
18
Win ays
Technology
Microsoft

Microsoft

Office 365 SSO
Lako i jednostavno

Vladimir Stefanović
Superadmins - Belgrade

Who am I

- Vladimir Stefanović
- System Engineer @Superadmins
- Techical Trainer @ATC
- MCSA, MCSE, MCT, IAMCT Regional Lead, Speaker
- vladimir@superadmins.com
- www.tech-trainer.info
- https://github.com/Wladinho/Presentations

Windays 18

Microsoft

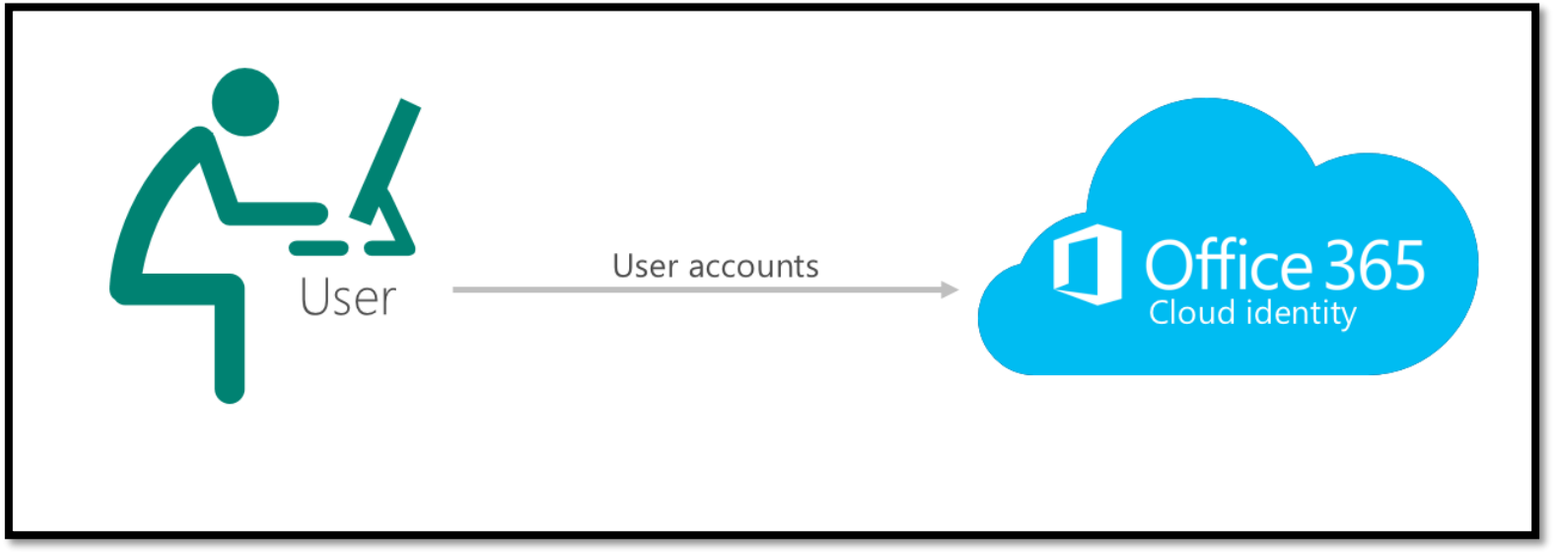
Agenda

- Identity models
- Pros and cons
- Seamless SSO
- Demo - ADFS & PTA
- Q & A

Identity models

Cloud identity

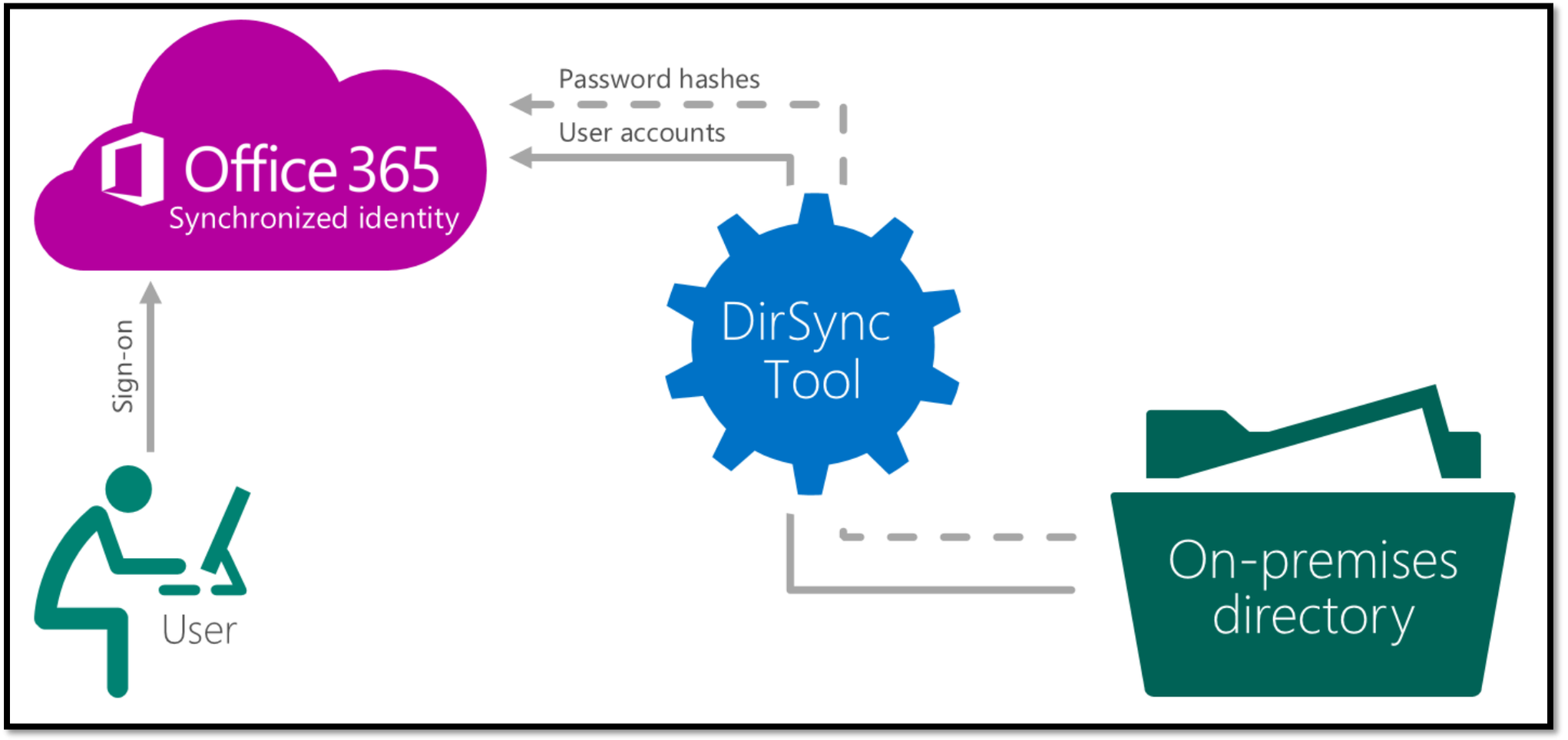
- User is created and managed in Office 365 and stored in Azure Active Directory
- Identity is verified by Azure AD
- There is no equivalent user account on-premises



Synchronized Identity - PHS & PTA

- User identity is created and managed in an on-premises server
- Accounts and **password hashes* are synchronized to the cloud
  - **With PTA, user passwords don't need to be synchronized with cloud*
- The user enters the same password on-premises as they do in the cloud
- Identity is verified by Azure AD / On-premise AD
- This model uses the Microsoft Azure AD Sync Tool

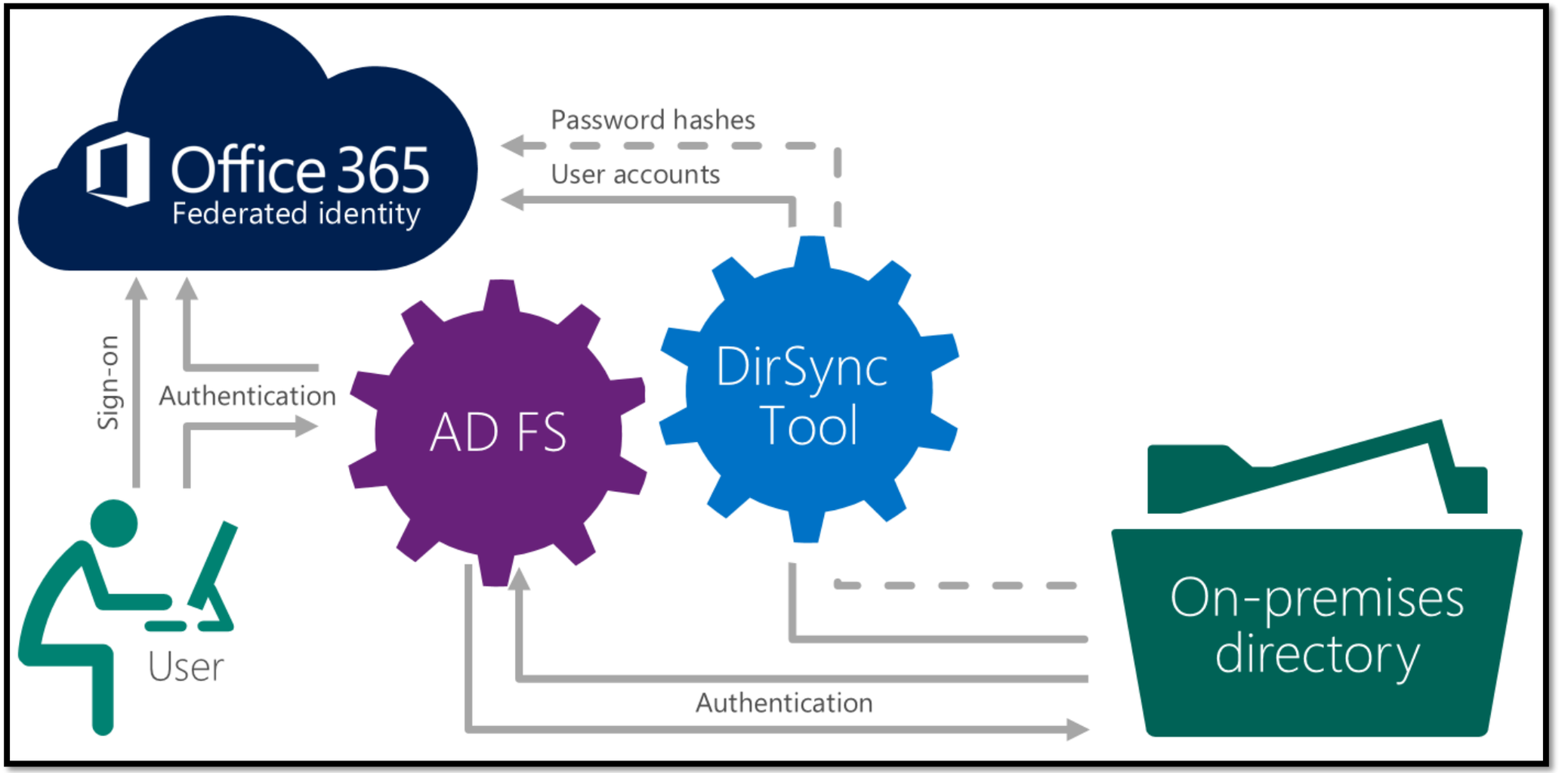
Synchronized Identity - PHS & PTA



Federated Identity - ADFS

- This model requires a synchronized identity
- Big difference - the user password is verified by the on-premises identity provider
- Password hash does not need to be synchronized to Azure AD
- This model uses AD FS or a third- party identity provider

Federated Identity - ADFS



Identity models - Pros and cons

Cloud Identity

- Pros:
  - *Quick implementation*
  - *Self-service password reset is available for Office 365 accounts*
  - *No need to dedicate servers or infrastructure for SSO*
  - *Can be used if AD is not deployed or most clients are not AD joined*
- Cons:
  - *No SSO for end users*

Identity models - Pros and cons

Password Synchronization

- Pros:
  - *Users have one password to remember for on-premise and cloud*
  - *The same server sync user data and passwords*
  - *No downtime for cloud apps if local AD is down*
- Cons:
  - *Domain-joined clients will still be prompted for password*
  - *Self-service password reset require Azure AD Premium or Enterprise Mobility + Security Suite licenses*

Identity models - Pros and cons

Pass Through Authentication

- Pros:
  - *True SSO for domain joined PCs in Outlook (2013 or later) and web browser*
  - *Similar experiences to password sync for external or non-domain PCs*
  - *Built into Azure AD Connect*
  - *Can deploy additional agents for redundancy*
  - *Security requirements that prohibit syncing a password hash*
- Cons:
  - *Redundancy can be a challenge for companies without resources*
  - *Browser based SSO still requires an initial "challenge" to determine where to redirect authentication*

Identity models - Pros and cons

Federated Identity

- Pros:
  - *Full SSO capabilities in the web browser and Outlook*
  - *Advanced security configurations available including the ability to filter connection on source IP address*
  - *No need to sync a password hash*
  - *ADFS farm can be reused with other cloud services that support SAML*
- Cons:
  - *Additional infrastructure requirements and cost to setup*
  - *Additional points of failure*
  - *SSL certificate from a public CA is required*

Azure AD Seamless SSO - PHS and PTA

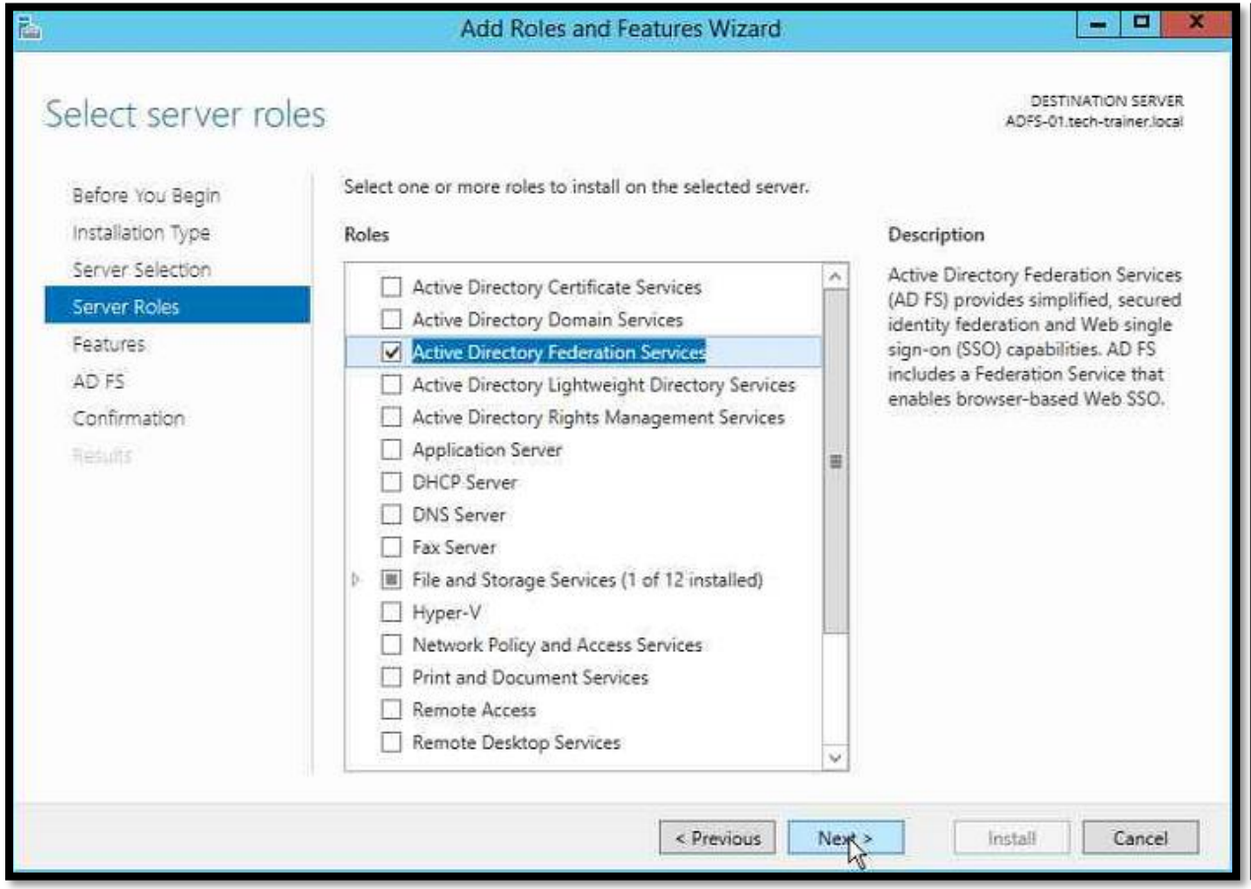
- Great user experience
  - *Users are automatically signed into on-premises and cloud-based apps*
  - *Users don't have to enter their passwords*
- Easy to deploy & administer
  - *No additional components needed on-premises*
  - *Works with Password Hash Synchronization or Pass-through Authentication*
  - *Can be rolled out to some or all your users using Group Policy*
- Seamless SSO is an opportunistic feature. If it fails for any reason, the user sign-in experience goes back to its regular behavior

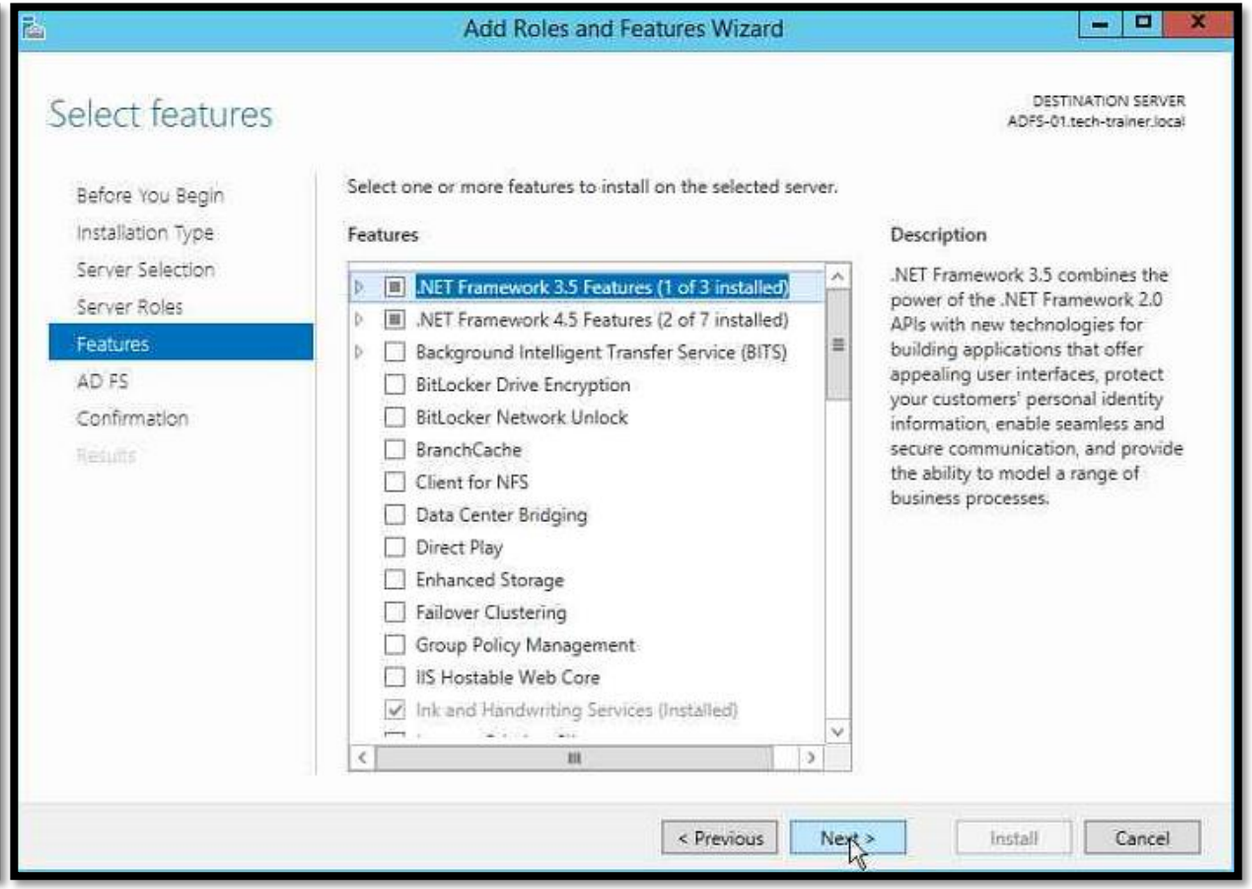
Do not forget

- Athe following Azure AD URL to the users *Intranet zone settings* by using GPO
  - *https://autologon.microsoftazuread-sso.com*
  - *https://aadg.windows.net.nsatc.net*

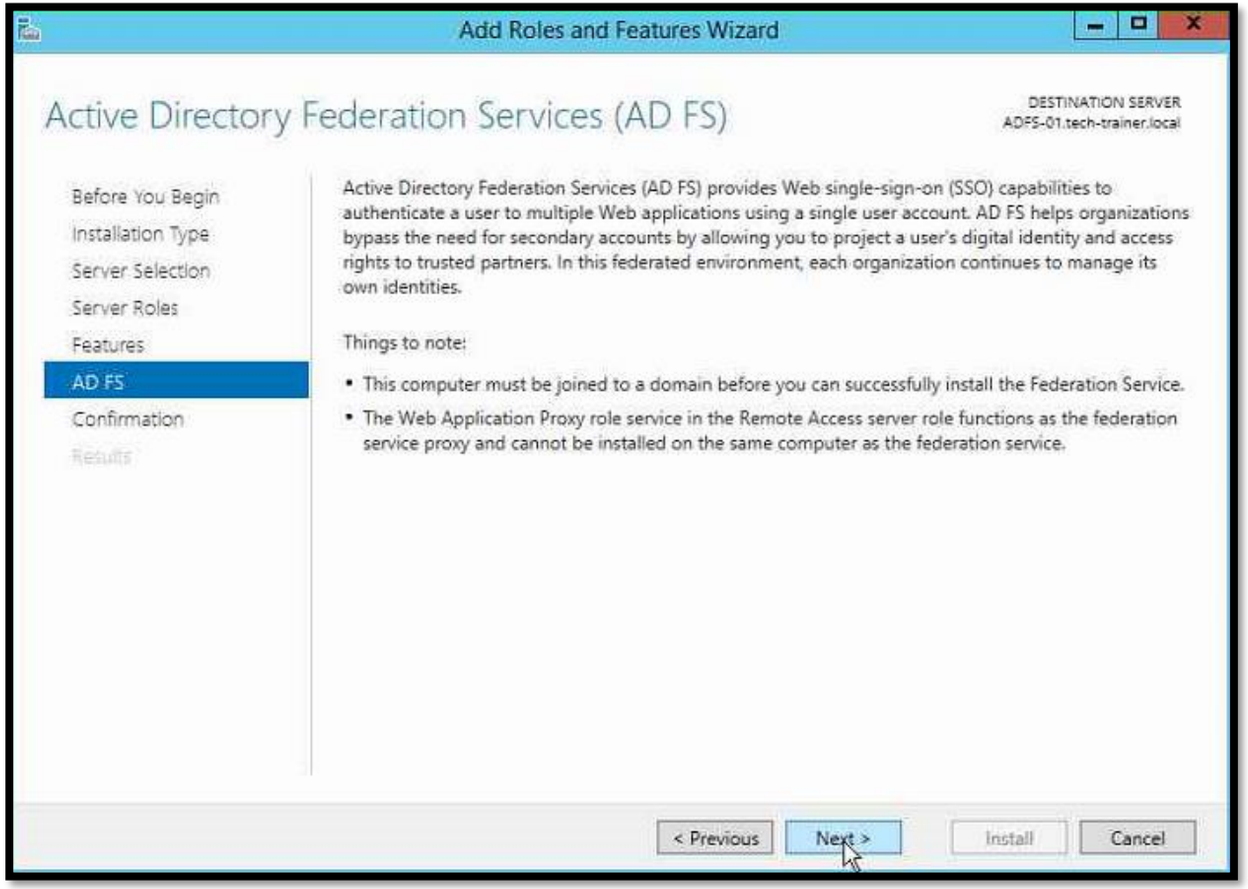
Demo - ADFS

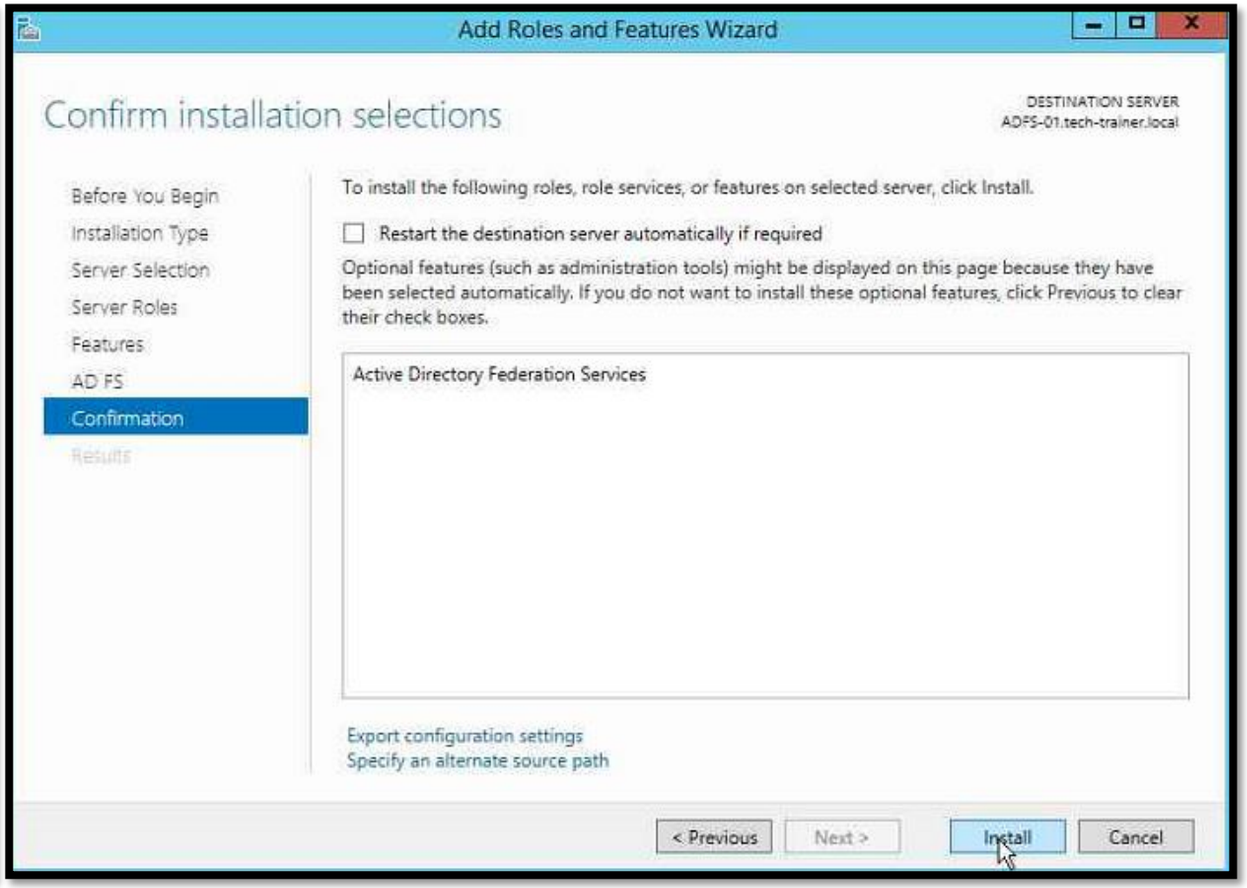
ADFS - Step-by-step





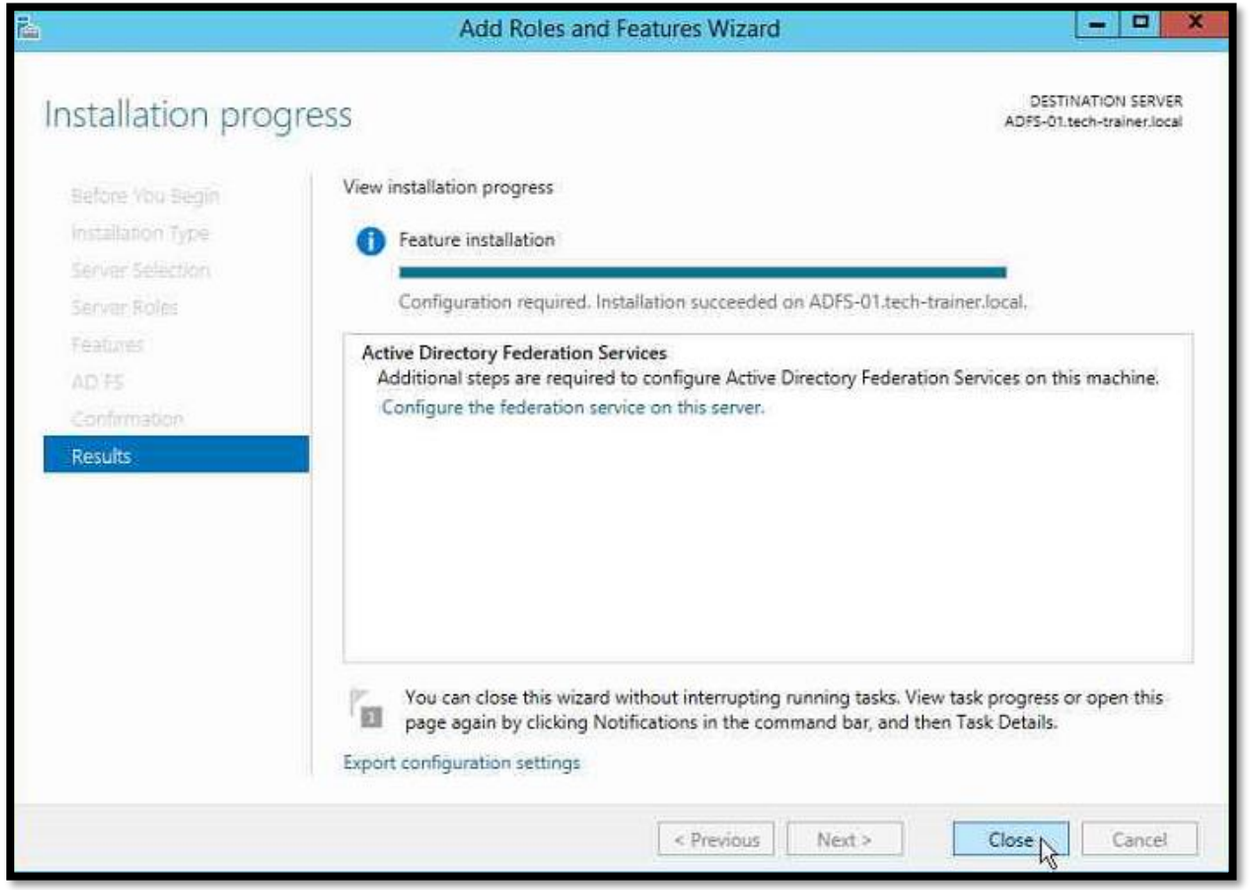
ADFS - Step-by-step

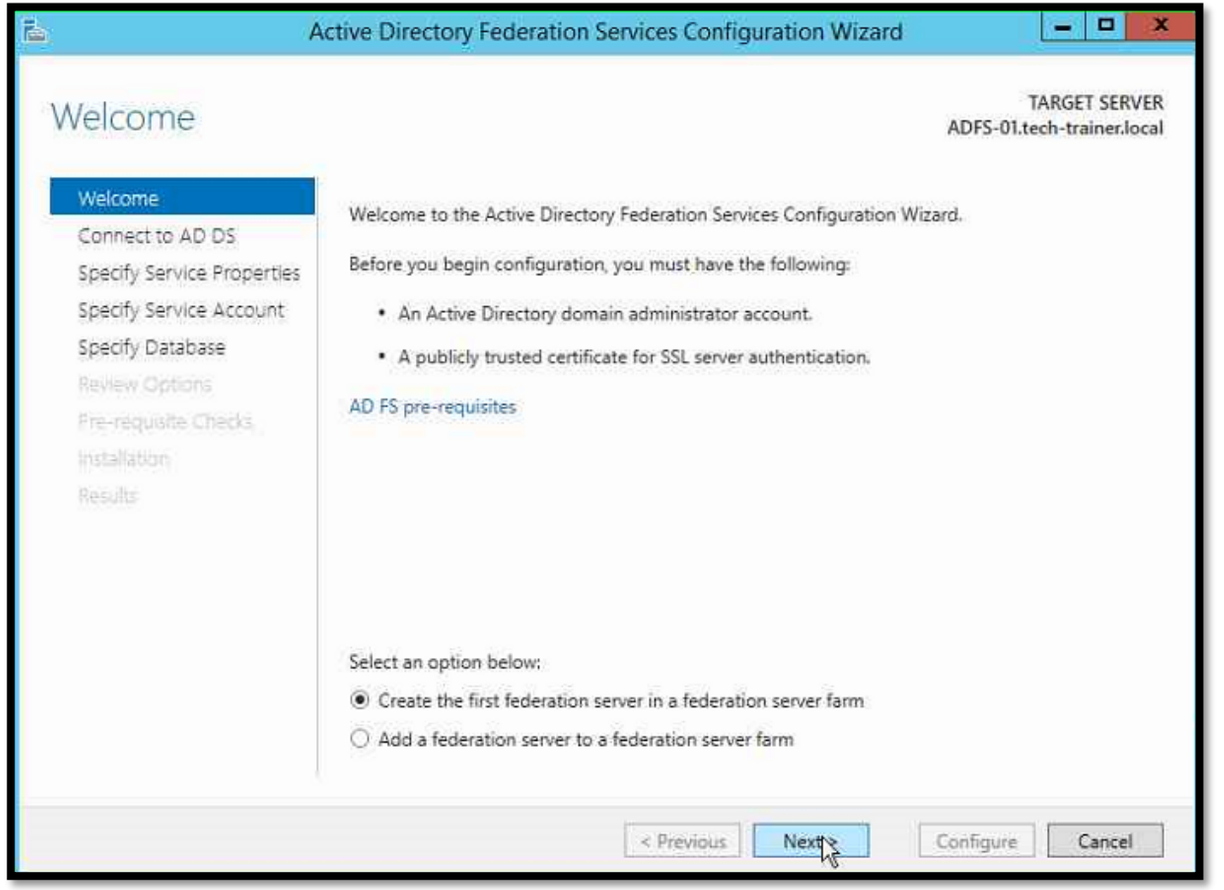




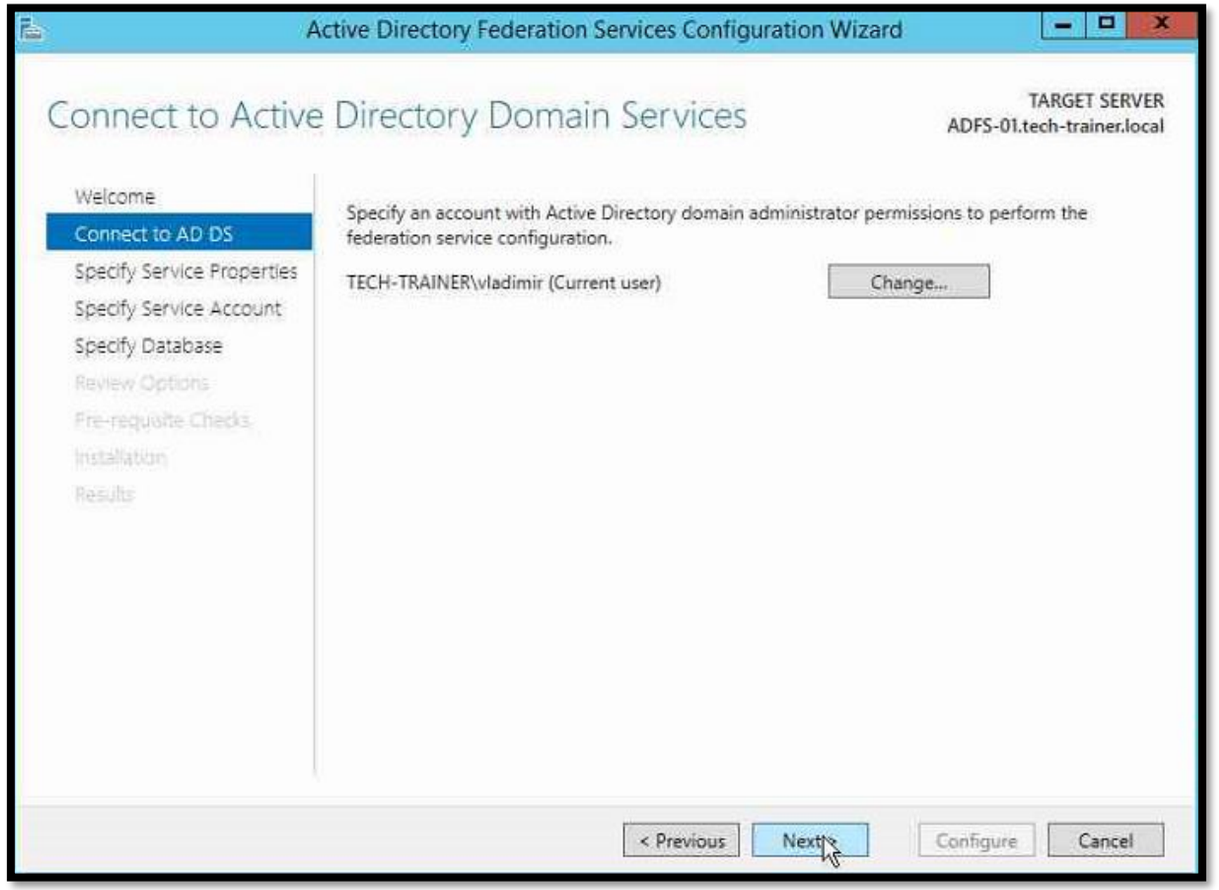
Windays 18

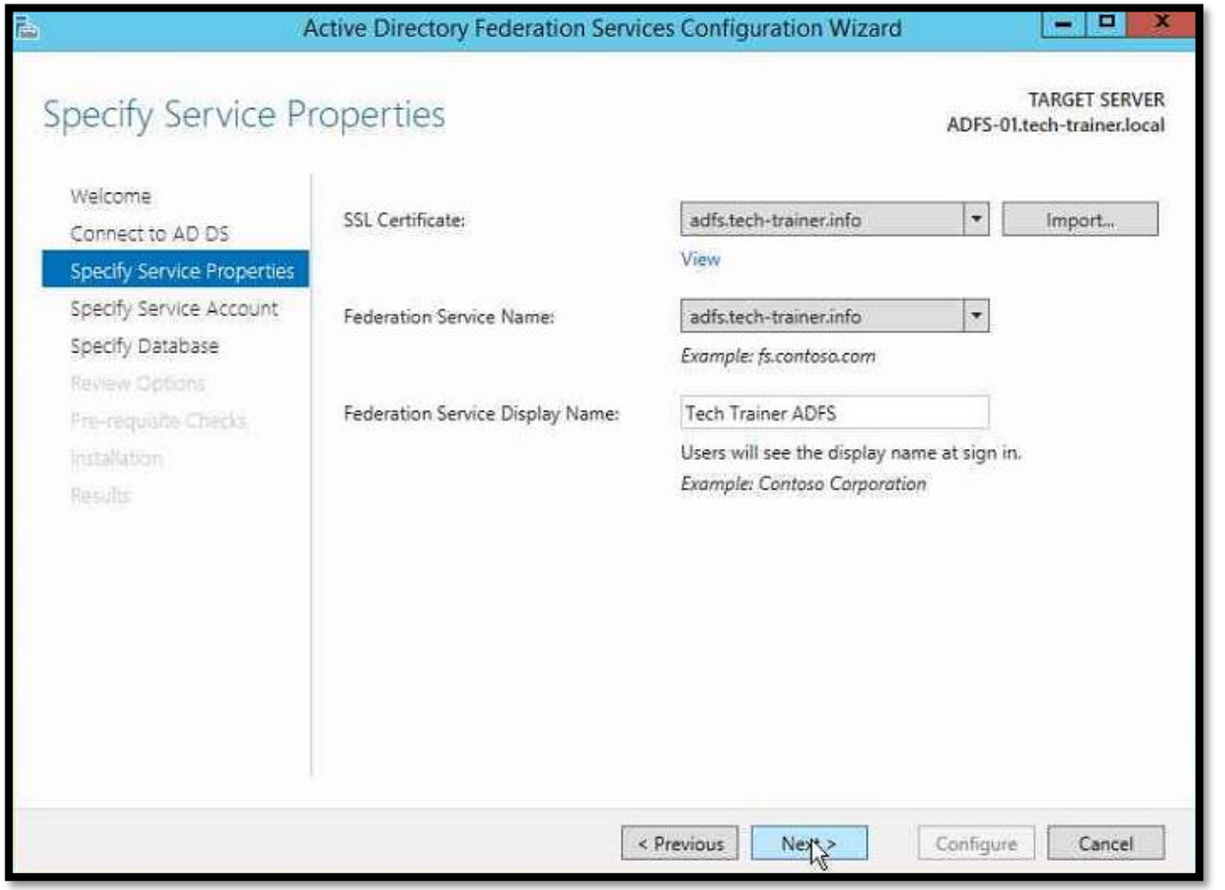
ADFS - Step-by-step





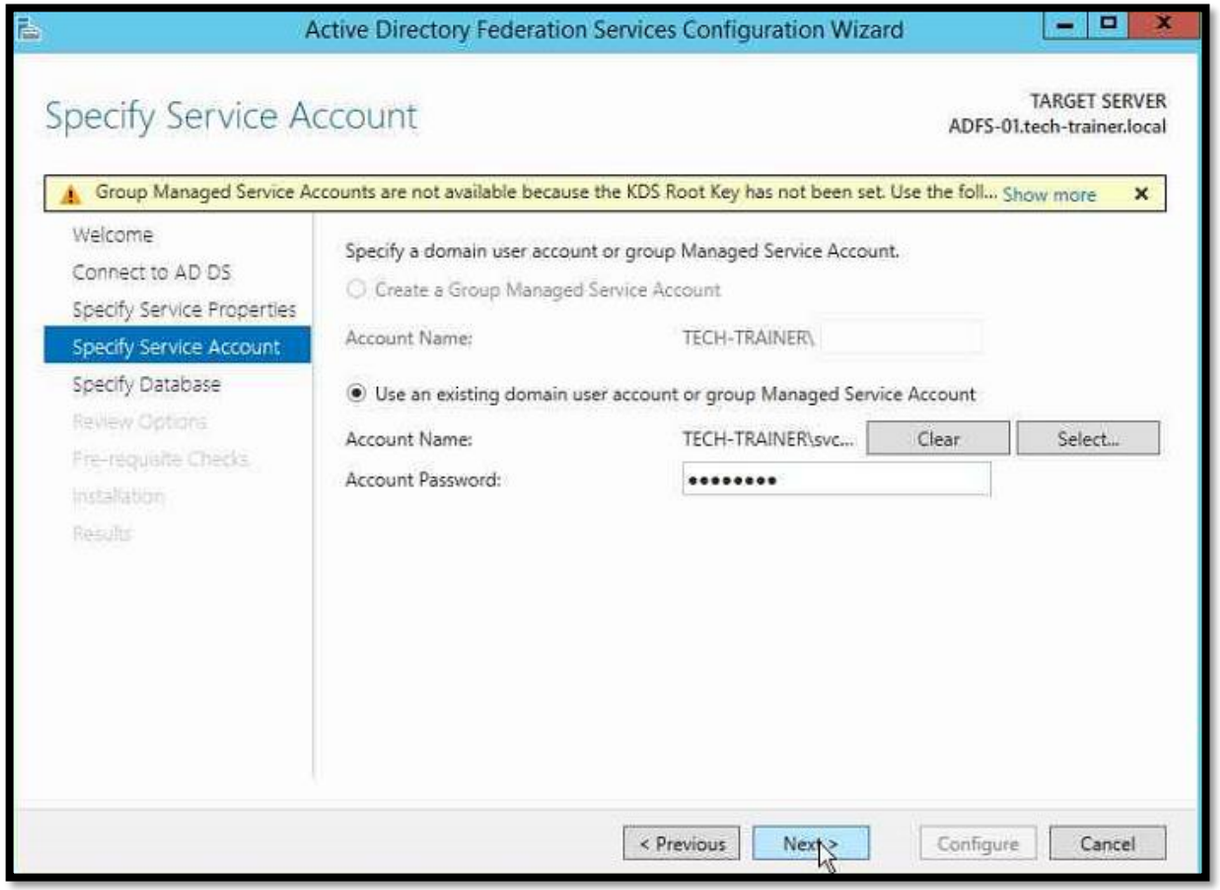
ADFS - Step-by-step

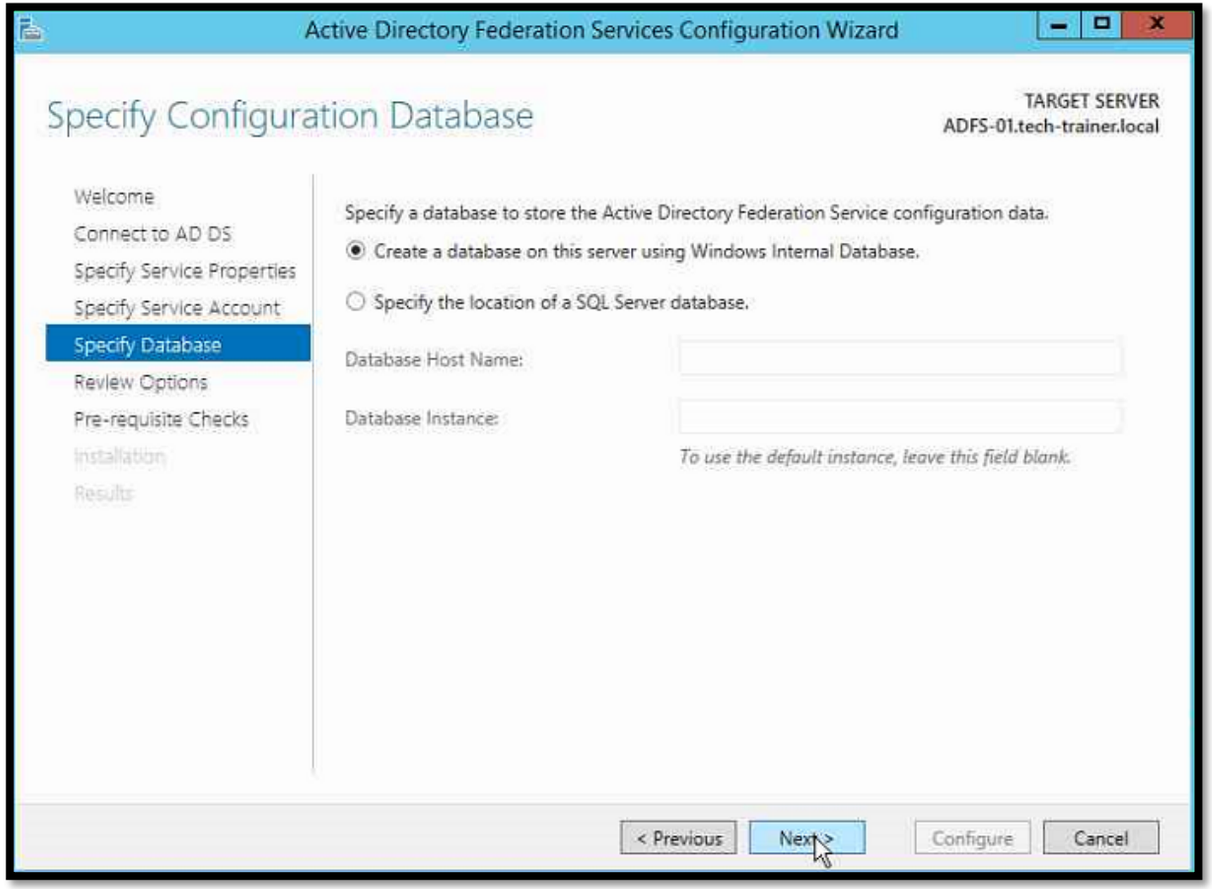




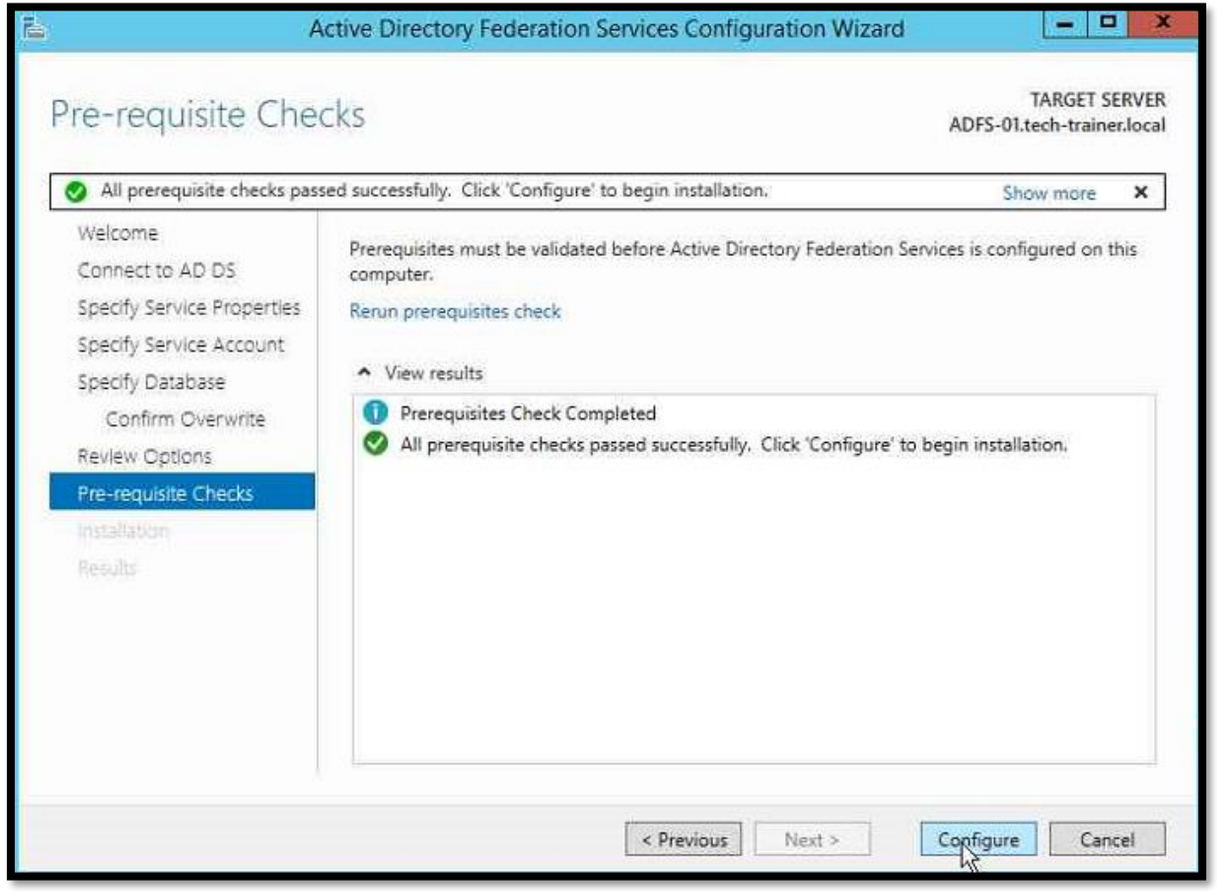
Windays 18

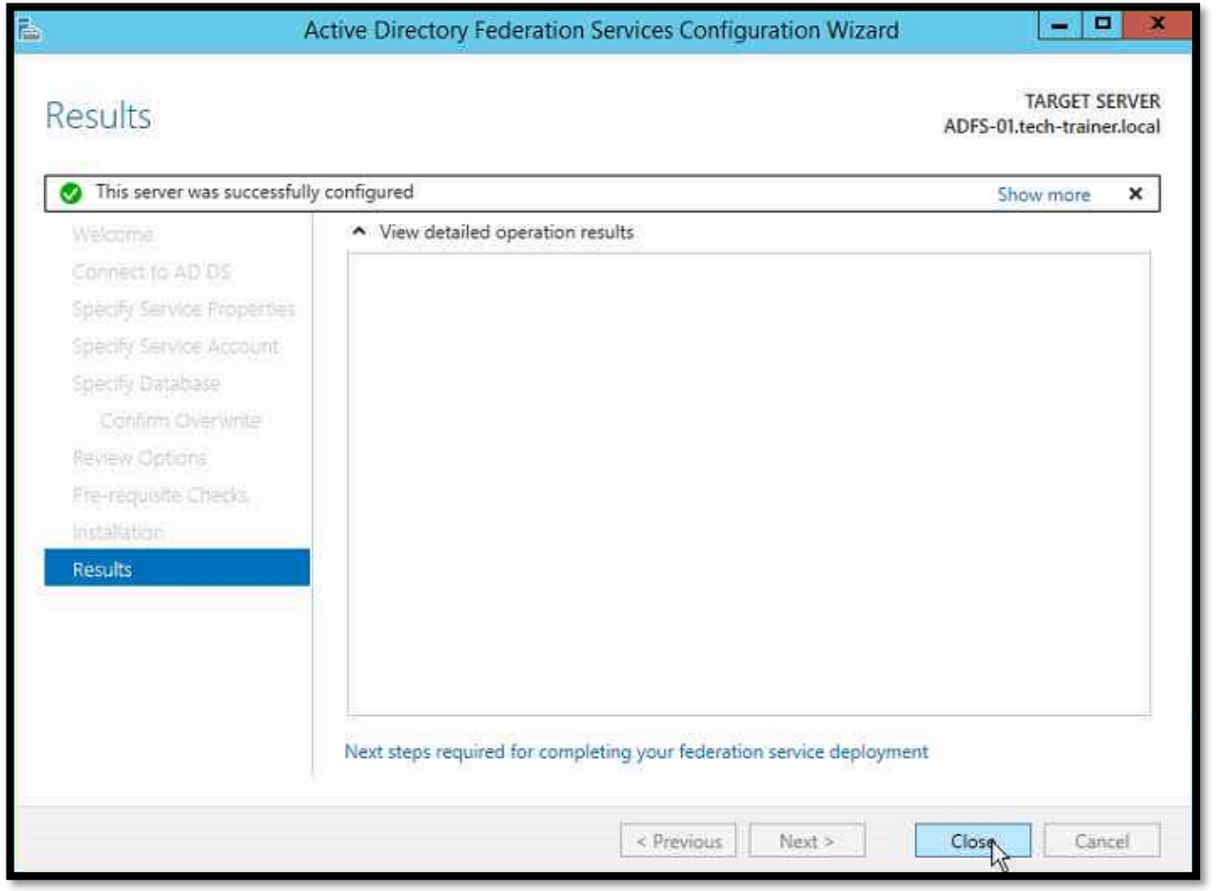
ADFS - Step-by-step





ADFS - Step-by-step

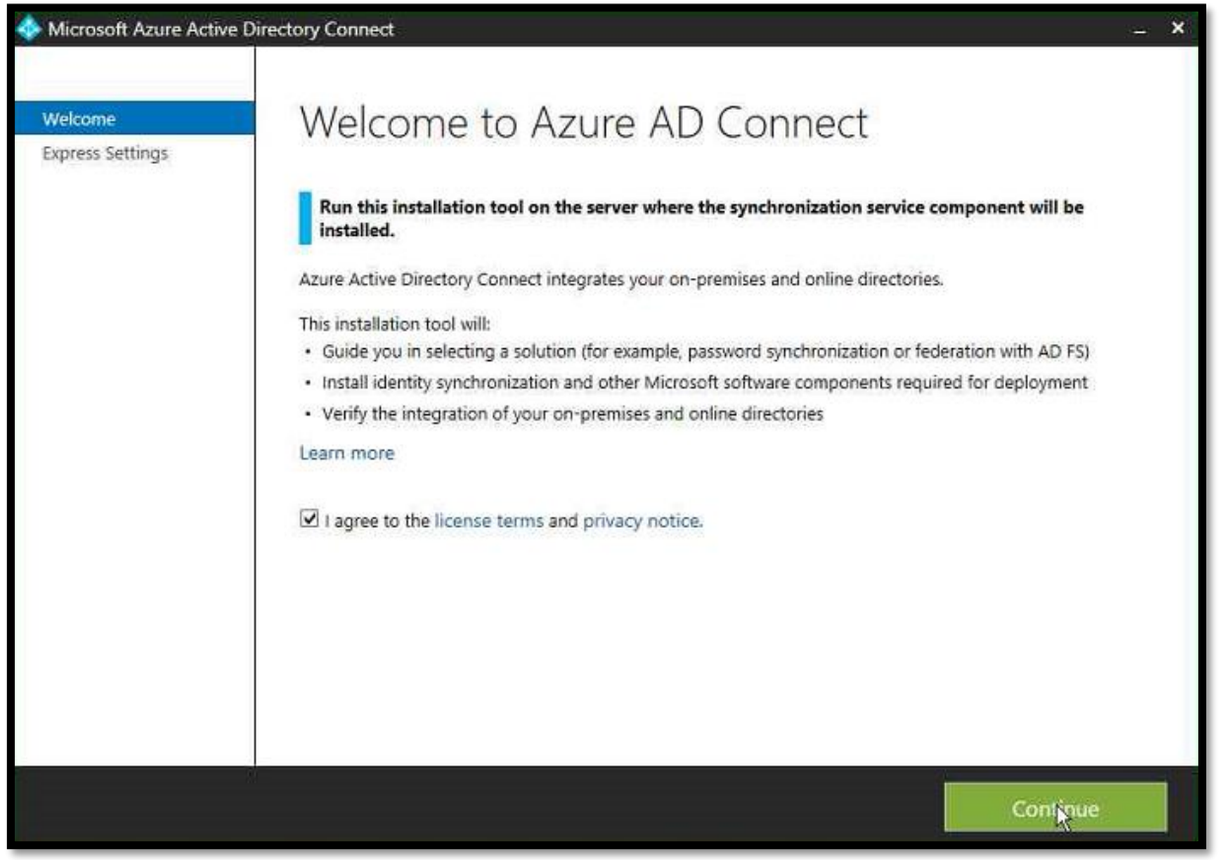


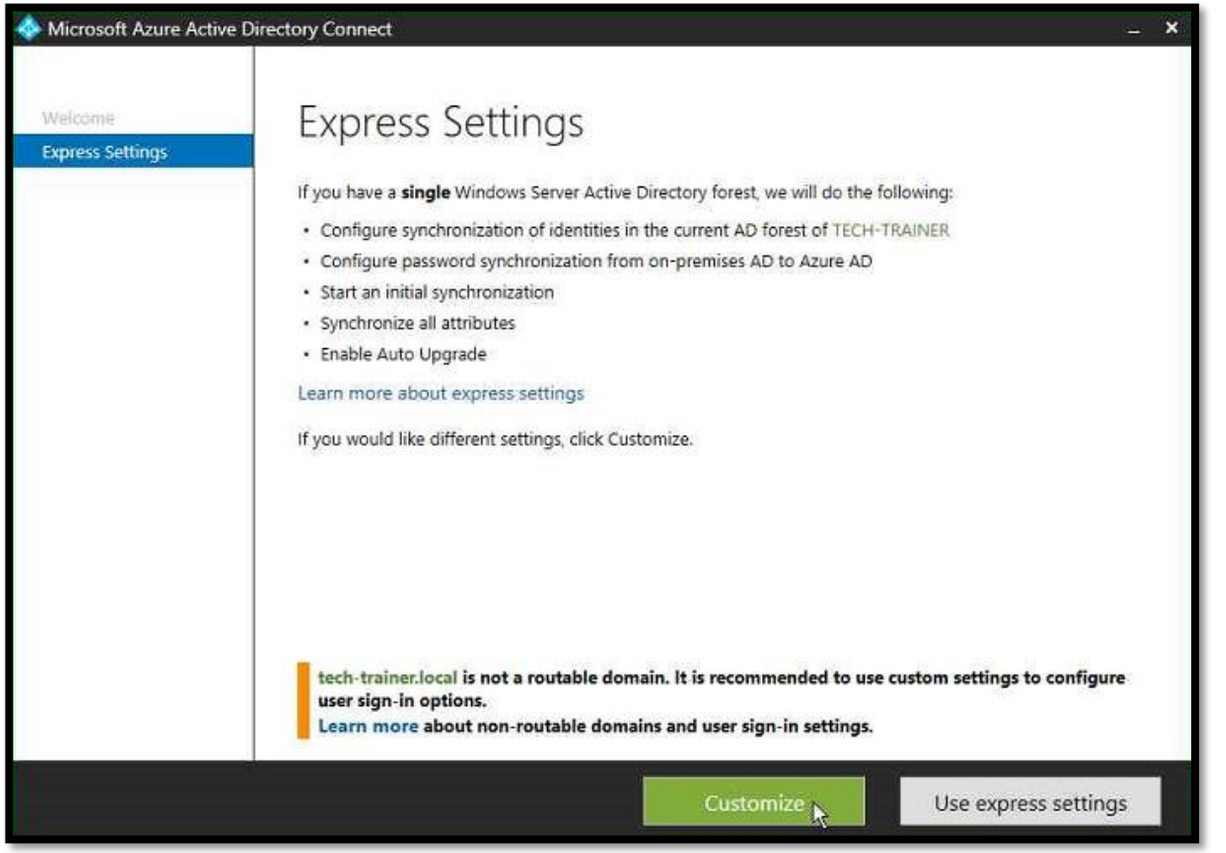


ADFS - Step-by-step

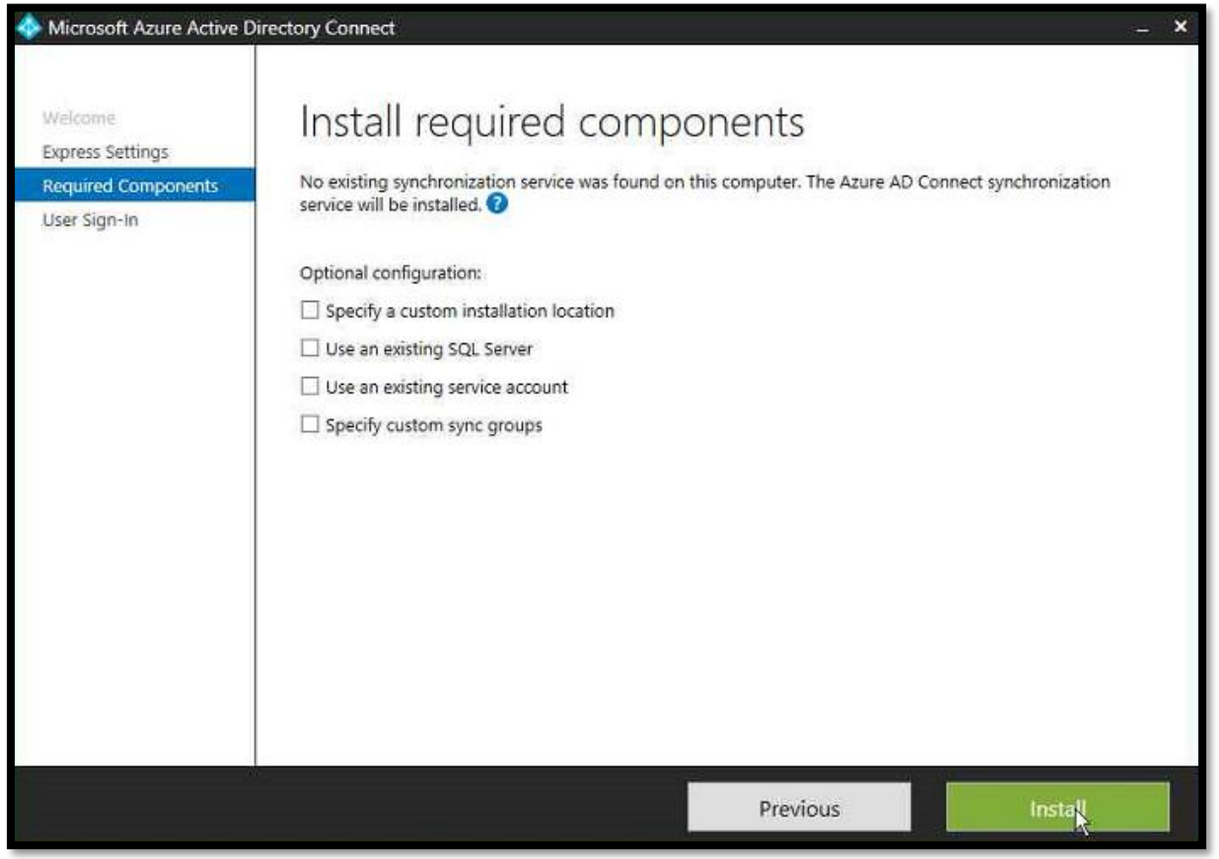
- Install Microsoft Azure AD Module for PowerShell
- Connect to Office 365 tenant with **Connect-MSOLService**
- Run following commands
  - `Enable-PSRemoting`
  - `Set-MsolADFSContext -Computer “local FQDN of ADFS server”`

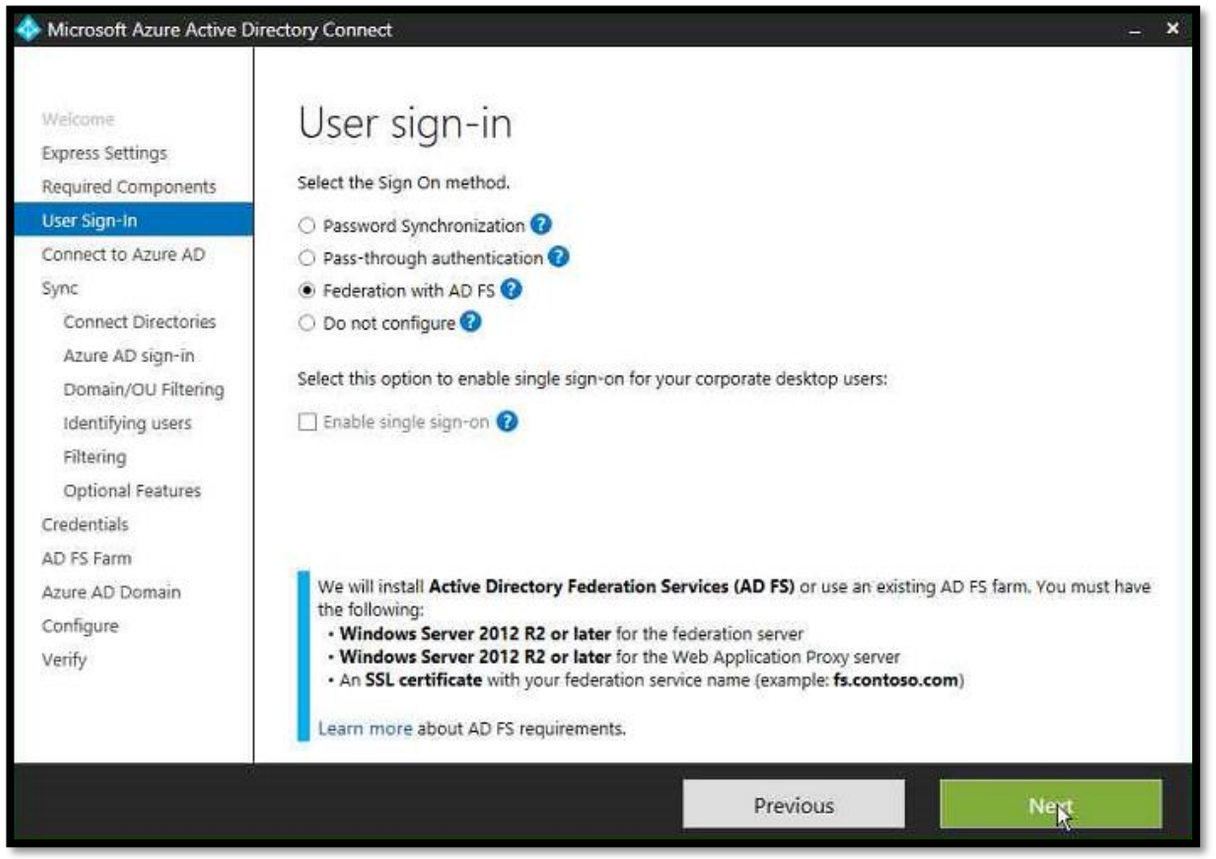
ADFS - Step-by-step





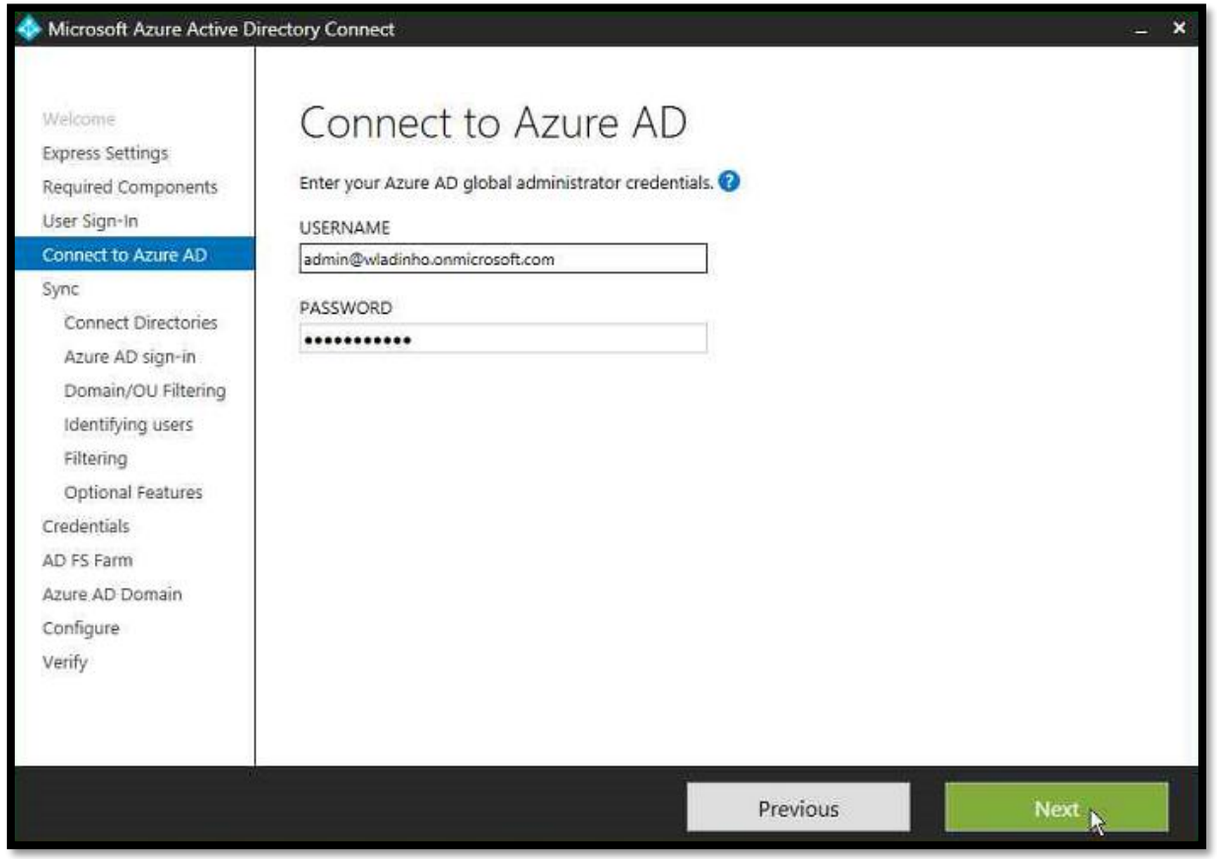
ADFS - Step-by-step

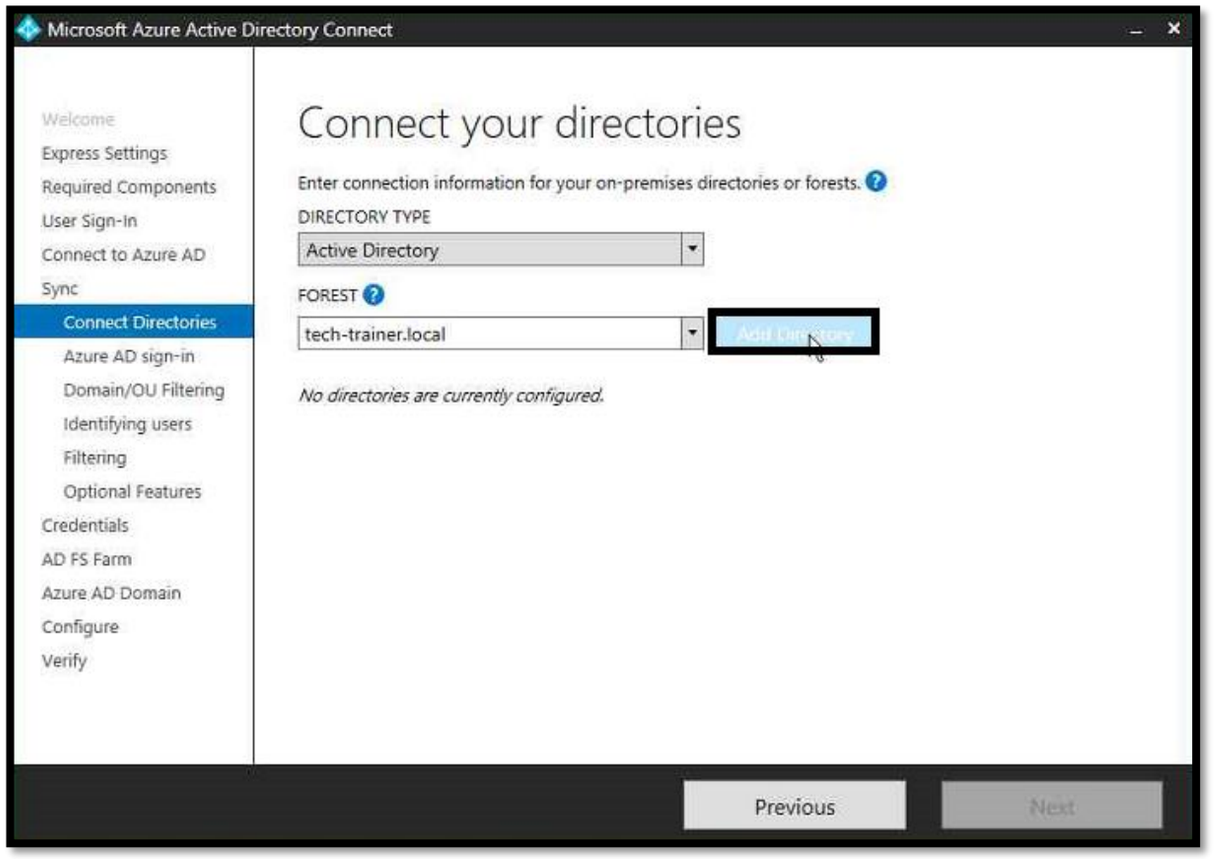




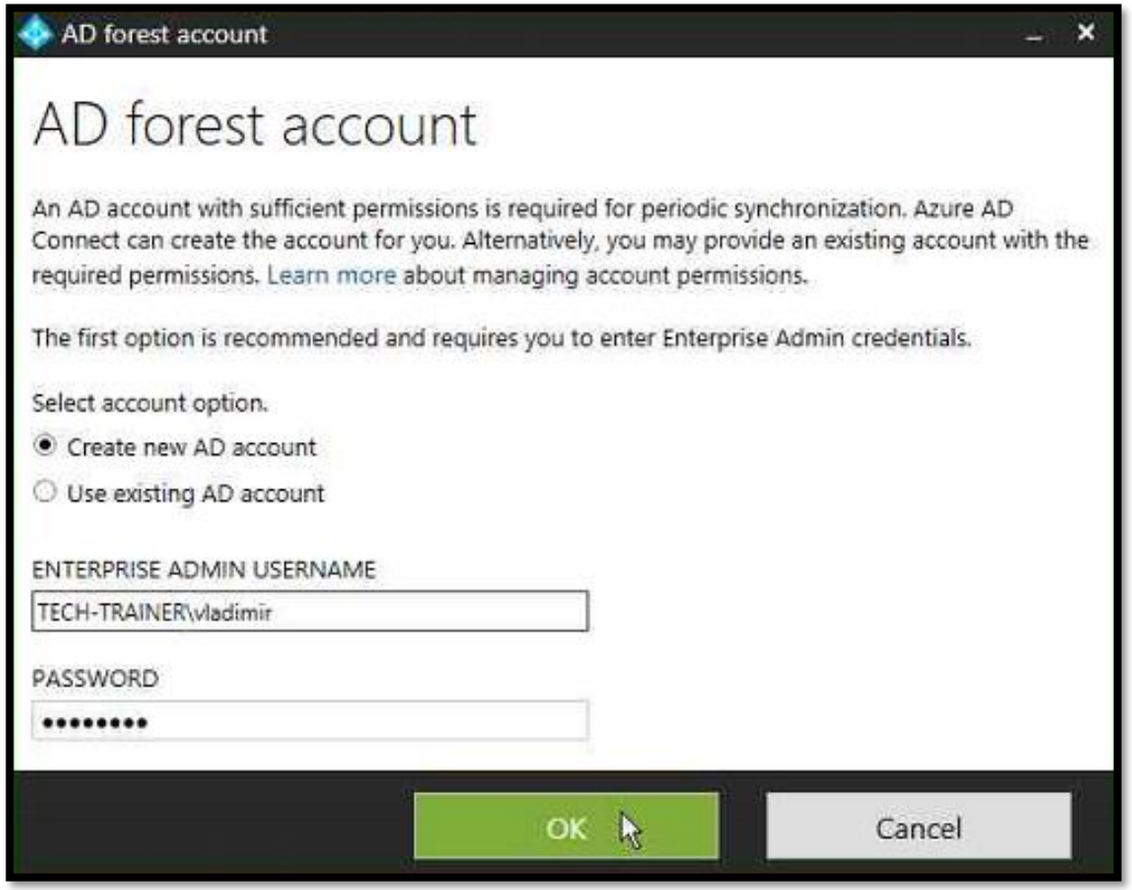
Windays 18

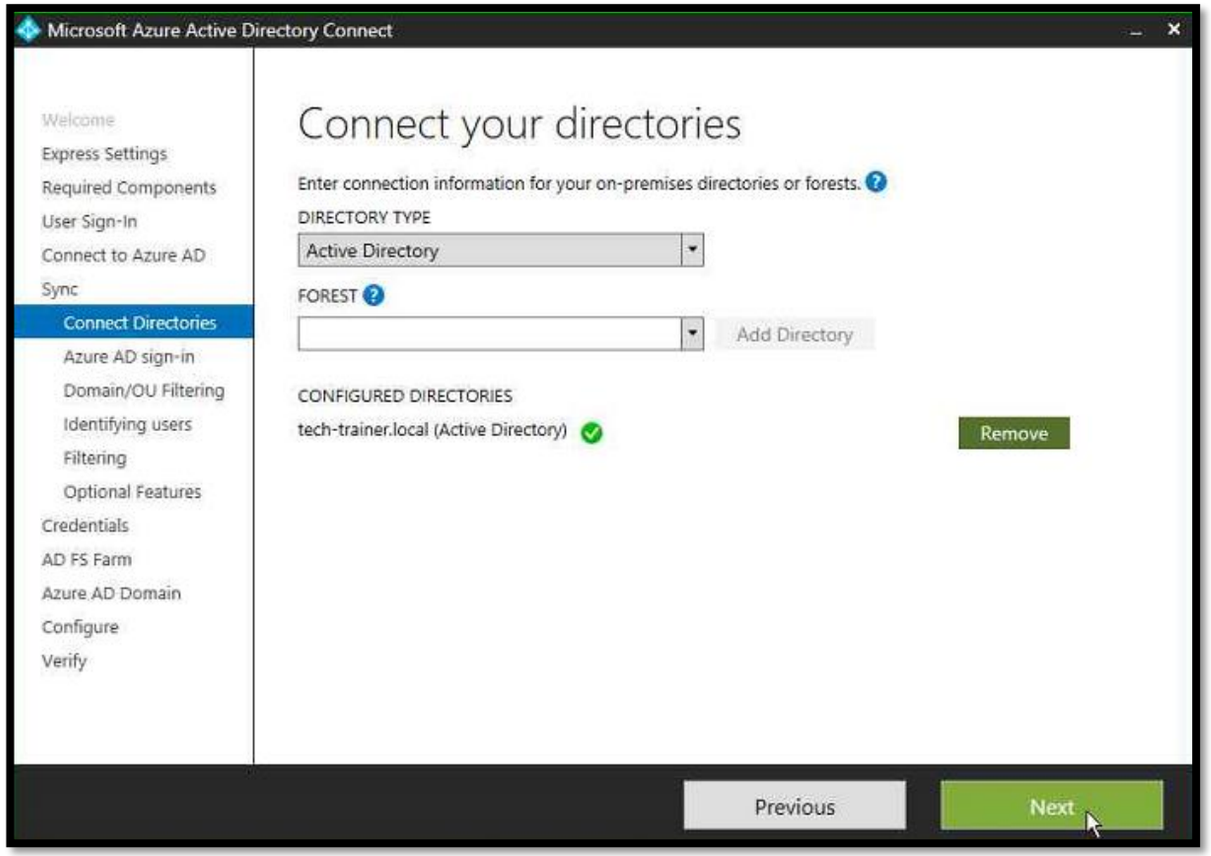
ADFS - Step-by-step



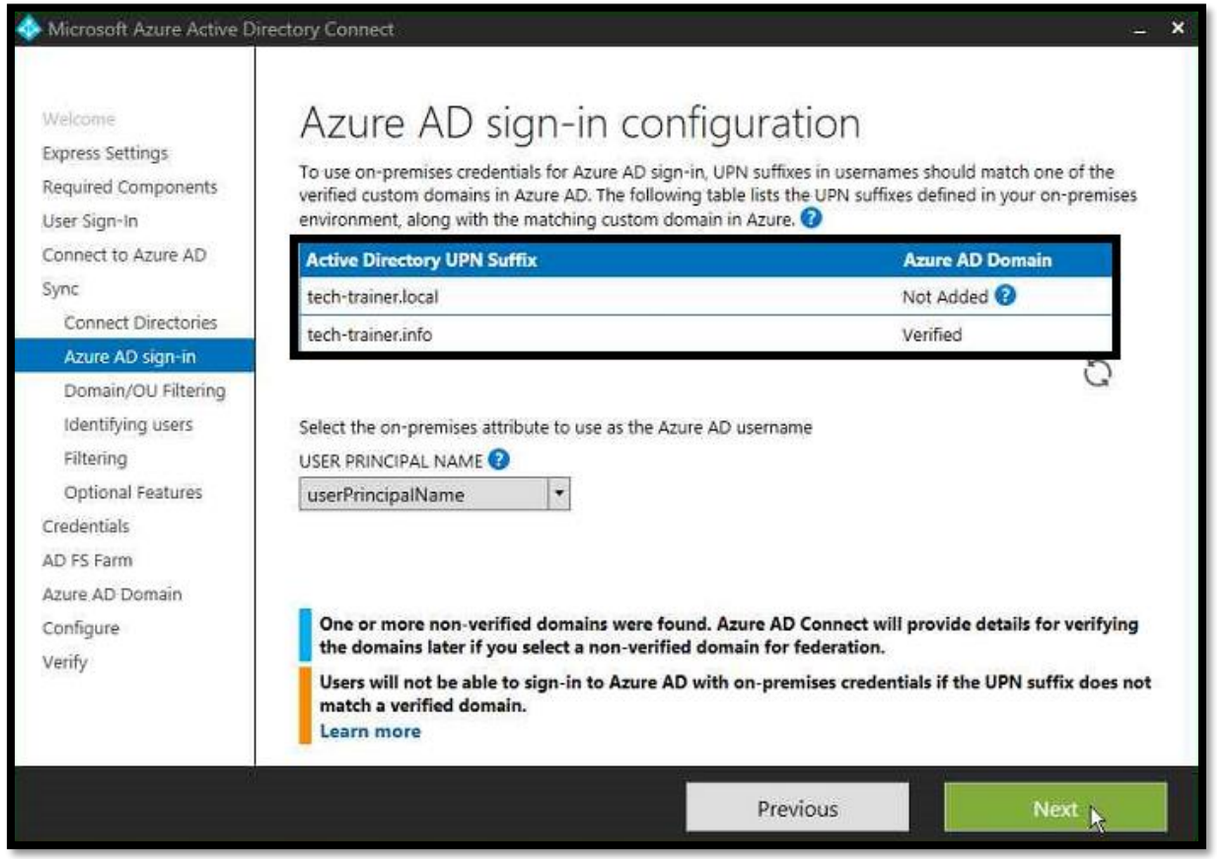


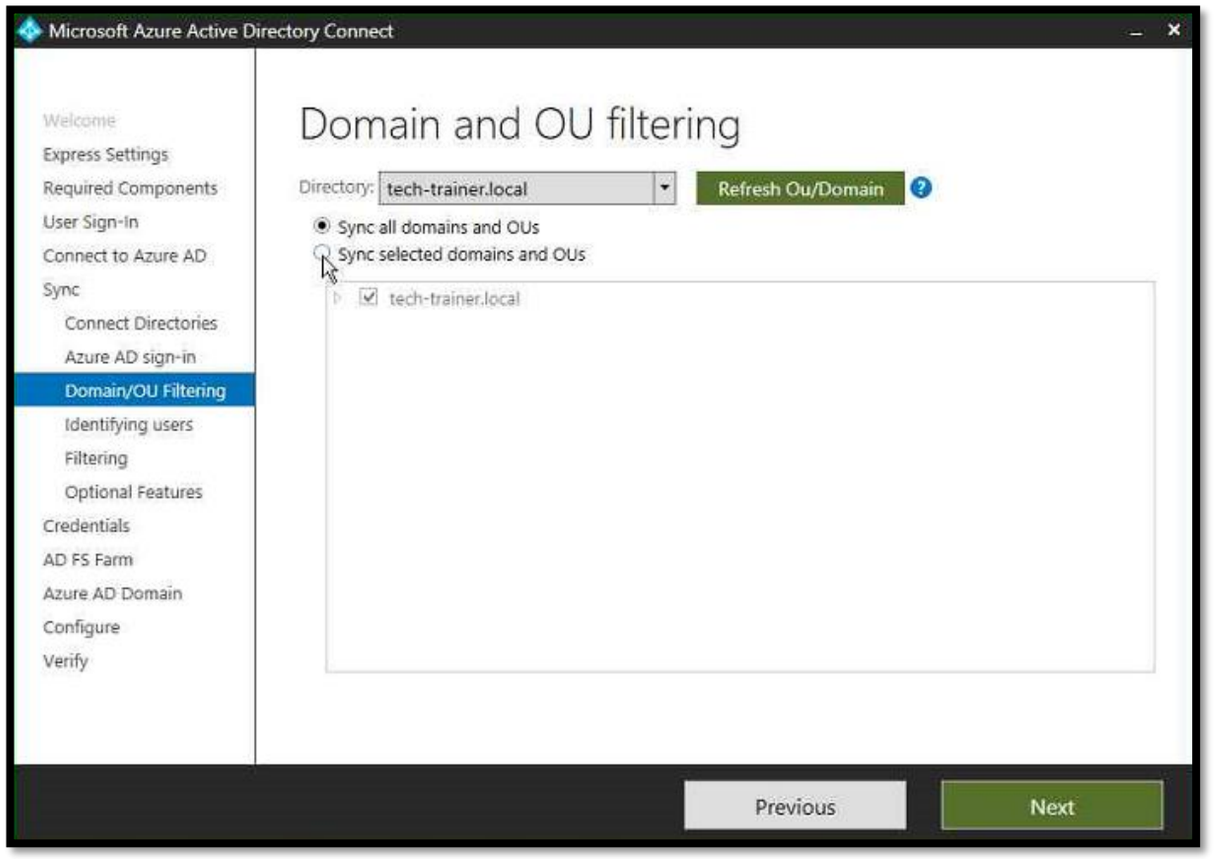
ADFS - Step-by-step





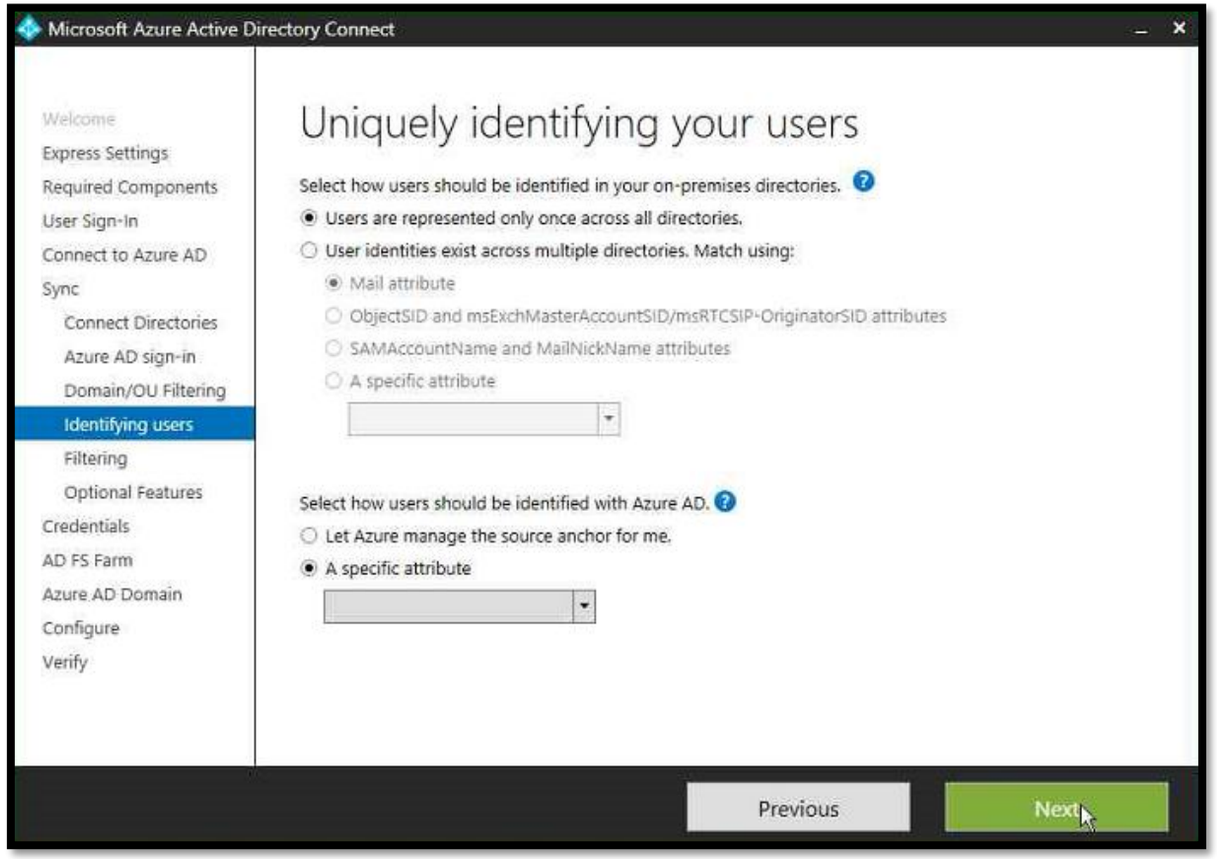
ADFS - Step-by-step

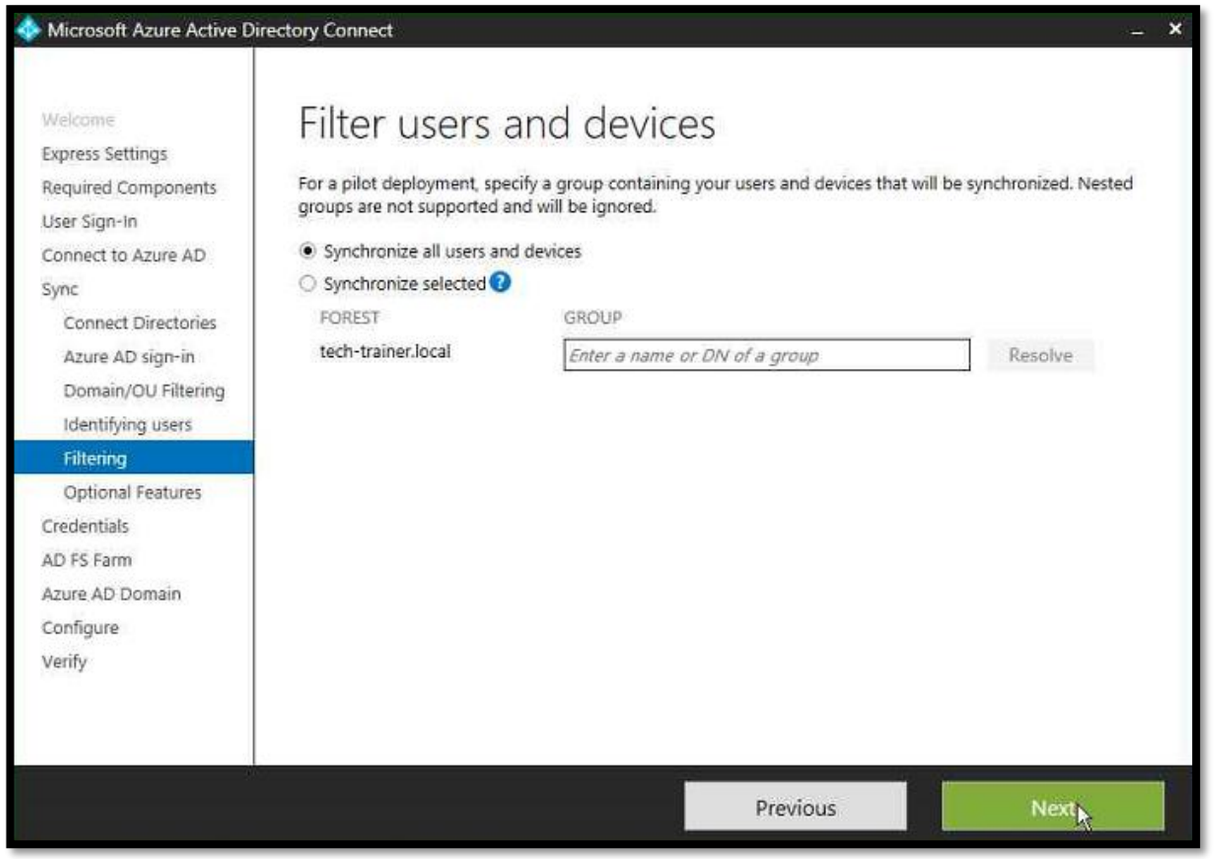




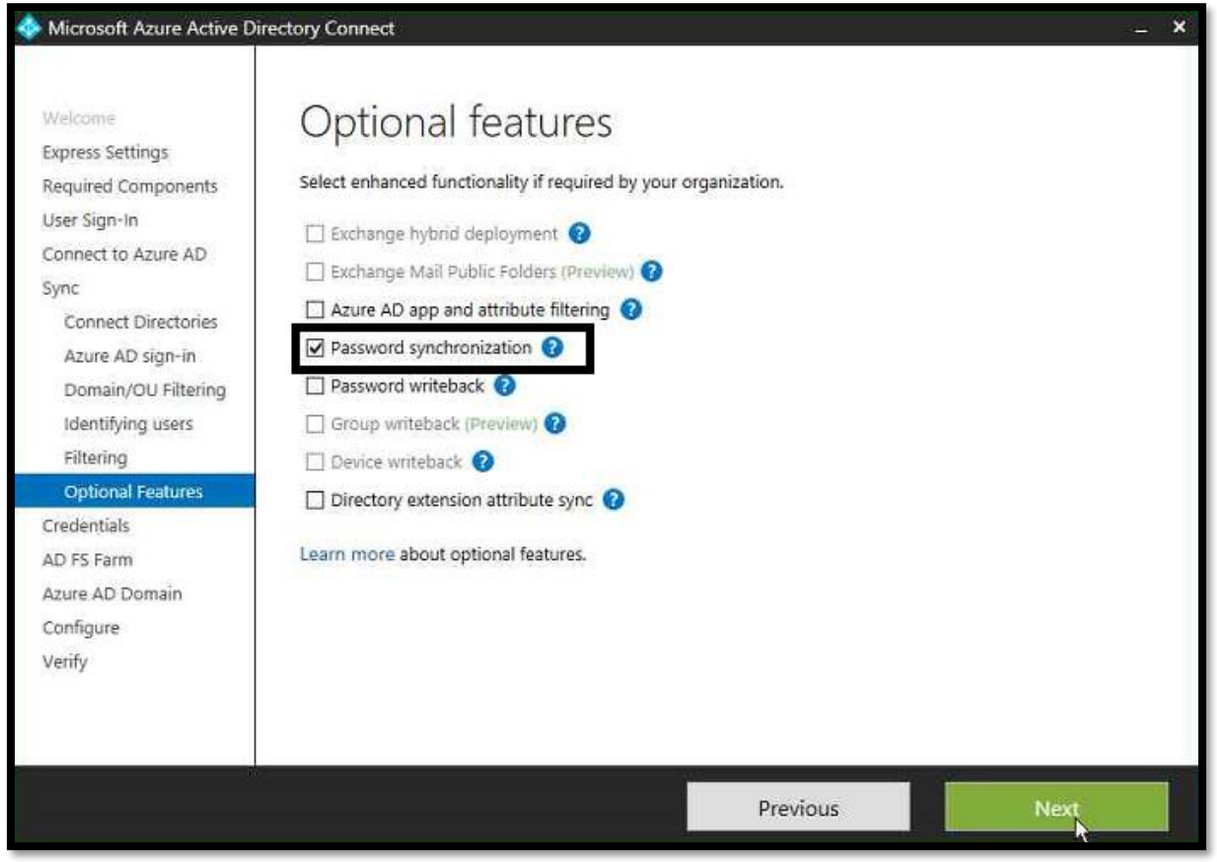
Windays 18

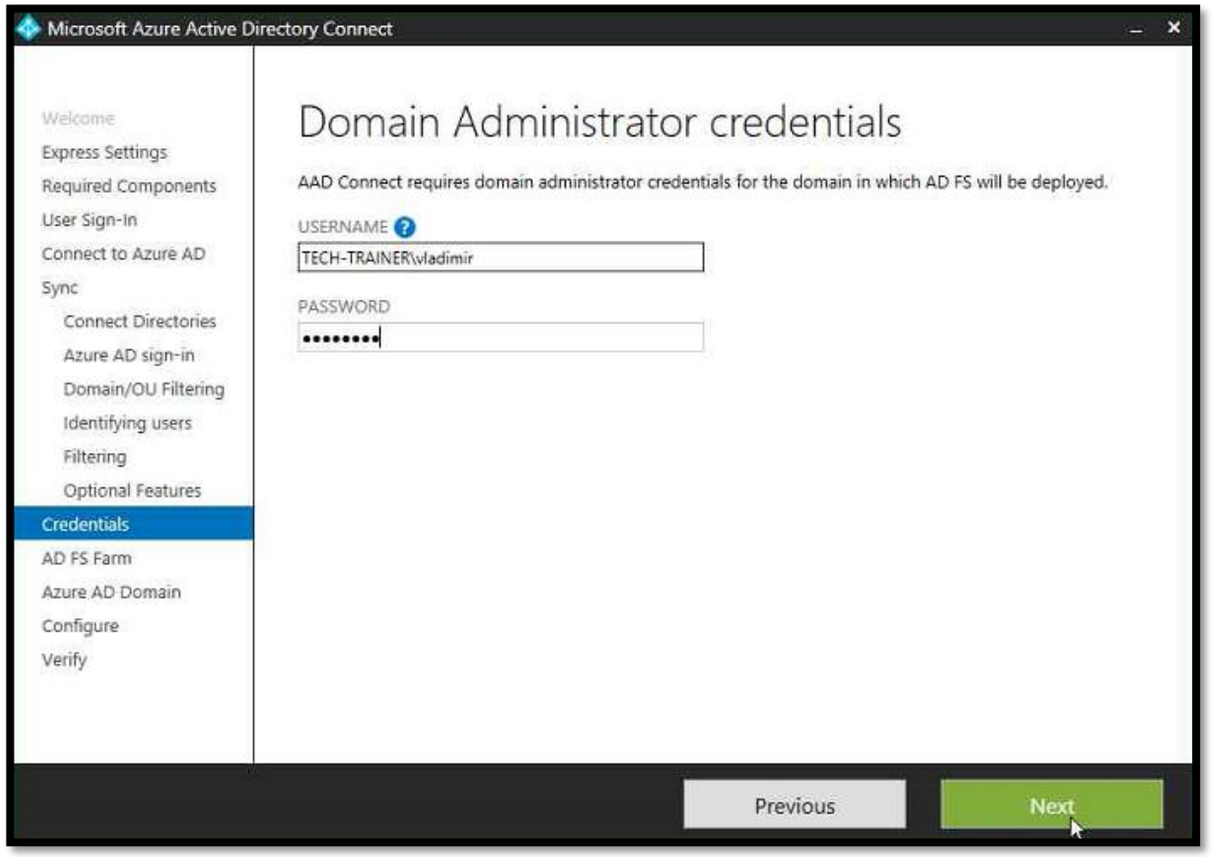
ADFS - Step-by-step



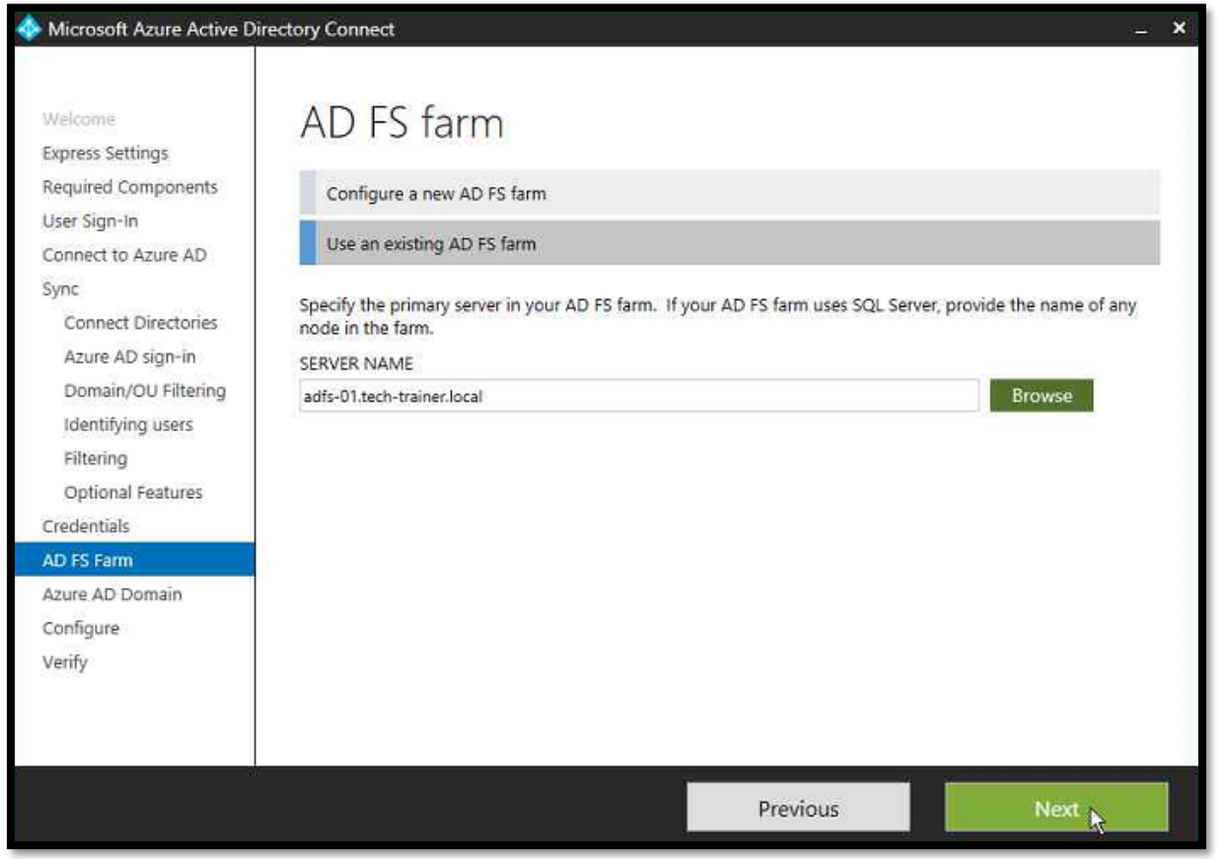


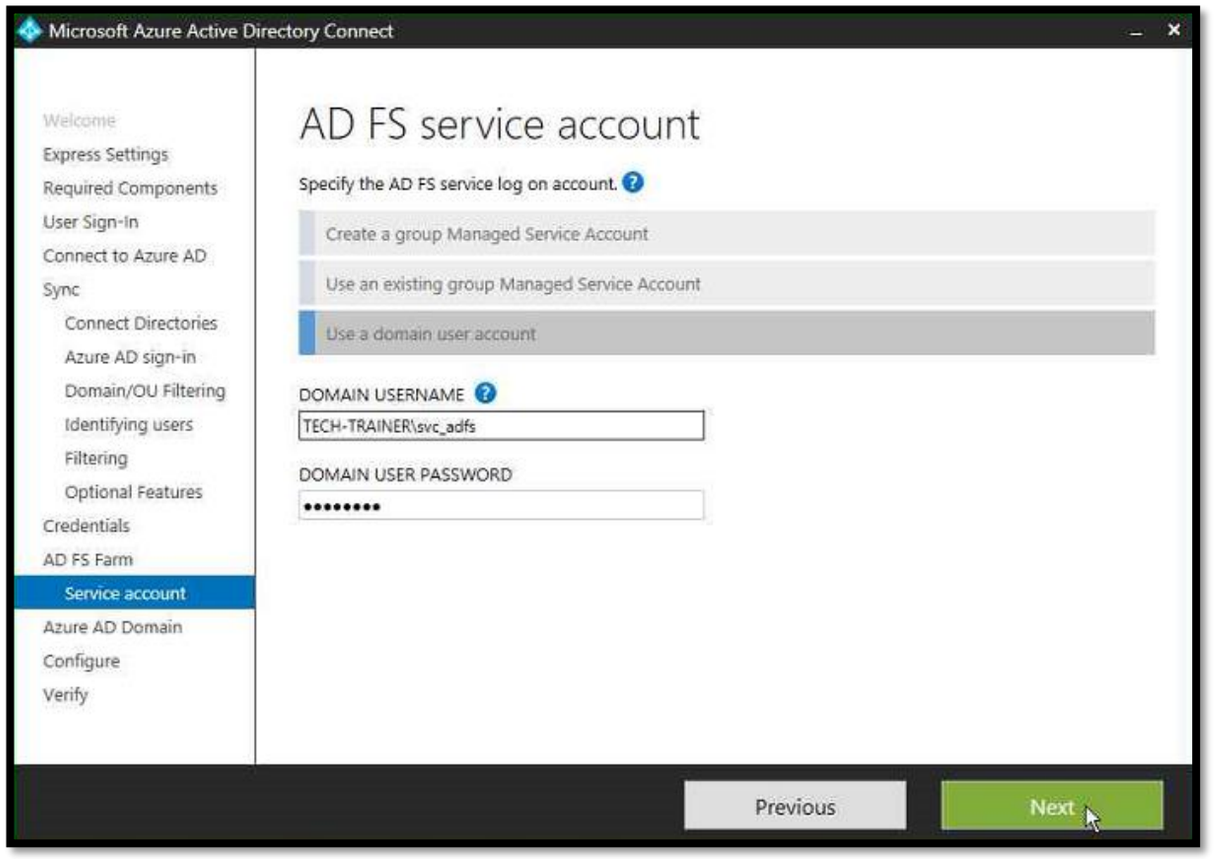
ADFS - Step-by-step



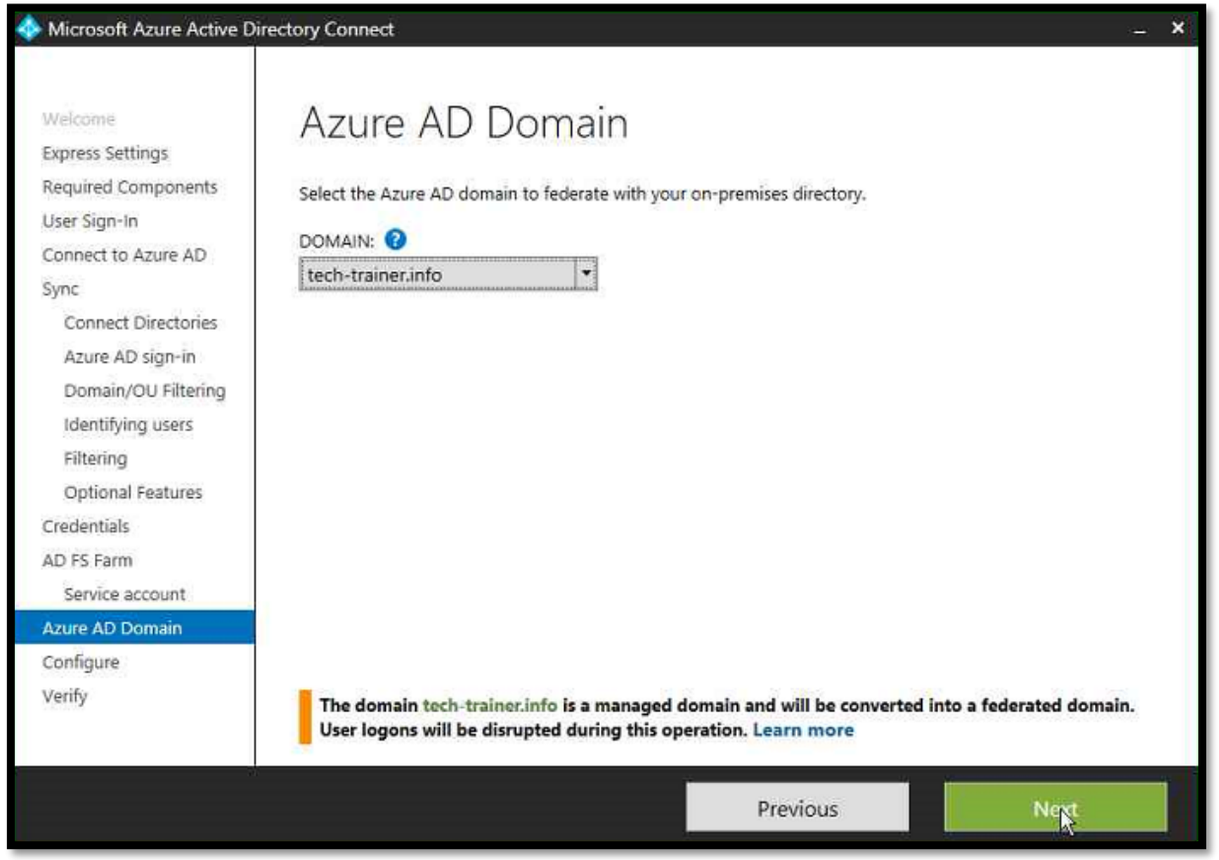


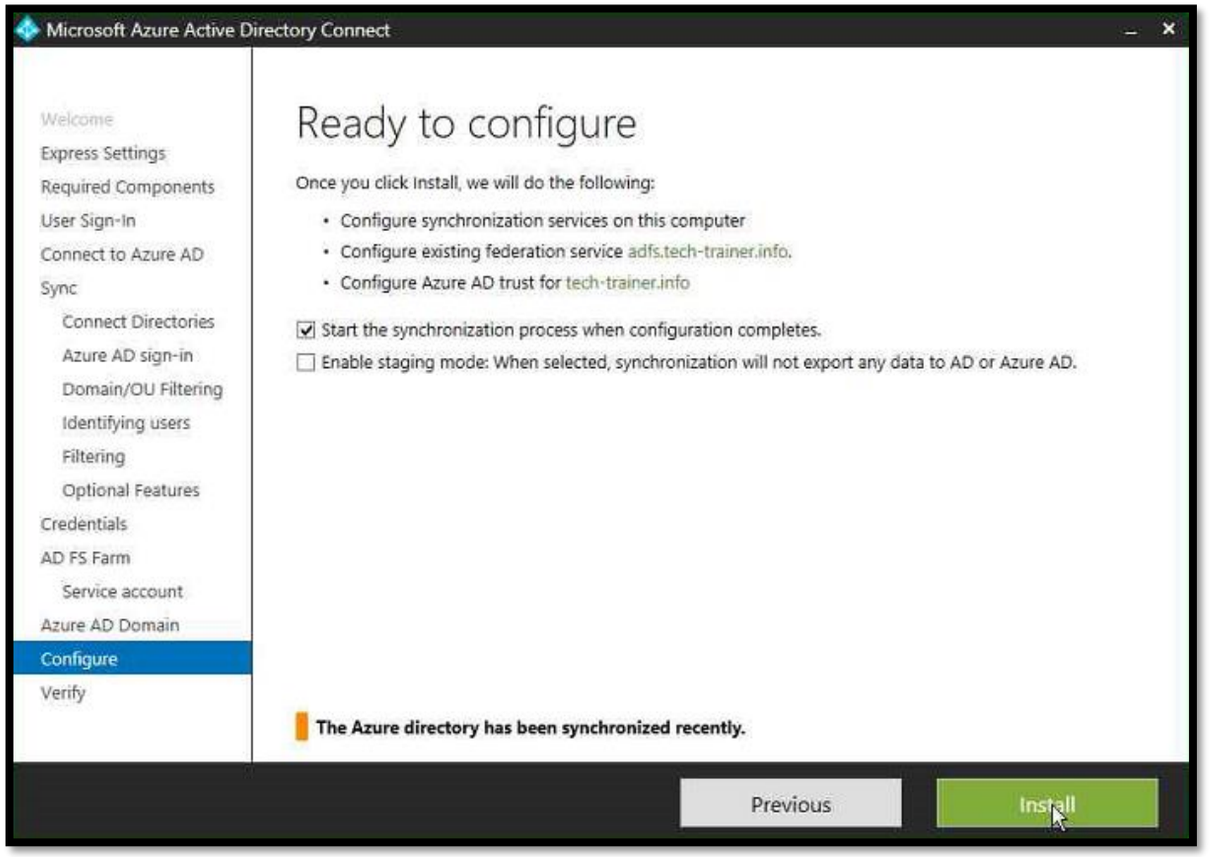
ADFS - Step-by-step



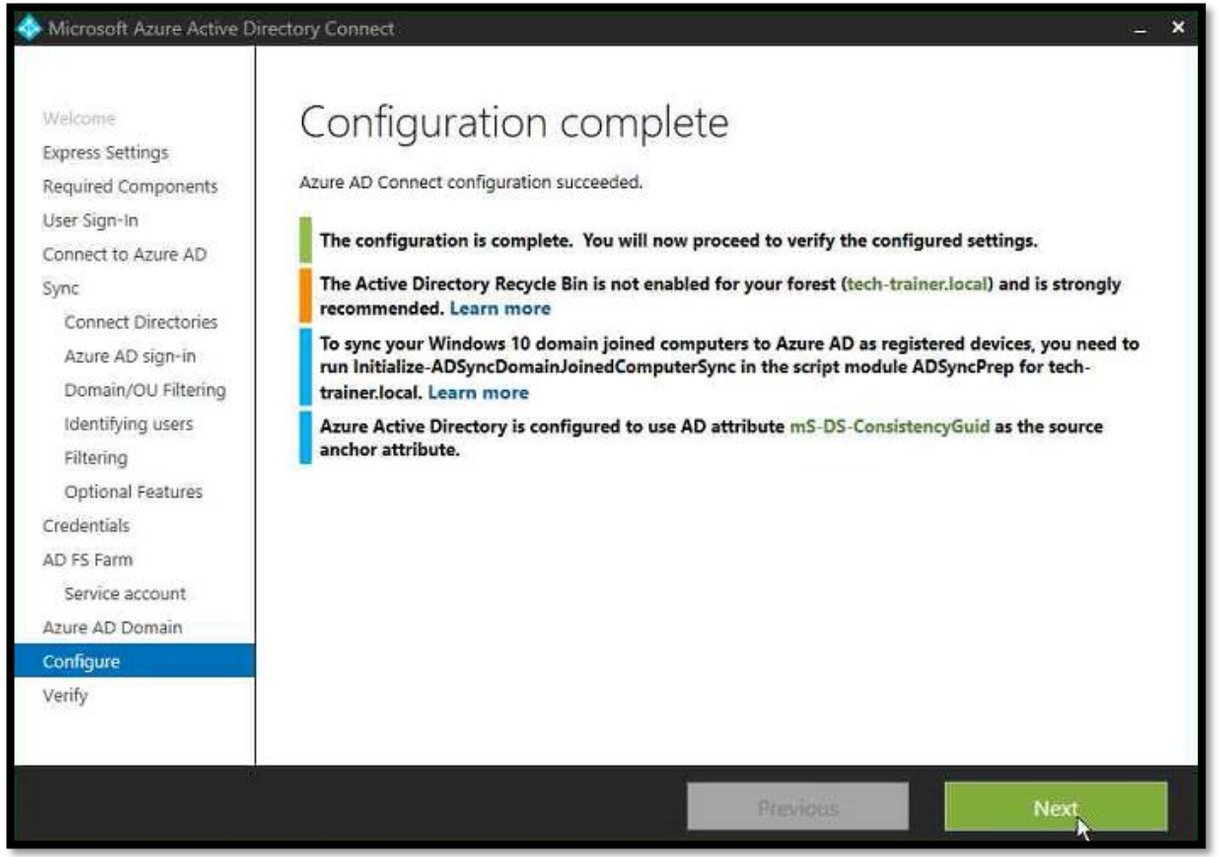


ADFS - Step-by-step



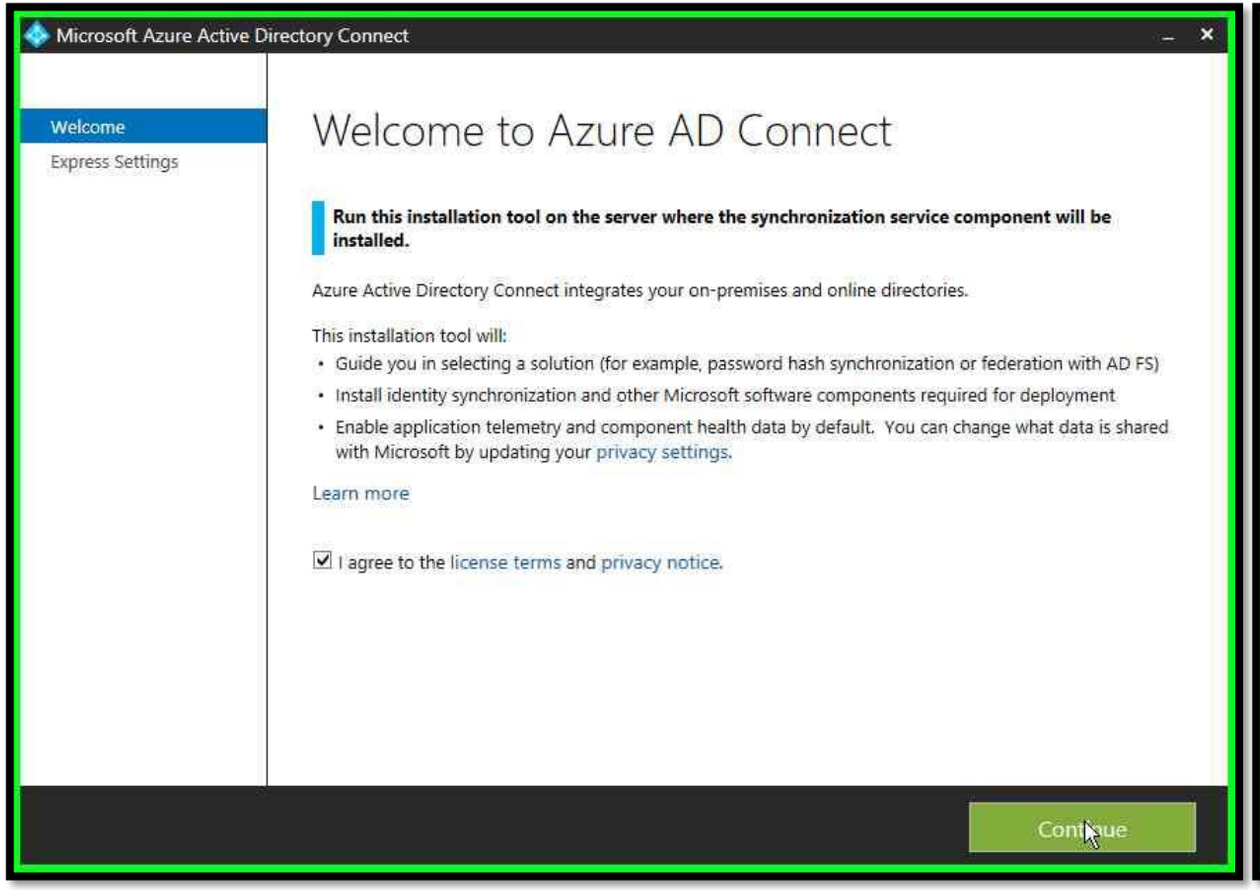


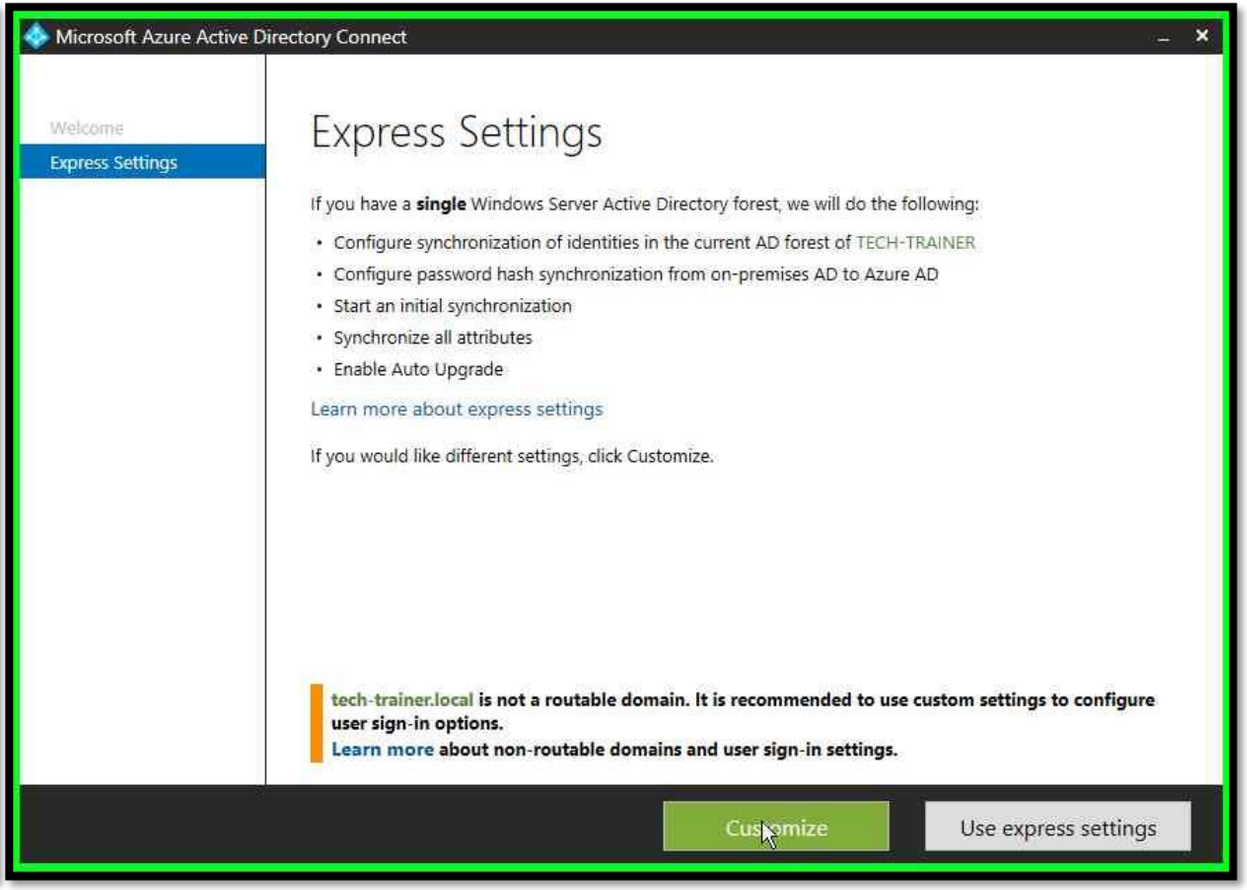
ADFS - Step-by-step



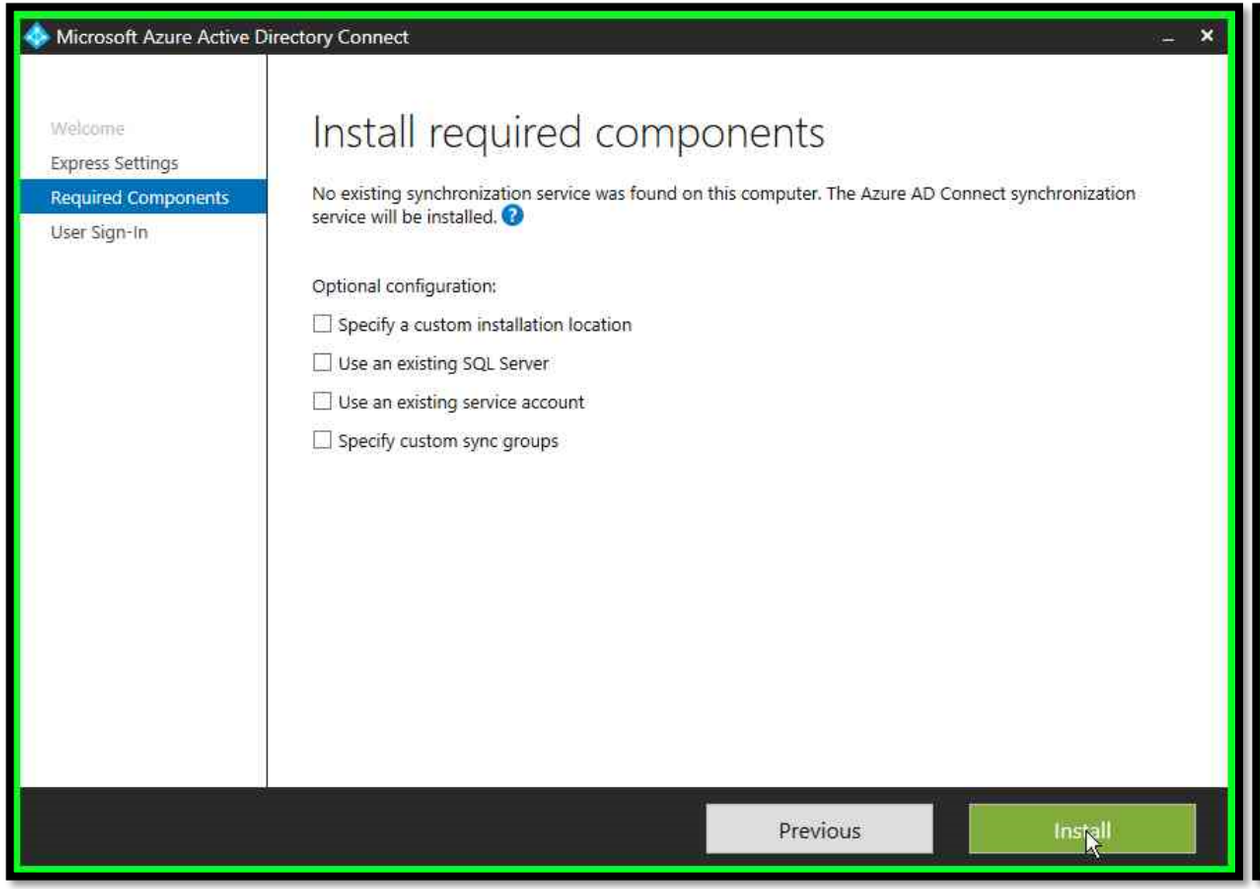
Demo *(Slideshow)* – PTA

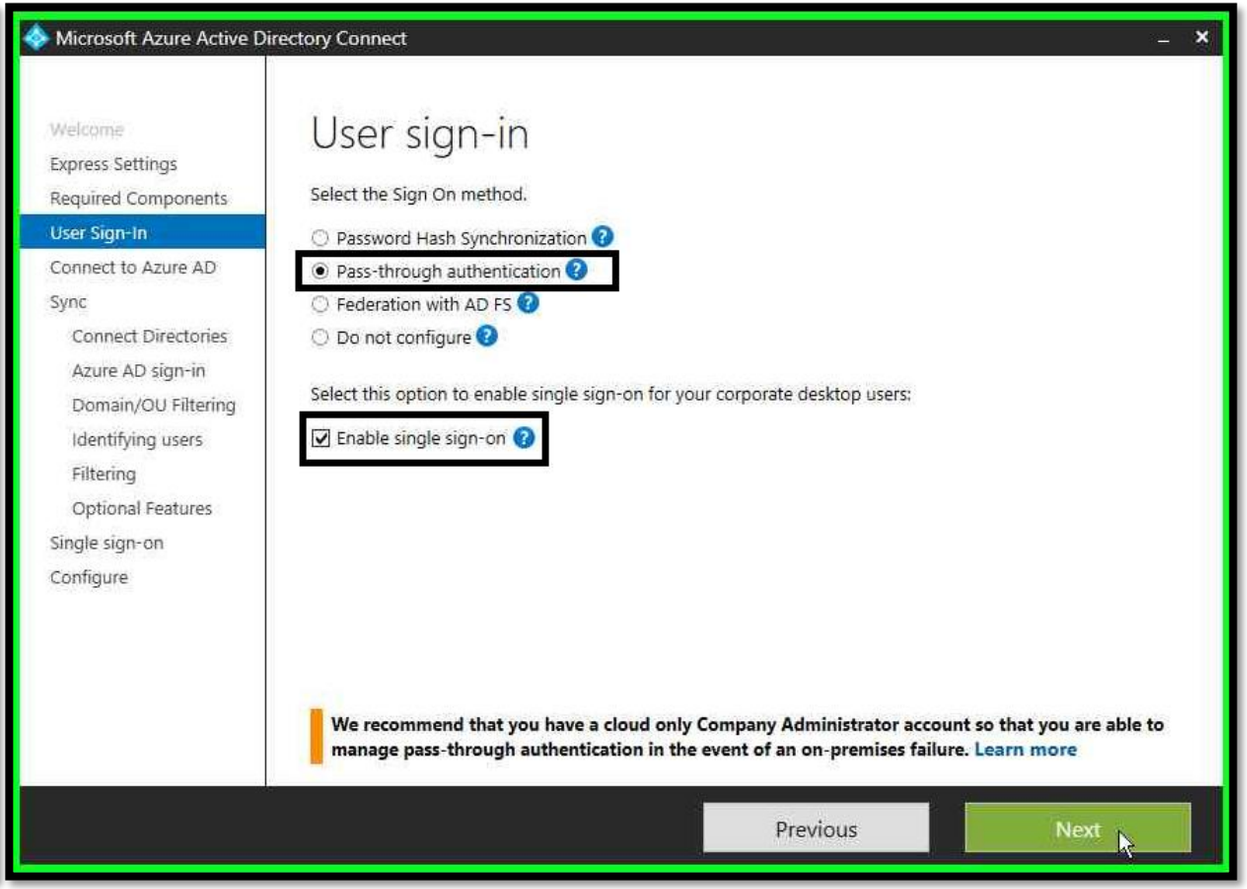
PTA - Step-by-step





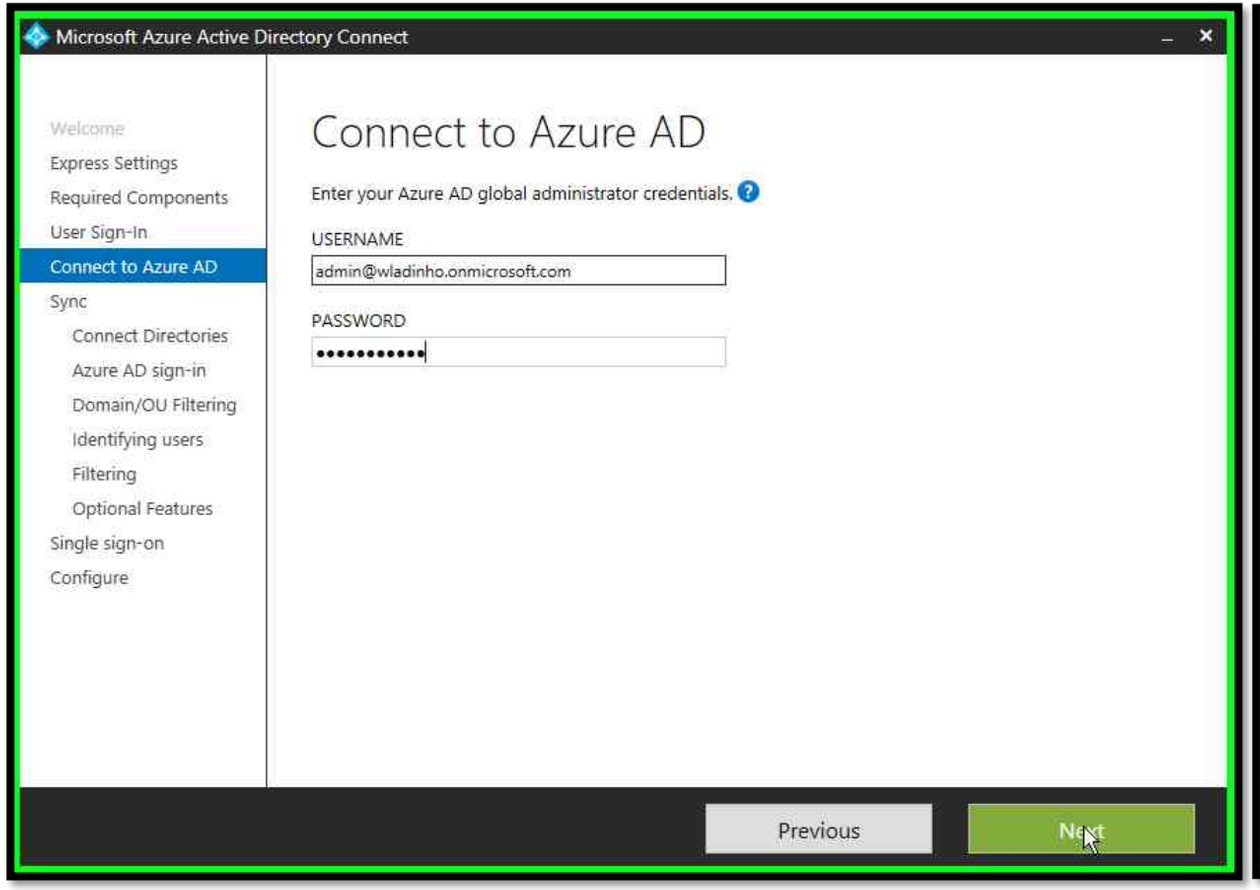
PTA - Step-by-step

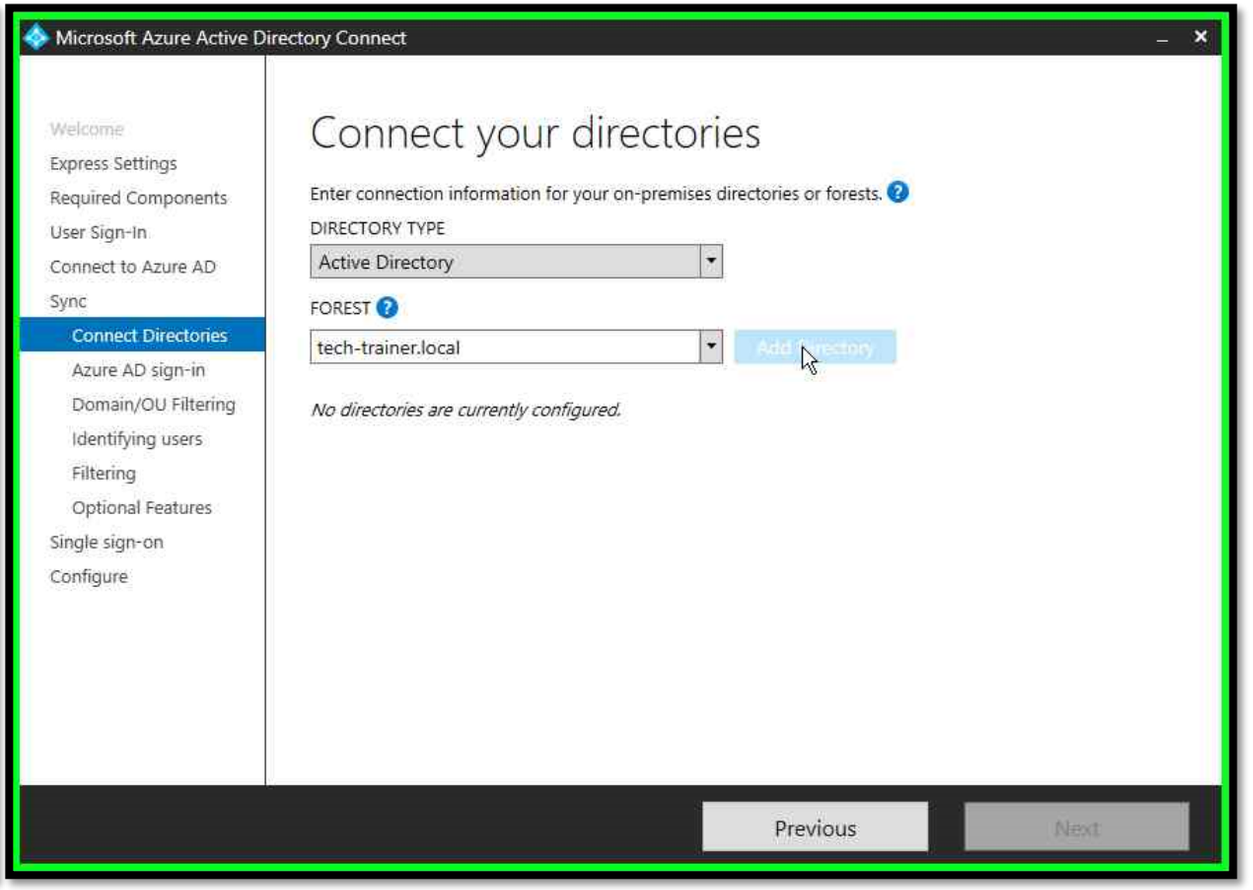




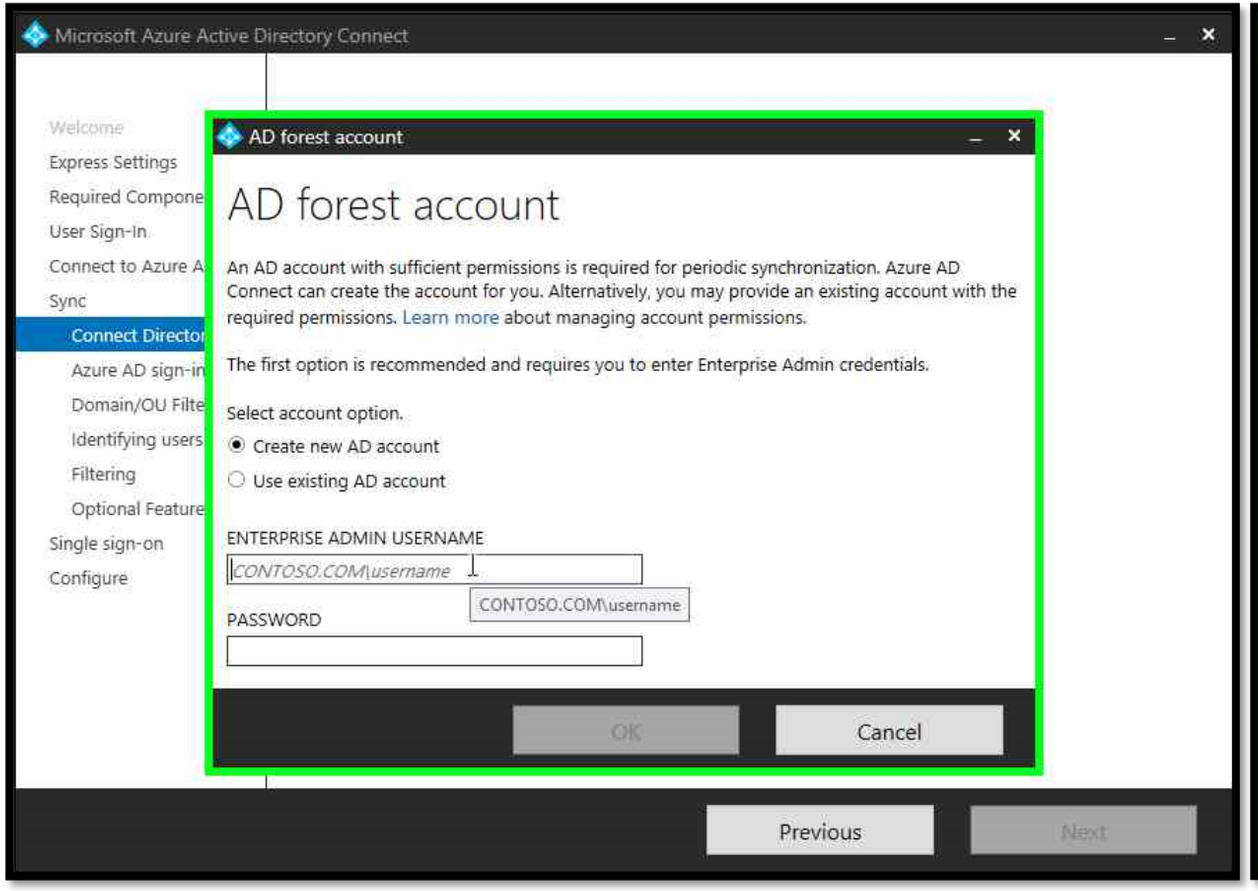
Windays 18

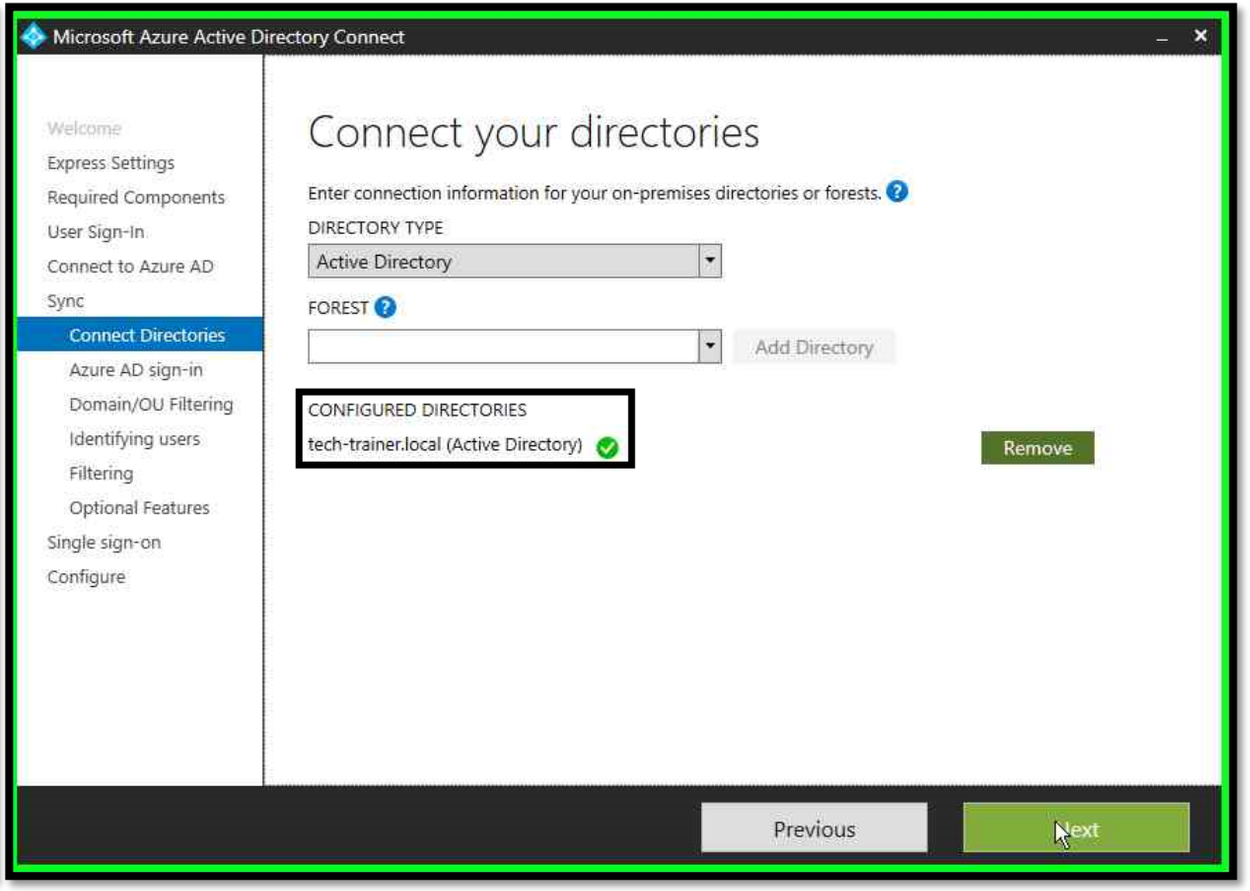
PTA - Step-by-step



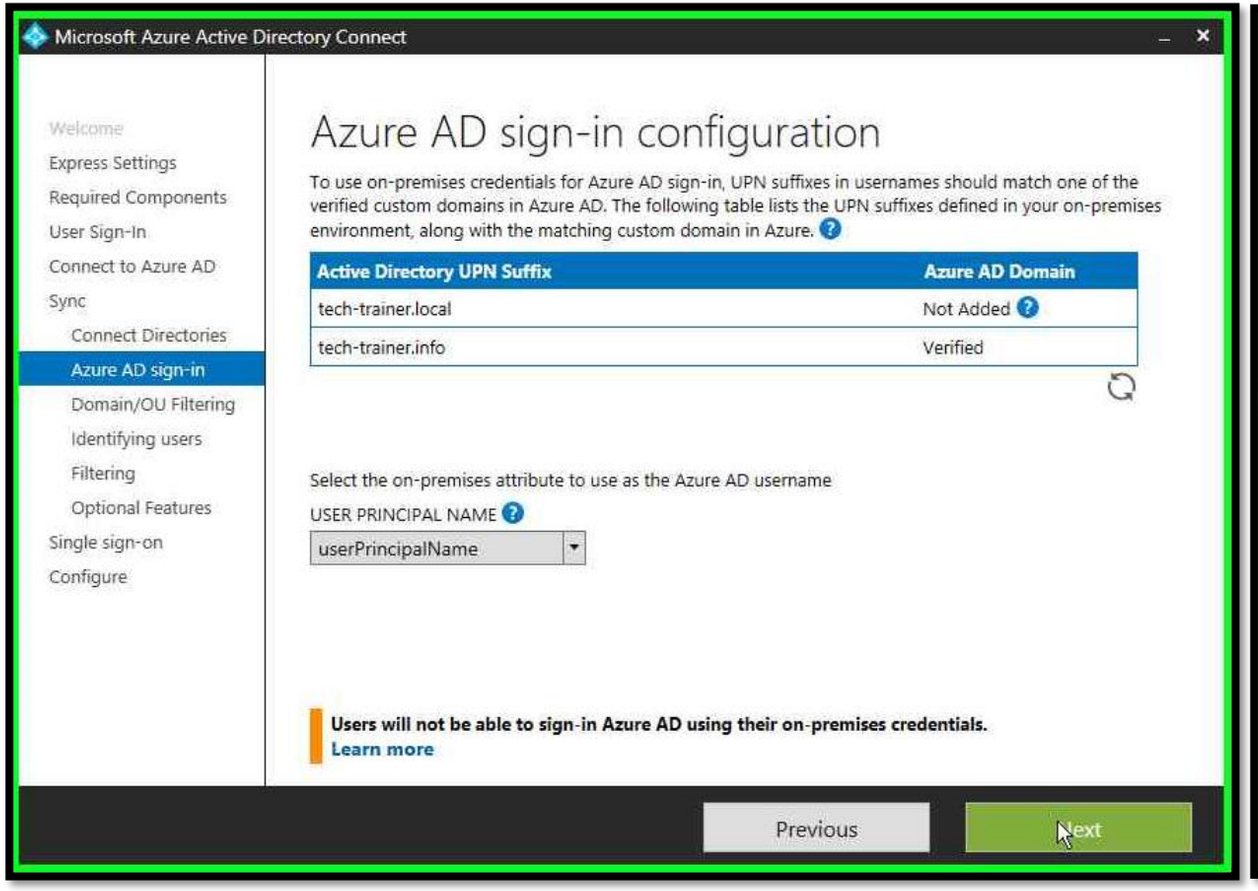


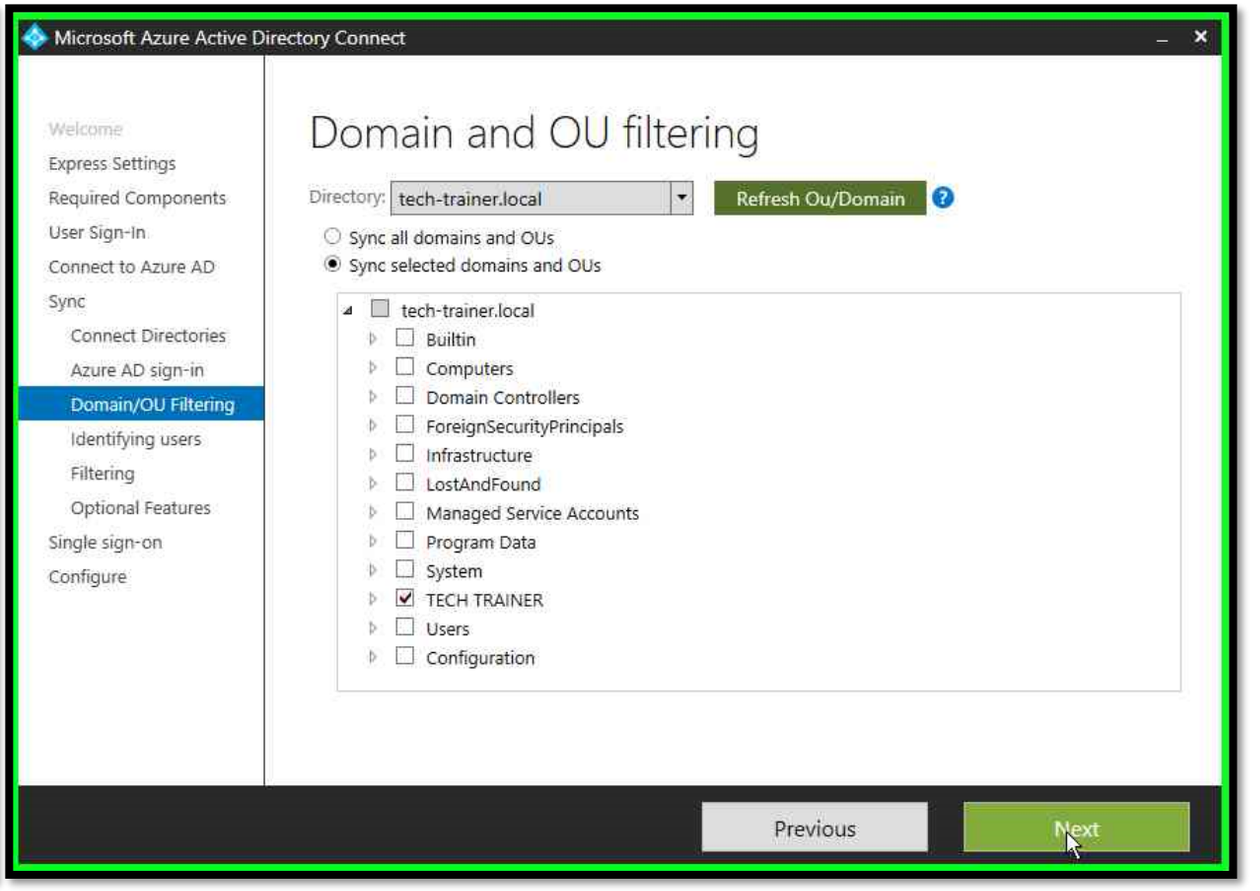
PTA - Step-by-step



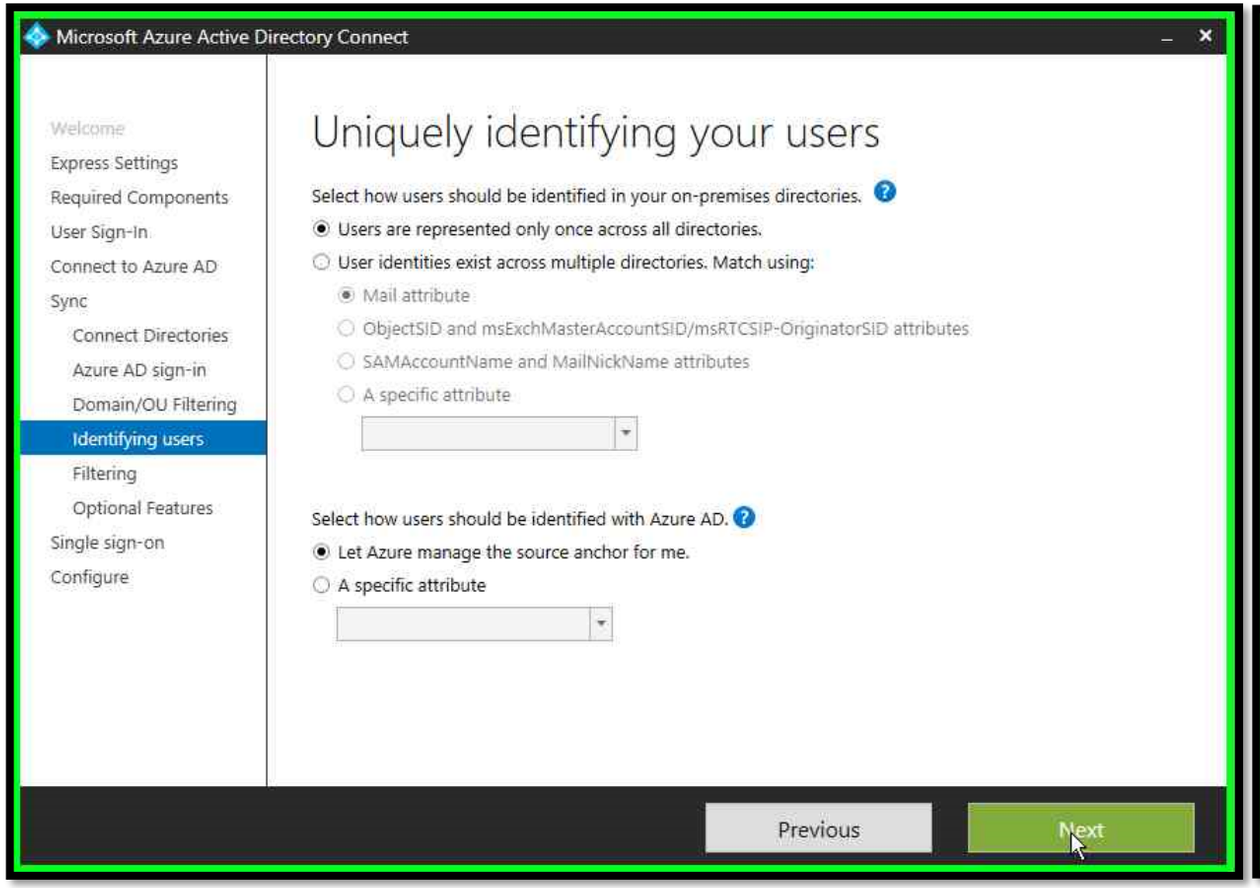


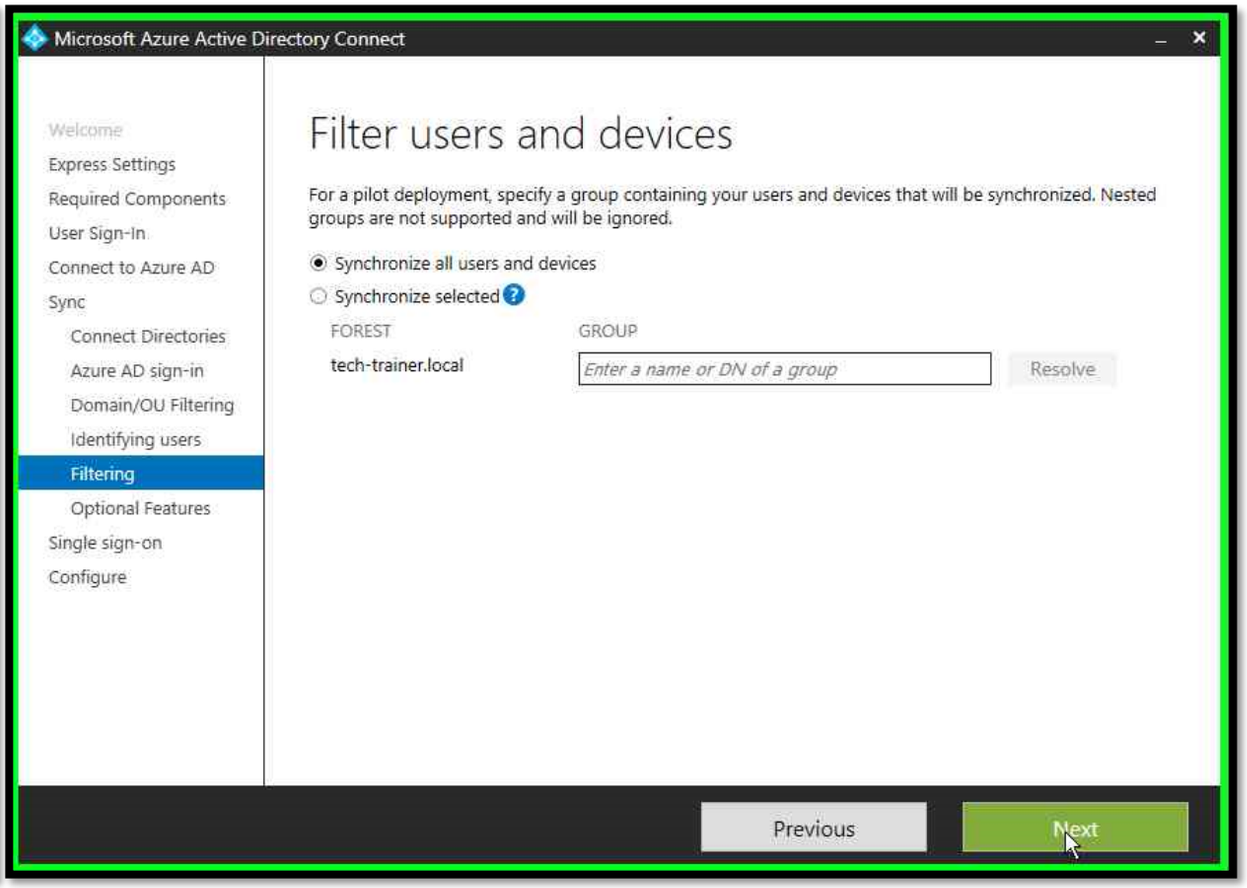
PTA - Step-by-step



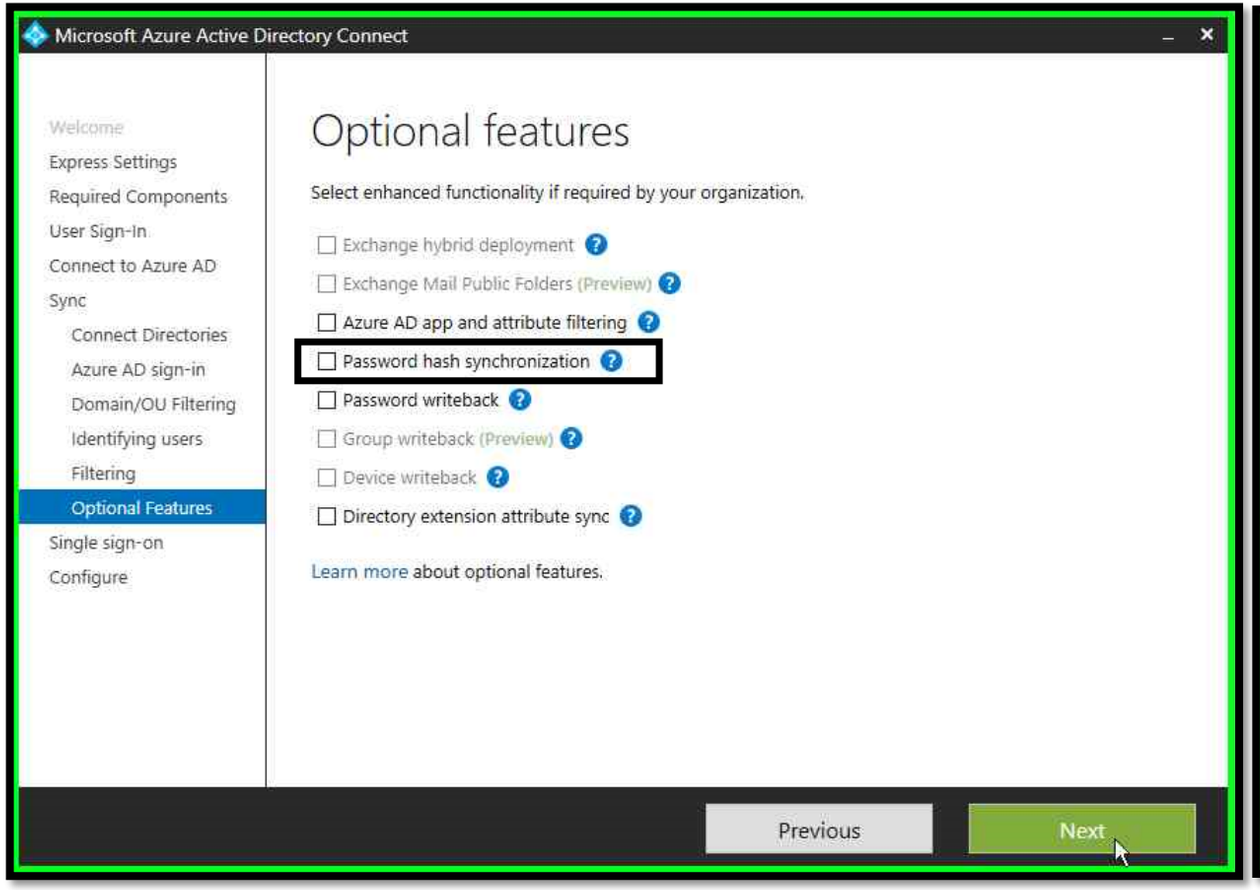


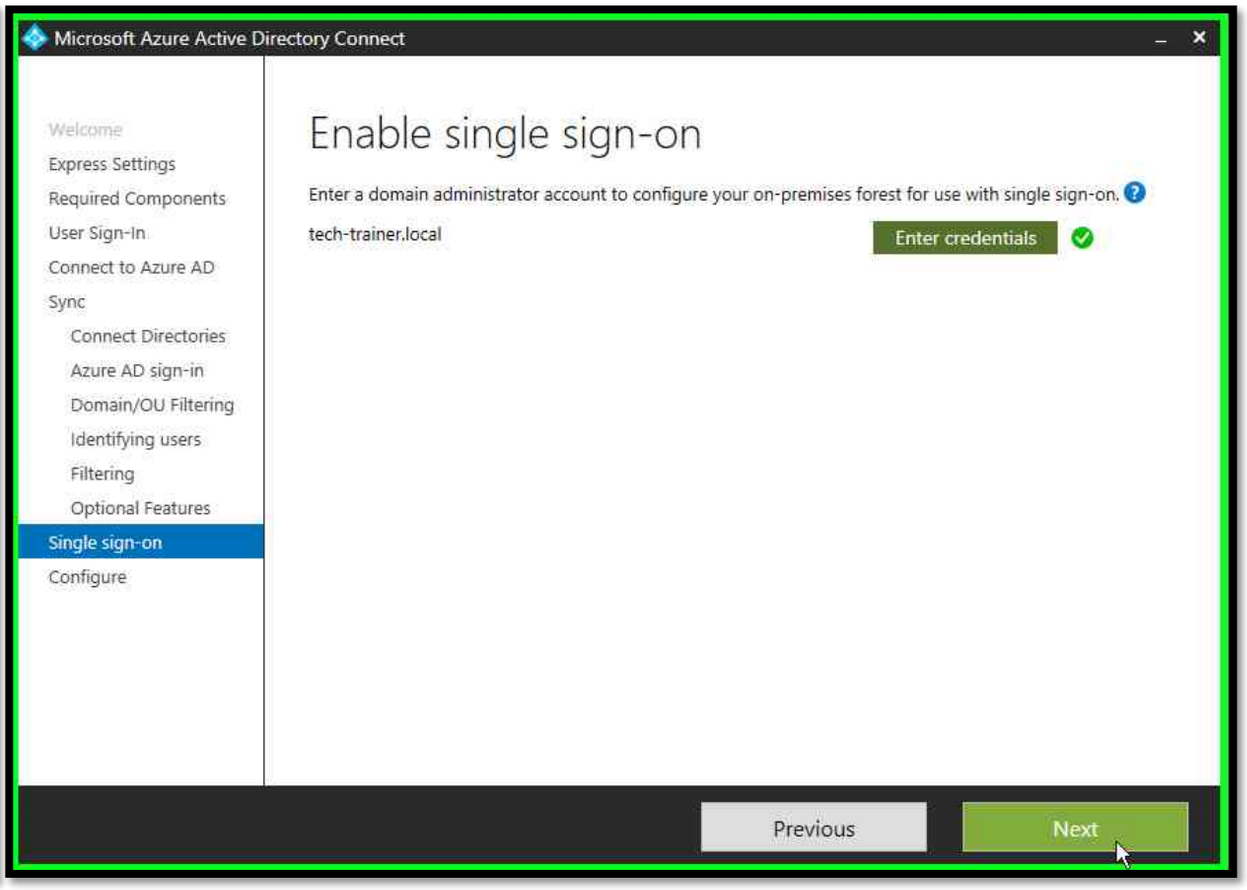
PTA - Step-by-step



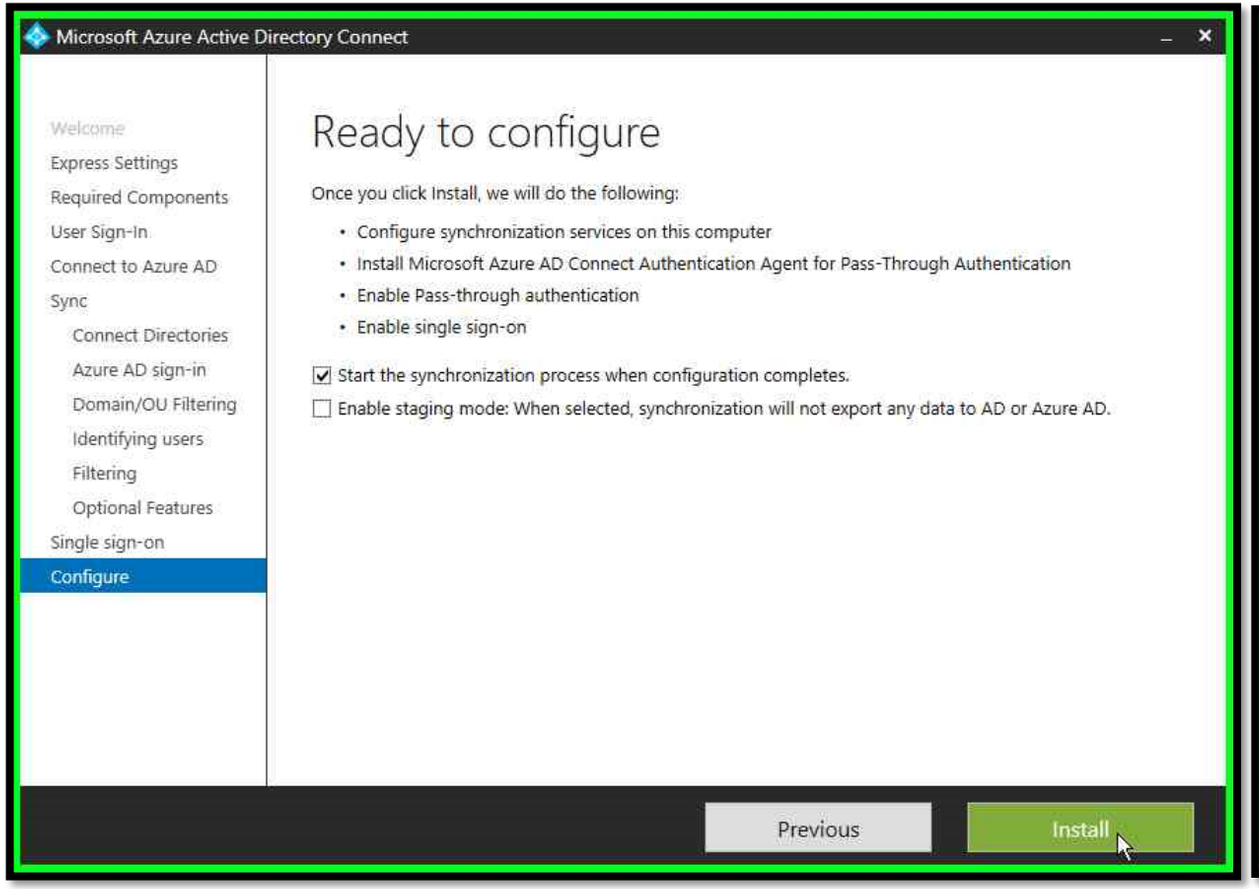


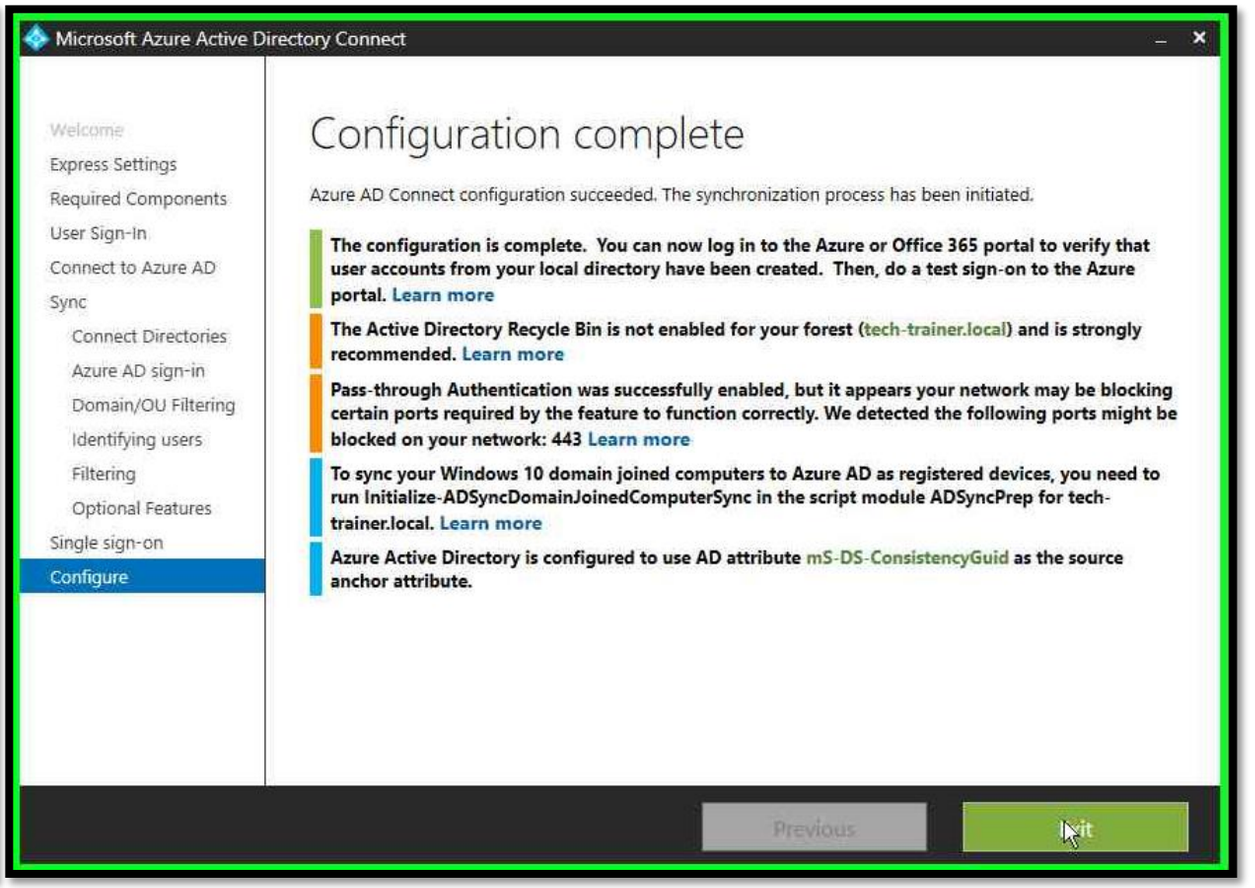
PTA - Step-by-step





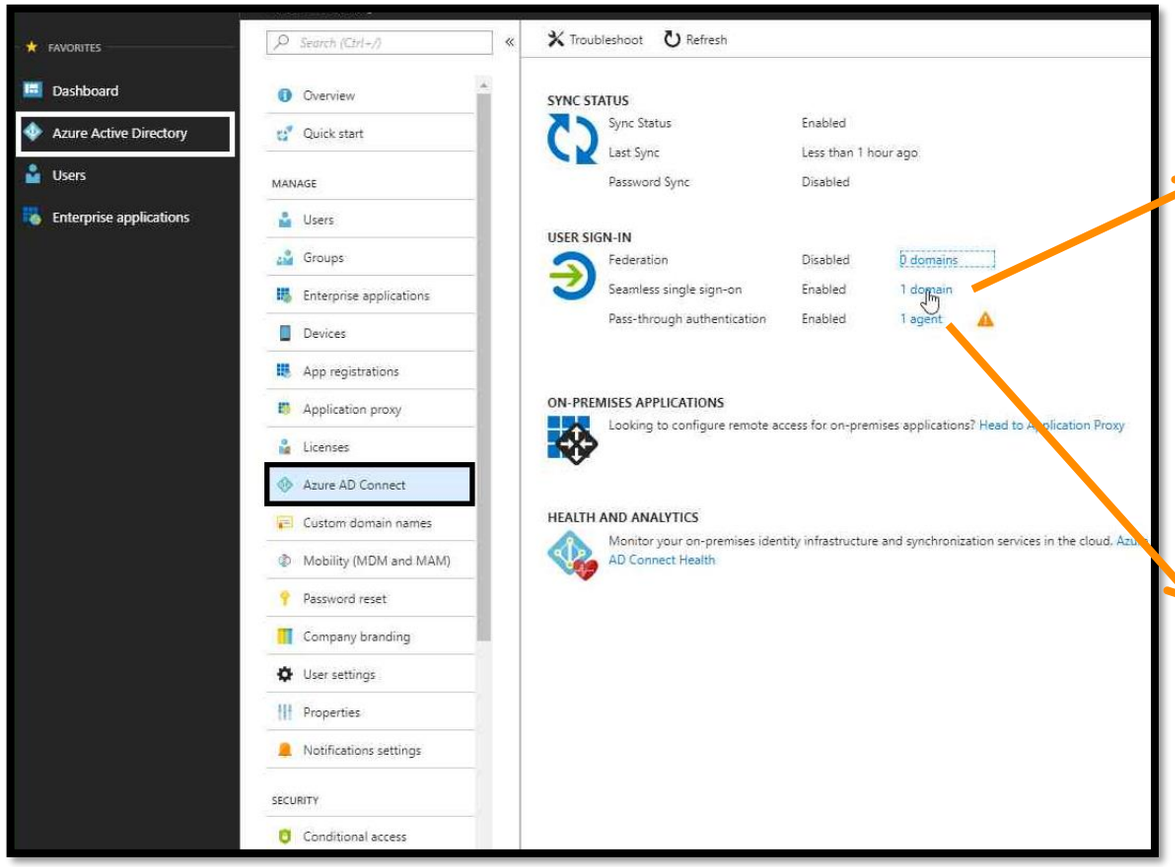
PTA - Step-by-step

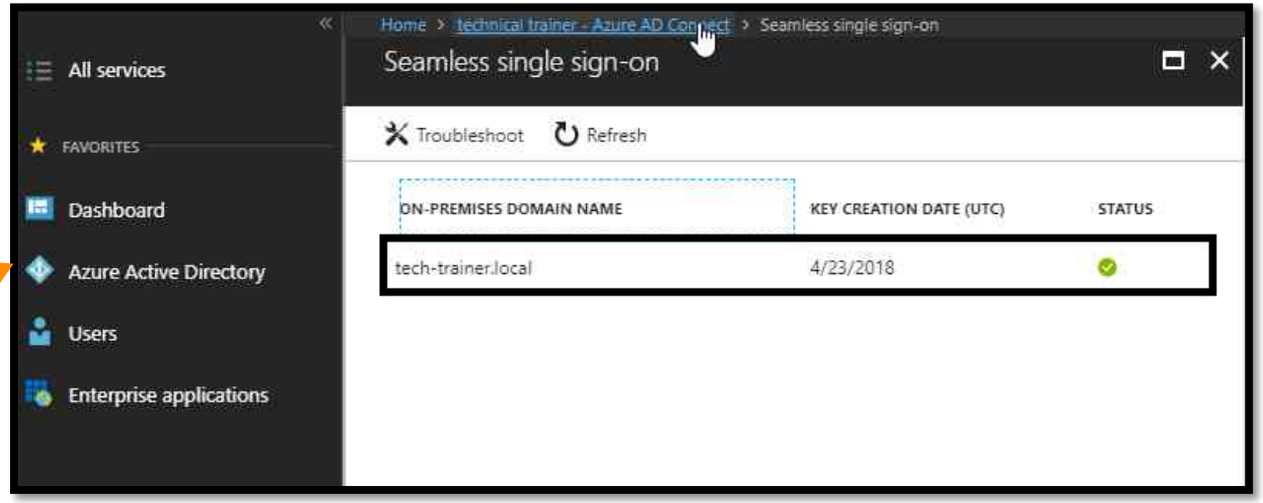


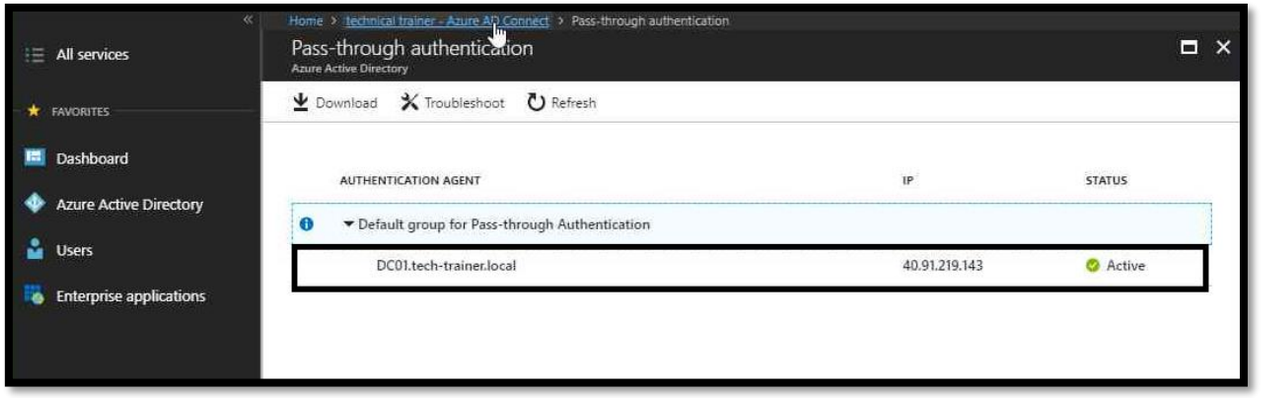


Windays 18

PTA - Step-by-step







Windays 18

Q & A

Thank you for your attention

Technology

Microsoft