Azure Identity and access management (IAM)

Secure access to your resources with Azure identity and access management solutions. Protect your applications and data at the front gate with Azure identity and access management solutions. Defend against malicious login attempts and safeguard credentials with risk-based access controls, identity protection tools, and strong authentication options—without disrupting productivity.

Azure Active Directory (Azure AD) is the Azure solution for identity and access management. Azure AD is a multitenant, cloud-based directory and identity management service from Microsoft. It combines core directory services, application access management, and identity protection into a single solution.

Cloud-based identity and mobile device management that provides user account and authentication services for resources such as Office 365, the Azure portal, or SaaS applications. Azure AD can be synchronized with an on-premises AD DS environment to provide a single identity to users that works natively in the cloud.

Azure AD offers some of the same features in the cloud, as AD DS offers on-premises. However, just because they both have AD in their names, doesn't mean they are identical services. Azure AD is a cloud-based identity service that offers the following:

- Cloud-based identification & authentication
- User and computer management
- Mobile Device Management (MDM)
- Access to Software as a service (SaaS) applications, Microsoft Azure portal, and Office 365 services

Because Azure AD is hosted and managed by Microsoft in the cloud, organizations don't have direct access to AD domain controllers the way they do in their on-premises environment. Microsoft exposes parts of the Azure AD to organizations through the web-based interface so they have enough control to run and customize the services, but Microsoft is responsible for managing the services and servers behind the scenes in its datacenters across the globe.