Microsoft

Azure Active Directory

Customer and Partner Identity Management

Table of contents

Introduction

Every organization has the opportunity and imperative to digitally transform to achieve greater productivity and competitive growth while securing their digital estate.

Every relationship in the modern business environment is becoming digital—not just between employees, but with customers and clients, constituents, distributors, supply chain partners, and service providers. Today, organizations must be able to collaborate across the boundaries of their business and create customized experiences for consumers.

Enabling seamless and secure identity experiences for all users outside your organization is central to unlocking greater productivity, deeper brand engagement and loyalty, and business-to-business collaboration. As organizations increasingly rely on collaboration and engagement with external users, you need an identity approach that enables flexibility to customize the experiences offered to each user and protect your organization's assets with built-in compliance, scale, and intelligent security.

Simplify the way you manage your employee, customer, and partner identities with Microsoft Azure Active Directory (Azure AD), the world's most trusted identity service, with over 254 million monthly active users and an average of 30 billion authentication requests per day—more than any other identity provider on the market. Azure AD provides the security to protect users and the oversight to govern them, along with the freedom to sign into thousands of SaaS apps with single sign-on (SSO). With a single identity solution, your organization is equipped to harness the power of your digital relationships.

Empowering the user experience

Digital relationships are built on a strong identity foundation.

At Microsoft, we believe a strong identity foundation is one in which our customers can manage all their identities from the cloud, connect all their apps, ensure strong identity governance, and leverage our industry-leading security capabilities.

With Azure AD's capabilities for customer and partner identity, organizations can leverage this foundation to offer seamless and secure experiences to all of their external users. Recognizing that different users have different needs, Azure AD allows admins to configure the access, controls, and user experience to fit these needs, enabling secure access for each type of user while meeting scalability, security, and compliance requirements.

We also recognize that the increasingly complex business landscape will require new, intelligent ways of fulfilling your business needs and addressing dynamic security risks. Our vision for Azure AD reflects our understanding of the future of business, where organizations will create new business value by eliminating siloes and deepening relationships across boundaries. Relationships are dynamic, and so are the policies and experiences tailored to the user. Just as these relationships evolve, organizations will benefit from an identity approach that offers a spectrum of customization alongside the built-in intelligence, security, and scale to enable future growth.

Today, Azure AD offers B2B collaboration features that enable organizations to collaborate safely and securely with users from other organizations. For common B2B commerce and B2C scenarios, Azure AD B2C provides citizens and customers with secure access to their apps with fully customizable signup experiences.

Our vision for Azure AD encompasses new ways of collaborating and engaging with external users. Today, we see five common end-user experiences that shape organizations' relationships with their customers and partners: collaborating for productivity with partners; collaborating with line-of-business and SaaS apps; collaborating with commercial customers; connecting with consumers, customers, and citizens; and providing identity as a service.

01 Collaborating for productivity with partners

In today's workforce, your business partners can be any individuals outside the customer's domain, including individuals in the supply chain, distributors, subsidiary partners, professional services clients, vendors, contractors, freelancers, employees of other organizations, or others providing outsourced business functions. Azure AD's B2B collaboration features enable your organization to collaborate with external users while maintaining complete control over your own corporate data and to allow enterprise developers to write applications to bring multiple organizations together more securely.

With Azure AD, your employees can grant access to users from any organization that has a federated identity provider, users with a Google social ID, or any user with an email address to join Teams or to review, edit, and collaborate in SharePoint. Users sign in to shared resources through a simple invitation and redemption process with their work, school, or other email account. Administrators can set up policies that determine who is allowed to invite guests and what data guests are allowed to see.

02 Collaborating with line-of-business and SaaS apps

Beyond productivity in Teams, SharePoint, and other Microsoft 365 tools, organizations can also share line-of-business (LOB) and SaaS applications, processes, and other services with guest users from any organization. Organizations using Azure AD have the ability to customize the look and feel of the end-user experience, and to configure which attributes to collect and which identity providers to enable for signup.

External users can access these apps with a simple invitation and redemption flow, or follow tenant-specific links to a portal with all the apps for which they have access. Individual users can also register for access through a sign-up experience using their email address or social identity provider. Administrators can set up policies for what apps and resources users have access to according to company or role, can approve sign-up requests, and can determine how long partner access will last.

Centrica

Centrica PLC, an international energy and services company focused on satisfying the changing needs of its business and consumer customers, relies heavily on its partnerships. Traditionally, Centrica's partners and other external users were treated as if they were internal employees, meaning Centrica's IT team had to distribute and manage each account. After Centrica enabled Azure AD entitlement management, Centrica was able to address access controls and governance requirements, remove collaboration barriers between internal and external users, and provide one simplified identity solution across all departments.

https://customers.microsoft.com/en-us/story/757467-centrica-energy-azure

> **"By centralizing and streamlining, we can be more confident that the data is in one place, our regulatory compliance can be validated, and everything is properly managed."**
>
> James Simms
> Senior Solutions Architect
> Centrica

03 Collaborating with commercial customers

In many industries, organizations manage complex partnerships in which subsidiaries, distributors, vendors, and other partners may also be clients or customers of the business. These commercial customers may require access to productivity tools, internal commercial applications, and even public-facing apps transacting products or services. Facilitating both B2B collaboration and commerce requires tools that offer intelligent security and control to manage these dynamic commercial relationships.

For organizations seeking to provide greater collaboration capabilities, Azure AD also provides a user experience that can be customized by the service provider and tailored according to the relationship with the end user.

04 Connecting with consumers, customers, and citizens

Eliminating friction in the end-user experience is a top priority for organizations and developers engaging consumers, customers, or citizens. With Azure AD B2C, organizations and developers have the flexibility to tailor the identity experience of their customer-facing apps and services so it's aligned with their brand and business requirements—without sacrificing security.

With Azure AD B2C, you can provide simple, reliable, and secure SSO access to customer-facing apps with customers using their preferred, already-established social, enterprise, or local account identities. This allows users to connect using their preferred professional or personal identities in situations where customers may sign up to purchase or resell products and services from a vendor, join membership and loyalty programs, or receive customer service from companies or the government.

For customizing the user journey, Azure AD B2C sign-up and sign-in policies allow you to control behavior by configuring settings, such as account types that consumers use, attributes that are collected from the consumer during sign-up, multi-factor authentication (MFA) usage, and the look and feel of all registration and authentication pages. Designed to offer you flexibility and control, these customization capabilities include white-label features that allow you to design the entire user experience to blend seamlessly with your web and mobile applications.

Los Angeles Clippers

With Azure AD B2C, the Los Angeles Clippers are able to engage with fans more effectively. They can see what parts of their platform are driving the most interest and interaction, which social platforms are being used for sharing, and where they might be housing stale data. By moving to the cloud and taking advantage Microsoft's built-in automation, the LA Clippers have been able to scale their small IT team while delighting fans.

https://customers.microsoft.com/en-us/story/la-clippers-media-entertainment-microsoft-365

> **"Given the choice between spending hours on security each day and making sure our employees and customers have everything they need, I'd choose the users every time. Now I don't need to choose."**
>
> Charles Sims
> Head of Technology
> Los Angeles Clippers

05 Providing identity as a service

Organizations may find themselves providing identity services and operating as an identity provider to subsidiaries, distribution channels, government agencies, and other external users. With Azure AD B2C, organizations can create an identity experience tailored to their brand and policies. Individual users are able to create accounts with this service, and use that identity with other affiliated services.

These five common identity experiences for external users are enabled by Microsoft's foundational security and compliance to establish a strong identity foundation.

Securing digital relationships

While connecting and collaborating are key, digital relationships are dependent on trust, making the security of both the user and the organization critical to the brand.

With Microsoft's intelligent security stack, Azure AD is the most trusted and compliant platform that allows you to securely engage with your customers and partners.

Organizations can leverage our industry-leading security capabilities by enabling strong authentication, conditional access, and identity protection.

Strong authentication

According to the Verizon data breach report, 81 percent of breaches use stolen or weak passwords. Turning on MFA is the simplest way to reduce the risk of compromise by 99.9 percent, according to research by Microsoft. Azure AD supports a broad range of authentication options to fit the needs of your external users. You can customize access policies to minimize disruption and prompt for MFA only when necessary.

Conditional Access

As organizations create business value by working and connecting with external users, you want to guarantee that only the right people with the right resources on secure devices can access your data where they are.

Microsoft’s Conditional Access provides this protection without compromising productivity. Conditional Access enables organizations to fine-tune access policies based on contextual user, device, location, and session risk information. You can use additional challenges, such as MFA, terms of use, or access restrictions, to further decide whether to allow, deny, or control access to a given user. These policies offer you greater control over how and when your external users access corporate resources.

Identity protection

While Conditional Access protects resources from suspicious requests, identity protection provides ongoing risk detection and remediation for suspicious user accounts. With identity protection from Microsoft, you can proactively prevent compromised customer or partner identities from being abused.

Using machine learning, Microsoft technology analyzes over 171 terabytes (TB) of identity-related security signals—including user behavior, location, state of device, application being accessed, and the risk score of the sign-in. This intelligence then informs the appropriate policy to apply for access to a resource, such as allowing, limiting, or blocking access, or additional verification measures.

By enabling identity protection, Azure AD customers benefit from real-time continuous detection of sign-in and user risk, automated remediation for common risk scenarios, and connected intelligence that surfaces potential vulnerabilities.

Together, the strong authentication, Conditional Access, and identity protection available within Azure AD empowers your organization to deepen customer and partner relationships without sacrificing your security.

Conclusion

Managing your organization's relationships with a diversity of external users is critical to uncovering potential business value through collaboration with partners and connection with customers.

As a leader in identity and access management, Azure AD offers a seamless, secure approach to managing and protecting these users' identities today, as well as for tomorrow's increasingly complex business needs and security challenges.

→ Activate your free Azure AD Premium trial today.

→ Get started with Azure AD B2C with a free tier of 50,000 active users per month. Pay only for your active users above the first 50,000. Existing customers are eligible to opt into the new monthly active user meter and take advantage of the expanded free tier.

→ Read the Azure AD and Azure AD B2C documentation to learn more.

Microsoft