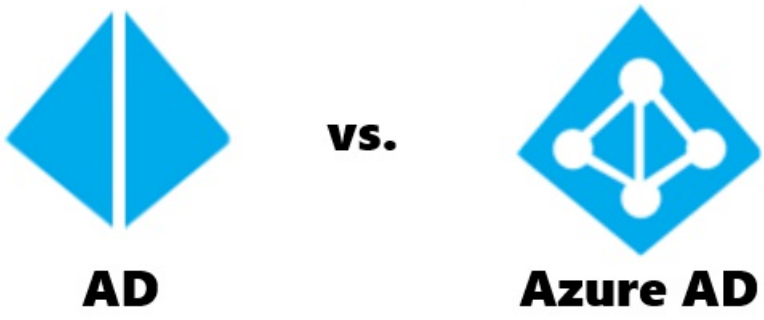
Difference between Azure AD vs Active Directory (AD)

Ajay Chadha

Table of Contents

Are you confused about the difference between Active Directory (AD) vs Azure AD? In this article, we'll explore the key differences between Active Directory (AD) and the Azure Active Directory (Azure AD).



To begin, it is important to understand that Azure AD is NOT the cloud replacement for Active Directory. Rather, Azure AD works on top of Active Directory implementations primarily to provide single sign-on (SSO) access to a variety of SaaS applications like Office 365, Salesforce, DropBox, and many others as well as being the user management system for Azure. In essence, it is designed as a bridge between your existing legacy Active Directory instance and Microsoft's catalog of compatible cloud-delivered services. While it is possible to sync your Active Directory instance with Azure AD, in itself Azure AD is not a complete cloud-based directory service.

This is because Azure AD does not act as the authoritative source of truth of user identities (unless you are just using Office 365 or Azure resources). This role is still within the domain of Active Directory for many organizations, thus requiring traditional on-prem devices and dedicated IT staff to create and maintain. While Azure AD is meant to be a cloud identity platform, unfortunately, the true source of identity management is still firmly grounded with the legacy directory service, Active Directory.

What Is Active Directory (AD)?

In order to understand what Active Directory is, you'll need to understand the basics of a Domain Controller. A Domain Controller is a server on the network that centrally manages access for users, PCs, and servers on the network. It does this using AD.

Active Directory is a database that organizes your company's users and computers. It provides authentication and authorization to applications, file services, printers, and other resources on the network. It uses protocols such as Kerberos and NTLM for authentication and LDAP to query and modify items in the Active Directory databases.

Key Functions of Active Directory (AD)

Active Directory Domain Services run on the Domain Controller and have the following key functions:

- Secure Object store, including Users, Computers and Groups
- Object organization – Organisational Units (OU), Domains and Forests
- Common Authentication and Authorization provider
- LDAP, NTLM, Kerberos (secure authentication between domain-joined devices)
- Group Policy – for fine-grained control and management of PCs and Servers on the domain

So basically AD has a record of all your users, PCs, and Servers and authenticates the users signing in (the network logon). Once signed in, AD also governs what the users are, and are not, allowed to do or access (authorization). For example, it knows that John Smith is in the Sales Group and is not allowed to access the HR folder on the file server. It also allows control and management of PCs and Servers on the network via Group Policy (so for example you could set all users' home page on their browser to be your intranet, or you can prevent users from installing other software, etc).

Most established businesses will have AD running on one or more Domain Controllers on their network.

What is an Azure Active Directory?

Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service, which helps your employees sign in and access resources in:

- External resources, such as Microsoft 365, the Azure portal, and thousands of other SaaS applications.
- Internal resources, such as apps on your corporate network and intranet, along with any cloud apps developed by your own organization.

Azure Active Directory is the next evolution of identity and access management solutions for the cloud. Microsoft introduced Active Directory Domain Services in Windows 2000 to give organizations the ability to manage multiple on-premises infrastructure components and systems using a single identity per user. Azure AD takes this approach to the next level by providing organizations with an Identity as a Service (IDaaS) solution for all their apps across the cloud and on-premises.

Azure AD is a multi-tenant cloud-based identity and access management solution for the Azure platform. Active Directory (AD) is great at managing traditional on-premise infrastructure and applications. Azure AD is great at managing user access to cloud applications. You can use both together, or if you want to have a purely cloud-based environment you can just use Azure AD.

What are the benefits of Azure Active Directory over AD?

Azure AD is not simply a cloud version of AD as the name might suggest. Although it performs some of the same functions, it is quite different. Azure Active Directory is a secure online authentication store, which can contain users and groups. Users have a username and a password which are used when you sign in to an application that uses Azure AD for authentication. So for example all of the Microsoft Cloud services use Azure AD for authentication: Office 365, Dynamics 365, and Azure. If you have Office 365, you are already using Azure AD under the covers.

As well as managing users and groups, Azure AD manages access to applications that work with modern authentication mechanisms like SAML and OAuth. Applications are an object that exists in Azure AD, and this allows you to create an identity for your applications (or 3rd party ones) that you can grant access to users to. Besides seamlessly connecting to any Microsoft Online Services, Azure AD can connect to thousands of SaaS applications (e.g. Salesforce, Slack, etc) using a single sign-on.

When compared with AD, here is what Azure AD doesn't do:

- You can't join a server to it
- You can't join a PC to it in the same way – there is Azure AD Join for Windows 10 only (see later)
- There is no Group Policy
- There is no support for LDAP, NTLM, or Kerberos
- It is a flat directory structure – no OU's or Forests

So Azure AD does not replace AD. Active Directory (AD) is great at managing traditional on-premise infrastructure and applications. Azure AD is great at managing user access to cloud applications. They do different things with the area of overlap being user management.

Active Directory vs Azure Active Directory

Most IT administrators are familiar with Active Directory Domain Services concepts. The following table outlines the differences and similarities between Active Directory concepts and Azure Active Directory.

Comparison Table

Concept	Active Directory (AD)	Azure Active Directory
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 AD organizations use Azure AD Connect to sync identities to the cloud. Azure AD adds support to automatically create users from cloud HR systems. Azure AD can provision identities in SCIM enabled 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 AD forest, resulting in administration overhead to manage the lifecycle of external identities (guest users)	Azure AD provides a special class of identity to support external identities. Azure AD B2B will manage the link to the external user identity to make sure they are valid.

Forbidden

You don't have permission to access this resource.

Additionally, a 403 Forbidden error was encountered while trying to use an ErrorDocument to handle the request.

Concept	Active Directory (AD)	Azure Active Directory
Entitlement management and groups	Administrators make users members of groups. App and resource owners then give groups access to apps or resources.	Groups are also available in Azure AD and administrators can also use groups to grant permissions to resources. In Azure AD, administrators can assign membership to groups manually or use a query to dynamically include users to a group. Administrators can use Entitlement management in Azure AD 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 AD to delegate administrative rights to manage the directory and resources it controls.	Azure AD provides built-in roles with its Azure AD role-based access control (Azure AD RBAC) system, with limited support for creating custom roles to delegate privileged access to the identity system, the apps, and resources it controls. Managing roles can be enhanced with Privileged Identity Management (PIM) to provide just-in-time, time-restricted, or workflow-based access to privileged roles.
Credential management	Credentials in Active Directory is based on passwords, certificate authentication, and smartcard authentication. Passwords are managed using password policies that are based on password length, expiry, and complexity.	Azure AD uses intelligent password protection for cloud and on-premises. Protection includes smart lockout plus blocking common and custom password phrases and substitutions. Azure AD significantly boosts security through Multi-factor authentication and passwordless technologies, like FIDO2. Azure AD reduces support costs by providing users a self-service password reset system.
Apps		
Infrastructure apps	Active Directory forms the basis for many infrastructure on-premises components, for example, DNS, DHCP, IPSec, WiFi, NPS, and VPN access	In a new cloud world, Azure AD is the new control plane for accessing apps versus relying on networking controls. When users authenticate, Conditional access (CA), will control which users, will have access to which apps under required conditions.
Traditional and legacy apps	Most on-premises apps use LDAP, Windows-Integrated Authentication (NTLM and Kerberos), or Header-based authentication to control access to users.	Azure AD can provide access to these types of on-premises apps using Azure AD application proxy agents running on-premises. Using this method Azure AD can authenticate Active Directory users on-premises using Kerberos while you migrate or need to coexist with legacy apps.
SaaS apps	Active Directory doesn't support SaaS apps natively and requires a federation system, such as AD FS.	SaaS apps supporting OAuth2, SAML, and WS-* authentication can be integrated to use Azure AD for authentication.
Line of business (LOB) apps with modern authentication	Organizations can use AD FS with Active Directory to support LOB apps requiring modern authentication.	LOB apps requiring modern authentication can be configured to use Azure AD for authentication.
Mid-tier/Daemon services	Services running in on-premises environments normally use AD service accounts or group Managed Service Accounts (gMSA) to run. These apps will then inherit the permissions of the service account.	Azure AD provides managed identities to run other workloads in the cloud. The lifecycle of these identities is managed by Azure AD and is tied to the resource provider can't be used for other purposes to gain backdoor access.

403

Forbidden

You don't have permission to access this resource.

Additionally, a 403 Forbidden error was encountered while trying to use an ErrorDocument to handle the request.

Devices Concept	Active Directory (AD)	Azure Active Directory
Mobile	Active Directory doesn't natively support mobile devices without third-party solutions.	Microsoft's mobile device management solution, Microsoft Intune, is integrated with Azure AD. Microsoft Intune provides device state information to the identity system to evaluate during authentication.
Windows desktops	Active Directory provides the ability to domain join Windows devices to manage them using Group Policy, System Center Configuration Manager, or other third-party solutions.	Windows devices can be joined to Azure AD. Conditional access can check if a device is Azure AD joined as part of the authentication process. Windows devices can also be managed with Microsoft Intune. In this case, conditional access will consider whether a device is compliant (for example, up-to-date security patches and virus signatures) before allowing access to the apps.
Windows servers	Active Directory provides strong management capabilities for on-premises Windows servers using Group Policy or other management solutions.	Windows servers virtual machines in Azure can be managed with Azure AD Domain Services. Managed identities can be used when VMs need access to the identity system directory or resources.
Linux/Unix workloads	Active Directory doesn't natively support non-Windows without third-party solutions, although Linux machines can be configured to authenticate with Active Directory as a Kerberos realm.	Linux/Unix VMs can use managed identities to access the identity system or resources. Some organizations, migrate these workloads to cloud container technologies, which can also use managed identities.

AD vs Azure AD – Which one should you use?

If you have a traditional on-premise set up with AD and also want to use Azure AD to manage access to cloud applications (e.g. Office 365 or any of thousands of SaaS apps) then you can happily use both.

If you are using Office 365 then your users will have a username and password for that (managed by Azure AD), as well as a username and password for their network logon (managed by AD). These two sets of credentials are un-related. This is fine and just means that if you have a password change policy that users will have to do this twice (and they could of course choose the same password for both).

Or you can synchronize AD with Azure AD so that the users only have one set of credentials which they use for both their network login and access to Office 365. You use Azure AD Connect to do this, it is a small free piece of Microsoft software that you install on a server to perform the synchronization.

If you are a new business or one that is looking to transition away from having any traditional on-premise infrastructure and using purely cloud-based applications, then you can operate purely using Azure AD.

AD vs Azure AD Summary

To summarize, Azure AD is not simply a cloud version of AD, they do quite different things. AD is great at managing traditional on-premise infrastructure and applications. Azure AD is great at managing user access to cloud applications. You can use both together, or if you want to have a purely cloud-based environment you can just use Azure AD.

Frequently Asked Questions about Azure AD

Here are some of the commonly asked questions about Azure AD vs AD.

Can Azure AD replace Active Directory?

Azure AD is not a replacement for Active Directory. Azure Active Directory is not designed to be the cloud version of Active

Directory. It is not a domain controller or a directory in the cloud that will provide the exact same capabilities as AD.

Does Azure AD replace ADFS?

Microsoft released an update to Azure AD Connect in June 2017 called Seamless Single Sign-On (also known as SSO) that offers a simpler and more cost-effective SSO solution for Office 365 than ADFS.

Does Azure AD support LDAP?

To communicate with your Azure Active Directory Domain Services (Azure AD DS) managed domain, the Lightweight Directory Access Protocol (LDAP) is used. ... With Azure AD DS, you can configure the managed domain to use secure Lightweight Directory Access Protocol (LDAPS).

Is Azure AD SaaS or PaaS?

Office 365 is a SaaS, which provides an online version of MS Office Suite (Office Web Apps) along with SharePoint Server, Exchange Server, and Lync Server. Windows Azure is both IaaS and PaaS, which makes the Windows Server operating system and other features available as services.

Does Office 365 have an Active Directory?

Microsoft 365 uses Azure Active Directory (Azure AD), cloud-based user identity and authentication service that is included with your Microsoft 365 subscription, to manage identities and authentication for Microsoft 365.

Does Azure AD support SAML?

Azure AD uses a certificate to sign the SAML tokens it sends to the application. You need this certificate to configure the trust between Azure AD and the application.

Does Azure AD support OAuth?

Azure Active Directory (Azure AD) supports all OAuth 2.0 flows.

403 Forbidden

You don't have permission to access this resource.

Additionally, a 403 Forbidden error was encountered while trying to use an ErrorDocument to handle the request.