**Compare Active Directory to Microsoft Entra ID**

|  |  |  |
| --- | --- | --- |
| **Concept** | **Windows Server Active Directory** | **Microsoft Entra ID** |
| Users |  |  |
| Provisioning: users | Organizations create internal users manually or use an in-house or automated provisioning system, such as the Microsoft Identity Manager, to integrate with an HR system. | Existing Microsoft Windows Server Active Directory organizations use [Microsoft Entra Connect](https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-sync-whatis) to sync identities to the cloud.  Microsoft Entra ID adds support to automatically create users from [cloud HR systems](https://learn.microsoft.com/en-us/entra/identity/app-provisioning/what-is-hr-driven-provisioning).  Microsoft Entra ID can provision identities in [System for Cross-Domain Identity Management (SCIM) enabled](https://learn.microsoft.com/en-us/entra/identity/app-provisioning/use-scim-to-provision-users-and-groups) software as a service (SaaS) apps to automatically provide apps with the necessary details to allow access for users. |
| Provisioning: external identities | Organizations create external users manually as regular users in a dedicated external Microsoft Windows Server Active Directory forest, resulting in administration overhead to manage the lifecycle of external identities (guest users) | Microsoft Entra ID provides a special class of identity to support external identities. [Microsoft Entra B2B](https://learn.microsoft.com/en-us/entra/external-id/) will manage the link to the external user identity to make sure they are valid. |
| Entitlement management and groups | Administrators make users members of groups. App and resource owners then give groups access to apps or resources. | [Groups](https://learn.microsoft.com/en-us/entra/fundamentals/how-to-manage-groups) are also available in Microsoft Entra ID and administrators can also use groups to grant permissions to resources. In Microsoft Entra ID, administrators can assign membership to groups manually or use a query to dynamically include users to a group.  Administrators can use [Entitlement management](https://learn.microsoft.com/en-us/entra/id-governance/entitlement-management-overview) in Microsoft Entra ID to give users access to a collection of apps and resources using workflows and, if necessary, time-based criteria. |
| Admin management | Organizations will use a combination of domains, organizational units, and groups in Microsoft Windows Server Active Directory to delegate administrative rights to manage the directory and resources it controls. | Microsoft Entra ID provides [built-in roles](https://learn.microsoft.com/en-us/entra/fundamentals/how-subscriptions-associated-directory) with its Microsoft Entra role-based access control (RBAC) system, with limited support for [creating custom roles](https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/custom-overview) to delegate privileged access to the identity system, the apps, and resources it controls.  Managing roles can be enhanced with [Privileged Identity Management (PIM)](https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-configure) to provide just-in-time, time-restricted, or workflow-based access to privileged roles. |
| Credential management | Credentials in Active Directory are based on passwords, certificate authentication, and smart card authentication. Passwords are managed using password policies that are based on password length, expiry, and complexity. | Microsoft Entra ID uses intelligent [password protection](https://learn.microsoft.com/en-us/entra/identity/authentication/concept-password-ban-bad) for cloud and on-premises. Protection includes smart lockout plus blocking common and custom password phrases and substitutions.  Microsoft Entra ID significantly boosts security [through multifactor authentication](https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mfa-howitworks) and [passwordless](https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-passwordless) technologies, like FIDO2.  Microsoft Entra ID reduces support costs by providing users a [self-service password reset](https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-howitworks) system. |