Contents

[Azure Active Directory 1](#_Toc49910993)

[Terminology 1](#_Toc49910994)

[Manage Azure Active Directory (AD) 3](#_Toc49910995)

[Azure AD licenses 3](#_Toc49910996)

[add custom domains 6](#_Toc49910997)

[configure Azure AD Identity Protection 7](#_Toc49910998)

[configure Azure AD Join 7](#_Toc49910999)

[configure self-service password reset 8](#_Toc49911000)

[implement conditional access policies 8](#_Toc49911001)

[manage multiple directories 8](#_Toc49911002)

[perform an access review 10](#_Toc49911003)

[Implement and manage hybrid identities 10](#_Toc49911004)

[install and configure Azure AD Connect 10](#_Toc49911005)

[configure federation 11](#_Toc49911006)

[configure single sign-on 11](#_Toc49911007)

[manage and troubleshoot Azure AD Connect 11](#_Toc49911008)

[troubleshoot password sync and writeback 11](#_Toc49911009)

[Create a new tenant in Azure Active Directory 11](#_Toc49911010)

[Associate or add an Azure subscription to your Azure Active Directory tenant 12](#_Toc49911011)

[Azure Key Vault 12](#_Toc49911012)

# Azure Active Directory

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis>

Azure Active Directory (Azure AD) is Microsoft’s cloud-based **Identity And Access Management** service.

## Terminology

To better understand Azure AD and its documentation, we recommend reviewing the following terms.

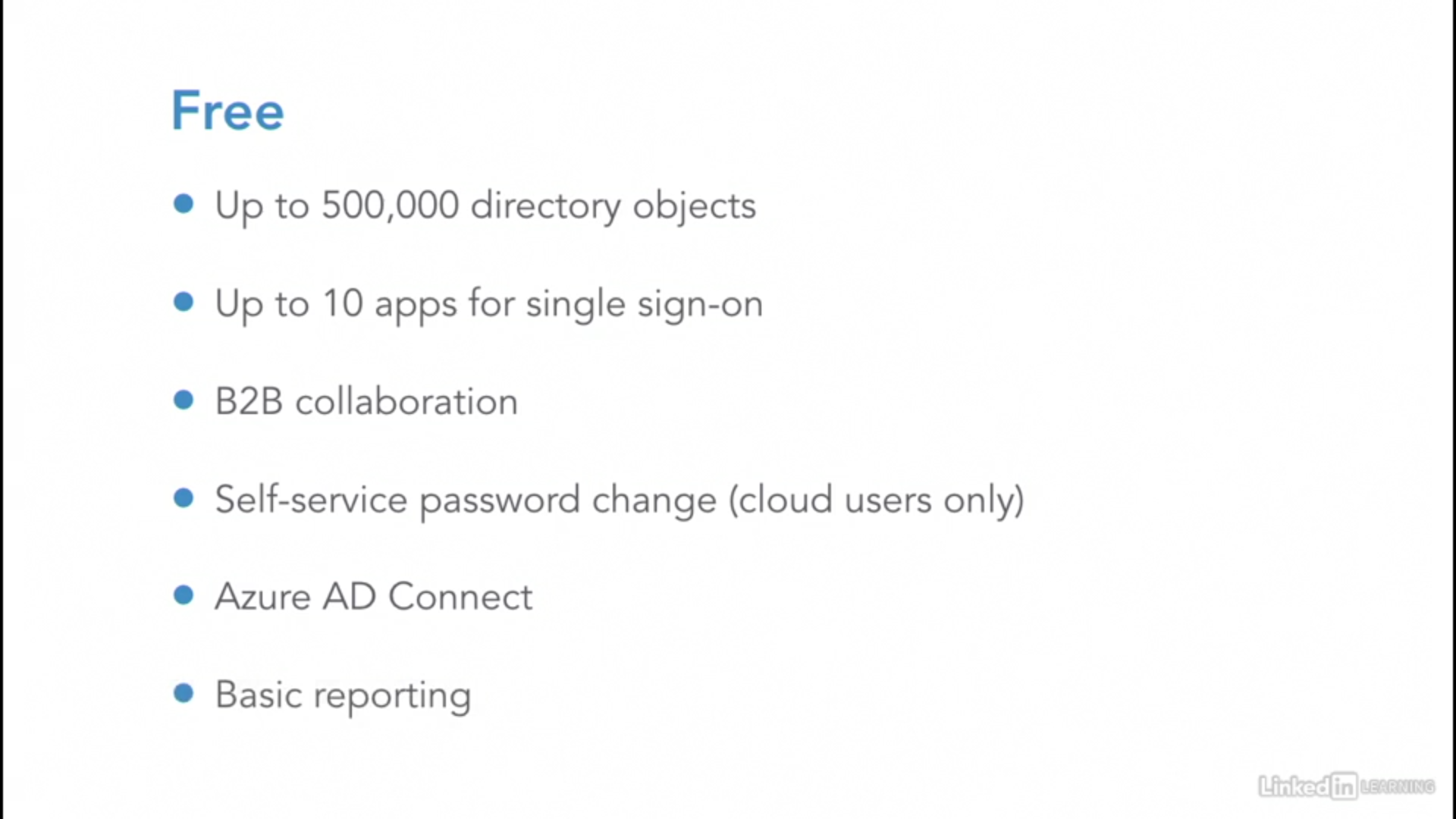
| **Term or concept** | **Description** |
| --- | --- |
| Identity | A thing that can get authenticated. An identity can be a user with a username and password. Identities also include applications or other servers that might require authentication through secret keys or certificates. |
| Account | **An identity that has data associated with it. You cannot have an account without an identity**. |
| Azure AD account | An identity created through Azure AD or another Microsoft cloud service, such as Office 365. Identities are stored in Azure AD and accessible to your organization's cloud service subscriptions. **This account is also sometimes called a Work or school account.** |
| Account Administrator | This classic subscription administrator role is conceptually the billing owner of a subscription. This role has access to the [Azure Account Center](https://account.azure.com/Subscriptions) and enables you to manage all subscriptions in an account. For more information, see [Classic subscription administrator roles, Azure roles, and Azure AD administrator roles](https://docs.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles). |
| Service Administrator | This classic subscription administrator role enables you to manage all Azure resources, including access. This role has the equivalent access of a user who is assigned the Owner role at the subscription scope. For more information, see [Classic subscription administrator roles, Azure roles, and Azure AD administrator roles](https://docs.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles). |
| Owner | This role helps you manage all Azure resources, including access. **This role is built on a newer authorization system called Azure role-base access control (Azure RBAC) that provides fine-grained access management to Azure resources**. For more information, see [Classic subscription administrator roles, Azure roles, and Azure AD administrator roles](https://docs.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles). |
| Azure AD Global administrator | This administrator role is automatically assigned to whomever created the Azure AD tenant. Global administrators can do all of the administrative functions for Azure AD and any services that federate to Azure AD, such as Exchange Online, SharePoint Online, and Skype for Business Online. You can have multiple Global administrators, but only Global administrators can assign administrator roles (including assigning other Global administrators) to users. Note that this administrator role is called Global administrator in the Azure portal, but it's called **Company administrator** in the Microsoft Graph API and Azure AD PowerShell.For more information about the various administrator roles, see [Administrator role permissions in Azure Active Directory](https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles). |
| Azure subscription | Used to pay for Azure cloud services. **You can have many subscriptions** and they're linked to a credit card. |
| Azure tenant | **A dedicated and trusted instance of Azure AD that's automatically created when your organization signs up for a Microsoft cloud service subscription**, such as Microsoft Azure, Microsoft Intune, or Office 365. **An Azure tenant represents a single organization.** |
| Single tenant | Azure tenants that access other services in a dedicated environment are considered single tenant. |
| Multi-tenant | Azure tenants that access other services in a shared environment, across multiple organizations, are considered multi-tenant. |
| Azure AD directory | **Each Azure tenant has a dedicated and trusted Azure AD directory.** **The Azure AD directory includes the tenant's users, groups, and apps and is used to perform identity and access management functions for tenant resources.** |
| Custom domain | Every new Azure AD directory comes with an initial domain name, domainname.onmicrosoft.com. In addition to that initial name, you can also add your organization's domain names, which include the names you use to do business and your users use to access your organization's resources, to the list. Adding custom domain names helps you to create user names that are familiar to your users, such as alain@contoso.com. |
| Microsoft account (also called, MSA) | Personal accounts that provide access to your consumer-oriented Microsoft products and cloud services, such as Outlook, OneDrive, Xbox LIVE, or Office 365. Your Microsoft account is created and stored in the Microsoft consumer identity account system that's run by Microsoft. |

## Manage Azure Active Directory (AD)

### Azure AD licenses

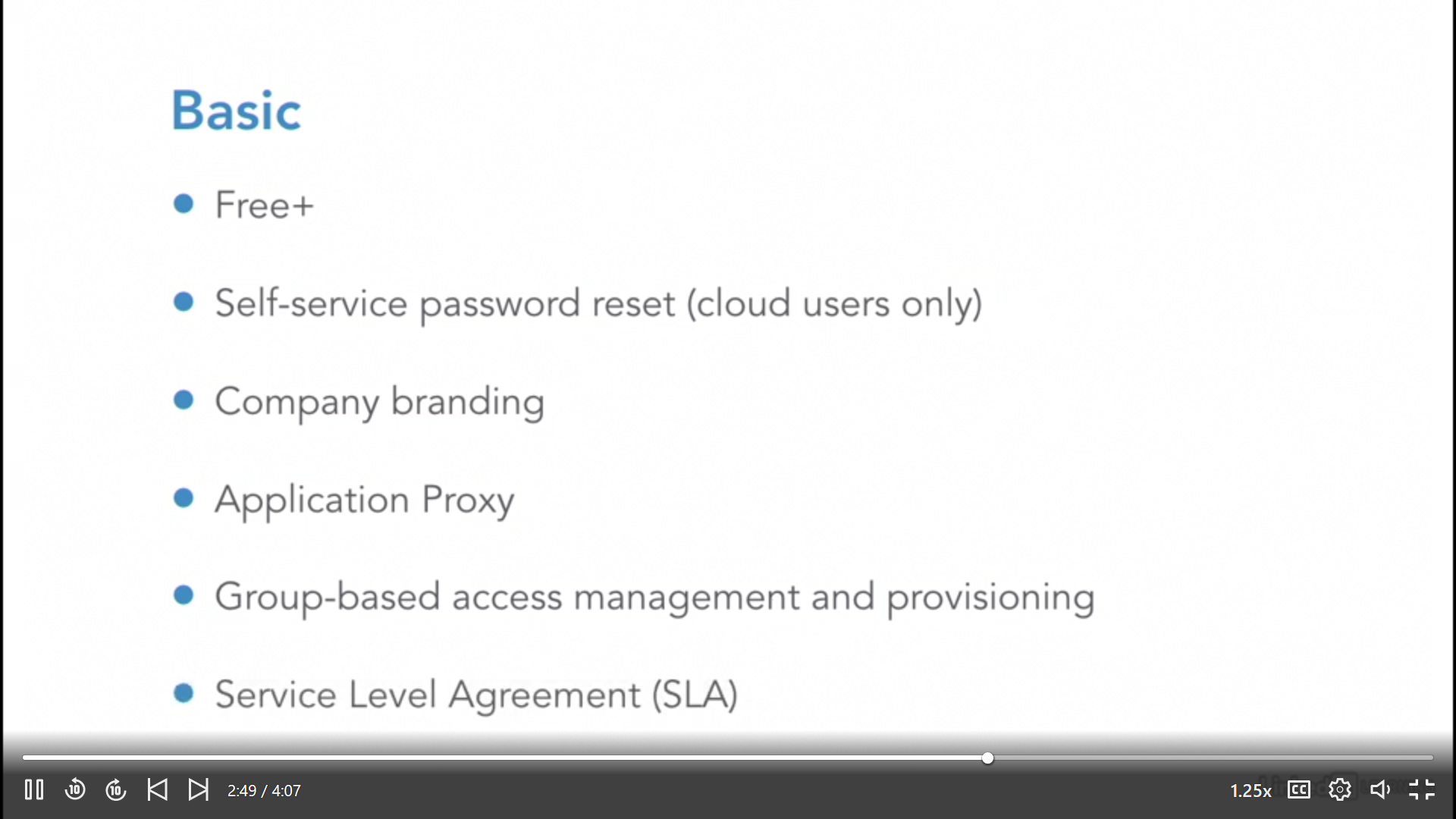
<https://azure.microsoft.com/en-in/pricing/details/active-directory/>

**Azure Active Directory Free.**

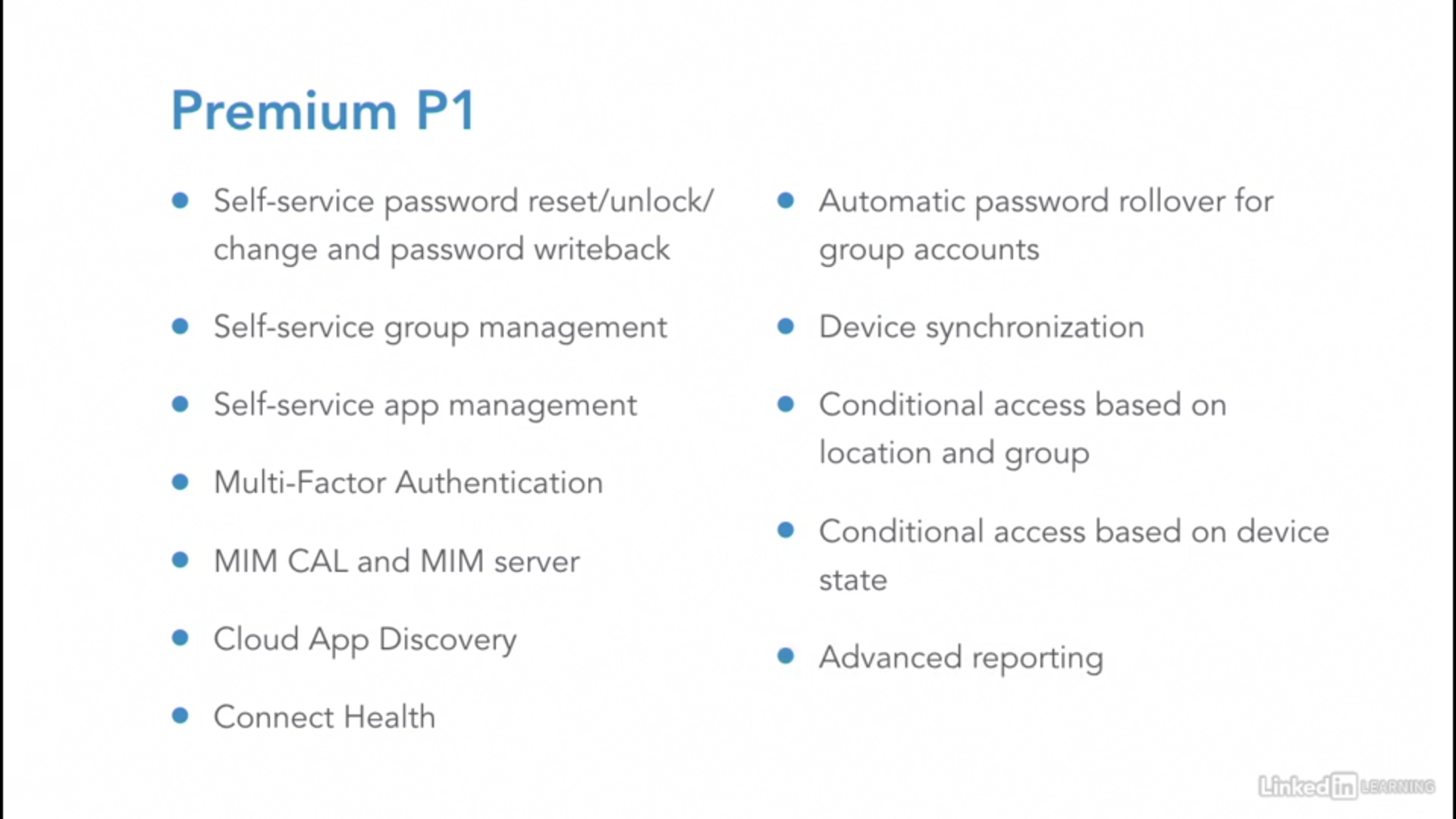


**Azure Active Directory Basic.**

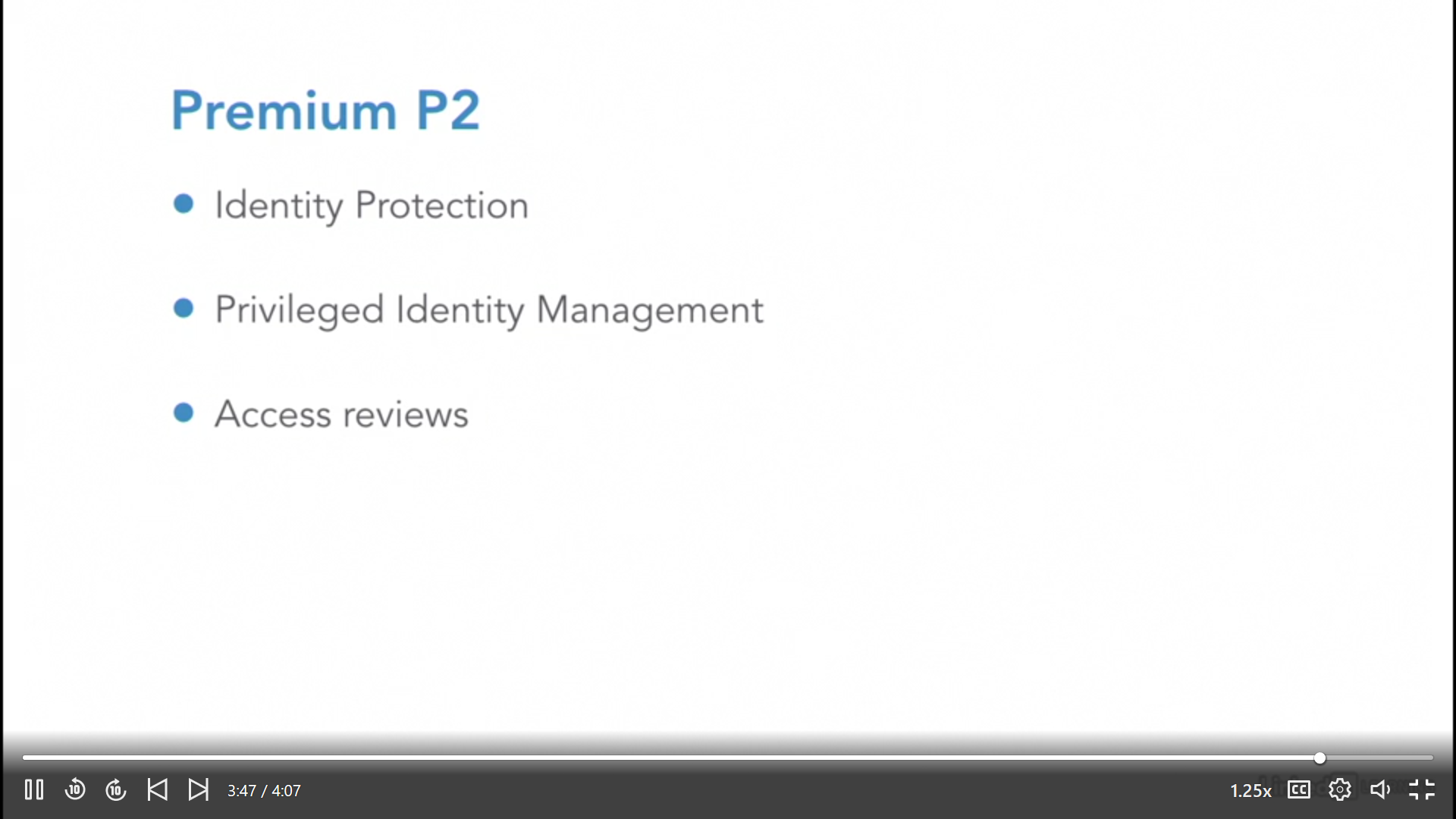
**Password reset**

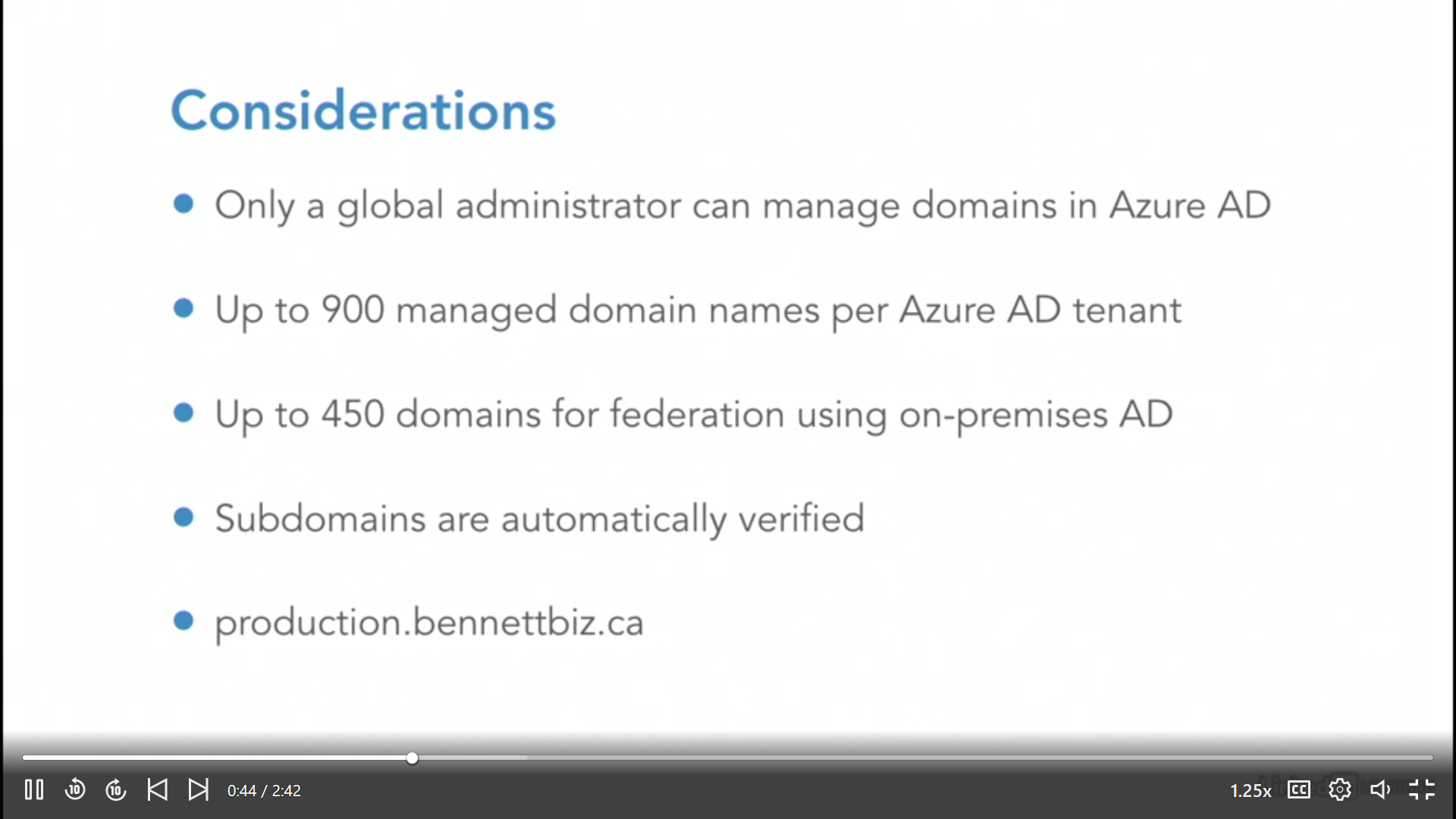


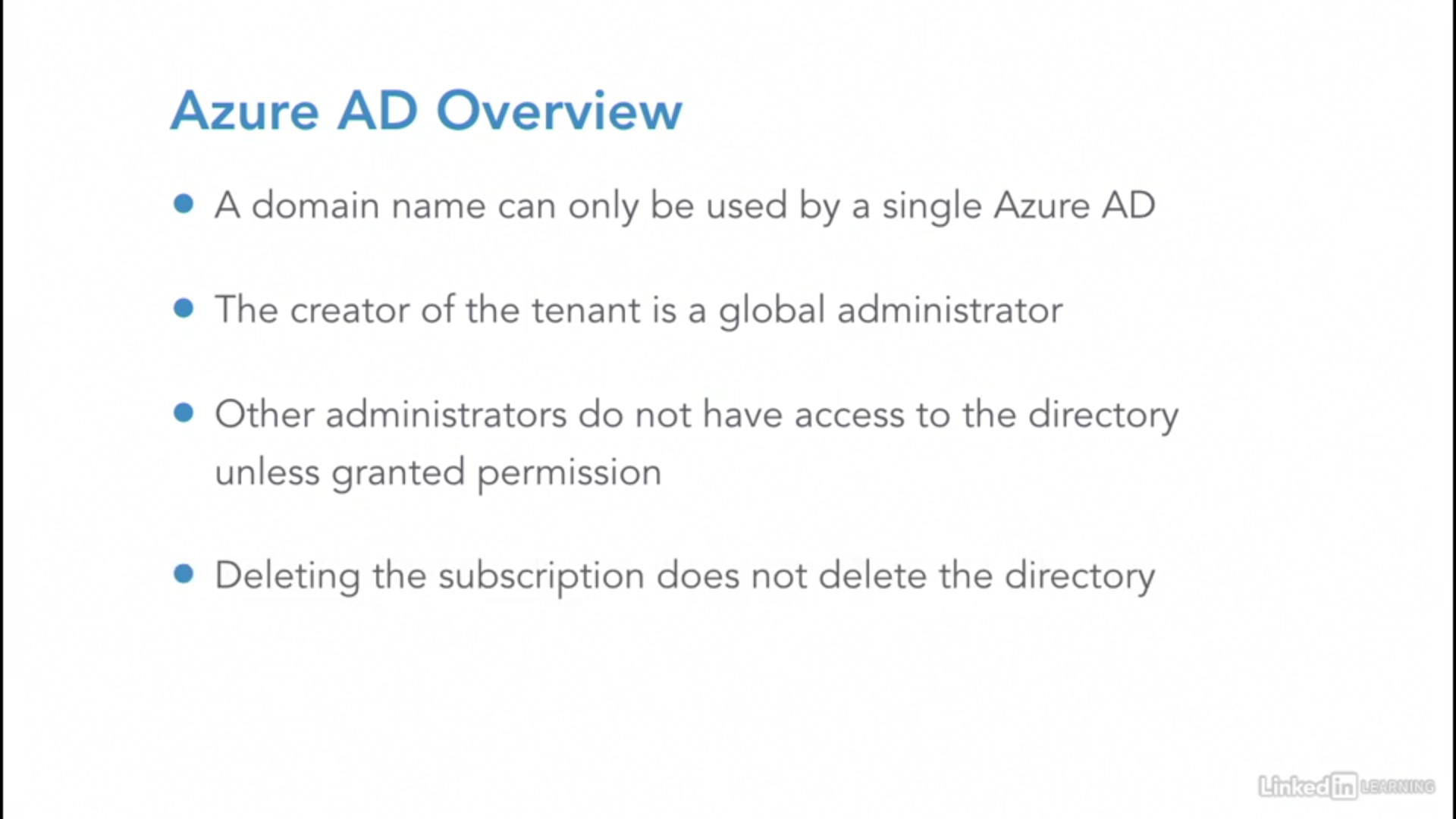
**Azure Active Directory Premium P1.**



**Azure Active Directory Premium P2.**







### add custom domains

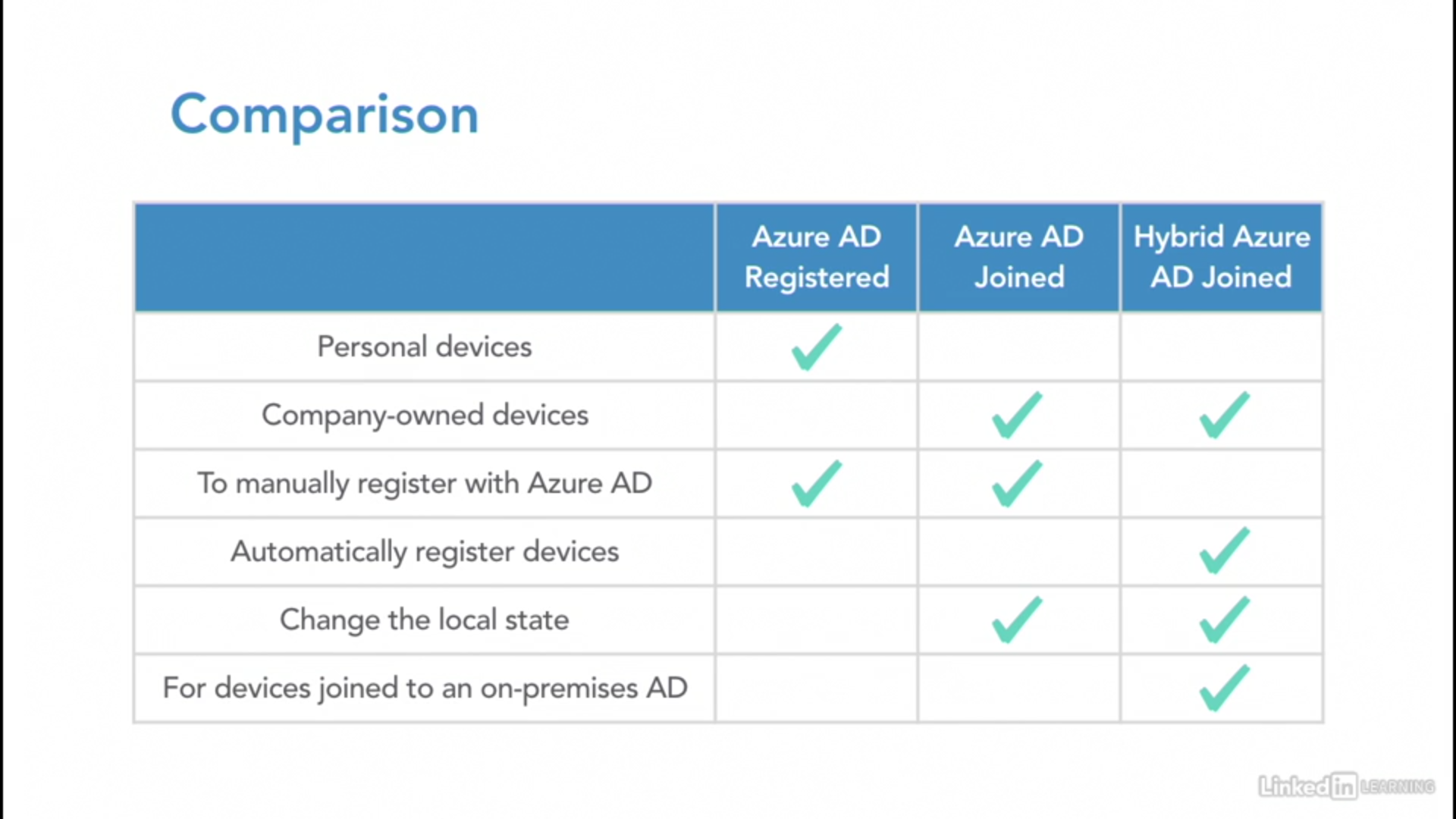
<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-custom-domain>

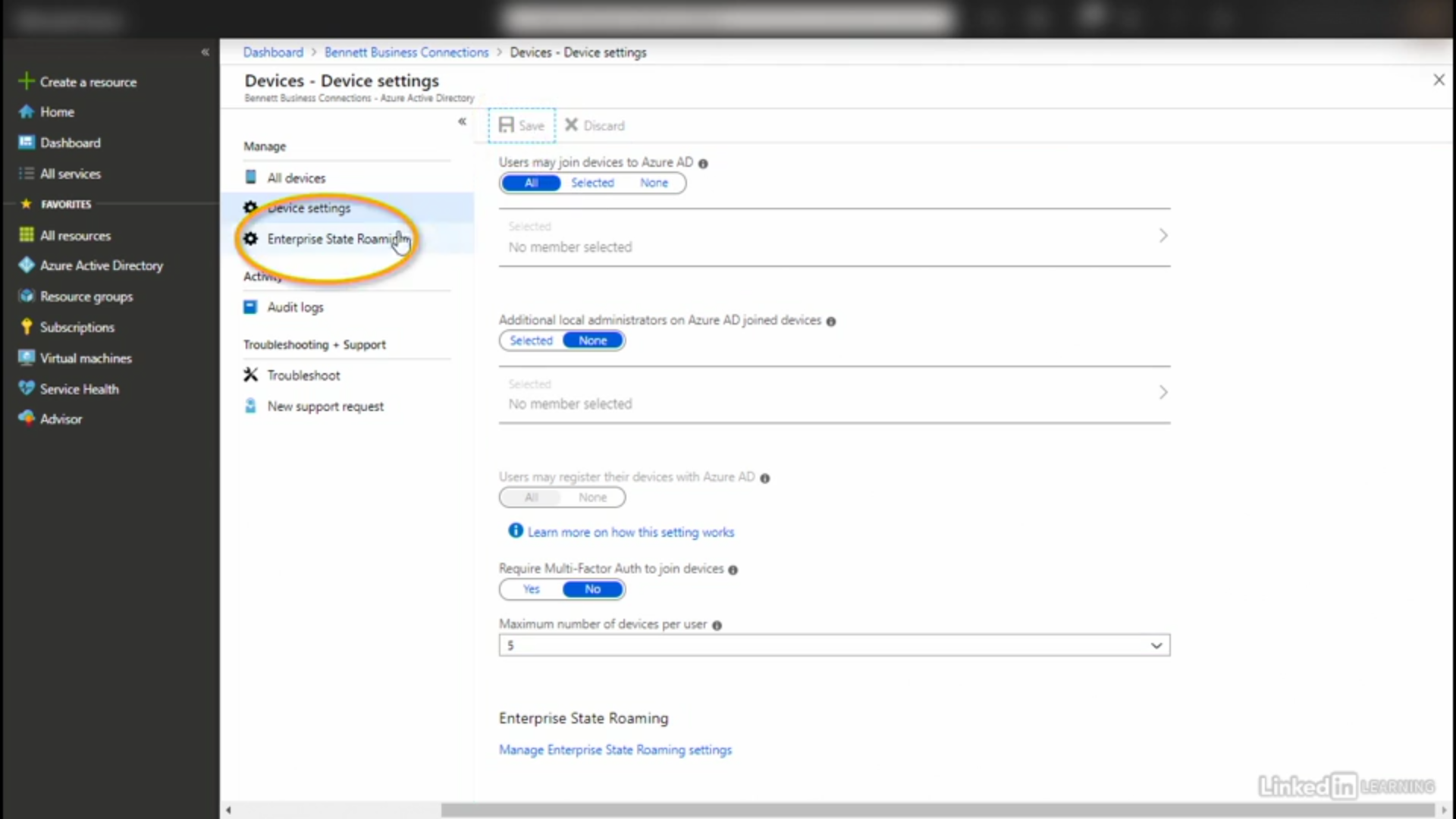
### configure Azure AD Identity Protection

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection>

### configure Azure AD Join

Allowing corporate resource access to users via laptop, mobile phone etc





### configure self-service password reset

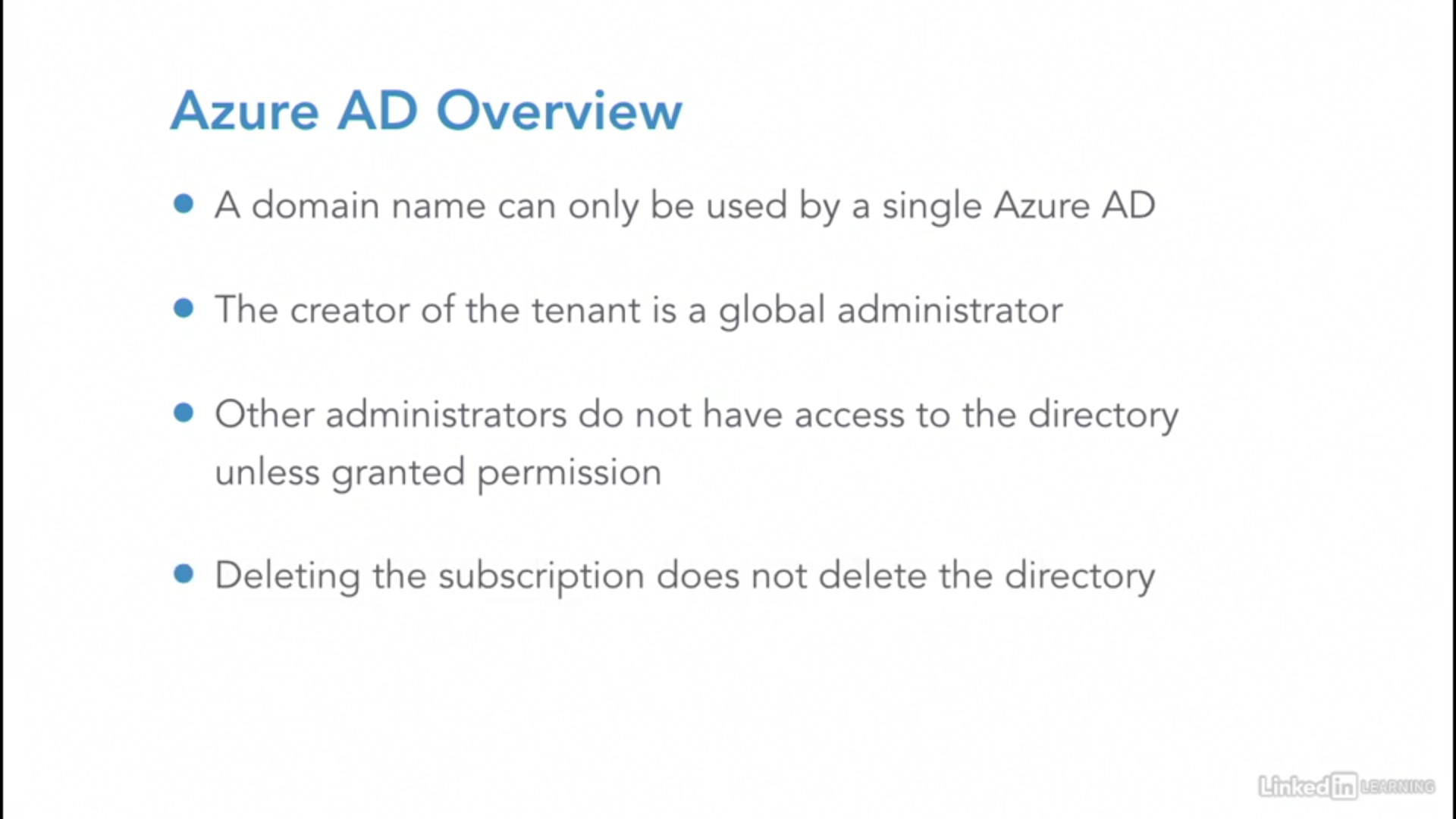
1. First enable password reset from portal
2. Then choose authentication method

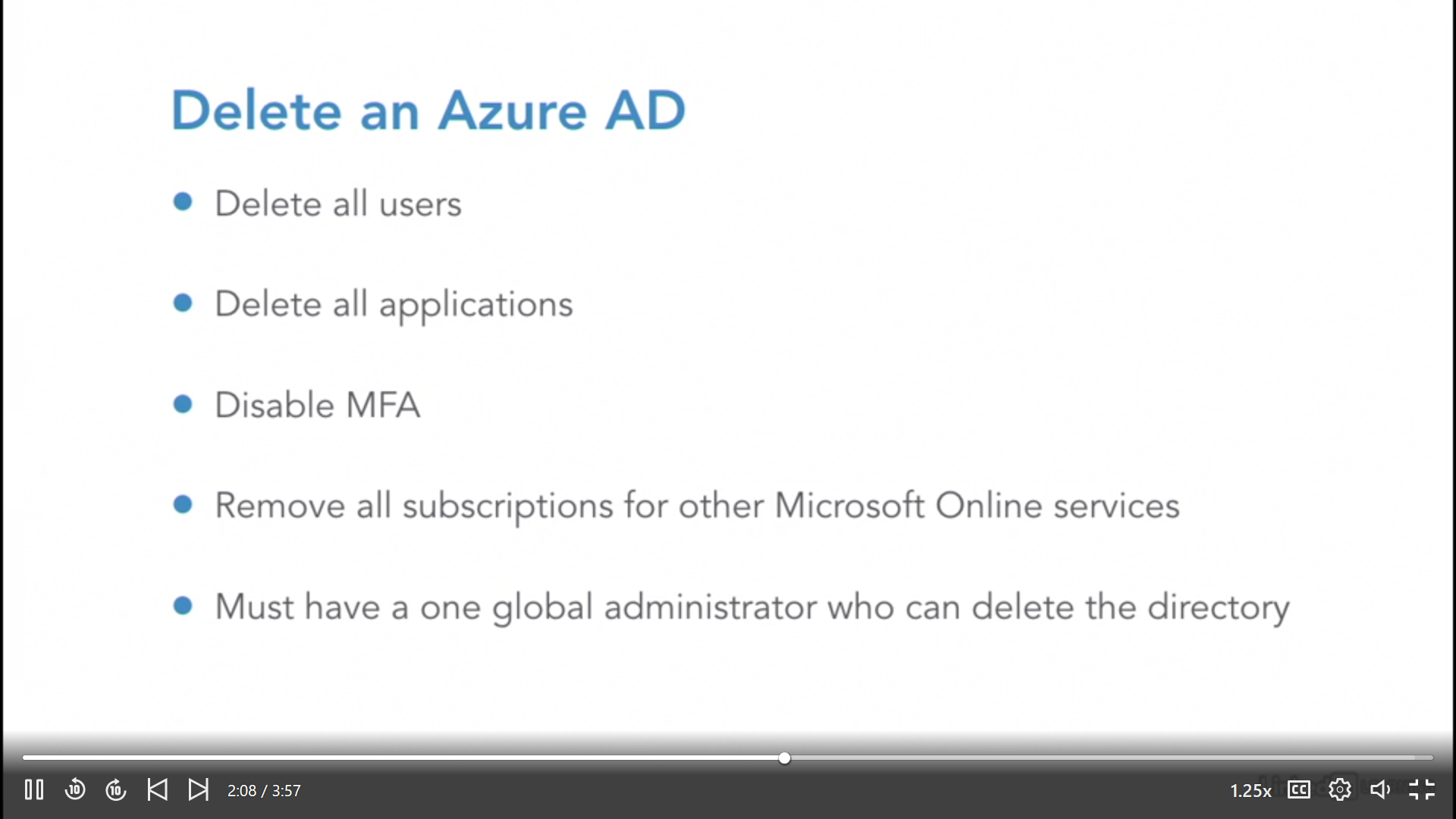
<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks>

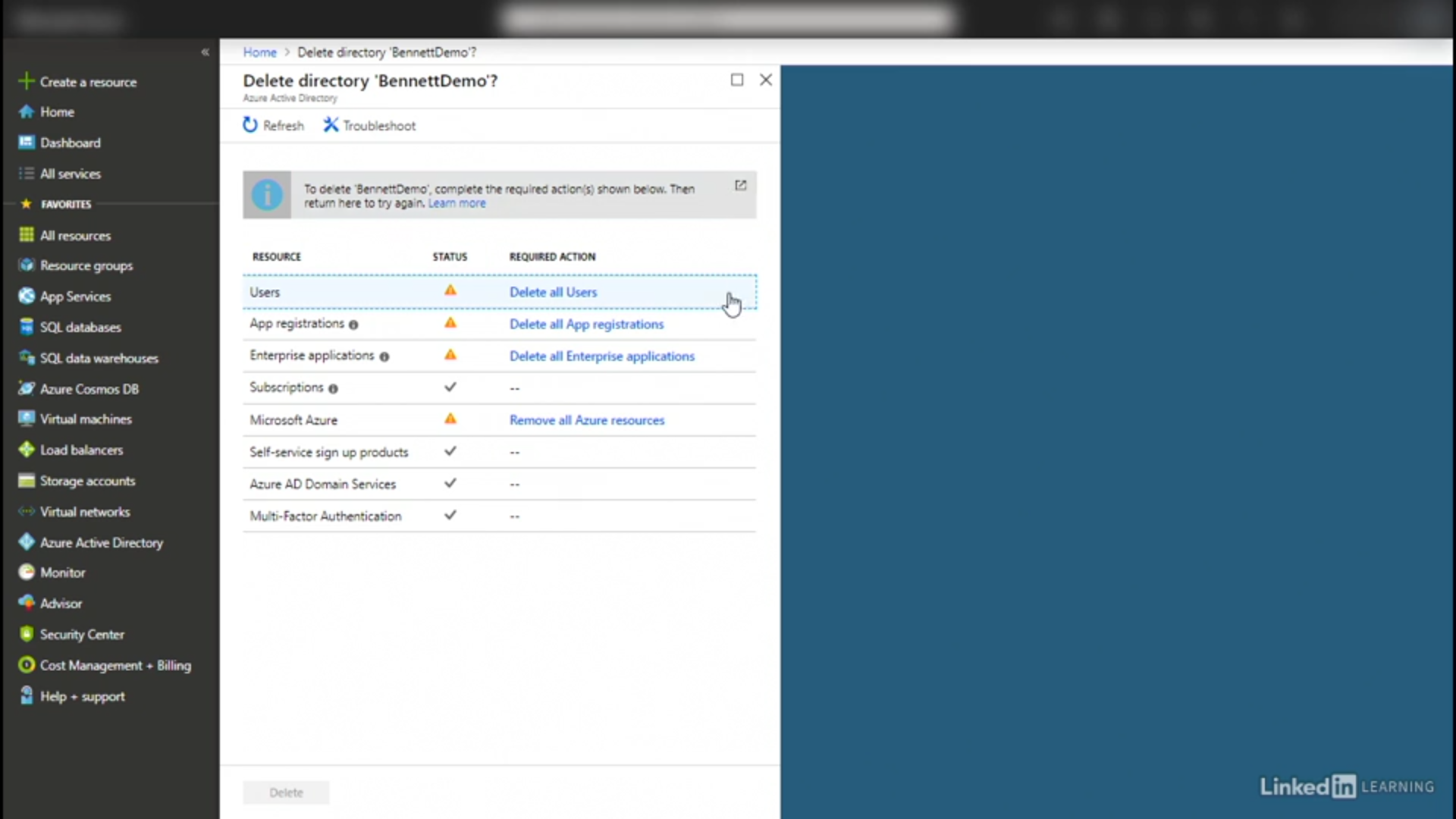
### implement conditional access policies

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-azure-mfa>

### manage multiple directories







### perform an access review

<https://www.youtube.com/watch?v=6KB3TZ8Wi40>

<https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview>

## Implement and manage hybrid identities

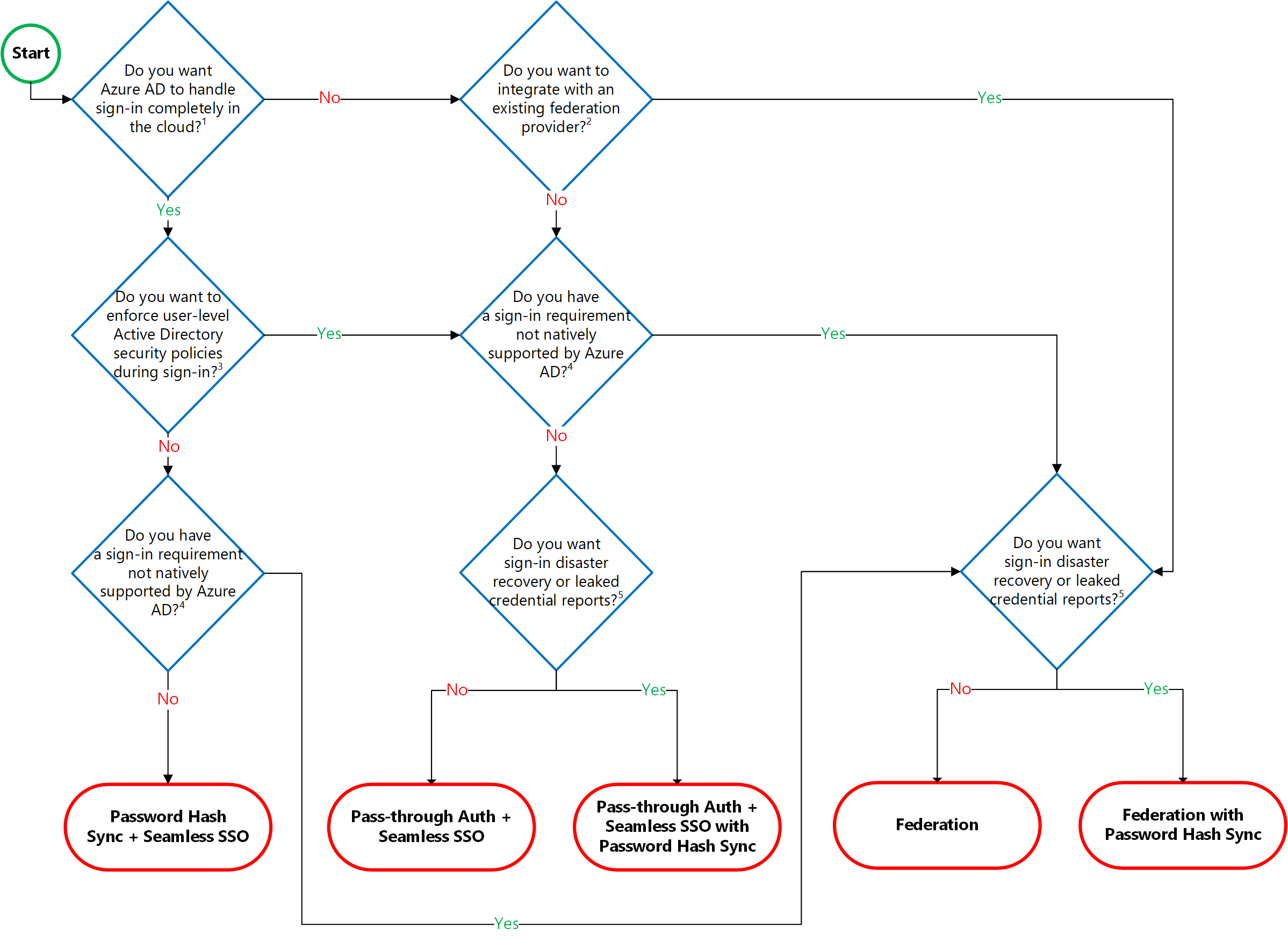
### install and configure Azure AD Connect

<https://youtu.be/YtW2cmVqSEw>

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-hybrid-identity#install-azure-ad-connect>

To achieve hybrid identity with Azure AD, one of three authentication methods can be used, depending on your scenarios. The three methods are:

* [**Password hash synchronization (PHS)**](https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-phs)
* [**Pass-through authentication (PTA)**](https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta)
* [**Federation (AD FS)**](https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fed)



<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn>

### configure federation

### configure single sign-on

### manage and troubleshoot Azure AD Connect

### troubleshoot password sync and writeback

## Implement Multi-Factor Authentication (MFA)

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted>

### Type of MFA:

1. MFA in cloud
   1. MFA for office 365 ( Free )
   2. MFA for Azure AD Global Administrator ( Free )
   3. Azure MFA ( full version , PAID )
2. MFA Servers on premises

### Prerequisites

Before starting a deployment of Azure Multi-Factor Authentication, there are prerequisite items that should be considered.

| Prerequisites | |
| --- | --- |
| **Scenario** | **Prerequisite** |
| **Cloud-only** identity environment with modern authentication | **No additional prerequisite tasks** |
| **Hybrid** identity scenarios | [Azure AD Connect](https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-hybrid-identity) is deployed and user identities are synchronized or federated with the on-premises Active Directory Domain Services with Azure Active Directory. |
| On-premises legacy applications published for cloud access | Azure AD [Application Proxy](https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy) is deployed. |
| Using Azure MFA with RADIUS Authentication | A [Network Policy Server (NPS)](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-nps-extension) is deployed. |
| Users have Microsoft Office 2010 or earlier, or Apple Mail for iOS 11 or earlier | Upgrade to [Microsoft Office 2013 or later](https://support.microsoft.com/help/4041439/modern-authentication-configuration-requirements-for-transition-from-o) and Apple mail for iOS 12 or later. Conditional Access is not supported by legacy authentication protocols. |

### configure user accounts for MFA

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates>

### configure fraud alerts

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#fraud-alert>

### configure bypass options

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#one-time-bypass>

### configure Trusted IPs

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#trusted-ips>

### configure verification methods

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#selectable-verification-methods>

## Create a new tenant in Azure Active Directory

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-access-create-new-tenant>

## Associate or add an Azure subscription to your Azure Active Directory tenant

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-how-subscriptions-associated-directory>

NOTE:

Multiple subscriptions can trust the same Azure AD directory. Each subscription can only trust a single directory.

By default, when a user signs up for a Microsoft cloud service, an Azure AD tenant is created and the user is made a member of the Global Administrators role. When you add a subscription to an existing directory, you aren't assigned to the Global Administrator role.

If your subscription expires, you lose access to all the other resources associated with the subscription. However, the Azure AD directory remains in Azure. You can associate and manage the directory using a different Azure subscription.

# Azure Key Vault

**Key Management Service** tool for securely storing and accessing secrets. A secret is anything that you want to tightly control access to, such as API keys, passwords, or certificates. A vault is a logical group of secrets.