Introduction

Completed 100 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. 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

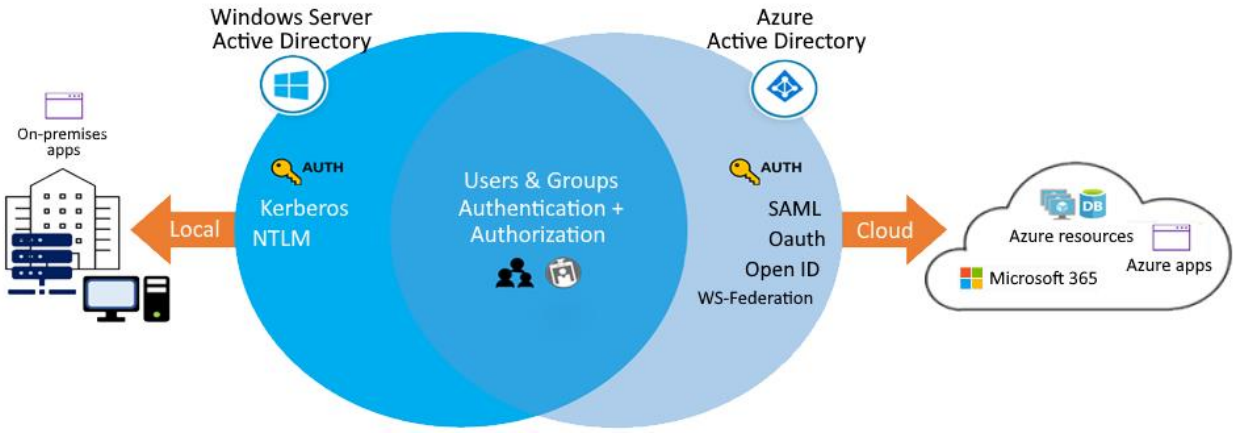
Completed 100 XP

- 3 minutes

Azure Active Directory (Azure AD) 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 and NTLM authentication 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-prem 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 commo Users can launch apps from a personalized web-based access panel, mobile app, Microso by using their existing work credentials.
Secure remote access	Azure AD enables secure remote access for on-premises web apps. Secure access can inc (MFA), conditional access policies, and group-based access management. Users can acce 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, p environments.
Sensitive data protection	Azure AD offers unique identity protection capabilities to secure your sensitive data and suspicious sign-in activity and potential vulnerabilities in a consolidated view of users an
Self-service support	Azure AD lets you delegate tasks to company employees that might otherwise be comple privileges. Providing self-service app access and password management through verifica 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

Completed 100 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.

Azure AD concept	Description
Identity	An *identity* is an object that can be authenticated. The identity can be a user with a username and password. Identities can also be applications or other servers that require authentication by using secret keys or certificates. Azure AD is the underlying product that provides the identity service.
Account	An *account* is an identity that has data associated with it. To have an account, you must first have a valid identity. You can't have an account without an identity.
Azure AD account	An *Azure AD account* is an identity that's created through Azure AD or another Microsoft cloud service, such as Microsoft 365. Identities are stored in Azure AD and are accessible to your organization's cloud service subscriptions. The Azure AD account is also called a *work or school account*.
Azure tenant (directory)	An Azure *tenant* is a single dedicated and trusted instance of Azure AD. Each tenant (also called a *directory*) represents a single organization. When your organization signs up for a Microsoft cloud service subscription, a new tenant is automatically created. Because each tenant is a dedicated and trusted instance of Azure AD, you can create multiple tenants or instances.
Azure subscription	An Azure subscription is used to pay for Azure cloud services. Each subscription is joined to a single tenant. You can have multiple subscriptions.

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

Completed 100 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

Select Azure Active Directory editions

Completed 100 XP

- 3 minutes

Azure Active Directory comes in four editions: **Free**, **Microsoft 365 Apps**, **Premium P1**, and **Premium P2**. The Free edition is included with an Azure subscription. The Premium editions are available through a Microsoft Enterprise Agreement, the Open Volume License Program, and the Cloud Solution Providers program. Azure and Microsoft 365 subscribers can also buy Azure Active Directory Premium P1 and P2 online.

Things to know about Azure AD editions

Consider the following features that distinguish the different editions of Azure AD. After you review the features and descriptions, think about which edition works best for your organization. An x indicates the feature is supported.

Feature	Free	Microsoft 365 Apps	Premium P1	Premium P2
Directory Objects	500,000	Unlimited	Unlimited	Unlimited
Single Sign-on	Unlimited	Unlimited	Unlimited	Unlimited
Core Identity and Access Management	x	x	x	x
Business-to-business Collaboration	x	x	x	x
Identity and Access Management for Microsoft 365 apps		x	x	x
Premium Features			x	x
Hybrid Identities			x	x
Advanced Group Access Management			x	x
Conditional Access			x	x
Identity Protection				x
Identity Governance				x

Azure Active Directory Free

The Free edition provides user and group management, on-premises directory synchronization, and basic reports. Single sign-on access is supported across Azure, Microsoft 365, and many popular SaaS apps.

Azure Active Directory Microsoft 365 Apps

This edition is included with Microsoft 365. In addition to the Free features, this edition provides Identity and Access Management for Microsoft 365 apps. The extra support includes branding, MFA, group access management, and self-service password reset for cloud users.

Azure Active Directory Premium P1

In addition to the Free features, the Premium P1 edition lets your hybrid users access both on-premises and cloud resources. This edition supports advanced administration like dynamic groups, self-service group management, and cloud write-back capabilities. P1 also includes Microsoft Identity Manager, an on-premises identity and access management suite. The extra features in P1 allow self-service password reset for your on-premises users.

Azure Active Directory Premium P2

In addition to the Free and P1 features, the Premium P2 edition offers Azure AD Identity Protection to help provide risk-based Conditional Access to your apps and critical company data. Privileged Identity Management is included to help discover, restrict, and monitor administrators and their access to resources, and to provide just-in-time access when needed.

Tip

The **Azure Active Directory pricing** page has detailed information on what's included in each edition.

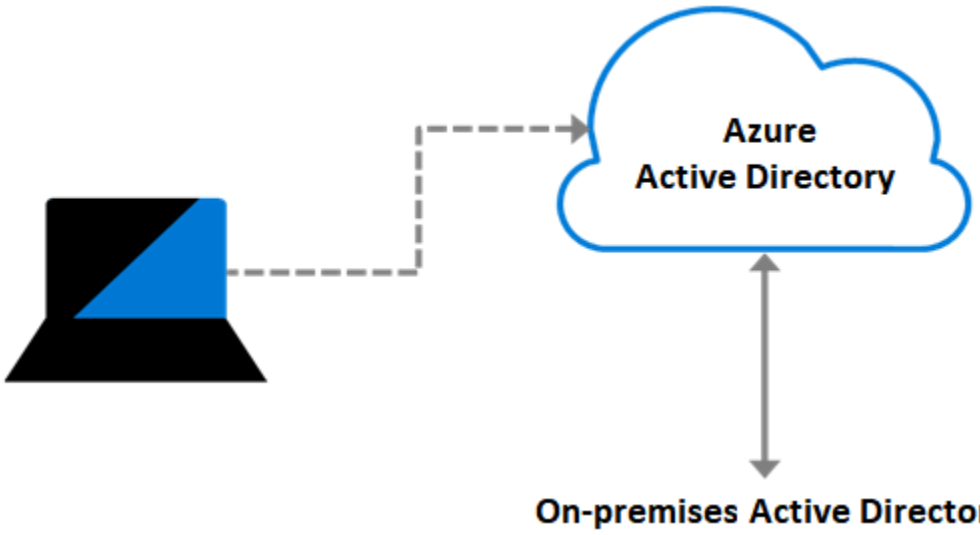
Next unit: Implement Azure Active Directory join

Implement Azure Active Directory join

Completed 100 XP

- 2 minutes

Azure Active Directory enables single sign-on (SSO) to devices, applications, and services from anywhere. To support SSO, IT admins must ensure corporate assets are protected, and devices meet standards for security and compliance.



The Azure AD join feature works with SSO to provide access to organizational apps and resources, and to simplify Windows deployments of work-owned devices.

Things to know about the Azure AD join feature

Let's look at some of the benefits of using joined devices:

Benefit	Description
Single-Sign-On (SSO)	Joined devices offer SSO access to your Azure-managed SaaS apps and services. Your users wo when they access work resources. The SSO functionality is available even when users aren't co
Enterprise state roaming	Starting in Windows 10, your users can securely synchronize their user settings and app setting state roaming reduces the time to configure a new device.
Access to Microsoft Store for Business	When your users access Microsoft Store for Business by using an Azure AD account, they can c pre-selected by your organization.
Windows Hello	Provide your users with secure and convenient access to work resources from joined devices.

Benefit	Description
Restriction of access	Restrict user access to apps from only joined devices that meet your compliance policies.
Seamless access to on-premises resources	Joined devices have seamless access to on-premises resources, when the device has line of sig controller.

Things to consider when using joined devices

Your organization is interested in using joined devices in their management strategy. As you plan for how to implement the feature, review these configuration points:

- **Consider connection options**. Connect your device to Azure AD in one of two ways:
    - **Register** your device to Azure AD so you can manage the device identity. Azure AD device registration provides the device with an identity that's used to authenticate the device when a user signs into Azure AD. You can use the identity to enable or disable the device.
    - **Join** your device, which is an extension of registering a device. Joining provides the benefits of registering, and also changes the local state of the device. Changing the local state enables your users to sign into a device by using an organizational work or school account instead of a personal account.
- **Consider combining registration with other solutions**. Combine registration with a mobile device management (MDM) solution like Microsoft Intune, to provide other device attributes in Azure AD. You can create conditional access rules that enforce access from devices to meet organization standards for security and compliance.
- **Consider other implementation scenarios**. Although AD Join is intended for organizations that don't have an on-premises Windows Server Active Directory infrastructure, it can be used for other scenarios like branch offices.

Next unit: Implement Azure Active Directory self-service password reset

Implement Azure Active Directory self-service password reset

Completed 100 XP

- 2 minutes

Many helpdesk calls are requests to reset passwords for users. The Azure Active Directory **self-service password reset** (SSPR) feature lets you give users the ability to bypass helpdesk and reset their own passwords.

Things to know about the Azure AD SSPR feature

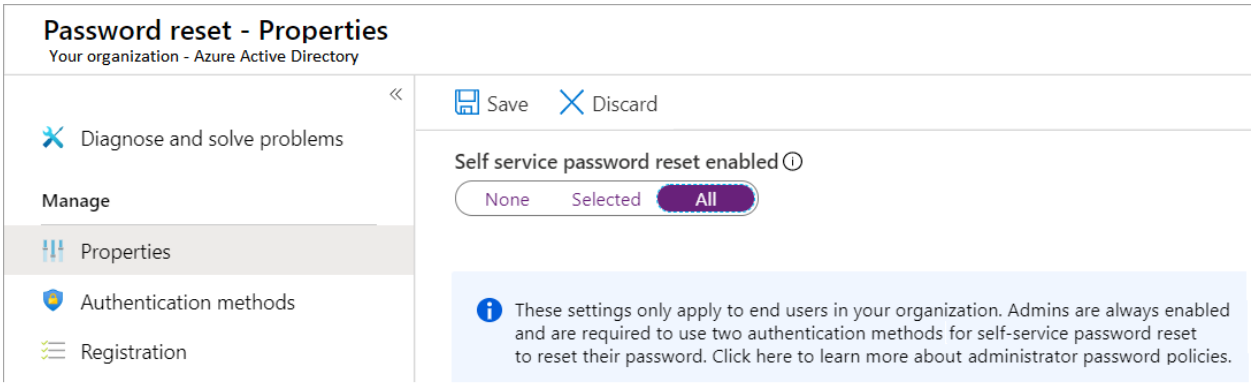
Examine the following characteristics and requirements of the SSPR feature:

- SSPR requires an Azure AD account with Global Administrator privileges to manage SSPR options. This account can always reset their own passwords, no matter what options are configured.
- SSPR uses a security group to limit the users who have SSPR privileges.
- All user accounts in your organization must have a valid license to use SSPR.

Things to consider when using SSPR

Your organization wants to implement support for SSPR in their management solution. As you plan for your configuration, review the following points:

- **Consider who can reset their passwords**. Decide which users in your organization should be enabled to use the feature. In the Azure portal, there are three options for the SSPR feature: **None**, **Selected**, and **All**.



The **Selected** option is useful for creating specific groups who have SSPR enabled. You can create groups for testing or proof of concept before applying the feature to a larger group. When you're ready to deploy SSPR to all user accounts in your Azure AD tenant, you can change the setting.

- **Consider your authentication methods**. Determine how many authentication methods are required to reset a password, and select the authentication options for users.
    - Your system must require at least one authentication method to reset a password.
    - A strong SSPR plan offers multiple authentication methods for the user. Options include email notification, text message, or a security code sent to the user's mobile or office phone. You can also offer the user a set of security questions.
    - You can require security questions to be registered for the users in your Azure AD tenant.
    - You can configure how many correctly answered security questions are required for a successful password reset.
- **Consider combining methods for stronger security**. Security questions can be less secure than other authentication methods. Some users might know the answers for a particular user's questions, or the questions might be easy to solve. If you support security questions, combine this option with other authentication methods.

Next unit: Knowledge check

Knowledge check

Completed200 XP

- 4 minutes

Suppose your company is looking for a strong identity solution. It's your job to decide whether Azure Active Directory or Active Directory Domain Services (AD DS) is the optimal choice. If you choose Azure AD, you need to select the edition that best supports your organization's needs and determine which features to implement.

Here are some requirements for your design:

- **Users can sign-in to devices, apps, and services from anywhere**.
- **The IT team wants users to manage their own passwords and do related tasks**.
- **The Legal department requests protection for sensitive data to meet governance compliance standards**.

Answer the following questions

Choose the best response for each of the questions below. Then select **Check your answers**.

1.

Which choice correctly describes Azure Active Directory?

Azure AD can be queried through LDAP.

Azure AD is primarily an identity solution.
Correct. Azure AD is primarily an identity solution. It's designed for internet-based applications by using HTTP and HTTPS communications.

Azure AD uses organizational units (OUs) and group policy objects (GPOs).
2.

What term defines a dedicated and trusted instance of Azure Active Directory?

Azure tenant
Correct. A tenant is a dedicated and trusted instance of Azure AD. A tenant is automatically created when an organization signs up for a Microsoft cloud service subscription.

Identity

Azure AD account

3.

Your users want to sign-in to devices, apps, and services from anywhere. Users want to sign-in by using an organizational work or school account instead of a personal account. What should you do first?

Enable the device in Azure AD.

Join the device to Azure AD.
Correct. Joining the device provides the features you need.

Register the device with Azure AD.

Next unit: Summary and resources

Summary and resources

Completed 100 XP

- 1 minute

Azure Administrators must be familiar with Azure Active Directory and its concepts.

In this module, you learned about Azure AD features and explored implementation scenarios. You reviewed the main components of Azure AD, including tenants, identities, and accounts, and learned how they're related. You compared Active Directory Domain Services to Azure AD, and discovered how different Azure AD editions support features. You explored the benefits of the Azure AD join and self-service password reset (SSPR) features, and considered how to implement them for your organization.

Learn more with Azure documentation

- Read more about Azure Active Directory.
- Join devices by using Azure AD device identity.
- Configure Azure AD self-service password reset.

Learn more with self-paced training

- Manage device identity with Azure AD join and Enterprise State Roaming.
- Implement and manage hybrid identity.

Learn more with optional hands-on exercises

- Allow users to reset their password with Azure Active Directory self-service password reset (sandbox).

Module complete: