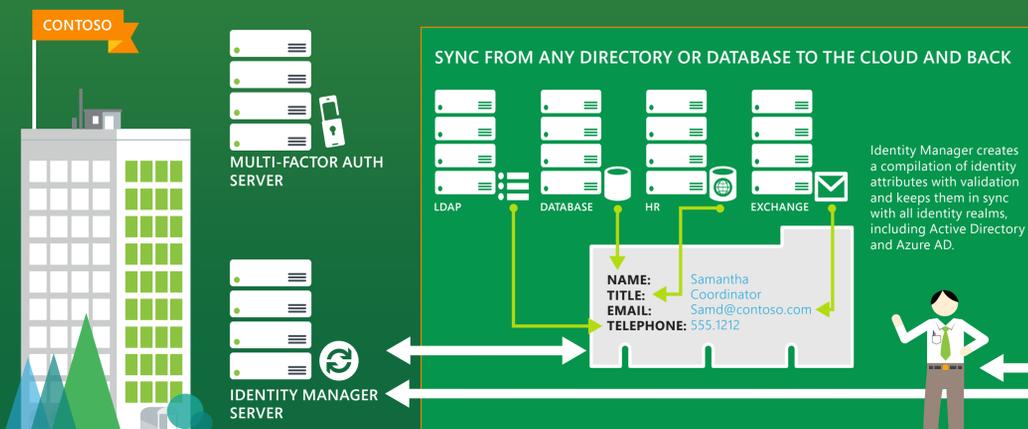
Give all users in your directory the capability to change and reset their passwords—whether they are in the cloud or on-premises.

CLOUD

ON-PREMISES

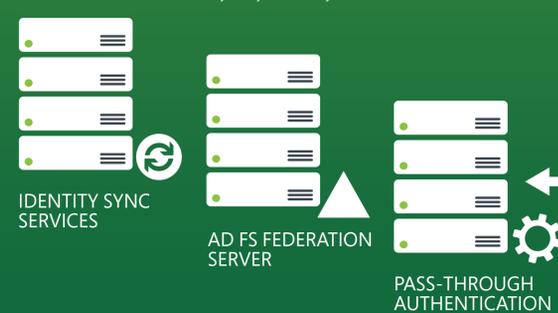
HYBRID IDENTITY SOLUTIONS

Provide users with a common identity across on-premises and cloud-based services, leveraging Windows Server Active Directory and Azure AD capabilities.



SYNC USERS, GROUPS, DEVICES, PASSWORDS, AND CHOOSE AUTHENTICATION METHOD

Azure Active Directory Connect is a tool that connects Active Directory and Azure Active Directory in a few clicks. Azure AD Connect will guide you to synchronize only the data you really need from single or multi-forest environments and will enable single sign on via password sync, federation with AD FS or pass-through authentication to Office 365 and thousands of other SaaS and on-premises applications. Azure AD Connect Health monitors your hybrid identity infrastructure.



WEB APPLICATION SERVER



WINDOWS SERVER ACTIVE DIRECTORY

