Microsoft

Manage and secure access to your applications with Azure Active Directory

Section 1

What is identity and access management?

What is identity and access management?

Identity is the foundation of digital transformation

Cloud computing and mobile devices have transformed the modern workplace. An increasingly global workforce has the flexibility to work from anywhere using free and low-cost software as a service (SaaS) applications to solve productivity and collaboration challenges. Large enterprises are migrating applications and computing to the cloud to modernize their architecture, and lines of businesses are taking advantage of new cloud services to build custom apps for their specific needs. The enterprise has benefited from the surge of new technology with greater productivity, but digital transformation has also introduced three new challenges.

New challenges

Security risk: Before the cloud revolution, IT served as a technology gatekeeper. The apps and platforms you managed and secured were contained within the network perimeter, and everyone that signed into your corporate resources was first validated by the firewall. Those days are over. Your workforce has more control over the technology they use, much of which is accessed via the internet. Cyber attackers have learned to exploit these vulnerabilities. Even when a password is presented, that does not mean it is presented by a legitimate user.

Administrative burden: The explosion of endpoints provides users more ways to connect but this also creates an administrative nightmare. Many enterprises aren't aware of all the tools employees use and even when they do have a good inventory, the sheer number of cloud apps means you need to manage multiple identity systems, increasing costs and compounding existing security risks.

Poor user experience: Users also feel the pain. They love the flexibility but are frustrated by the number of credentials they need to remember.

Challenges due to digital transformation

Security risk
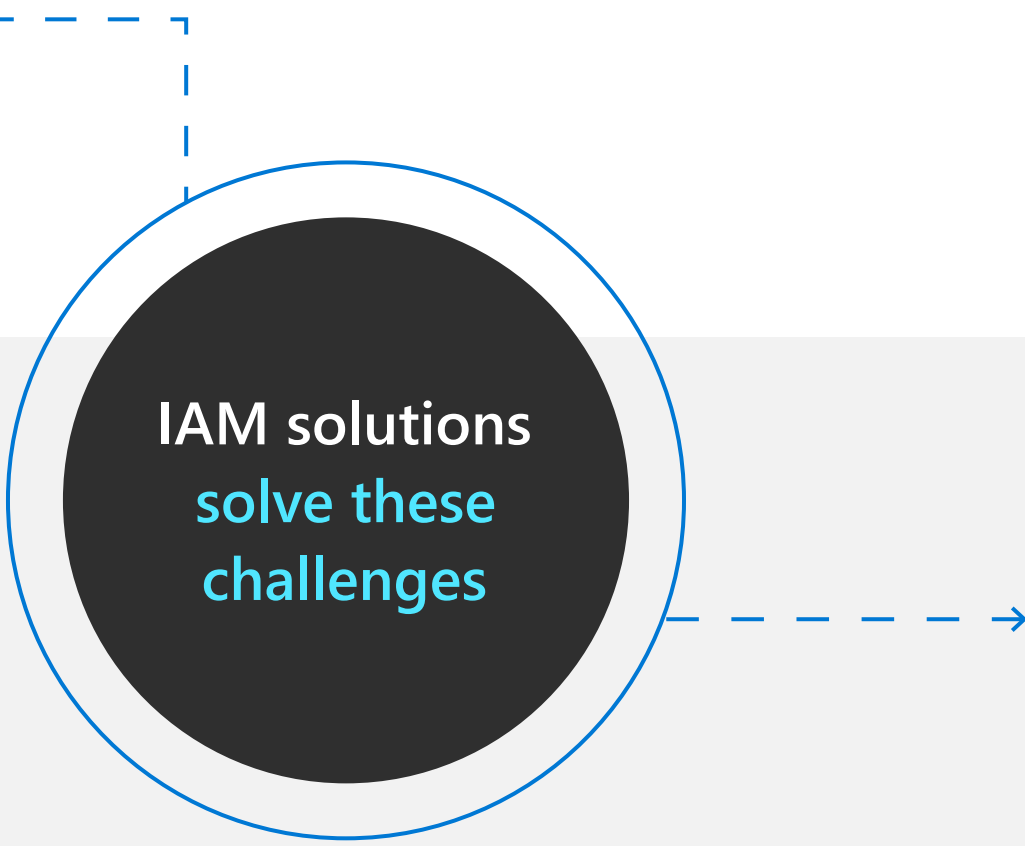
Administrative burden

Poor user experience

What is identity and access management?

Identity as the control plane

The common denominator across these pain points is inefficient systems for verifying identity. Identity has replaced the network perimeter as the new control plane. You need solutions that connect the disparate tools, architecture, devices, services, and clouds across the enterprise to better protect the organization and manage access for both employees and external partners.

Identity and access management (IAM) solutions unite access under one system, giving you more control. They provide seamless collaboration across the boundaries of your organization while improving the security of your corporate resources. A good IAM solution lets you connect your users to all their work applications—whether they are in the cloud or on-premises—through one set of credentials. IAM solutions are designed to give users access to only the resources they need and block unauthorized users from accessing data they shouldn't. You manage user access rights and permissions from a centralized portal, reducing much of the manual processes involved in provisioning and deprovisioning user accounts. IAM solutions also provide tools to manage security policies across your identities and apps. The best IAM solutions safeguard identities, improve the user experience, and increase administrative efficiency.

IAM solutions
solve these challenges

Better safeguard identities

Improve the user experience

Increase administrative efficiency

Section 2

What is Azure Active Directory?

What is Azure Active Directory?

A universal identity platform

Microsoft Azure Active Directory (Azure AD) is a comprehensive IAM solution in the cloud, and a leader in the market for directory management, application access, and advanced identity protection. Azure AD empowers organizations to manage and secure identities for employees, partners, and customers to access the apps and services they need. Azure AD helps thousands of organizations manage and secure over one billion identities.

Connect your workforce to any app

Manage and secure access to your organization's data and resources on-premises and in the cloud. Connect all your users, applications, and devices to the cloud for seamless, secure access and greater visibility and control. Automate workflows and enable self-service options help keep costs down and improve productivity for your users.
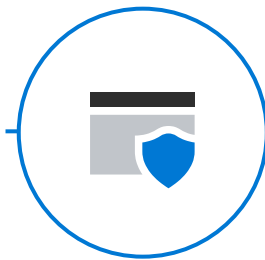
Protect and govern access

With the high volume of attacks on user credentials every day, the way to prevent compromise is to continuously track normal and abnormal behavior across the broadest set of signals possible, apply artificial intelligence and automate the responses. Balance productivity and security with timely access to the right resources and regular access reviews and policy enforcement.
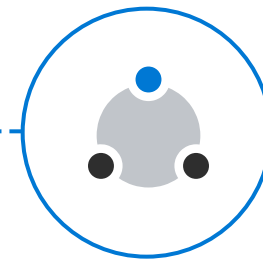
Engage with customers and partners

Expand your business with a reliable cloud service that can scale to millions of users with industry-leading security and flexibility. Connect with your external users and empower them to be productive with user-friendly, self-service experiences and built-in security controls.
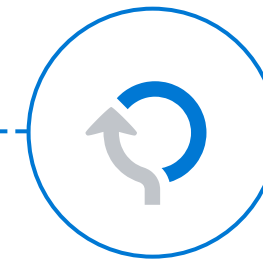
Accelerate adoption of your apps

Build applications that give users an easy way to sign in with their Microsoft personal, work or school account or with their social accounts. Start connecting to the Microsoft Graph, the gateway to data and intelligence in Microsoft 365, and build rich applications. Enable single sign on and automate user provisioning and reach the world's largest organizations.

Section 3

Azure AD for all your applications

Azure AD for all your applications

One identity for all of your apps

Azure AD lets you manage a common identity for each user across your hybrid infrastructure to access all the applications they need, including cloud and on-premises line of business applications. Manage all your identities from a universal platform, increasing administrative efficiency and giving you more control. Apply granular security policies to each of the applications used in your organization.

Azure AD for all your applications

Save time and money

Azure AD is pre-integrated with thousands of applications, including popular options like Workday, ServiceNow, SuccessFactors, Adobe, Concur, and Workplace by Facebook, making it simpler for you to make those apps available to your users. With one console, deploy consistent policies and monitor access rights. You can automate workflows for user provisioning and lifecycle management and save time and resources with self-service account management. You can also inbound user information from HR tools as a source-of-truth, eliminating the need for custom scripts or manual processes to manage user attributes.

Apps configured through Azure AD enable single sign-on (SSO) for seamless access, meaning users don't have to remember credentials for each app account or reuse weak passwords and risk a data breach. Accounts that have been configured for automatic provisioning give users immediate access to new resources. For inbound provisioning from HR tools, Azure AD ensures new hires have access to all of their relevant resources on day one.

Time and money savings

Built-in SaaS integrations

Single sign-on

Day one user access

Azure AD for all your applications

Provide more secure access to all your apps

Azure AD gives you comprehensive identity protection across all your apps – both SaaS apps and your on-premises line of business apps. Whether the user is requesting access into Microsoft Word or Box, Azure AD ensures their identity is confirmed before granting access. You can also institute access governance policies to ensure users only have access to what they need, when they need it. You can require users to request permission for access, and you can set a time limit for how long they can access the application and conduct regular compliance reviews of the access.

Azure AD also leverages the power of the Microsoft Intelligent Security Graph and machine learning to analyze trillions of signals across all our products and services to uncover atypical behavior and assign relative risk to each session. Azure AD looks at device, location, and other contextual information to evaluate the risk of the sign-in. You can establish Azure AD Conditional Access policies that automatically apply security measures, such as blocking an access request or requiring a password reset when a sign-in is deemed risky or particular policy conditions are met.

Application security measures

Identity protection

Access governance

Conditional Access policies

Section 4

How to manage and secure apps with Azure AD

Azure AD makes it simple to stay in control and reduce costs using automation, self-service, and policy enforcement.

How to manage and secure apps with Azure AD

Azure AD integrations

The Azure AD application gallery makes it easy to configure and connect any one of the thousands of pre-integrated apps to your tenant. These apps all support a SSO experience, and it is simple to configure the apps for Azure AD Conditional Access on a per-app basis or for enterprise-wide policies. Once you've added the app and configured it for your needs, users with authorized access can easily find it in the Azure AD My Apps portal, a centralized portal for end-user app discovery and launch.

If you have built an app or need one integrated for your org, you can also request to have it listed in the Azure AD application gallery.

[Explore the thousands of pre-integrated apps >](#)

Secure hybrid access

Use Azure AD Application Proxy to provide secure, remote access to claims-based on-premises web application without the need for VPN. App Proxy requires a light-weight connector installation, and grants the same IT and end-user experience as SaaS apps connected through the Azure AD application gallery.

Or leverage existing infrastructure investments, such as with partners like F5, Zscaler, Citrix, Akamai, and Aryaka to connect other types of apps like those that use header-based or Kerberos authentication protocols, and still gain the centralization and security benefits of Azure AD.

[Read how to add an on-premises application though App Proxy >](#)

[Connect other partner app networks and clouds >](#)

How to manage and secure apps with Azure AD

Automated provisioning

Azure AD lets you automate the creation, maintenance, and removal of user identities in popular SaaS applications. You can automatically create new accounts in the right systems for new people when they join your team or organization. When people leave a team or organization, you can set policies that will automatically deactivate their accounts from the right systems. By automating these tasks, you can ensure that the identities in your apps and systems are kept up-to-date based on changes in the directory, or your human resources system, reducing errors and time.

Learn more about setting up automated providing and deprovisioning to SaaS apps >

Group management

Azure AD helps you give access to your organization's resources by providing access rights to a single user or to an entire Azure AD group. Using groups lets the resource owner set access permissions for all the members of the group, instead of having to provide the rights one-by-one. This is a more secure method as you are less likely to accidentally give an individual inappropriate access, and it can save you time. You can also dynamically scale your group management by having enrollment be automated through identity attribute-based policies."

Learn how to create a group in the Azure portal >

How to manage and secure apps with Azure AD

Simplified user access

Some tasks don't require an IT professional to complete, and Azure AD lets you delegate those to others in the organization. You can empower users to create and manage their own security groups in Azure AD. Group owners can approve or deny membership requests, or they can delegate control of group membership.

Set up self-managed groups >

Users can also discover and explore the breadth of their access from the My Apps portal, and easily SSO to any app they have been granted access to. My Apps will show any SaaS app, on-premises app, and custom app as well as key corporate portals where access has been granted on a per-user basis, and apps can be grouped into collections to streamline visibility.

Navigate your access via My Apps >

Modernize authentication

If you currently use on-premises authentication like Active Directory Federation Services (AD FS), consider migrating your apps to Azure AD. You keep the same user benefits like SSO, but gain scalability and security benefits available from the cloud like applying granular per-application access controls using Azure AD Conditional Access or granting partners access to resources with Azure AD B2B collaboration. Apps that use the SAML 2.0, WS-Federation, OAuth, or OpenID Connect standards for federated sign-on can all be migrated.

Build Azure AD Conditional Access policies to secure access to your apps >

Use Azure AD B2B to seamlessly collaborate with your external partners >

Securely connect **any app**, on **any** cloud or server to Azure AD.

Over 2 million active, unique apps connected.

Get started today.

[Start a free one month trial of Azure AD](#) to see how simple it is to manage users access to all your apps and secure your enterprise.