**Introduction**

Completed100 XP

* 1 minute

Transitioning workloads to the cloud involves more than just moving servers, websites, and data. Companies need to think about how to secure their resources and identify authorized users.

In this module, your company is planning to implement Azure Active Directory (Azure AD) and features like Azure AD Join and Self-Service Password Reset. You need to understand how to choose the Azure AD edition that works best for your organization, and explore how to implement required features.

**Learning objectives**

In this module, you learn how to:

* Define Azure AD concepts, including identities, accounts, and tenants.
* Describe Azure AD features to support different configurations.
* Understand differences between Azure AD and Active Directory Domain Services (AD DS).
* Choose between supported editions of Azure AD.
* Implement the Azure AD join feature.
* Use the Azure AD self-service password reset feature.

**Skills measured**

The content in the module helps you prepare for [Exam AZ-104: Microsoft Azure Administrator](https://learn.microsoft.com/en-us/certifications/exams/az-104). The module concepts are covered in:

Manage identities and governance in Azure (15-20%)

* Manage Azure Active Directory objects
  + Configure self-service password reset
  + Configure Azure AD join

**Prerequisites**

None.

**Next unit: Describe Azure Active Directory benefits and features**

**Describe Azure Active Directory benefits and features**

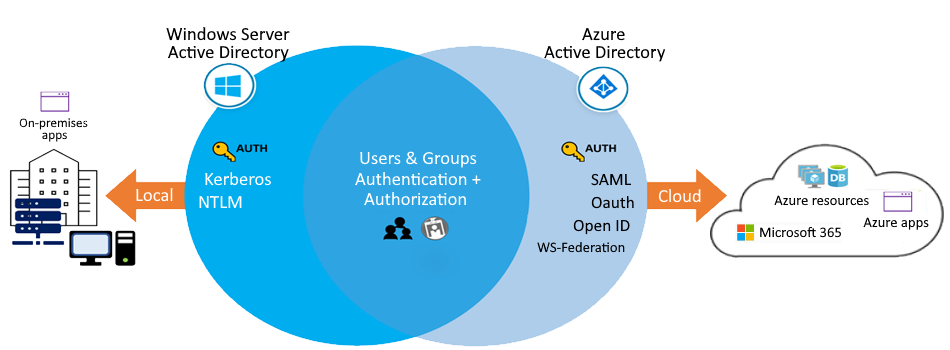
Completed100 XP

* 3 minutes

[Azure Active Directory (Azure AD)](https://learn.microsoft.com/en-us/azure/active-directory/) is Microsoft's multi-tenant cloud-based directory and identity management service. Azure AD helps to support user access to resources and applications, such as:

* Internal resources and apps located on your corporate network.
* External resources like Microsoft 365, the Azure portal, and SaaS applications.
* Cloud apps developed for your organization.

The following diagram shows an example implementation of Azure AD. In this scenario, Windows Server AD is using [Kerberos](https://learn.microsoft.com/en-us/windows-server/security/kerberos/kerberos-authentication-overview) and [NTLM authentication](https://learn.microsoft.com/en-us/windows-server/security/kerberos/ntlm-overview) to on-premises applications.



**Things to know about Azure AD features**

Let's examine some of the prominent features of Azure AD.

| **Azure AD feature** | **Description** |
| --- | --- |
| **Single sign-on (SSO) access** | Azure AD provides secure single sign-on (SSO) to web apps on the cloud and to on-premises apps. Users can sign in with the same set of credentials to access all their apps. |
| **Ubiquitous device support** | Azure AD works with iOS, macOS, Android, and Windows devices, and offers a common experience across the devices. Users can launch apps from a personalized web-based access panel, mobile app, Microsoft 365, or custom company portals by using their existing work credentials. |
| **Secure remote access** | Azure AD enables secure remote access for on-premises web apps. Secure access can include multifactor authentication (MFA), conditional access policies, and group-based access management. Users can access on-premises web apps from everywhere, including from the same portal. |
| **Cloud extensibility** | Azure AD can extend to the cloud to help you manage a consistent set of users, groups, passwords, and devices across environments. |
| **Sensitive data protection** | Azure AD offers unique identity protection capabilities to secure your sensitive data and apps. Admins can monitor for suspicious sign-in activity and potential vulnerabilities in a consolidated view of users and resources in the directory. |
| **Self-service support** | Azure AD lets you delegate tasks to company employees that might otherwise be completed by admins with higher access privileges. Providing self-service app access and password management through verification steps can reduce helpdesk calls and enhance security. |

**Things to consider when using Azure AD features**

Azure AD offers many features and benefits. Consider which features can be used to best support your corporate scenarios.

* **Consider enabling single sign-on access**. Enable SSO access for your users to connect to the cloud or use on-premises apps. Azure AD SSO supports Microsoft 365 and thousands of SaaS apps, such as Salesforce, Workday, DocuSign, ServiceNow, and Box.
* **Consider UX and device support**. Build a consistent user experience that works for all devices and directory access points. You can design custom company portals and personalized web-based access for your employees that lets them connect with their existing work credentials.
* **Consider benefits of secure remote access**. Protect your on-premises web apps by implementing secure remote access with MFA and access policies.
* **Consider advantages of cloud extensibility**. Connect Active Directory and other on-premises directories in the cloud to Azure AD in just a few steps. You can make it easier for your admins to manage the same users, groups, passwords, and devices across all supported environments.
* **Consider advanced protection for sensitive data**. Enhance the security of your sensitive data and apps by using the built-in protection features of Azure AD. Your admins can utilize advanced security reports, notifications, remediation recommendations, and risk-based policies.
* **Consider reduced costs, self-service options**. Take advantage of the Azure AD self-service features to help reduce costs for your organization. Delegate certain tasks like resetting passwords, or creating and managing groups to your non-admin users.

In the next unit, we explore the Azure AD concepts that make these features possible.

**Next unit: Describe Azure Active Directory concepts**

**Describe Azure Active Directory concepts**

Completed100 XP

* 2 minutes

To implement Azure Active Directory in your corporate configuration, you need to understand the key components of the service. The following table describes the main components and concepts of Azure AD and explains how they work together to support service features.

Graphical user interface, text, application, email

Description automatically generated

If you're a Microsoft 365, Azure, or Dynamics CRM Online customer, you might already be using Azure AD! Every Microsoft 365, Azure, and Dynamics CRM tenant is already an Azure AD tenant. You can start using your tenant to manage access to thousands of other cloud apps that integrate with Azure AD.

**Next unit: Compare Active Directory Domain Services to Azure Active Directory**

# Compare Active Directory Domain Services to Azure Active Directory

Completed100 XP

* 2 minutes

Active Directory Domain Services (AD DS) is the traditional deployment of Windows Server-based Active Directory on a physical or virtual server. AD DS is commonly considered to be primarily a directory service, but it's only one component of the Windows Active Directory suite of technologies. The suite also includes Active Directory Certificate Services (AD CS), Active Directory Lightweight Directory Services (AD LS), Active Directory Federation Services (AD FS), and Active Directory Rights Management Services (AD RMS).

**Important**

Although you can deploy and manage AD DS in Azure Virtual Machines, we recommend you use Azure Active Directory, unless your configuration targets IaaS workloads that depend specifically on AD DS.

### Things to consider when using Azure AD rather than AD DS

Azure AD is similar to AD DS, but there are significant differences. It's important to understand that using Azure AD for your configuration is different from deploying an Active Directory domain controller on an Azure virtual machine and then adding it to your on-premises domain.

As you plan your identity strategy, consider the following characteristics that distinguish Azure AD from AD DS.

* **Identity solution**: AD DS is primarily a directory service, while Azure AD is a full identity solution. Azure AD is designed for internet-based applications that use HTTP and HTTPS communications. The features and capabilities of Azure AD support target strong identity management.
* **REST API queries**: Azure AD is based on HTTP and HTTPS protocols. Azure AD tenants can't be queried by using LDAP. Azure AD uses the REST API over HTTP and HTTPS.
* **Communication protocols**: Because Azure AD is based on HTTP and HTTPS, it doesn't use Kerberos authentication. Azure AD implements HTTP and HTTPS protocols, such as SAML, WS-Federation, and OpenID Connect for authentication (and OAuth for authorization).
* **Federation services**: Azure AD includes federation services, and many third-party services like Facebook.
* **Flat structure**: Azure AD users and groups are created in a flat structure. There are no organizational units (OUs) or group policy objects (GPOs).
* **Managed service**: Azure AD is a managed service. You manage only users, groups, and policies. If you deploy AD DS with virtual machines by using Azure, you manage many other tasks, including deployment, configuration, virtual machines, patching, and other backend processes.

## Next unit: Select Azure Active Directory editions