Introduction to Azure AD

What Is Azure Active Directory?

Azure Active Directory (Azure AD) is Microsoft's multi-tenant cloud based directory and identity management service.

Azure AD also includes a full suite of

- identity management capabilities including multi-factor authentication,
- device registration,
- self-service password management,
- self-service group management,
- privileged account management,
- role based access control,
- application usage monitoring,
- rich auditing and security monitoring and alerting.

These capabilities can help secure cloud based applications, streamline IT processes, cut costs and help assure corporate compliance goals are met.

What are the benefits of Azure AD?

Your organization can use Azure AD to improve employee productivity, streamline IT processes, improve security and cut costs in many ways:

- Quickly adopt cloud services, providing employees and partners with an easy single-sign on experience powered by Azure AD's fully automated SaaS app access management and provisioning services capabilities.
- Empower employees with access to world class cloud apps and service and self-services capabilities from wherever they need to work on the devices they love to use.
- Easily and securely manage employee and vendor access to your corporate social media accounts.
- Improve application security with Azure AD multifactor authentication and conditional access.
- Implement consistent, self-service application access management, empowering business owners to move quickly while cutting IT costs and overhead.
- Monitor application usage and protect your business from advanced threats with security reporting and monitoring.
- Secure mobile (remote) access to on-premises applications.

Azure AD Features Free, Basic, and Premium editions

		Azure Active Directory Free	Azure Active Directory Basic	Azure Active Directory Premium	Office 365 apps only
Common features	Directory objects[1]	500,000 object limit	No object limit	No object limit	No object limit for Office 365 user accounts
	User/group management (add/update/delete)/user-based provisioning, device registration	Yes	Yes	Yes	Yes
	SSO to SAAS apps/custom apps/application proxy apps	10 apps per user[2]	10 apps per user[2]	No limit	10 apps per user[2]
	Self-service password change for cloud users	Yes	Yes	Yes	Yes
	Connect (sync engine that extends on-premises directories to Azure Active Directory)	Yes	Yes	Yes	Yes
	Preview: B2B collaboration	Yes	Yes	Yes	Yes
	Security/usage reports	Basic reports	Basic reports	Advanced reports	Basic reports
Premium + Basic features	Group-based access management/provisioning		Yes	Yes	
	Self-service password reset for cloud users		Yes	Yes	Yes
	Company branding (logon pages/access panel customization)		Yes	Yes	Yes
	Application proxy		Yes	Yes	
	SLA 99.9%		Yes	Yes	Yes
Premium features	Self-service group management/self-service application addition/ dynamic group membership			Yes	

	Self-service password reset/change/unlock with on-premises write-back			Yes	
	Multi-factor authentication (cloud and on-premises (MFA server))			Yes	Limited cloud only for Office 365 Apps
	MIM CAL + MIM Server3			Yes	
	Cloud app discovery			Yes	
	Connect Health			Yes	
	Automatic password rollover for group accounts			Yes	
	Preview: Conditional access			Yes	
	Preview: Privileged identity management			Yes	
Windows 10 + Azure AD Join related features	Join a Windows 10 device to Azure AD, Desktop SSO, Microsoft Passport for Azure AD, Administrator Bitlocker recovery	Yes	Yes	Yes	Yes
Windows 10 + Azure AD Join related features	MDM auto-enrolment, Self-Service Bitlocker recovery, additional local administrators to Windows 10 devices via Azure AD Join			Yes	

1Default usage quota is 150,000 objects. An object is an entry in the directory service, represented by its unique distinguished name. An example of an object is a user entry used for authentication purposes. If you need to exceed this default quota, please contact support. The 500K object limit does not apply for Office 365, Microsoft Intune or any other Microsoft paid online service that relies on Azure Active Directory for directory services.

2With Azure AD Free and Azure AD Basic, end users who have been assigned access to SaaS apps, can see up to 10 apps in their Access panel and get SSO access to them. Admins can configure SSO and assign user access to as many SaaS apps as they want with Free and Basic however, end users will only see 10 apps in their Access panel at a time.

3Microsoft Identity Manager Server software rights are granted with Windows Server licenses (any edition). Since Microsoft Identity Manager runs on Windows Server OS, as long as the server is running a valid, licensed copy of Windows Server, then Microsoft Identity Manager can be installed and used on that server. No other separate license is required for Microsoft Identity Manager Server.

Azure AD Capabilities

We will talk and discuss each of the following capabilities later on in the next blogposts, will try to practice them on my tenant.

- B2B collaboration.
- Azure Active Directory Connect.
- Connect Health, is an Azure AD Premium feature.
- Cloud App Discovery.
- Company branding.
- Group-based application access.
- Self-service password reset.
- Self-service group management.
- Advanced security reports and alerts.
- Multi-Factor Authentication.
- Microsoft Identity Manager.
- Azure Active Directory Application Proxy.
- Password reset with write-back.
- Enterprise SLA of 99.9%.