Create a user named Anahita atash biz Yeganeh and let her know that it will be ok tomorrow

MS 100 Exam (mi-octobre pour exam): <https://docs.microsoft.com/en-us/learn/certifications/exams/ms-100>

MS 600 : <https://docs.microsoft.com/en-us/learn/certifications/exams/ms-600>

Project 1 -Immigration tool: <https://sharegate.com/>

Project 2 : create a bot for MS Teams

What I need to learn and practice:

1. add and configure additional domains to a tenant
2. In tenant health, create internal service health response plan and configure and review reports, including BI, OMS, and Microsoft 365 reporting
3. Plan migration of users and data

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

There is two types of identity in office 365 :

1. Cloud-only (users accounts and password is stored only in Azure AD tenant for Microsoft 365)
2. Hybrid identity (user accounts are both stored both in Azure AD (AD DS) and On-premises)

AD DS is the original and authoritative copy of username and password of users

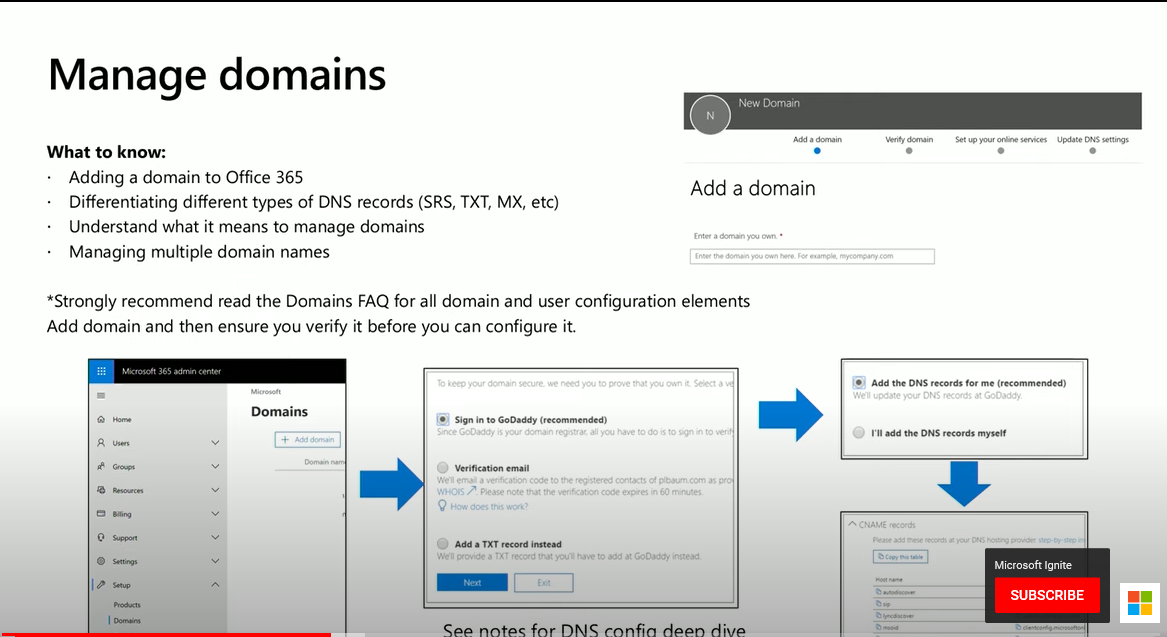
Saas= software as service

Paas = platform as service

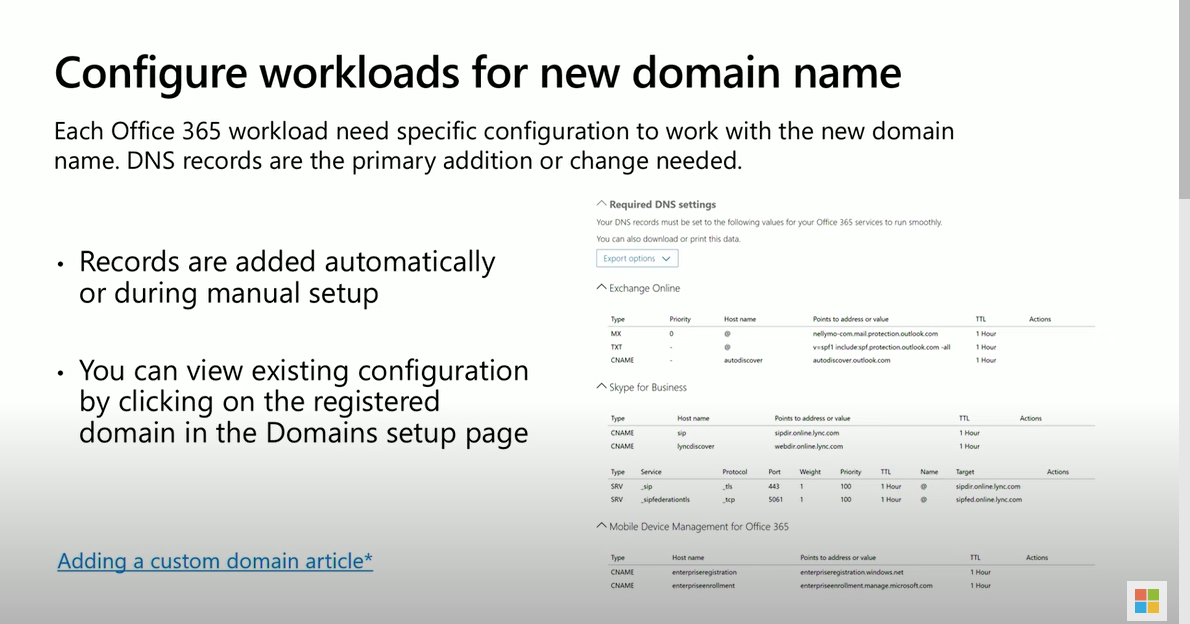
There are different ways to set up authentication for hybrid identity:

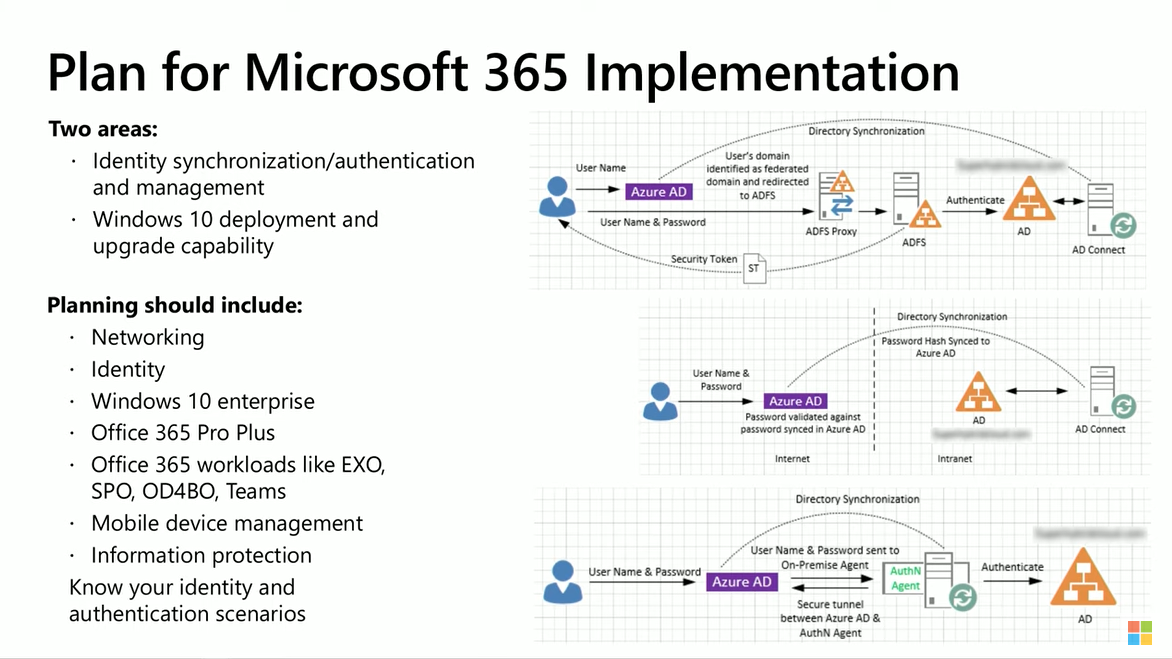
1. Managed (by Azure AD) – with this we have two options – password hash synchronization(PHS) – pass through authentication (PTA)
2. Federated (by an identity provider), they don’t have hash function so they are redirected to another identity provider to authenticate account

Adding a domain to O365

Types of DNS records(SRS,TXT,MX,…)

Read the Domains FAQ





* Know all the protocols for M365 implementation
* Know differences in different licenses (ex: difference between E5 and F1 ?)

PowerShell command to get the licenses:

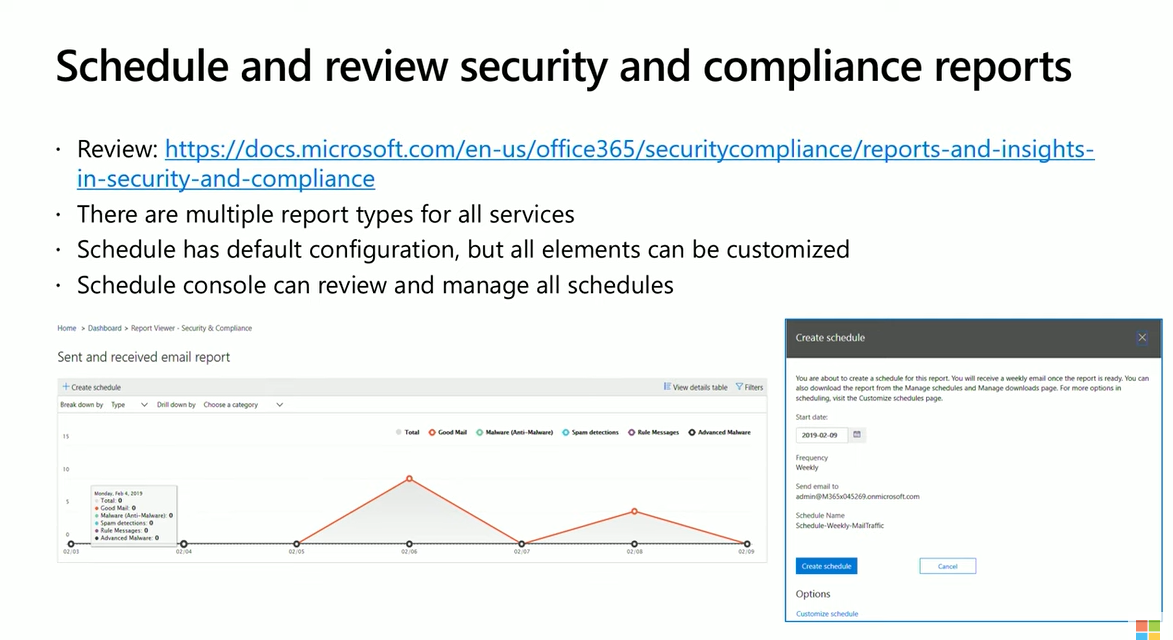
(Get-MsolAccountSku| where {$\_.AccountSkuId -eq ´TenantName:name ´}).ServiceStatus

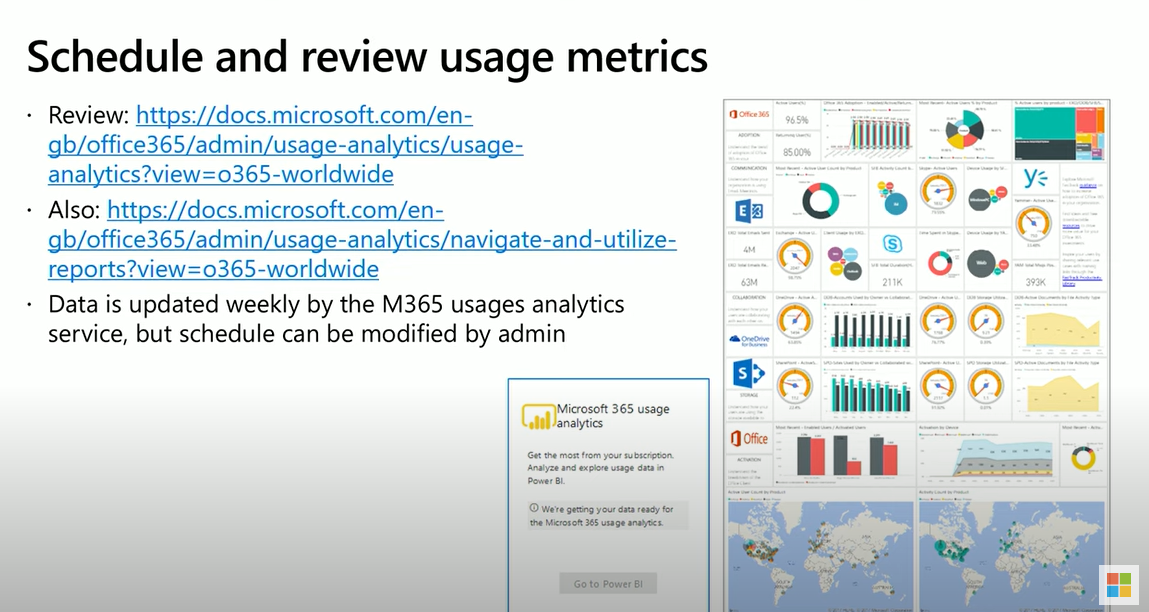
Know everything about tenant health

* Know how to raise a service request



* Security and compliance





**Migration**

Multiple ways to migrate document data into M365:

1. File share migration using SPMT (<http://aka.ms/spmt>)
2. SharePoint on-premises migration using SPMT

**Different types of migrating emails: hybrid, staged, cut-over**

**cut-over migration:** When you migrate the contents of user mailboxes from a source email system to Microsoft 365 or Office 365 **all at one time**, it's called a cutover migration. (<https://docs.microsoft.com/en-us/exchange/mailbox-migration/cutover-migration-to-office-365>)

Choosing a cutover migration is suggested when:

* Your current on-premises Exchange organization is Microsoft Exchange Server 2003 or later.
* Your on-premises Exchange organization has fewer than 2,000 mailboxes.
* A maximum of 2,000 mailboxes can be migrated to Microsoft 365 or Office 365 by using a cutover Exchange migration. However, it is recommended that you only migrate 150 mailboxes.

**Staged migration:** when we migrate emails **over-time** from a source to office365

(<https://docs.microsoft.com/en-us/exchange/mailbox-migration/what-to-know-about-a-staged-migration#:~:text=As%20part%20of%20a%20Microsoft,it's%20called%20a%20staged%20migration.&text=Consider%20using%20a%20cutover%20migration%20or%20a%20hybrid%20email%20migration%20instead.>)

A staged migration is recommended when:

* Your source email system is Microsoft Exchange Server 2003 or Microsoft Exchange Server 2007.
* You have more than 2,000 mailboxes.
* You can migrate only user mailboxes and resource mailboxes. Other recipient types, such as distribution groups, contacts, and mail-enabled users are migrated to Microsoft 365 or Office 365 through the process of directory synchronization.
* Out of Office messages aren't migrated with user mailboxes.

IMAP: used to migrate mailboxes from Gmail to O365. It only migrates items in a user’s mailbox and other mail folders. It does NOT migrate contacts, calendar, or tasks. We can migrate max of 500,000 items from a user’s mailbox. The biggest email we can migrate is 35 MB.

<https://docs.microsoft.com/en-us/exchange/mailbox-migration/migrating-imap-mailboxes/migrating-imap-mailboxes>

**Manage user identity and roles :**

<https://docs.microsoft.com/en-us/microsoft-365/enterprise/prepare-a-non-routable-domain-for-directory-synchronization?view=o365-worldwide>

* Know about critical roles (global , security, reader , …)
* Plan directory synchronization using AD Connect
* <https://docs.microsoft.com/en-us/Exchange/permissions/feature-permissions/policy-and-compliance-permissions?view=exchserver-2019>
* When you synchronize your on-premises directory with Microsoft 365 you have to have a verified domain in Azure Active Directory (Azure AD). Only the User Principal Names (UPN) that are associated with the on-premises domain are synchronized. However, any UPN that contains an non-routable domain, for example .local (like billa@contoso.local), will be synchronized to an .onmicrosoft.com domain (like [billa@contoso.onmicrosoft.com](mailto:billa@contoso.onmicrosoft.com)).
* The most recent tool you can use for synchronizing your AD DS to Azure AD is named Azure AD Connect. For more information, see [Integrating your on-premises identities with Azure AD](https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/identity/azure-ad). Azure AD Connect synchronizes your users' UPN and password so that users can sign in with the same credentials they use on-premises.

Azure AD Connect runs on an on-premises server and synchronizes your AD DS with the Azure AD tenant. Along with directory synchronization, you can also specify these authentication options:

* Password hash synchronization (PHS)

Azure AD performs the authentication itself.

* Pass-through authentication (PTA)

Azure AD has AD DS perform the authentication.

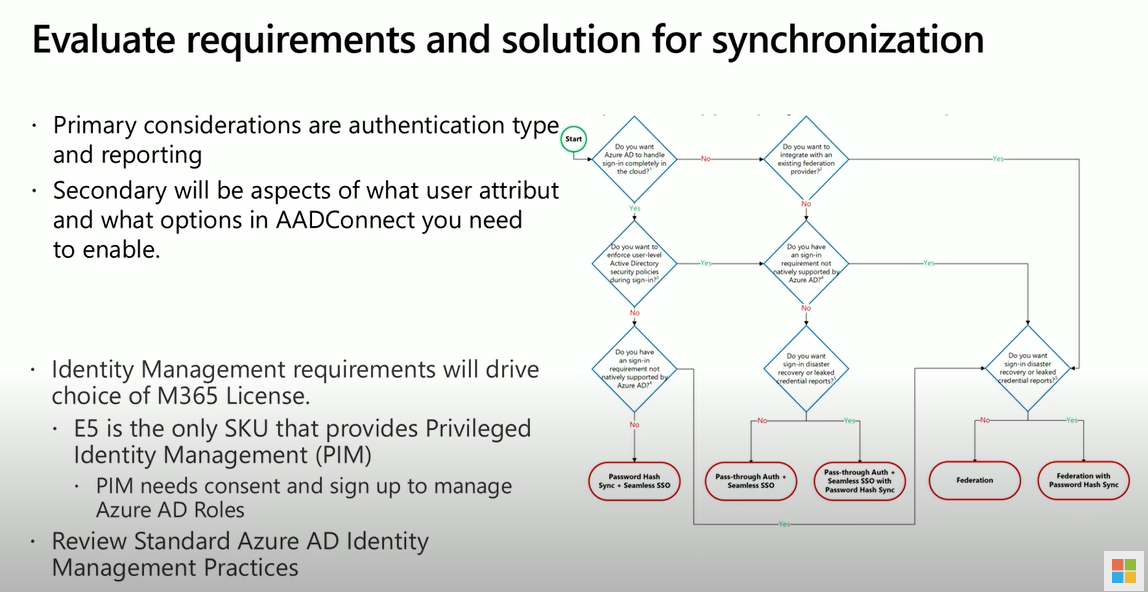
* Federated authentication

Azure AD redirects the client computer requesting authentication to contact another identity provider.

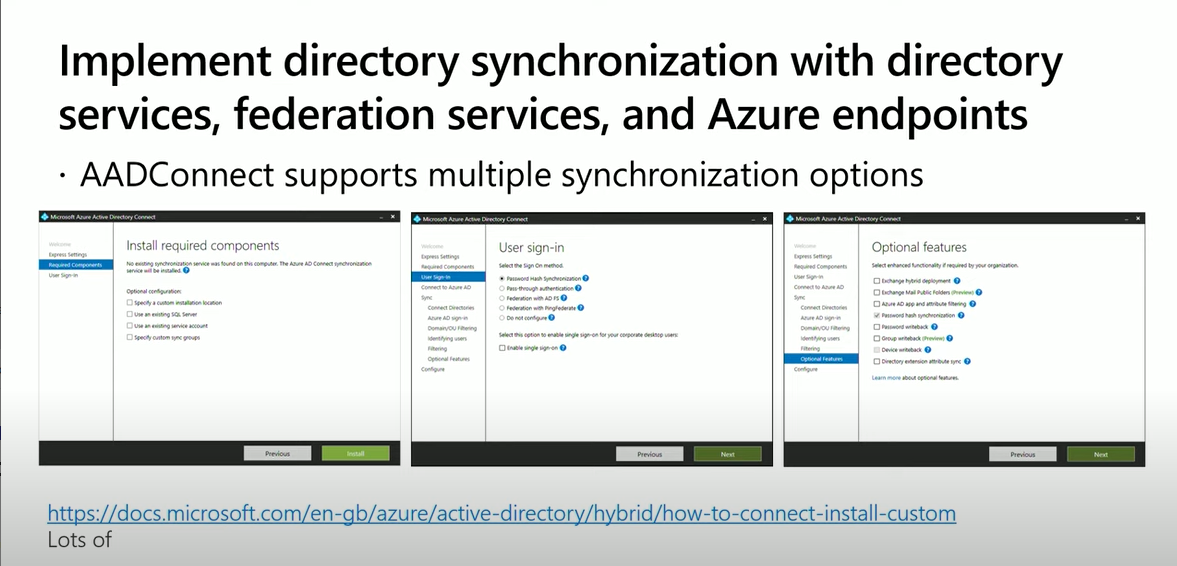
Multiple Azure AD tenants:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-topologies#multiple-azure-ad-tenants>

There's a 1:1 relationship between an Azure AD Connect sync server and an Azure AD tenant. For each Azure AD tenant, you need one Azure AD Connect sync server installation. The Azure AD tenant instances are isolated by design. That is, users in one tenant can't see users in the other tenant. If you want this separation, this is a supported configuration. Otherwise, you should use the single Azure AD tenant model.

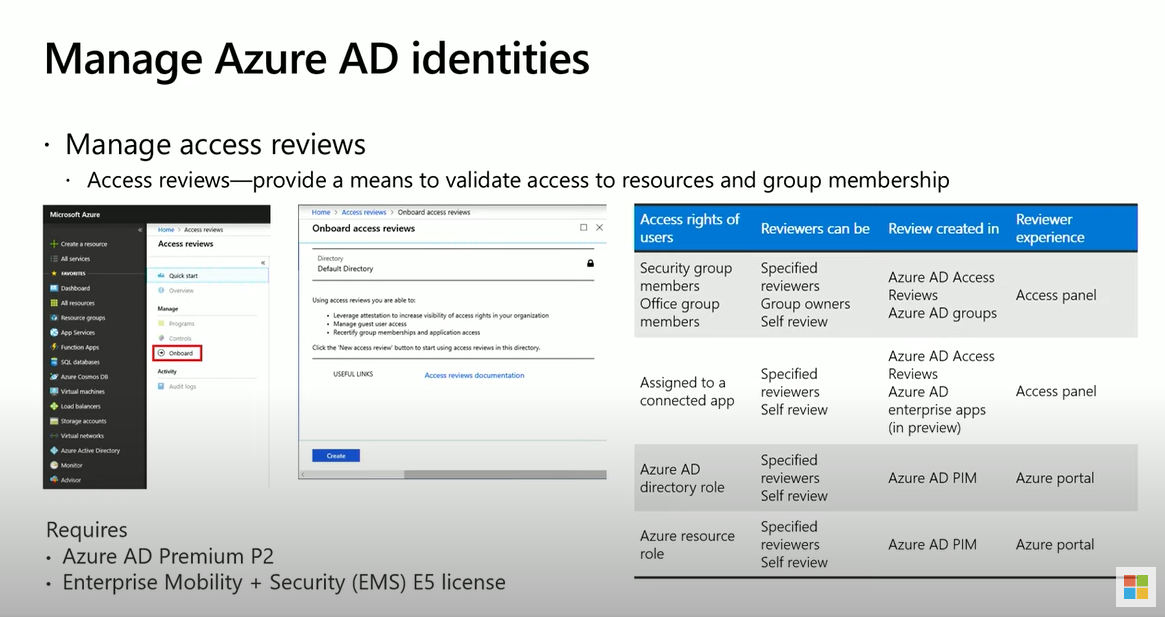


AD Connect tool:



Manage identity synchronization by using Azure AD Connect :

Monitor Azure AD Connect Health (support is available for monitoring Sync,ADFS, AAD DS)



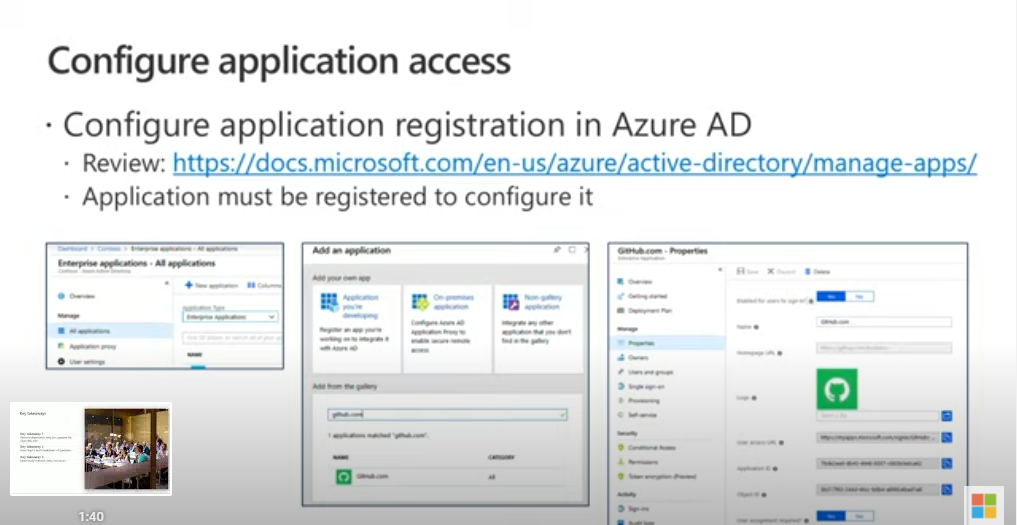
* Get AD premium and build groups and explore them to know Azure AD user and group management

**Manage authentication**:

* MFA
* Application access (<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/>

Azure AD needs to know what applications are using it as an identity system. The process of keeping Azure AD aware of these applications, and how it should handle them, is known as application management.

We manage applications on the Azure Active Directory portal > Enterprise applications blade



IAM (Identity and Access Management system) : An IAM system provides a single place to keep track of user identities. Azure AD is the IAM system for the Microsoft cloud.

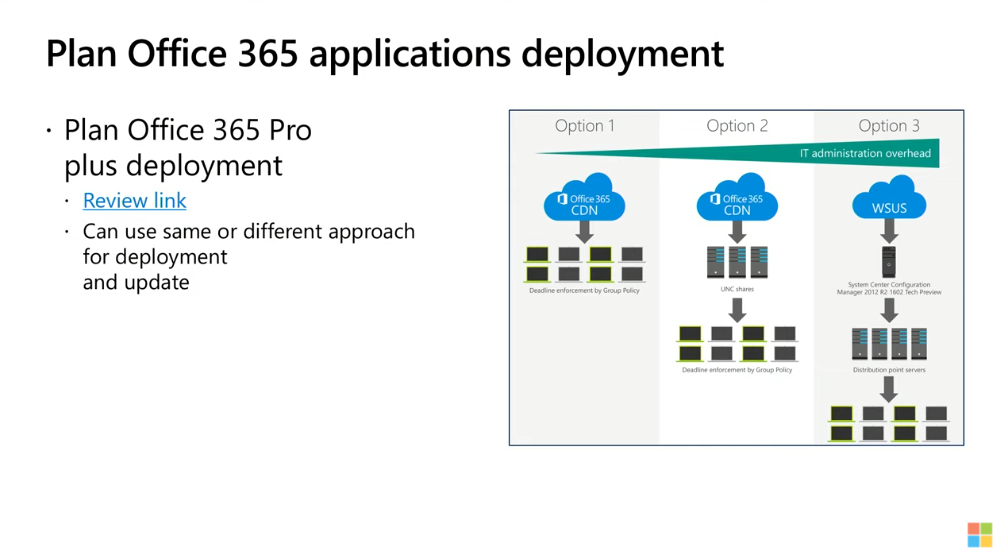
You can add your software as a service (SaaS) applications, on-premises applications, and line of business (LOB) apps to Azure AD. Then users sign in once to securely and seamlessly access these applications, along with Office 365 and other business applications from Microsoft. You can reduce administrative costs by [automating user provisioning](https://docs.microsoft.com/en-us/azure/active-directory/app-provisioning/user-provisioning). You can also use multi-factor authentication and Conditional Access policies to provide secure application access.

With Azure AD Application Proxy, you can integrate your on-premises web apps with Azure AD to support single sign-on. Then end users can access your on-premises web apps in the same way they access Office 365 and other SaaS apps.

SSO (Single Sign on ) : Single sign-on means a user doesn't have to sign in to every application they use. The user logs in once and that credential is used for other apps too.

Tutorial for integrating SaaS applications with Azure AD : <https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/tutorial-list>

* Create B2B accounts (<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/what-is-b2b>)



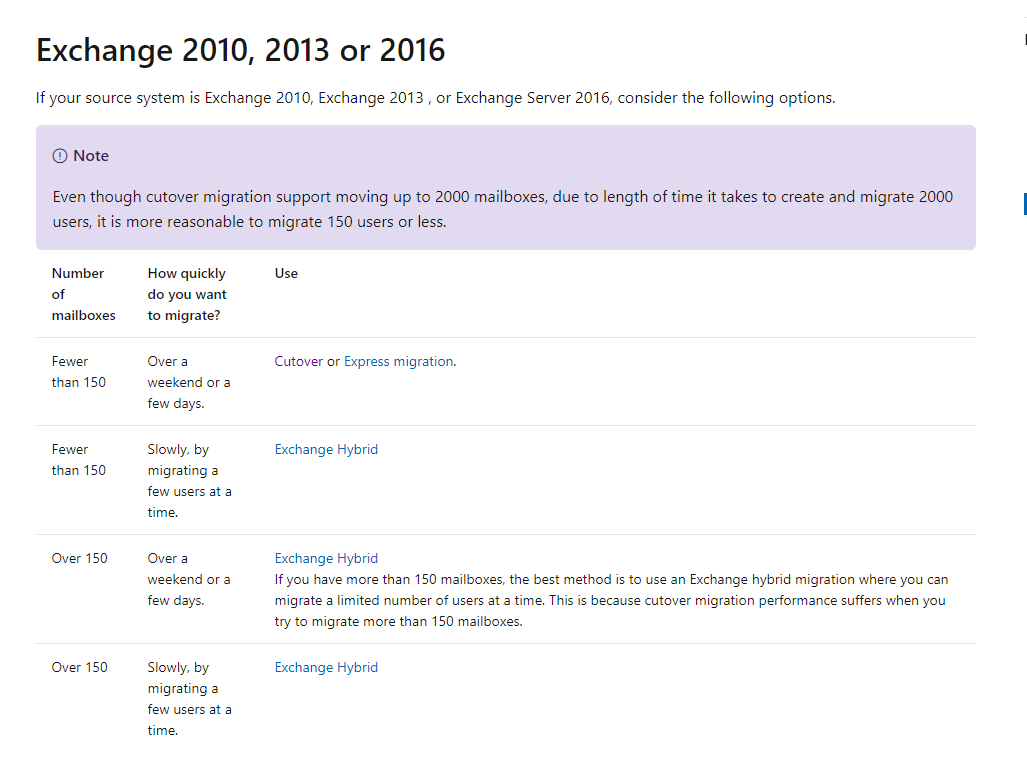
* A Cloud discovery anomaly detection policy enables you to set up and configure continuous monitoring of unusual increases in cloud application usage. Increases in downloaded data, uploaded data, transactions, and users are considered for each cloud application. Each increase is compared to the normal usage pattern of the application as learned from past usage. The most extreme increases trigger security alerts.

**Security and compliance roles:** <https://docs.microsoft.com/en-gb/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center?view=o365-worldwide#mapping-of-role-groups-to-assigned-roles>

How create sign-in risk policy : <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies>

**Exchange server 2003 or Exchange server2007 migration**

****

****

Windows 10 deployment scenarios : <https://docs.microsoft.com/en-us/windows/deployment/windows-10-deployment-scenarios%20>

Your company has a Microsoft Azure Active Directory (Azure AD) directory tenant named contoso.onmicrosoft.com.  
All users have client computers that run Windows 10 Pro and are joined to Azure AD.  
The company purchases a Microsoft 365 E3 subscription.  
You need to upgrade all the computers to Windows 10 Enterprise. The solution must minimize administrative effort.  
You assign licenses from the Microsoft 365 admin center.  
What should you do next?

* A. Add a custom domain name to the subscription.
* B. Deploy Windows 10 Enterprise by using Windows Autopilot.
* C. Create provisioning package, and then deploy the package to all the computers.
* D. Instruct all the users to log off of their computer, and then to log in again.

You have an on-premises web application that is published by using a URL of https://app.contoso.local.  
You purchase a Microsoft 365 subscription.  
Several external users must be able to connect to the web application.  
You need to recommend a solution for external access to the application. The solution must support multi-factor authentication.  
Which two actions should you recommend? Each correct answer presents part of the solution.  
NOTE: Each correct selection is worth one point.

* A. From an on-premises server, install a connector and then publish the app.
* B. From the Azure Active Directory admin center, enable an Application Proxy.
* C. From the Azure Active Directory admin center, create a conditional access policy.
* D. From an on-premises server, install an Authentication Agent.
* E. Republish the web application by using https://app.contoso.local.