Microsoft Azure

Simple and secure access management

Azure Active Directory

Azure Active Directory provides single sign-on to thousands of cloud (SaaS) apps and access to web apps you run on-premises. Built for ease of use, Azure Active Directory features Multi-Factor Authentication (MFA), access control based on device health, user location, and identity and holistic security reports, audits, and alerts. Azure Active Directory is available in 3 editions: Free, Basic and Premium.

Benefits of Azure Active Directory

Single sign-on to any cloud and on-premises web app
Azure Active Directory provides secure single sign-on to cloud and on-premises applications including Microsoft Office 365 and thousands of SaaS applications such as Salesforce, Workday, DocuSign, ServiceNow, and Box.

Easily extend Active Directory to the cloud
Connect Active Directory and other on-premises directories to Azure Active Directory in just a few clicks and maintain a consistent set of users, groups, passwords, and devices across both environments.

Works with iOS, Mac OS X, Android, and Windows devices
Users can launch applications from a personalized web-based access panel, mobile app, Office 365, or custom company portals using their existing work credentials—and have the same experience whether they're working on iOS, Mac OS X, Android and Windows devices.

Protect sensitive data and apps
Enhance application access security using rule-based Azure Multi-Factor Authentication for both on-premises and cloud applications. Protect your business with security reporting, auditing, alerting, and "shadow IT" application discovery. Take advantage of unique machine learning-based capabilities that identify potential threats.

Protect on-premises web apps with secure remote access
Access your on-premises web applications from everywhere and protect with multi-factor authentication, conditional access policies, and group-based access management. Users can access SaaS and on-premises web apps from the same portal.

Reduce costs and enhance security with self-service
Delegate important tasks such as resetting passwords and the creation and management of groups to your employees. Providing self-service application access and password management through verification steps can reduce helpdesk calls and enhance security.

Enterprise scale and SLA
Azure Active Directory Premium offers enterprise-grade scale and reliability. As the directory for Office 365, it already hosts hundreds of millions of users and handles billions of authentications every day. The high availability service is hosted in globally distributed datacenters in 17 regions, with worldwide technical support that provides a 99.9% SLA.

Like it? Get it.

Created by the Azure poster team
Email: AzurePoster@microsoft.com

Cloud Identity and Access Management

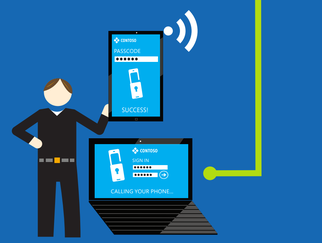
Microsoft

EMPOWER YOUR USERS

Enable users to work from any location using any device. Give them always-on access to all their work resources using a single set of credentials protected with Multi-Factor Authentication. After a user has signed in, they get single sign-on access to their apps and data.

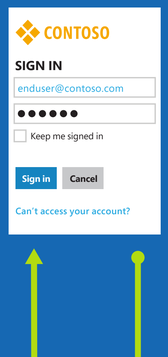
CORPORATE OFFICE

HOME OFFICE



ON THE GO

CLOUD

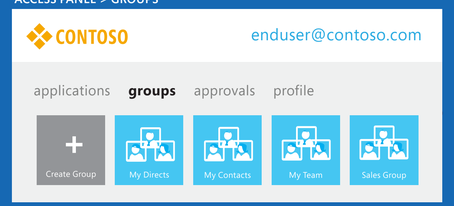


ACCESS PANEL

SELF-SERVICE CAPABILITIES

Minimize support costs and keep users up and running by configuring self-service experiences. With web-based tools such as Access Panel and Password Reset, give users a personalized, company-branded portal to access SaaS applications.

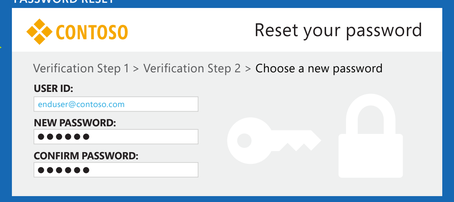
ACCESS PANEL > GROUPS



USERS CREATE AND MANAGE THEIR OWN GROUPS

Empower users to create their own groups, assign members to groups they own, approve join requests, and more.

PASSWORD RESET

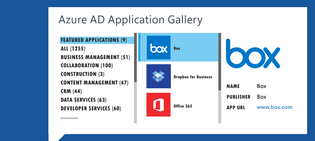


USERS CHANGE AND RESET THEIR OWN PASSWORDS

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

MANAGE YOUR SAAS APPLICATIONS

Add and manage SaaS applications in the public cloud by using the Azure AD Application Gallery. Users can then quickly sign in to your Microsoft and third-party SaaS apps from the Access Panel. Set up user provisioning to automatically sync users to your app and back.



NON-MICROSOFT APPS

MICROSOFT APPS + SERVICES

ON-PREMISES WEB APPS

APPS YOU BUILD

PREVENT MALICIOUS ATTACKS

Monitor access and anomaly reports to help secure your Azure AD directory. Get visibility into security risks so that you can mitigate them.

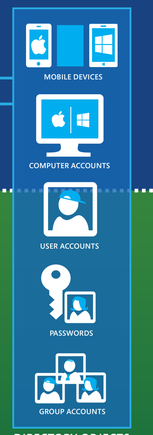
INTEGRATE YOUR LOB AND SAAS APPS

Build line-of-business (LOB) or SaaS applications using standard development tools and integrate your applications with Azure AD for use in one organization (single tenant) or many organizations (multi-tenant). Integrated applications leverage Azure AD for single sign-on, identity and access management, querying the directory, and more.

Publish your app to the Azure AD Application Gallery. An administrator then adds it to the Access Panel for use by any user or group that has been assigned access.

APPLICATION PROXY

AZURE ACTIVE DIRECTORY



DIRECTORY OBJECTS

ON-PREMISES

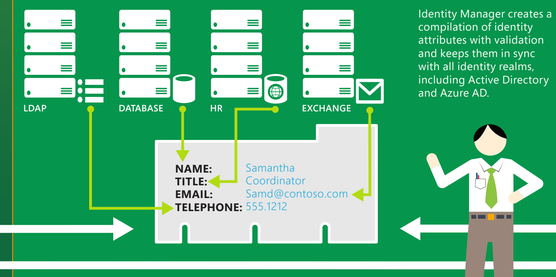
HYBRID IDENTITY SOLUTIONS

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

MULTI-FACTOR AUTH SERVER

IDENTITY MANAGER SERVER

SYNC FROM ANY DIRECTORY OR DATABASE TO THE CLOUD AND BACK



Identity Manager creates a compilation of identity attributes with validation and keeps them in sync with all identity realms, including Active Directory and Azure AD.

APPLICATION SERVER

CONNECTOR

SYNC USERS, GROUPS, DEVICES, PASSWORDS, AND MORE

Azure Active Directory Connect, the simple, fast and lightweight tool to connect on-premises directories to Azure Active Directory in a few clicks, will synchronize only the data needed from single or multi-forest environments and will enable single sign on via password sync or federation with AD FS to Office 365 and thousands of other SaaS applications.

IDENTITY SYNC SERVICES

WINDOWS SERVER ACTIVE DIRECTORY