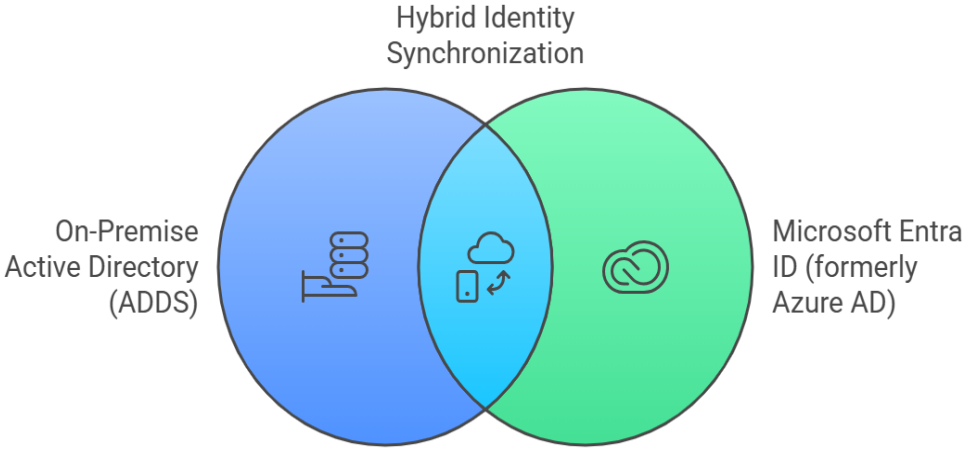
Identities in Microsoft Entra ID

examlabpractice.com

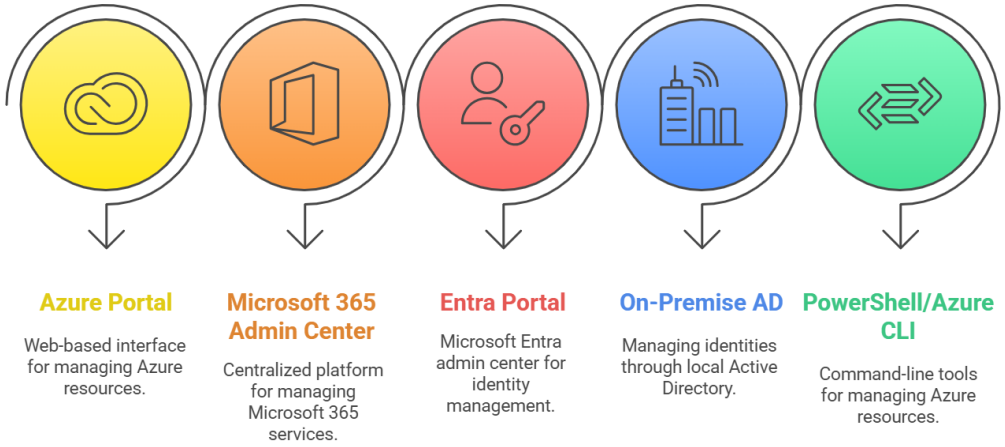
Microsoft’s Identity Based Management System

- You’ll see the term identity vs account these days
- Entra ID (formerly Azure AD) is the central directory services store
- Identities can be sync’d with your on premise Active Directory (ADDS)



The Multiple ways to Manage Identities

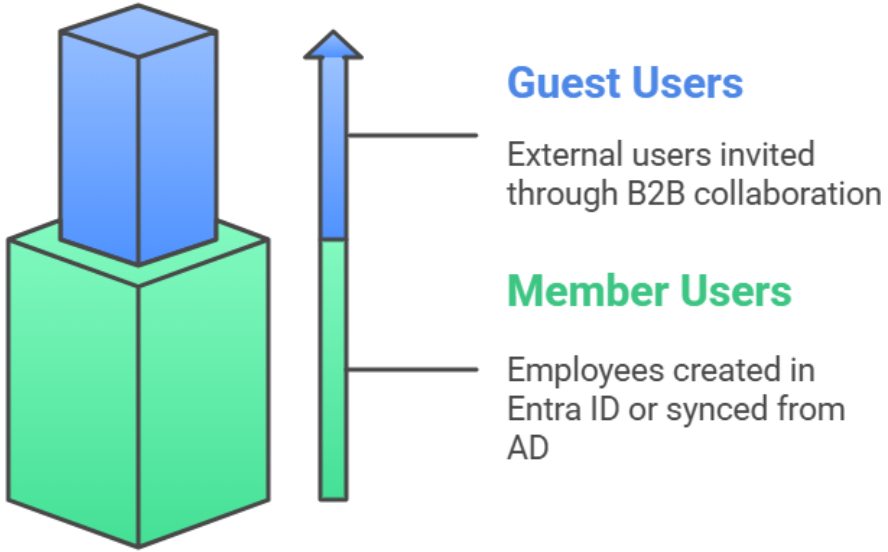
- Azure Portal (portal.azure.com)
- Microsoft 365 Admin Center (admin.microsoft.com)
- Entra Portal (entra.Microsoft.com)
- On-Premise Active Directory Domain Services with account sync through Azure AD Connect
- PowerShell / Azure CLI (Bash)



User Identities

These are human users who access Microsoft services.

- **Member users**: Typically, employees created directly in Entra ID or synced from on-premises Active Directory.
- **Guest users**: External users invited through B2B collaboration. Their identity is managed in their home directory but granted limited access.



Service Principals

These represent applications or services that need to authenticate and access resources.

- Created automatically when an app is registered in Entra ID.
- Used for assigning permissions, running automation, or secure access without human interaction.

Example: A web app that needs to read/write from Microsoft Graph or access Azure Key Vault.

Application Authentication

Ensures secure access for applications and services

Automated Permissions

Facilitates permission assignments without human intervention

Secure Access

Provides secure resource access without human interaction

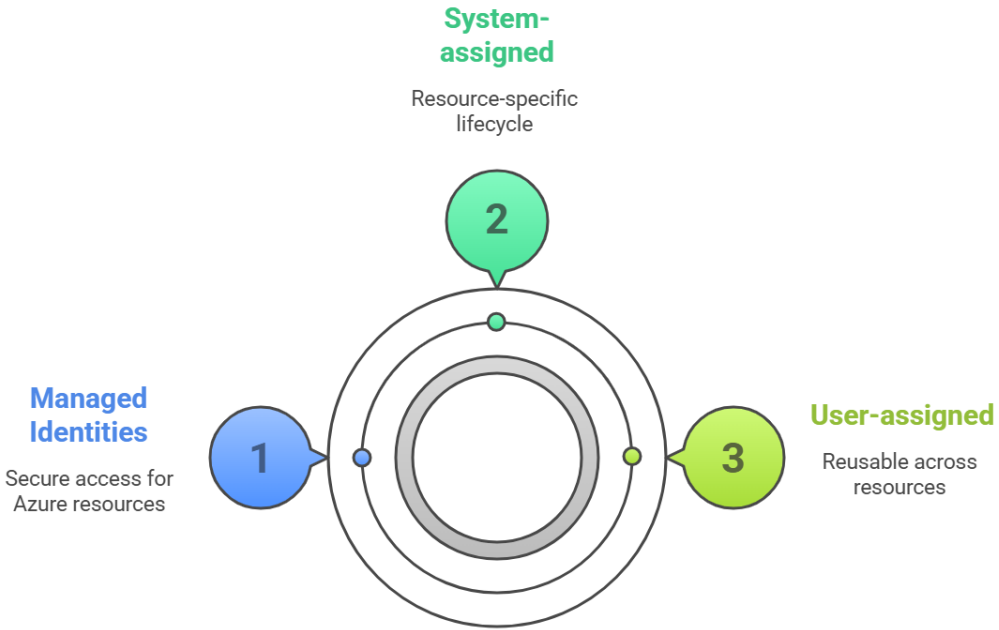
Managed Identities

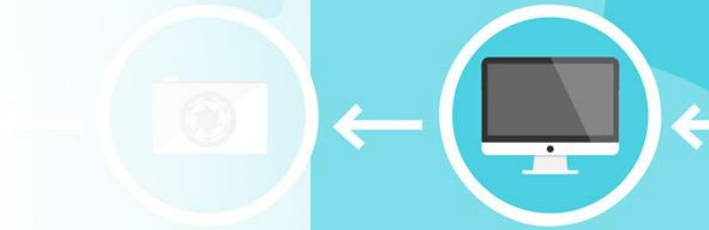
These are special identities for Azure resources (like VMs or Function Apps) to access other Azure services securely — without storing credentials.

Two types:

- System-assigned: Tied to one resource; lifecycle matches the resource.
- User-assigned: Standalone identity reusable across multiple resources

Example: An Azure VM accessing a storage account using a system-assigned identity.





Device Identities

Each device that joins Microsoft Entra ID (or is hybrid-joined) gets an identity.

- Used for Conditional Access, compliance, and Intune management.
- Devices can be:
  - Entra ID joined
  - Hybrid AD joined
  - Entra ID registered (BYOD)