Describe Azure AD

Azure AD is MS's cloud-based identity and access management service. Covers:

- Internal resources (apps on corp network, cloud apps)
- External services (M365, Azure portal, any SaaS apps used by org)

Simplifies the way you manage auth and access by providing a single identity system for cloud and on-prem apps.

Available Azure AD Editions

Azure AD Free:

- Administer users and create groups
- Create basic reports
- Configure SSPR
- Enable SSO across Azure, M365 and other SaaS apps
- Is included with subscriptions to Office 365, Azure, Dynamics 365, Intune, Power Platform

Office 365 Apps:

- All of the above included in Free
- Two way sync between on-prem directories and Azure AD
- Is included in subscriptions to Office 365 E1, E3, E5, F1, and F3

Azure AD Premium P1:

- Includes all above
- Supports advanced administration (dynamic groups, self-service group management, MS Identity Manager)

Azure AD Premium P2:

- Includes all above
- Azure AD Identity Protection

- PIM

Azure AD Identity Types

User

Representation of something that's managed by Azure AD. Employees and guests are represented as users in Azure AD. If you have several users with the same access needs, create a group.

Service Principal

Essentially an identity for an application. For an application to delegate its identity and access functions to Azure AD, it must be registered to enable its integration. When registered, a service principle is created in each Azure AD tenant where the application is used.

Managed Identity

A type of service principal that are automatically generated in Azure AD and remove the need for developers to manage credentials. Provides an identity for apps to use when connecting to Azure resources that support Azure AD auth.

Two types of managed identity:

- System assigned: some Azure services allow you to enable managed identity directly on service instance, which is tied to its lifecycle. When you delete the resource, the identity goes with it. Only that Azure resource can use the identity to request tokens from Azure AD
- User assigned: You can create a managed identity as a standalone resource. This can then be assigned to one or more instances of an Azure service. The identity is then managed separately from the resources using it.

Device

Azure AD Registered

Provide users with support for BYOD, meaning they can access company resources on personal devices without needing an organisation account to sign in.

Azure AD Joined

A device joined to Azure AD via an organisational account (also used to sign in to the device itself).

Hybrid Azure AD joined

Organisations with existing on-prem AD implementations can benefit from Azure AD functionality. They are joined to the on.prem AD and Azure AD requiring org acccount sign in.

Both Registered and Joined allows SSO to cloud-baed resources. Intune can be used for MDM to control how devices are used.

Types of External Identities

A set of capabilities enabling organisations to allow access to external users such as customers or partners. Customers and partners can "bring their own identities" to sign in. Admins can set up federation with identity providers so external users can sign in with existing social or enterprise accounts rather than creating a separate one just for your application.

Two different Azure AD External Identities: B2B and B2C.

B2B

Azure AD B2B allows you to share your orgs apps and services with guests from other orgs whilst maintaining control over your own data. By accepting an invite they complete the same flow as your own orgs employees so tey can call be managed the same way and added to the same groups. SSO to all Azure AD connected apps supported.

B2C

A Customer Identity Access Management (CIAM) solution. It allows external uers to sign in with their preferred social, enterprise or local account identities to get SSO to your apps.

External users are managed in the Azure AD B2C directory separate from the organisations employee and partner directory.

Azure AD External Identities is a feature of Premium P1 and P2 editions. Pricing is based on Monthly Active Users.

Hybrid Identity

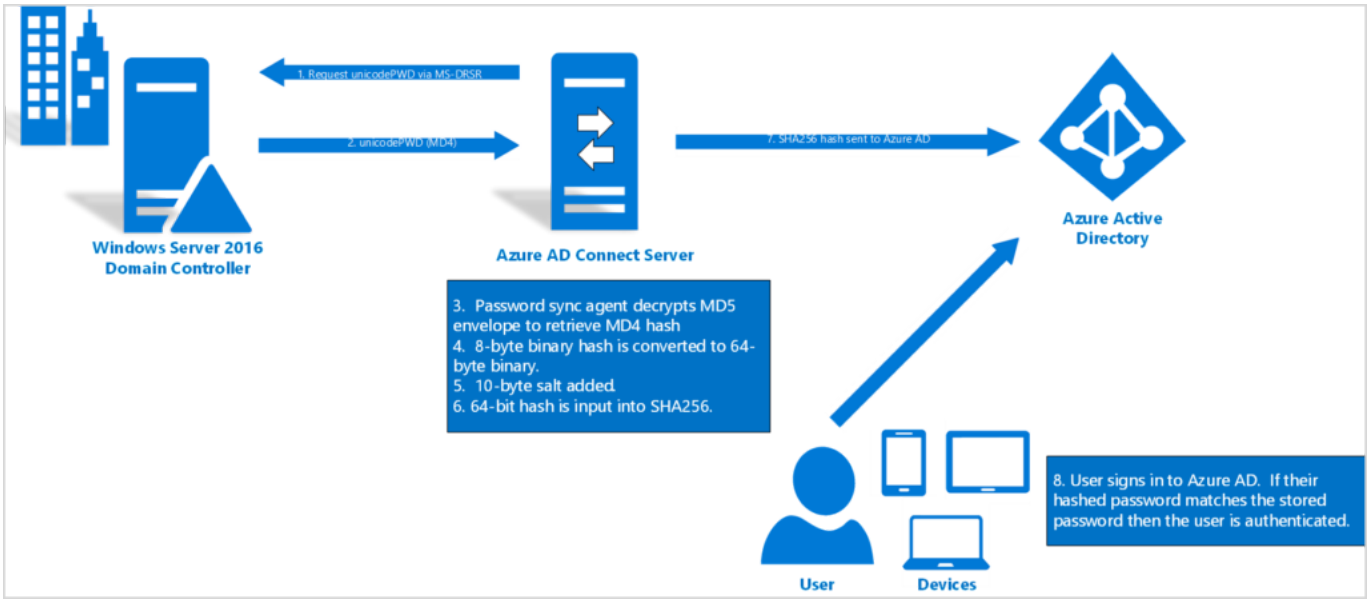
A way to create a common user identity for authentication and auth to all resources regardless of location.

It is important to determine the right authentication method because it acts as the foundation for the organisations' IT infra. Once a method is chosen it is difficult and disruptive to users to change.

There are many was of hybrid identity auth:

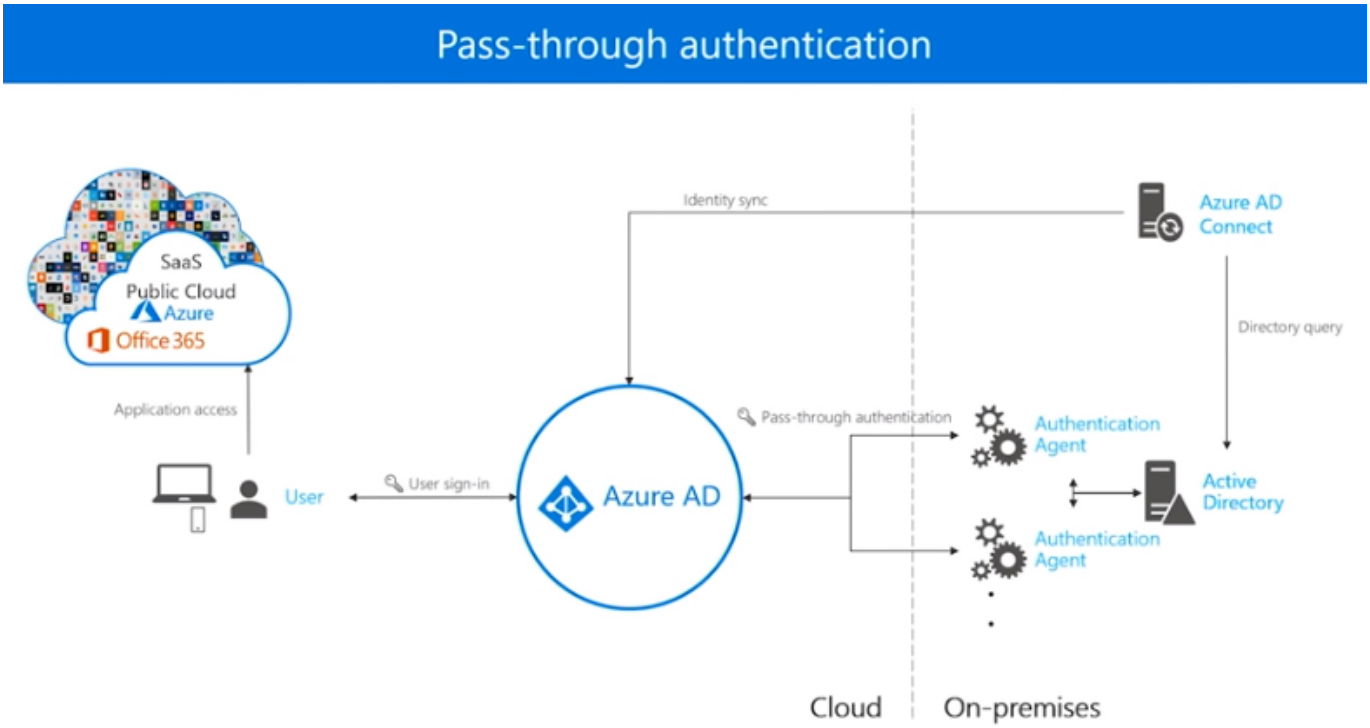
Azure AD Password hash sync (PHS)

The simplest way of authentication for on-prem directory objects in Azure AD. Users can sign into Azure AD services using the same credentials used to sign into their on-prem AD. Azure AD handles the sign-in process.



Azure AD Pass-through auth

Allows users to sign into both on-prem and cloud based apps using hte same passwords (similar to PHS). The key difference from PHS is that the users password is validated directly against on.prem AD (no cloud involved). Important for orgs who want to enforce their own on-prem AD security and password policies.



Federated auth

Recommended for orgs that have advanced features not currently supported in Azure AD including sign-on using smart cards or certificates, on-prem MFA server or sign on using third party authentication.

Azure AD hands off the authentication process to a separate trusted system such as on-prem AD Federation services (AD FS) to validate the password. This method ensures all user authentication happens on-prem.

Those using Federation with AD FS can optionally set up PHS as backup incase AD FS infra fails.

Federated Authentication