Microsoft

A Crash Course in Azure Active Directory for Nonprofits

A Crash Course in Azure Active Directory for Nonprofits

Digital transformation is helping all types of organizations to create more collaborative environments. The goal: creating a digital space where users can work together more effectively and securely regardless of their device, application, or location. For nonprofits this presents both opportunities and challenges. Leaders of nonprofits need to ensure that staff, volunteers, board members, and donors all have access to the data they need. At the same time, that data needs to be protected against accidental or intentional security breaches.

A modern solution to those challenges is unified identity and access management (IAM). Organizations take advantage of IAM to apply controls based on role and need—no matter how the user connects. By authenticating and managing users as they access the organization's assets, nonprofits can protect data regardless of where it's stored, how it's accessed, or with whom it's shared. Azure Active Directory (AD) is a cloud-based directory and identity management service that delivers single sign-on (SSO) access to on-premises and cloud applications. This makes it easy for your general staff and volunteers to safely access the resources they need, to further your organization's mission. It also frees your IT staff from routine maintenance tasks so they can develop new ways to enhance your organization's services.

Gain intelligent security for your modern workplace

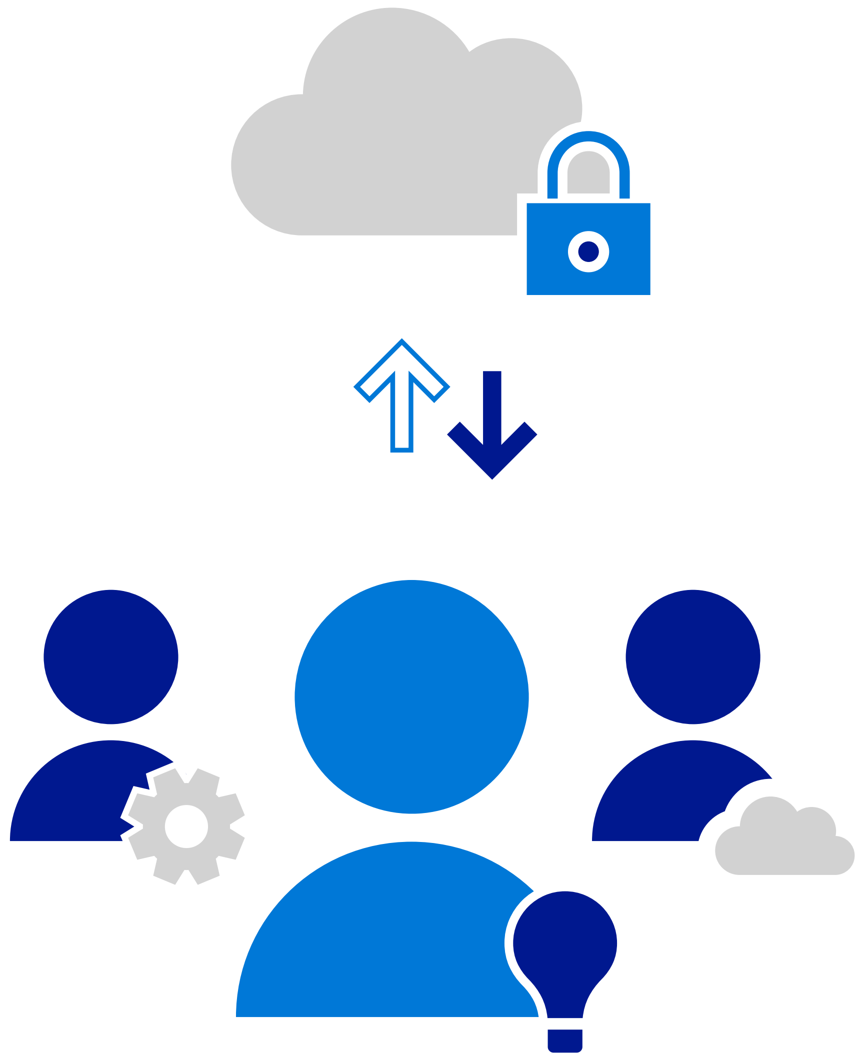
To make it easier for your organization to take advantage of unified IAM capabilities, the Azure Active Directory service is a core feature of Microsoft 365. Microsoft 365 combines Office 365, Windows 10, and Enterprise Mobility + Security (EMS) into a comprehensive, intelligent solution with built-in holistic, identity-driven protection for users, devices, apps, and data. With Microsoft 365, your internal and external users can access both cloud and on-premises resources with a single, common identity, to work together more creatively and securely from anywhere, on the device of their choice.

$1 billion cloud resources donated to nonprofits

At Microsoft, we are committed to helping nonprofits accelerate your mission by making the latest technologies more accessible, affordable, and relevant to your organization. Through the Microsoft Tech for Social Impact initiative, launched in late 2017, Microsoft Philanthropies has pledged $1 billion in donations and discounts on a variety of cloud computing resources to reach over 300,000 nonprofits by 2020. We've also built a growing ecosystem of partners who focus specifically on providing relevant technology and services, to help nonprofits of all sizes to scale and drive greater impact through the cloud.

How to use this e-book

This e-book offers a quick tour of all you can accomplish with Azure AD. It highlights everything from the benefits of SSO, to how to integrate on-premises Active Directory with Azure AD, to improving security without compromising productivity. It will help you discover the power of the cloud to support your digital transformation.



What is Azure AD?

Azure AD is Microsoft’s cloud-based directory and identity management service. It combines core directory services, advanced identity protection, and application access management. Azure AD delivers single sign-on (SSO) access to on-premises and cloud applications, helping users stay productive. Using Azure AD, developers can quickly integrate IAM into their applications.

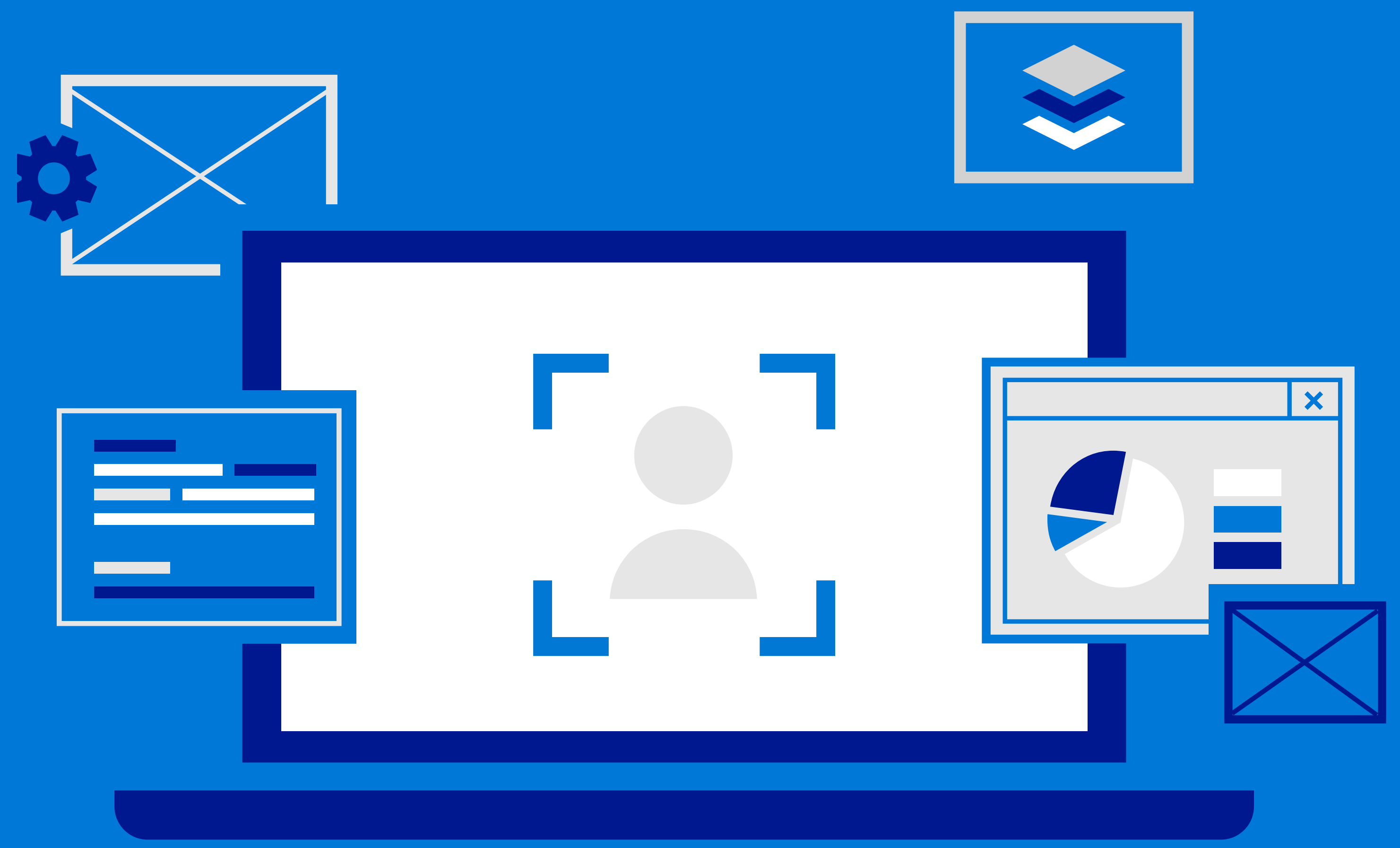
The solution provides a full range of modern IAM capabilities, including conditional access with multifactor authentication (MFA) and password-free login options, single sign-on, self-service password management, role-based access control, and intelligent security monitoring and alerting capabilities.

Because it is hosted as a fully managed cloud service, Azure AD is the ideal service for combining user accounts into a single, unified, highly secure identity. It employs the same Active Directory technology used by thousands of businesses around the world, supporting seamless synchronization from on-premises identity servers—yet with the accessibility and cross-platform capabilities of the cloud.

It includes solutions for authenticating users for software-as-a-service (SaaS), on-premises, web, and mobile applications using a unified identity. That identity also simplifies the process of monitoring and controlling application access, because all authentications flow through a single system. To maximize the value of Azure AD, the one-identity-per-user model should be prioritized.

01.

Improve the user experience



Save time and improve productivity with single sign-on

Workers use a variety of applications throughout the day. Managing passwords and logging in over and over slows people down. Azure AD single sign-on (SSO) extends on-premises AD to the cloud, so people can use their primary corporate identity to sign in to domain-joined devices, company resources, and web and software-as-a-service (SaaS) applications.

This frees users from the burden of managing multiple logins and enables organizations to provide or revoke access based on employee role. Azure AD manages the user lifecycle dynamically, integrating with Human Resources controls to provide automatic access to the apps users need based on team and role. As users join, move, and leave, access adapts based on preset policies.

Using Azure AD SSO, you can manage user access to SaaS applications directly from the Azure Portal, and even delegate application access decision-making and approvals to anyone in the organization for greater productivity. Built-in monitoring and reporting of user activity will help your organization identify and mitigate unauthorized access.

Use password-free login for security and ease

Keeping track of passwords can be a major headache for users, leading them to write credentials down in non-encrypted formats—and opening the door to security breaches. Azure AD provides password-free login options that make authenticating easier for users and more secure for businesses.

For example, using the Microsoft Authenticator app, employees can sign in by getting a notification on their phone. On a domain-joined Windows 10 device, where IT has integrated a device with Azure AD, Windows Hello can unlock both the device and apps by recognizing a PIN, smart card, or biometrics such as a fingerprint or face.

Simplify password management with Azure AD self-service password reset

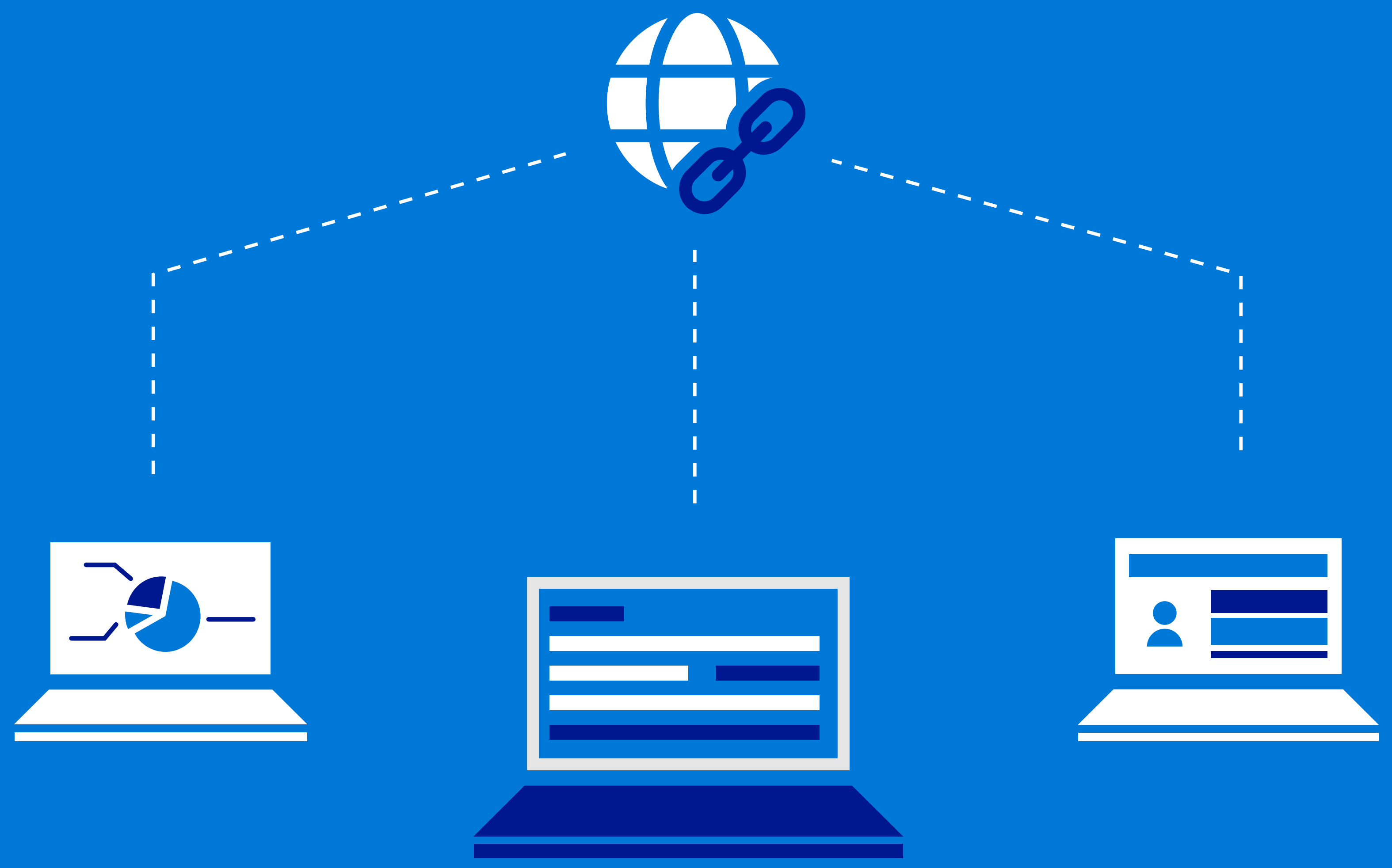
Your IT department should be able to prioritize strategic and mission critical work, rather than spending time resetting passwords. With Azure AD self-service password reset (SSPR), you can enable users to change their passwords and unlock their accounts without calling the helpdesk. It is a full-featured solution, enabling authentication by text message, phone call, email, or security questions.

Give users a consistent experience by adding your corporate branding

Apply your company's look and feel to your Azure AD sign-in page, which appears when users sign in to applications that use Azure AD as an identity provider. This option can be configured in the Azure AD admin center.

02.

Connect your on-premises and cloud applications into one ecosystem



Integrate on-premises directories with Azure AD Connect

If you use Active Directory on-premises, you can easily benefit from Azure AD by synchronizing the two using Azure AD Connect. By providing a single, common identity for accessing both cloud and on-premises resources, you can improve the user experience, support productivity, and enable advanced security capabilities. Azure AD Connect can work with Active Directory Federation Services (AD FS) to address complex deployment scenarios such as domain-joined SSO.

Azure AD Connect also includes Azure AD Connect Health to help you monitor and report on your hybrid directory environment. This helps you ensure that users can reliably access all the resources they need using a simple Azure AD Connect Health agent.

Enable easy remote access using AD Application Proxy

When you empower your employees to work on their own devices with access to on-premises applications from anywhere, you can significantly improve productivity. Some traditional access methods for remote workers—such as virtual private networks (VPNs) and demilitarized zones (DMZs)—can be complex and challenging to secure and manage.

Azure AD Application Proxy enables SSO and secure remote access for on-premises web applications such as SharePoint sites, Outlook Web Access on Exchange Server, or other line-of-business applications. Users can access on-premises and cloud applications using one identity, and there's no need to change network infrastructure or employ VPN.

Engage more effectively with Azure B2B collaboration

Employees aren't the only people who need secure access to your application ecosystem. You might also need to connect with vendors, partners, subsidiaries, or other external entities. Using Azure AD B2B collaboration, you can give guest users single sign-on access to applications of your choice, with powerful authentication policies managed by Azure AD.

03.

Secure identities more effectively

Improve security with Azure AD Conditional Access and MFA

In a world of growing cyber-threats, passwords just aren’t enough to protect sensitive information, but you don’t want to compromise productivity either. Azure AD Conditional Access simplifies multifactor authentication so that it is only required when conditions represent risk.

Conditional Access provides a risk score based on multiple criteria about the user, device, and location that is being used to sign on to determine if MFA, password reset, or limited functionality in the app is appropriate. Azure MFA enables you to add device-based or biometric security while giving users a streamlined sign-in process. You can use phone calls, text messages, or app-based verification as the secondary authentication method.

Detect and mitigate breaches with Azure AD Identity Protection

If an attacker steals a user's identity—even one with minimal privileges—they may still be able to gain access to critical systems and data. Azure AD Identity Protection helps you detect identity vulnerabilities, investigate and mitigate suspicious access, and configure automated responses to potential identity breaches. With Azure AD Identity Protection, you can protect all identities regardless of their privilege level and proactively prevent compromised identities from being abused.

The solution uses adaptive machine learning algorithms and heuristics to detect anomalies and suspicious incidents that indicate potentially compromised identities. Using this data, Identity Protection generates reports and alerts that enable you to evaluate the detected issues and take appropriate mitigation or remediation actions. You can also configure automated responses to potential identity breaches, including automatic blocking or remediation actions such as password resets and multifactor authentication enforcement.

Delegate application controls safely using Azure AD Privileged Identity Management

Users may need privileged access to administrative controls for a variety of reasons. However, dormant or rarely used account privileges can linger unseen and enable access beyond what individuals need—which creates security risk. Azure AD Privileged Identity Management (Azure AD PIM) enables you to provide granular access privileges to Azure AD resources and other Microsoft Online services on a temporary, as-needed, or on-request basis, as well as manage, control, and monitor those privileges to prevent problems.

Nonprofit Sales Desk

To learn more about nonprofit offers and to get help finding the right products for your organization, contact nonprofit sales via email or phone (Monday–Friday, 7 AM–7 PM Central Time).

→ Email us

→ Call us: (800) 258-6149

Microsoft Windows, Windows Vista and other product names are or may be registered trademarks in the U.S. and/or other countries. The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this document. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this document.