Microsoft Security

Crash course in Azure Active Directory

The sudden mandate to work remotely has accelerated many organisations' efforts to modernise their workplace by empowering employees to securely and efficiently collaborate. Now more than ever, IT is being asked to provide seamless access to the tools and data people need, wherever they are, from whichever device they're using. To help keep your 'new' workplace secure, you need to protect your data effectively as it traverses many applications and locations.

0.
Introduction

1.
What is Azure AD?

2.
Improve the user experience

3.
Connect to cloud and on-premises apps

4.
Secure and govern identities more effectively

0.

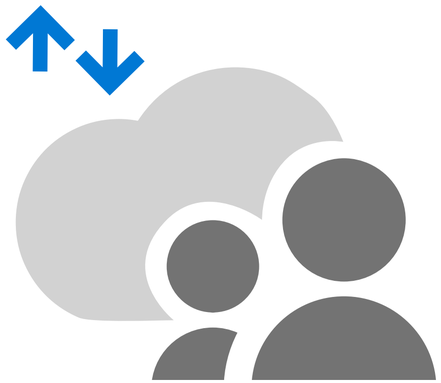
Introduction

A modern approach to identity and access management (IAM) can help you safely support a remote workforce.

At its core is the adoption of Azure Active Directory (Azure AD) to establish one, unified identity and provide an easy way to centralise authentication for many types of applications and services. By adopting Azure AD, you can enhance security and compliance while your users can focus on innovation and working effectively on dispersed teams. At the same time, Azure AD integrates once-disparate identity management tasks for IT simplicity and supports intelligent security. In this eBook, we'll take you on a quick tour of what you can accomplish with Azure AD and how to use it to its fullest potential to safely support a new digital workplace.

1.

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 strong, secure authentication into their applications.

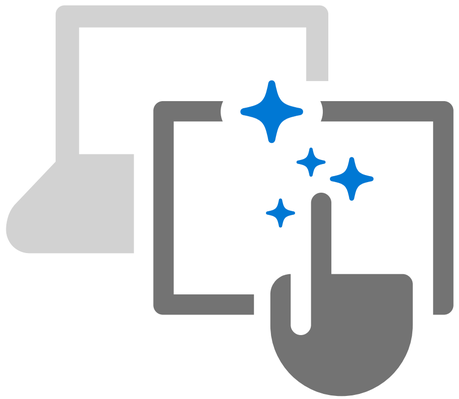
The solution provides a full range of modern IAM capabilities, including Conditional Access with multifactor authentication (MFA) and passwordless login options, single sign-on, self-service password management, role-based access control and intelligent security monitoring and alerting capabilities.

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 on-premises Active Directory (AD) technology used by thousands of businesses around the world, supporting seamless synchronisation from on-premises identity servers – yet with the accessibility, scalability 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 maximise the value of Azure AD, the one-identity-per-user model should be prioritised.

2.

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 SaaS applications.

This frees users from the burden of managing multiple logins and enables organisations 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. With SSO, you can manage user access to SaaS, on-premises and custom applications directly from the Azure Portal, and delegate application access decision-making and approvals to anyone in the organisation for greater productivity. Built-in monitoring and reporting of user activity will help your organisation to identify and mitigate unauthorised access. The Azure AD app gallery has thousands of SaaS apps with built-in integrations, making it easy for IT to connect new apps for users. With My Apps or the Office portal, users can discover, filter and launch their apps from a central, web-based portal.

Use passwordless 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 passwordless 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 recognising a PIN, smart card or biometrics such as a fingerprint or face. If a user can't access their workstation or mobile work device, they can use a FIDO2 security key to log in to their Azure AD account.

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 centre.

Simplify password management with Azure AD self-service password reset

Your IT department should be able to prioritise strategic and mission-critical work, rather than spending time and resources 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. When a user creates or manages their authentication methods, such as mobile app, email or security questions, you can enable SSPR to prompt them to enrol the same security information for MFA, helping to drive end-user adoption.

3.

Connect to cloud and on-premises apps

Integrate on-premises and cloud directories with Azure AD Connect

If you use Active Directory on-premises, you can easily benefit from Azure AD by synchronising 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. Multiple on-premises directory scenarios are possible, either to a single AD forest or to many isolated AD forests that are created by complex organisation structures or mergers and acquisitions (M&A). 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 enables you to maintain a small on-premises footprint while integrating complex directories into the cloud. 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 secure remote access to on-premises applications

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 demilitarised zones (DMZs) – can be complex and challenging to secure and manage. One lightweight agent is all that's required for Azure AD Application Proxy to enable 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. You can also pair the scalability and security of Azure AD with app platforms that already exist in your infrastructure, such as F5, Oracle, SAP and Zscaler.

Engage more effectively with 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 SSO access to applications of your choice, with powerful authentication policies managed by Azure AD. Guest users can even use their own company's identity provider for authentication and still access the approved apps and resources on your organisation's network.

By providing a single, common identity for guest users to access both cloud and on-premises resources, you can support the experience and productivity of company guests while keeping identities secure.

4.

Secure and govern 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-based outcome 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, and if you choose the Microsoft Authentication app as your method, you'll get MFA for free!

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, Azure AD 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 MFAi enforcement.

Delegate administrative controls and govern access compliance with Azure AD Identity Governance

Azure AD Identity Governance enables you to govern the identity and access lifecycles by ensuring that the right users have access to the right resources. Provision accounts for newly hired users from HR tools to enable day-one productivity and update user access if their role changes. Choose which internal and guest users are allowed to request access to resources, and bundle access into packages for better scalability. Azure AD access reviews help you to regularly assess current access status, as well as dynamically automate access and group membership based on identity attributes. Azure AD Privileged Identity Management helps you mitigate the risks of excessive or unnecessary elevation of roles and access rights.

To learn more about Azure AD, explore the
Azure Active Directory documentation >

Microsoft Security

Discover the benefits of cloud-based identity

The best way to experience the power of Azure AD is to try it yourself.

Start your free trial now

Contact us