Azure Identity and Management Solutions

Identity and Management Solutions

- To protect Applications and Data
- Defend against malicious login attempts and safeguard credentials with risk-based access controls
- Identity protection tools and strong authentication options—without disrupting productivity.

Azure Identity & Management Services

Azure Active Directory

Azure Active Directory External Identities

Azure Active Directory Domain Services

Microsoft Entra

Azure Active Directory Service

Azure Active Directory

Cloud-based identity and access management service

This service helps your employees access external resources, such as Microsoft 365, the Azure portal, and thousands of other SaaS applications

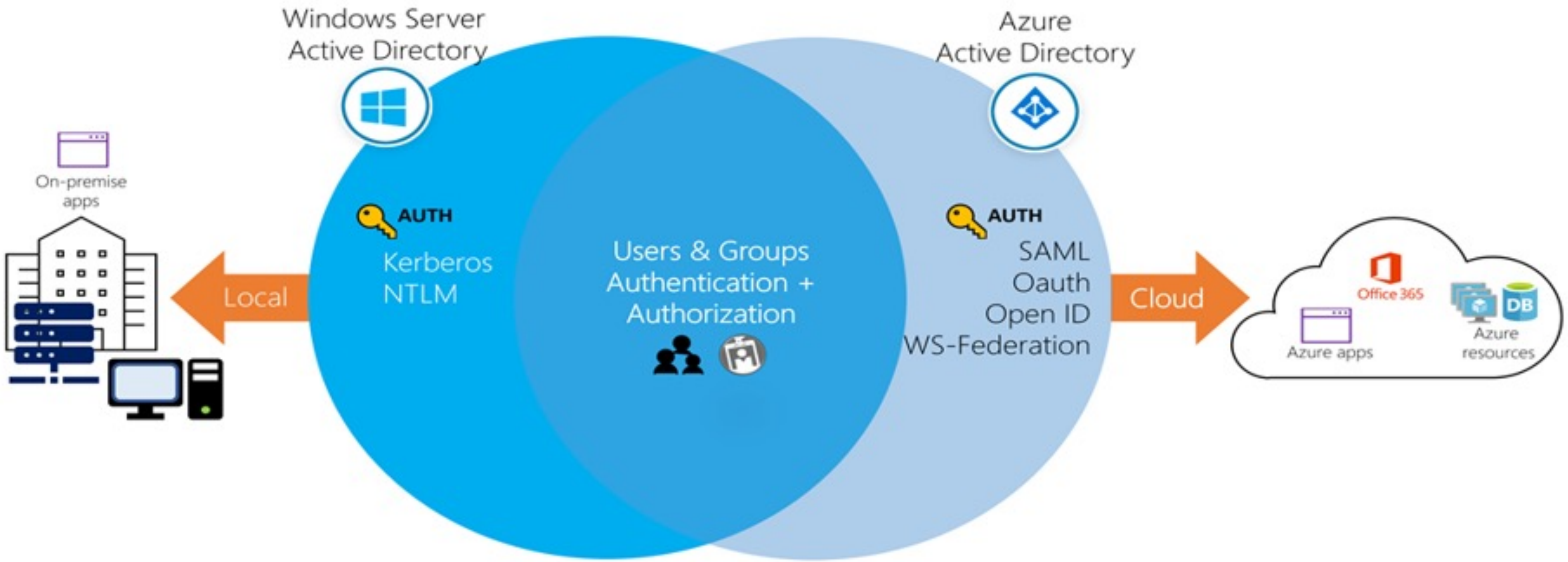
Also helps them access internal resources like apps on your corporate intranet network, along with any cloud apps developed for your own organization

Who Uses Azure AD?

IT Admins – Control Azure AD access

App Developers – Integrating SSO login for the applications which they develop

Microsoft365, Office 365 or Dynamic CRM online subscribers


Windows Server
Active Directory
Azure
Active Directory
On-premise
apps
AUTH
Kerberos
NTLM
Local
Users & Groups
Authentication +
Authorization
AUTH
SAML
Oauth
Open ID
WS-Federation
Cloud
Office 365
Azure apps
DB
Azure
resources

What are Azure AD Licenses?

- Azure Active Directory Free
- Azure Active Directory Premium P1
- Azure Active Directory Premium P2
- Pay As You Go feature licenses

Azure AD Editions

Feature	Free	Microsoft 365 Apps	Premium P1	Premium P2
Directory Objects	500,000	Unlimited	Unlimited	Unlimited
Single Sign-on	Unlimited	Unlimited	Unlimited	Unlimited
Core Identity and Access Management	X	X	X	X
Business-to-business Collaboration	X	X	X	X
Identity and Access Management for Microsoft 365 apps		X	X	X
Premium Features			X	X
Hybrid Identities			X	X
Advanced Group Access Management			X	X
Conditional Access			X	X
Identity Protection				X
Identity Governance				X

What is Tenant in Azure AD?

- An Azure AD tenant is a reserved Azure AD service instance that an organization receives and owns once it signs up for a Microsoft cloud service such as - Azure, Microsoft Intune, or Microsoft 365
- Each tenant represents an organization, and is distinct and separate from other Azure AD tenants

Azure AD Features

- Application Management
- Authentication
- Azure Active Directory For Developers
- Business-to-Business (B2B)
- Business-to-customer(B2B)
- Conditional Access
- Device Management
- Domain Services
- Enterprise users
- Hybrid Identity
- Identity Governance
- Identity Protection
- Managed Identities for Azure Resources
- Privileged Identity Management (PIM)
- Reports and Monitoring

Azure AD Features

Category	Description
Application management	Manage your cloud and on-premises apps using Application Proxy, single sign-on, the My Apps portal, and Software as a Service (SaaS) apps. For more information,
Authentication	Manage Azure Active Directory self-service password reset, Multi-Factor Authentication, custom banned password list, and smart lockout. For more information,
Azure Active Directory for developers	Build apps that sign in all Microsoft identities, get tokens to call Microsoft Graph, other Microsoft APIs, or custom APIs.
Business-to-Business (B2B)	Manage your guest users and external partners, while maintaining control over your own corporate data. For more information.
Business-to-Customer (B2C)	Customize and control how users sign up, sign in, and manage their profiles when using your apps. For more information, see Azure Active Directory B2C documentation.
Conditional Access	Manage access to your cloud apps. For more information, see Azure AD Conditional Access documentation.

Azure AD Features

Category	Description
Device Management	Manage how your cloud or on-premises devices access your corporate data
Domain services	Join Azure virtual machines to a domain without using domain controllers.
Enterprise users	Manage license assignments, access to apps, and set up delegates using groups and administrator roles. For more information
Hybrid identity	Use Azure Active Directory Connect and Connect Health to provide a single user identity for authentication and authorization to all resources, regardless of location (cloud or on-premises)
Identity governance	Manage your organization's identity through employee, business partner, vendor, service, and app access controls. You can also perform access reviews.

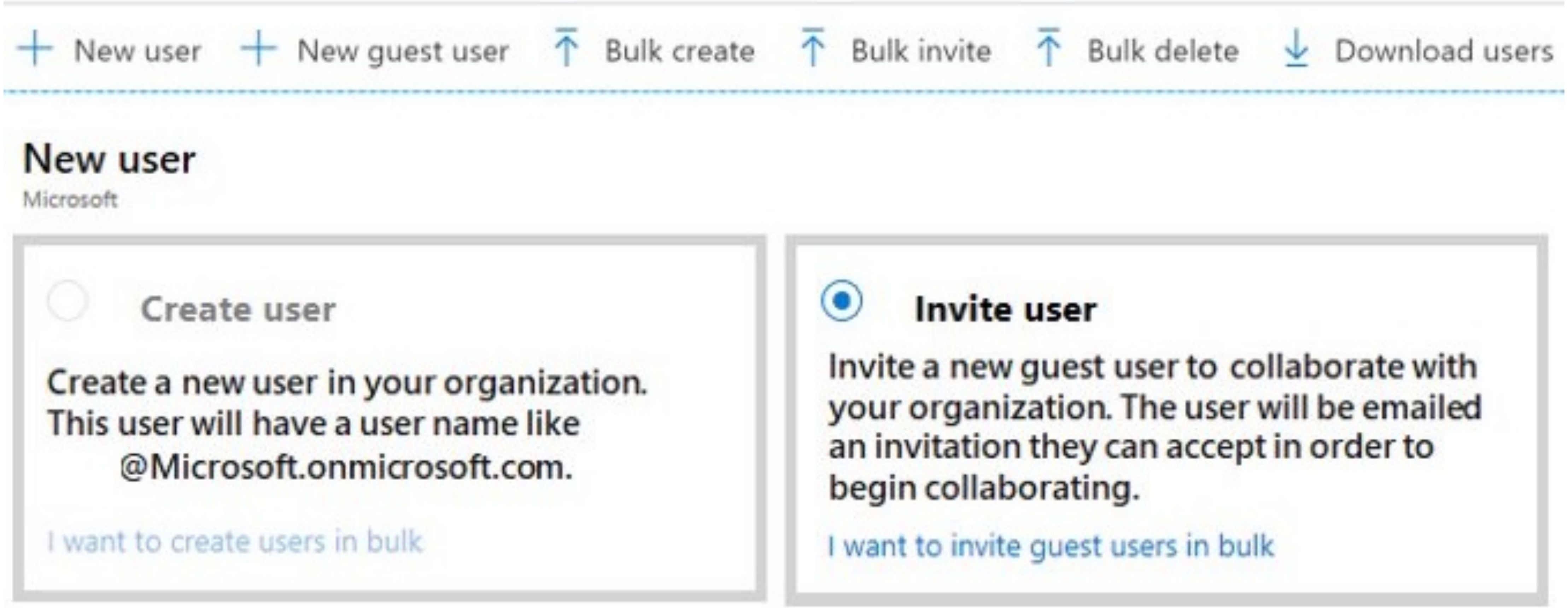
Azure AD Features

Category	Description
Identity Protection	Detect potential vulnerabilities affecting your organization's identities, configure policies to respond to suspicious actions, and then take appropriate action to resolve them.
Managed identities for Azure resources	Provide your Azure services with an automatically managed identity in Azure AD that can authenticate any Azure AD-supported authentication service, including Key Vault. For more information
Privileged identity management (PIM)	Manage, control, and monitor access within your organization. This feature includes access to resources in Azure AD and Azure, and other Microsoft Online Services, like Microsoft 365 or Intune
Reports and monitoring	Gain insights into the security and usage patterns in your environment

Users and Groups in Azure AD

User account	Description
Cloud identity	A user account with a cloud identity is defined only in Azure AD. This type of user account includes administrator accounts and users who are managed as part of your organization. A cloud identity can be for user accounts defined in your Azure AD organization, and also for user accounts defined in an external Azure AD instance. When a cloud identity is removed from the primary directory, the user account is deleted.
Directory-synchronized identity	User accounts that have a directory-synchronized identity are defined in an on-premises Active Directory. A synchronization activity occurs via Azure AD Connect to bring these user accounts in to Azure. The source for these accounts is Windows Server Active Directory.
Guest user	Guest user accounts are defined outside Azure. Examples include user accounts from other cloud providers, and Microsoft accounts like an Xbox LIVE account. The source for guest user accounts is Invited user. Guest user accounts are useful when external vendors or contractors need access to your Azure resources.

Users creation in Azure AD



New user

Microsoft

○ Create user

Create a new user in your organization. This user will have a user name like @Microsoft.onmicrosoft.com.

I want to create users in bulk

● Invite user

Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.

I want to invite guest users in bulk