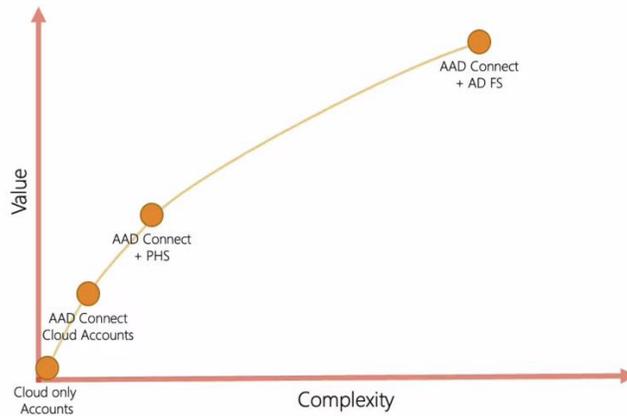


## SSO in Azure AD-Connect.

### 1. Step1:

# Sign-in Options today

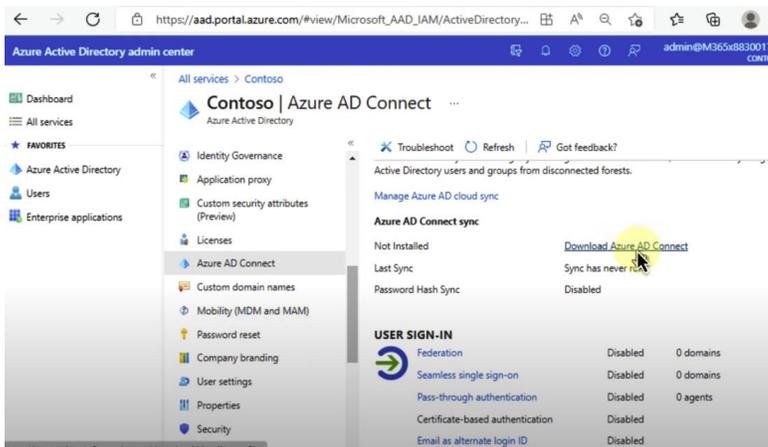


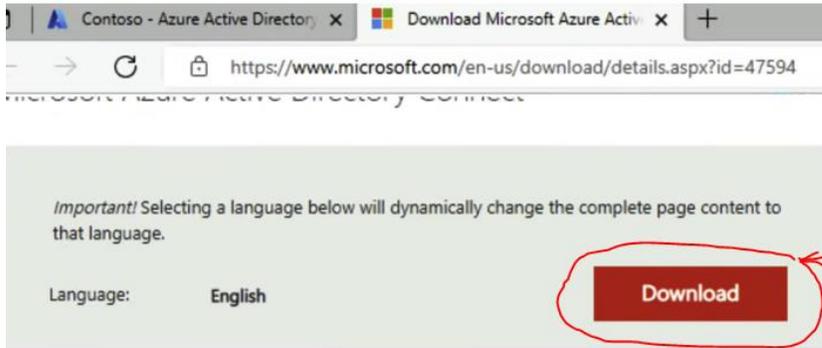
## Install Azure AD-Connect



- Install all dependencies:
  - SQL Express LocalDB, Sync, Sign-in assistant, AAD Connector
- With default settings:
  - Local service account w/ random password

### 2. Download & install : Global Admin to install

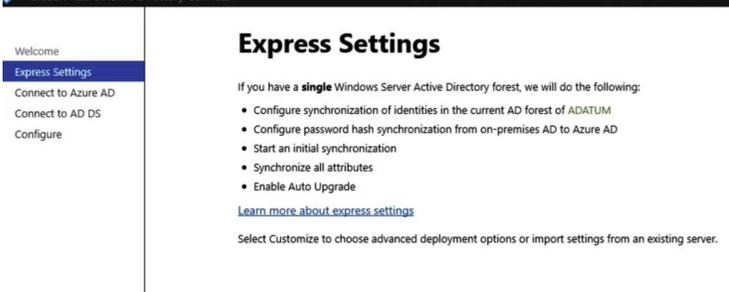
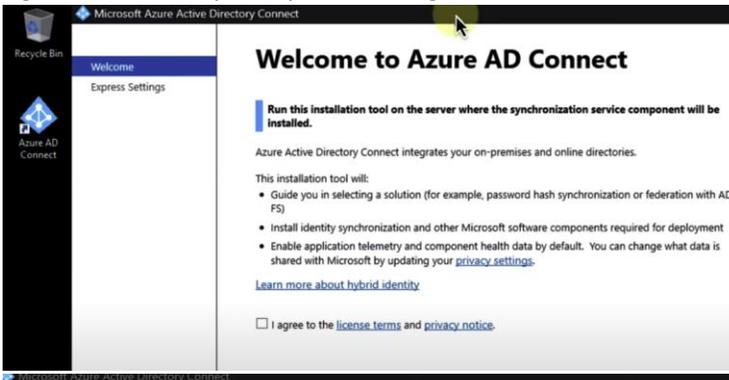




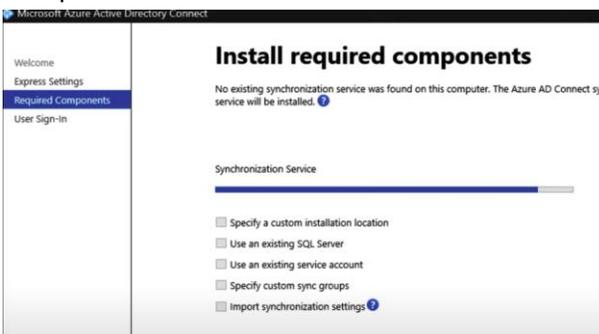
### 3. Install:



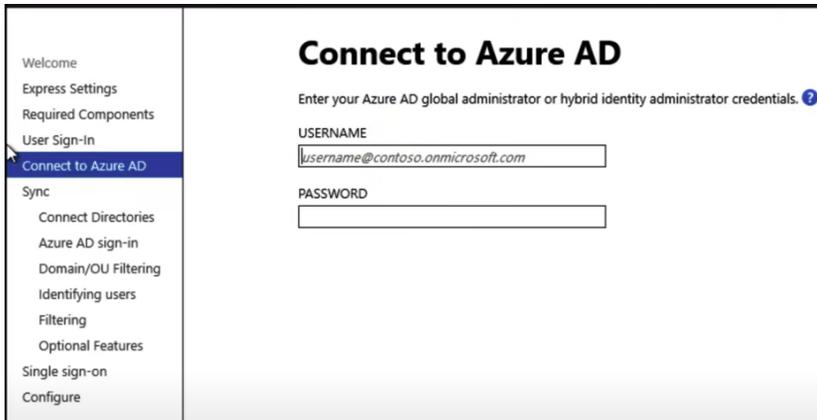
### 4. Agree & Accept - Express Setting.



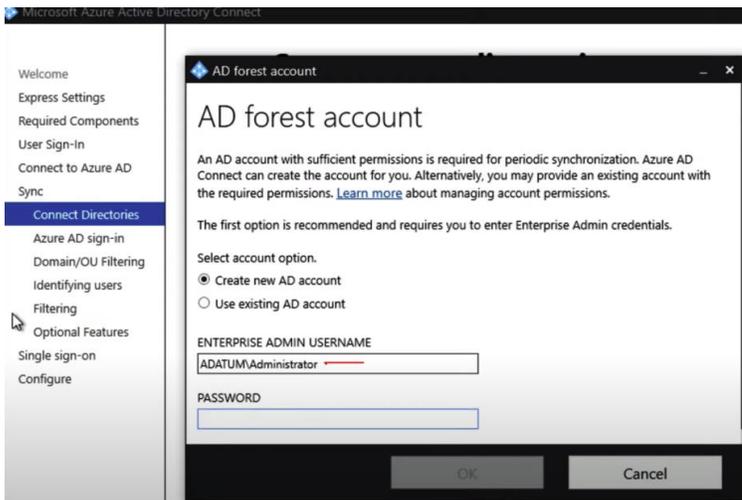
### 5. Accept & continue



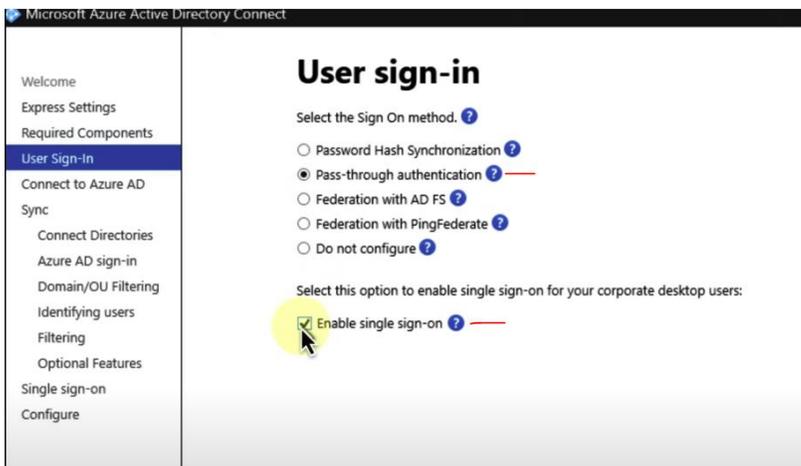
### 6. Connect AAD and use Global Admin/Domain Admin



### 7. Add AD admin



### 8. Select PTA & Enable SSO to continue



Connect to Azure AD

Welcome  
Express Settings  
Required Components  
User Sign-In  
**Connect to Azure AD**  
Sync  
Connect Directories  
Azure AD sign-in  
Domain/OU Filtering  
Identifying users  
Filtering  
Optional Features  
Single sign-on  
Configure

## Connect to Azure AD

Enter your Azure AD global administrator or hybrid identity administrator credentials. ?

USERNAME

PASSWORD

### Connect your AD

Welcome  
Express Settings  
Required Components  
User Sign-In  
Connect to Azure AD  
Sync  
**Connect Directories**  
Azure AD sign-in  
Domain/OU Filtering  
Identifying users  
Filtering  
Optional Features  
Single sign-on  
Configure

## Connect your directories

Enter connection information for your on-premises directories or forests. ?

DIRECTORY TYPE

FOREST ?

*No directories are currently configured.*

### Using Enterprise Admin to login

Welcome  
Express Settings  
Required Components  
User Sign-In  
Connect to Azure AD  
Sync  
**Connect Directories**  
Azure AD sign-in  
Domain/OU Filtering  
Identifying users  
Filtering  
Optional Features  
Single sign-on  
Configure

#### AD forest account

An AD account with sufficient permissions is required for periodic synchronization. Azure AD Connect can create the account for you. Alternatively, you may provide an existing account with the required permissions. [Learn more](#) about managing account permissions.

The first option is recommended and requires you to enter Enterprise Admin credentials.

Select account option.

Create new AD account  
 Use existing AD account

ENTERPRISE ADMIN USERNAME

PASSWORD

### Accept & check Continue

Welcome

Express Settings

Required Components

User Sign-In

Connect to Azure AD

Sync

Connect Directories

**Azure AD sign-in**

Domain/OU Filtering

Identifying users

Filtering

Optional Features

Single sign-on

Configure

## Azure AD sign-in configuration

To sign-in to Azure with the same credentials as your on-premises directory, a matching Azure AD Domain is required. The following table lists the UPN suffixes for your on-premises environment and the status of the associated Azure AD Domain. [?](#)

Active Directory UPN Suffix	Azure AD Domain
adatum.com	Not Added <a href="#">?</a>
microsoft.com	Not Added <a href="#">?</a>

Select the on-premises attribute to use as the Azure AD username

USER PRINCIPAL NAME [?](#)

userPrincipalName

Continue without matching all UPN suffixes to verified domains

**Users will not be able to sign-in to Azure AD with on-premises credentials if the UPN suffix does not match a verified domain.** [Learn more](#)

### 9. Select Domain, OU to synch

Microsoft Azure Active Directory Connect

Welcome

Express Settings

Required Components

User Sign-In

Connect to Azure AD

Sync

Connect Directories

Azure AD sign-in

**Domain/OU Filtering**

Identifying users

Filtering

Optional Features

Single sign-on

Configure

## Domain and OU filtering

Directory: adatum.com [Refresh Domains](#) [?](#)

Sync all domains and OUs [?](#)

Sync selected domains and OUs

- adatum.com
  - Builtin
  - Computers
  - Development
  - Domain Controllers
  - ForeignSecurityPrincipals
  - Infrastructure
  - IT
  - LostAndFound
  - Managed Service Accounts
  - Managers
  - Marketing
  - Program Data
  - Research
  - Sales
  - System
  - Users

### 10. Select Users and across all

Microsoft Azure Active Directory Connect

Welcome  
Express Settings  
Required Components  
User Sign-In  
Connect to Azure AD  
Sync  
Connect Directories  
Azure AD sign-in  
Domain/OU Filtering  
**Identifying users**  
Filtering  
Optional Features  
Single sign-on  
Configure

## Uniquely identifying your users

Select how users should be identified in your on-premises directories. ?

- Users are represented only once across all directories.
- User identities exist across multiple directories. Match using:
  - Mail attribute
  - ObjectSID and msExchMasterAccountSID/msRTCSIP-OriginatorSID attributes
  - SAMAccountName and MailNickName attributes
  - A specific attribute

Select how users should be identified with Azure AD. ?

- Let Azure manage the source anchor
- Choose a specific attribute

**Azure will write back unique source anchors to your on-premises directory if mS-DS-ConsistencyGuid is currently unused by your organization. [Learn more](#)**

### 11. Keep as it

Welcome  
Express Settings  
Required Components  
User Sign-In  
Connect to Azure AD  
Sync  
Connect Directories  
Azure AD sign-in  
Domain/OU Filtering  
Identifying users  
Filtering  
**Optional Features**  
Single sign-on  
Configure

## Optional features

Select enhanced functionality if required by your organization.

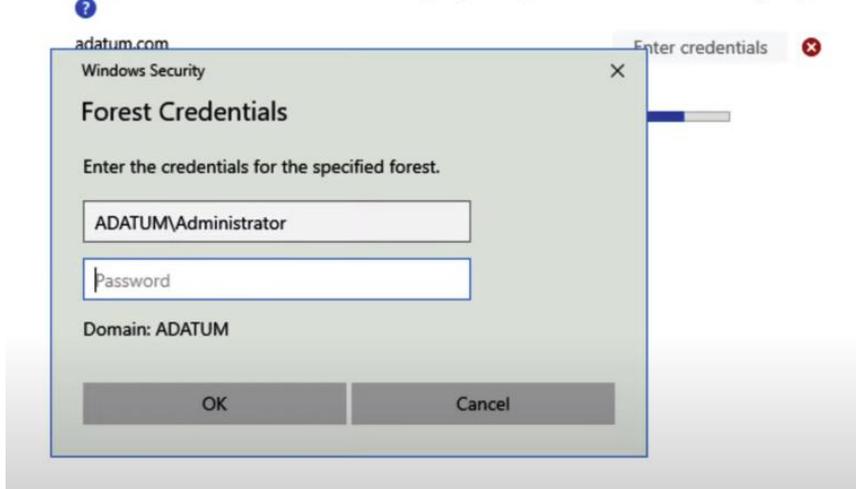
- Exchange hybrid deployment ?
- Exchange Mail Public Folders ?
- Azure AD app and attribute filtering ?
- Password hash synchronization ?
- Password writeback ?
- Group writeback ⚠
- Device writeback ?
- Directory extension attribute sync ?

[Learn more](#) about optional features.

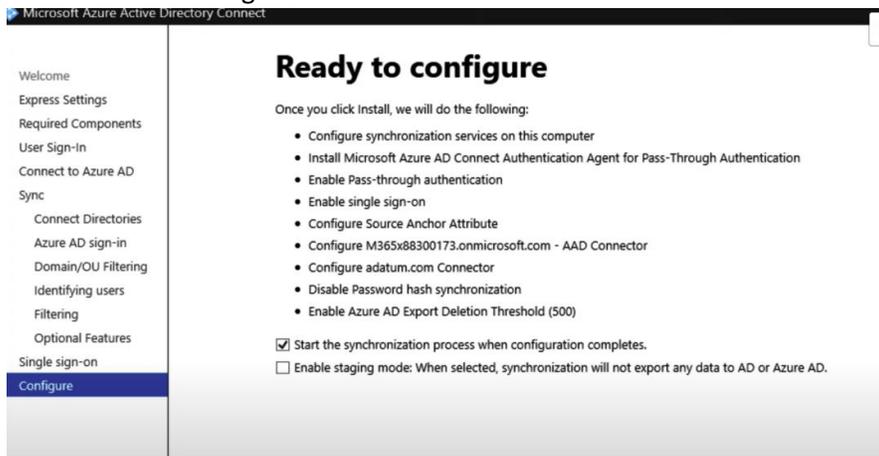
12. Click Enable SSO & login

## Enable single sign-on

Enter a domain administrator account to configure your on-premises forest for use with single sign-on.



13. Click Start and configure



14.

## Configuration complete

Azure AD Connect configuration succeeded. The synchronization process has been initiated.

**The configuration is complete. You can now log in to the Azure or Office 365 portal to verify that user accounts from your local directory have been created. Then, do a test sign-on to the Azure portal. [Learn more about the next steps and managing Azure AD Connect](#)**

**The Active Directory Recycle Bin is not enabled for your forest (adatum.com) and is strongly recommended. [Learn more about enabling the Active Directory Recycle Bin](#)**

**Azure Active Directory is configured to use AD attribute `mS-DS-ConsistencyGuid` as the source anchor attribute. [Learn more about configuring the source anchor attribute](#)**

**Provide your users a single sign-on experience by configuring Seamless SSO through Group Policy. [Learn more](#)**

15. Testing...Go each **user account** to unblock & add licenses

