

Understand Microsoft Entra ID

1. Introduction

<https://learn.microsoft.com/en-us/training/modules/understand-azure-active-directory/1-introduction>

Introduction

Completed

Welcome to the Microsoft Entra ID learning module! Microsoft Entra ID is a cloud-based identity and access management service provided by Microsoft. Microsoft Entra ID is a comprehensive solution for managing identities, enforcing access policies, and securing your applications and data in the cloud and on-premises.

This module aims to equip you with a comprehensive understanding of the following:

- Describe Microsoft Entra ID.
- Compare Microsoft Entra ID to Active Directory Domain Services (AD DS).
- Describe how Microsoft Entra ID is used as a directory for cloud apps.
- Describe Microsoft Entra ID P1 and P2.
- Describe Microsoft Entra Domain Services.

Whether you're a beginner or an experienced IT professional, this module provides you with the knowledge and skills necessary to understand Microsoft Entra ID effectively. So, let's explore the exciting world of Microsoft Entra ID!

2. Examine Microsoft Entra ID

[https://learn.microsoft.com/en-us/training/modules/understand-azure-active-directory/2-examine-azure-active-d
irectory](https://learn.microsoft.com/en-us/training/modules/understand-azure-active-directory/2-examine-azure-active-directory)

Examine Microsoft Entra ID

Completed

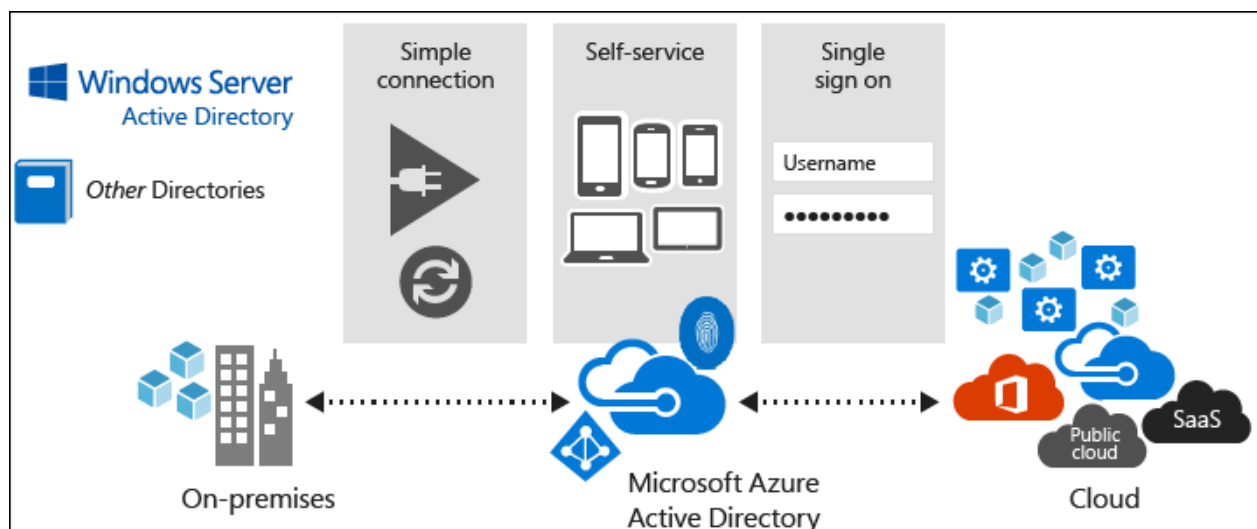
Students should be familiar with Active Directory Domain Services (AD DS or traditionally called just "Active Directory"). AD DS is a directory service that provides the methods for storing directory data, such as user accounts and passwords, and makes this data available to network users, administrators, and other devices and services. It runs as a service on Windows Server, referred to as a domain controller.

Microsoft Entra ID is part of the platform as a service (PaaS) offering and operates as a Microsoft-managed directory service in the cloud. It's not a part of the core infrastructure that customers own and manage, nor is it an Infrastructure as a service offering. While this implies that you have less control over its implementation, it also means that you don't have to dedicate resources to its deployment or maintenance.

With Microsoft Entra ID, you also have access to a set of features that aren't natively available in AD DS, such as support for multi-factor authentication, identity protection, and self-service password reset.

You can use Microsoft Entra ID to provide more secure access to cloud-based resources for organizations and individuals by:

- Configuring access to applications
- Configuring single sign-on (SSO) to cloud-based SaaS applications
- Managing users and groups
- Provisioning users
- Enabling federation between organizations
- Providing an identity management solution
- Identifying irregular sign-in activity
- Configuring multi-factor authentication
- Extending existing on-premises Active Directory implementations to Microsoft Entra ID
- Configuring Application Proxy for cloud and local applications
- Configuring Conditional Access for users and devices



Microsoft Entra constitutes a separate Azure service. Its most elementary form, which any new Azure subscription includes automatically, doesn't incur any extra cost and is referred to as the Free tier. If you subscribe to any Microsoft Online business services (for example, Microsoft 365 or Microsoft Intune), you automatically get Microsoft Entra ID with access to all the Free features.

Note

By default, when you create a new Azure subscription by using a Microsoft account, the subscription automatically includes a new Microsoft Entra tenant named Default Directory.

Some of the more advanced identity management features require paid versions of Microsoft Entra ID, offered in the form of Basic and Premium tiers. Some of these features are also automatically included in Microsoft Entra instances generated as part of Microsoft 365 subscriptions. Differences between Microsoft Entra versions are discussed later in this module.

Implementing Microsoft Entra ID isn't the same as deploying virtual machines in Azure, adding AD DS, and then deploying some domain controllers for a new forest and domain. Microsoft Entra ID is a different service, much more focused on providing identity management services to web-based apps, unlike AD DS, which is more focused on on-premises apps.

Microsoft Entra tenants

Unlike AD DS, Microsoft Entra ID is multi-tenant by design and is implemented specifically to ensure isolation between its individual directory instances. It's the world's largest multi-tenant directory, hosting over a million directory services instances, with billions of authentication requests per week. The term tenant in this context typically represents a company or organization that signed up for a subscription to a Microsoft cloud-based service such as Microsoft 365, Intune, or Azure, each of which uses Microsoft Entra ID. However, from a technical standpoint, the term tenant represents an individual Microsoft Entra instance. Within an Azure subscription, you can create multiple Microsoft Entra tenants. Having multiple Microsoft Entra tenants might be convenient if you want to test Microsoft Entra functionality in one tenant without affecting the others.

At any given time, an Azure subscription must be associated with one, and only one, Microsoft Entra tenant. This association allows you to grant permissions to resources in the Azure subscription (via RBAC) to users, groups, and applications that exist in that particular Microsoft Entra tenant.

Note

You can associate the same Microsoft Entra tenant with multiple Azure subscriptions. This allows you to use the same users, groups, and applications to manage resources across multiple Azure subscriptions.

Each Microsoft Entra tenant is assigned the default Domain Name System (DNS) domain name, consisting of a unique prefix. The prefix, derived from the name of the Microsoft account you use to create an Azure subscription or provided explicitly when creating a Microsoft Entra tenant, is

followed by the **onmicrosoft.com** suffix. Adding at least one custom domain name to the same Microsoft Entra tenant is possible and common. This name utilizes the DNS domain namespace that the corresponding company or organization owns. The Microsoft Entra tenant serves as the security boundary and a container for Microsoft Entra objects such as users, groups, and applications. A single Microsoft Entra tenant can support multiple Azure subscriptions.

Microsoft Entra schema

The Microsoft Entra schema contains fewer object types than that of AD DS. Most notably, it doesn't include a definition of the computer class, although it does include the device class. The process of joining devices to Microsoft Entra differs considerably from the process of joining computers to AD DS. The Microsoft Entra schema is also easily extensible, and its extensions are fully reversible.

The lack of support for the traditional computer domain membership means that you can't use Microsoft Entra ID to manage computers or user settings by using traditional management techniques, such as Group Policy Objects (GPOs). Instead, Microsoft Entra ID and its services define a concept of modern management. Microsoft Entra ID's primary strength lies in providing directory services; storing and publishing user, device, and application data; and handling the authentication and authorization of the users, devices, and applications. The effectiveness and efficiency of these features are apparent based on existing deployments of cloud services such as Microsoft 365, which rely on Microsoft Entra ID as their identity provider and support millions of users.

Microsoft Entra ID doesn't include the organizational unit (OU) class, which means that you can't arrange its objects into a hierarchy of custom containers, which is frequently used in on-premises AD DS deployments. However, this isn't a significant shortcoming, because OUs in AD DS are used primarily for Group Policy scoping and delegation. You can accomplish equivalent arrangements by organizing objects based on their group membership.

Objects of the Application and servicePrincipal classes represent applications in Microsoft Entra ID. An object in the Application class contains an application definition and an object in the servicePrincipal class constitutes its instance in the current Microsoft Entra tenant. Separating these two sets of characteristics allows you to define an application in one tenant and use it across multiple tenants by creating a service principal object for this application in each tenant. Microsoft Entra ID creates the service principal object when you register the corresponding application in that Microsoft Entra tenant.

3. Compare Microsoft Entra ID and Active Directory Domain Services

Compare Microsoft Entra ID and Active Directory Domain Services

Completed

You could view Microsoft Entra ID simply as the cloud-based counterpart of AD DS; however, while Microsoft Entra ID and AD DS share some common characteristics, there are several significant differences between them.

Characteristics of AD DS

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

When comparing AD DS with Microsoft Entra ID, it's important to note the following characteristics of AD DS:

- AD DS is a true directory service, with a hierarchical X.500-based structure.
- AD DS uses Domain Name System (DNS) for locating resources such as domain controllers.
- You can query and manage AD DS by using Lightweight Directory Access Protocol (LDAP) calls.
- AD DS primarily uses the Kerberos protocol for authentication.
- AD DS uses OUs and GPOs for management.
- AD DS includes computer objects, representing computers that join an Active Directory domain.
- AD DS uses trusts between domains for delegated management.

You can deploy AD DS on an Azure virtual machine to enable scalability and availability for an on-premises AD DS. However, deploying AD DS on an Azure virtual machine doesn't make any use of Microsoft Entra ID.

Note

Deploying AD DS on an Azure virtual machine requires one or more extra Azure data disks because you shouldn't use drive C for AD DS storage. These disks are needed to store the AD DS

database, logs, and the sysvol folder. The Host Cache Preference setting for these disks must be set to None.

Characteristics of Microsoft Entra ID

Although Microsoft Entra ID has many similarities to AD DS, there are also many differences. It's important to realize that using Microsoft Entra isn't the same as deploying an Active Directory domain controller on an Azure virtual machine and adding it to your on-premises domain.

When comparing Microsoft Entra ID with AD DS, it's important to note the following characteristics of Microsoft Entra ID:

- Microsoft Entra ID is primarily an identity solution, and it's designed for internet-based applications by using HTTP (port 80) and HTTPS (port 443) communications.
- Microsoft Entra ID is a multi-tenant directory service.
- Microsoft Entra users and groups are created in a flat structure, and there are no OUs or GPOs.
- You can't query Microsoft Entra ID by using LDAP; instead, Microsoft Entra ID uses the REST API over HTTP and HTTPS.
- Microsoft Entra ID doesn't use Kerberos authentication; instead, it uses HTTP and HTTPS protocols such as SAML, WS-Federation, and OpenID Connect for authentication, and uses OAuth for authorization.
- Microsoft Entra ID includes federation services, and many third-party services such as Facebook are federated with and trust Microsoft Entra ID.

4. Examine Microsoft Entra ID as a directory service for cloud apps

<https://learn.microsoft.com/en-us/training/modules/understand-azure-active-directory/4-examine-azure-directory-service-cloud-apps>

Examine Microsoft Entra ID as a directory service for cloud apps

Completed

When you deploy cloud services such as Microsoft 365 or Intune, you also need to have directory services in the cloud to provide authentication and authorization for these services. Because of this, each cloud service that needs authentication will create its own Microsoft Entra tenant. When a single

organization uses more than one cloud service, it's much more convenient for these cloud services to use a single cloud directory instead of having separate directories for each service.

It's now possible to have one identity service that covers all Microsoft cloud-based services, such as Microsoft 365, Azure, Microsoft Dynamics 365, and Intune. Microsoft Entra ID provides developers with centralized authentication and authorization for applications in Azure by using other identity providers or on-premises AD DS. Microsoft Entra ID can provide users with an SSO experience when using applications such as Facebook, Google services, Yahoo, or Microsoft cloud services.

The process of implementing Microsoft Entra ID support for custom applications is rather complex and beyond the scope of this course. However, the Azure portal and Microsoft Visual Studio 2013 and later make the process of configuring such support more straightforward.

In particular, you can enable Microsoft Entra authentication for the Web Apps feature of Azure App Service directly from the Authentication/Authorization blade in the Azure portal. By designating the Microsoft Entra tenant, you can ensure that only users with accounts in that directory can access the website. It's possible to apply different authentication settings to individual deployment slots.

For more information, see [Configure your App Service app to use Microsoft Entra login](#).

5. Compare Microsoft Entra ID P1 and P2 plans

<https://learn.microsoft.com/en-us/training/modules/understand-azure-active-directory/5-compare-azure-premium-p1-p2-plans>

Compare Microsoft Entra ID P1 and P2 plans

Completed

The Microsoft Entra ID P1 or P2 tier provides extra functionality as compared to the Free and Office 365 editions. However, premium versions require additional cost per user provisioning. Microsoft Entra ID P1 or P2 comes in two versions P1 and P2. You can procure it as an extra license or as a part of the Microsoft Enterprise Mobility + Security, which also includes the license for Azure Information Protection and Intune.

Microsoft provides a free trial period that can be used to experience the full functionality of the Microsoft Entra ID P2 edition. The following features are available with the Microsoft Entra ID P1 edition:

- **Self-service group management.** It simplifies the administration of groups where users are given the rights to create and manage the groups. End users can create requests to join other groups, and group owners can approve requests and maintain their groups' memberships.

- **Advanced security reports and alerts.** You can monitor and protect access to your cloud applications by viewing detailed logs that show advanced anomalies and inconsistent access pattern reports. Advanced reports are machine learning based and can help you gain new insights to improve access security and respond to potential threats.
- **Multi-factor authentication.** Full multi-factor authentication (MFA) works with on-premises applications (using virtual private network [VPN], RADIUS, and others), Azure, Microsoft 365, Dynamics 365, and third-party Microsoft Entra gallery applications. It doesn't work with non-browser off-the-shelf apps, such as Microsoft Outlook. Full multi-factor authentication is covered in more detail in the following units in this lesson.
- **Microsoft Identity Manager (MIM) licensing.** MIM integrates with Microsoft Entra ID P1 or P2 to provide hybrid identity solutions. MIM can bridge multiple on-premises authentication stores such as AD DS, LDAP, Oracle, and other applications with Microsoft Entra ID. This provides consistent experiences to on-premises line-of-business (LOB) applications and SaaS solutions.
- **Enterprise SLA of 99.9%.** You're guaranteed at least 99.9% availability of the Microsoft Entra ID P1 or P2 service. The same SLA applies to Microsoft Entra Basic.
- **Password reset with writeback.** Self-service password reset follows the Active Directory on-premises password policy.
- **Cloud App Discovery feature of Microsoft Entra ID.** This feature discovers the most frequently used cloud-based applications.
- **Conditional Access based on device, group, or location.** This lets you configure conditional access for critical resources, based on several criteria.
- **Microsoft Entra Connect Health.** You can use this tool to gain operational insight into Microsoft Entra ID. It works with alerts, performance counters, usage patterns, and configuration settings, and presents the collected information in the Microsoft Entra Connect Health portal.

In addition to these features, the Microsoft Entra ID P2 license provides extra functionalities:

- **Microsoft Entra ID Protection.** This feature provides enhanced functionalities for monitoring and protecting user accounts. You can define user risk policies and sign-in policies. In addition, you can review users' behavior and flag users for risk.
- **Microsoft Entra Privileged Identity Management.** This functionality lets you configure additional security levels for privileged users such as administrators. With Privileged Identity Management, you define permanent and temporary administrators. You also define a policy workflow that activates whenever someone wants to use administrative privileges to perform some task.

Note

Plans change frequently. Check Microsoft's website for the current plans and capabilities.

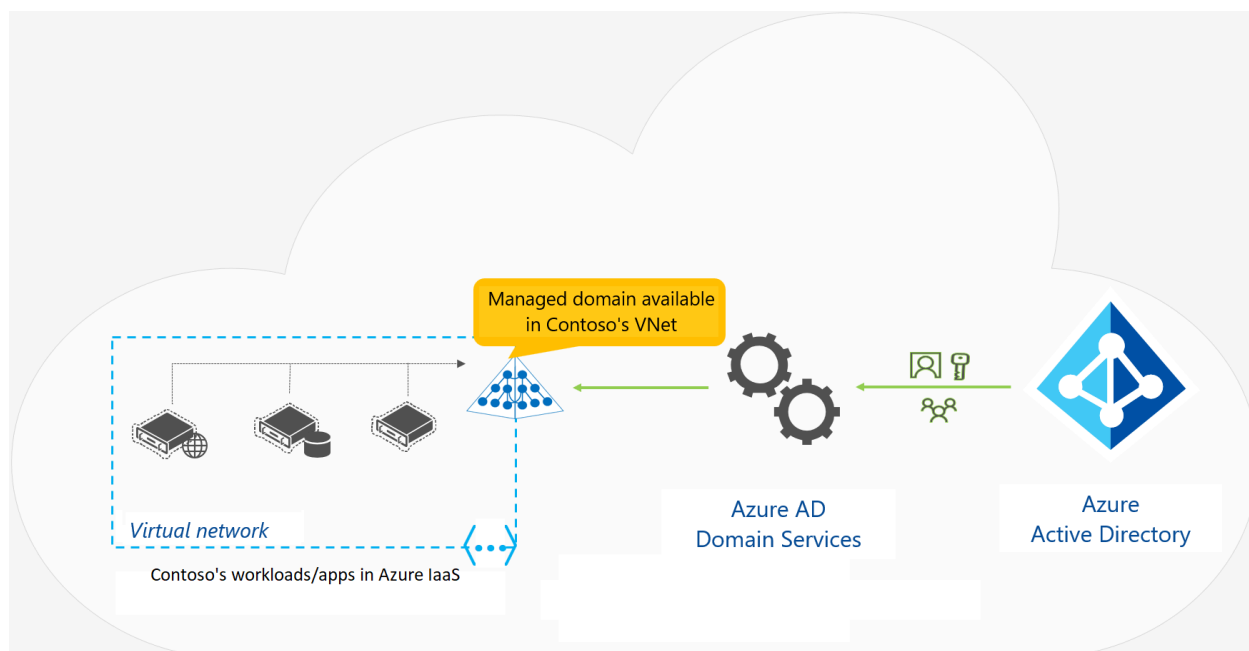
6. Examine Microsoft Entra Domain Services

Examine Microsoft Entra Domain Services

Completed

In most organizations today, line-of-business (LOB) applications are deployed on computers and devices that are domain members. These organizations use AD DS–based credentials for authentication, and Group Policy manages them. When you consider moving these apps to run in Azure, one key issue is how to provide authentication services to these apps. To satisfy this need, you can choose to implement a site-to-site virtual private network (VPN) between your local infrastructure and the Azure IaaS, or you can deploy replica domain controllers from your local AD DS as virtual machines (VMs) in Azure. These approaches can entail additional costs and administrative effort. Additionally, the difference between these two approaches is that with the first option, authentication traffic will cross the VPN, while in the second option, replication traffic will cross the VPN and authentication traffic stays in the cloud.

Microsoft provides Microsoft Entra Domain Services as an alternative to these approaches. This service, which runs as part of the Microsoft Entra ID P1 or P2 tier, provides domain services such as Group Policy management, domain joining, and Kerberos authentication to your Microsoft Entra tenant. These services are fully compatible with locally deployed AD DS, so you can use them without deploying and managing additional domain controllers in the cloud.



Because Microsoft Entra ID can integrate with your local AD DS, when you implement Microsoft Entra Connect, users can utilize organizational credentials in both on-premises AD DS and in Microsoft Entra Domain Services. Even if you don't have AD DS deployed locally, you can choose to use

Microsoft Entra Domain Services as a cloud-only service. This enables you to have similar functionality of locally deployed AD DS without having to deploy a single domain controller on-premises or in the cloud. For example, an organization can choose to create a Microsoft Entra tenant and enable Microsoft Entra Domain Services, and then deploy a virtual network between its on-premises resources and the Microsoft Entra tenant. You can enable Microsoft Entra Domain Services for this virtual network so that all on-premises users and services can use domain services from Microsoft Entra ID.

Microsoft Entra Domain Services provides several benefits for organizations, such as:

- Administrators don't need to manage, update, and monitor domain controllers.
- Administrators don't need to deploy and manage Active Directory replication.
- There's no need to have Domain Admins or Enterprise Admins groups for domains that Microsoft Entra ID manages.

If you choose to implement Microsoft Entra Domain Services, you need to be aware of the service's current limitations. These include:

- Only the base computer Active Directory object is supported.
- It's not possible to extend the schema for the Microsoft Entra Domain Services domain.
- The organizational unit (OU) structure is flat and nested OUs aren't currently supported.
- There's a built-in Group Policy Object (GPO), and it exists for computer and user accounts.
- It's not possible to target OUs with built-in GPOs. Additionally, you can't use Windows Management Instrumentation filters or security-group filtering.

By using Microsoft Entra Domain Services, you can freely migrate applications that use LDAP, NTLM, or the Kerberos protocols from your on-premises infrastructure to the cloud. You can also use applications such as Microsoft SQL Server or Microsoft SharePoint Server on VMs or deploy them in the Azure IaaS, without needing domain controllers in the cloud or a VPN to local infrastructure.

You can enable Microsoft Entra Domain Services by using the Azure portal. This service charges per hour based on the size of your directory.

7. Module assessment

<https://learn.microsoft.com/en-us/training/modules/understand-azure-active-directory/7-knowledge-check>

Module assessment

Completed

8. Summary

<https://learn.microsoft.com/en-us/training/modules/understand-azure-active-directory/8-summary>

Summary

Completed

Active Directory provides the core service of identity management. AD DS is the traditional on-premises solution, whereas Microsoft Entra ID is the cloud-based solution. Microsoft Entra ID is frequently adopted at first to facilitate authentication for cloud-based apps, but is capable of providing authentication services for the entire infrastructure. While they provide similar solutions, each offer different capability and are often used together to provide a best-of-breed solution. Microsoft Entra ID is offered as a free service, with paid tiers for additional capabilities, depending on an organization's needs.

Learn more

- [What is Microsoft Entra ID?](#)
- [Compare Active Directory to Microsoft Entra ID](#)