

Windays¹⁸

Technology



Office 365 SSO Lako i jednostavno

Vladimir Stefanović
Superadmins - Belgrade

Technology

A large white word "Technology" is positioned on the right side of the slide. The letter "y" is replaced by a 3D blue cube with white edges, which has a small white square on its top face.

Who am I

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



Agenda

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



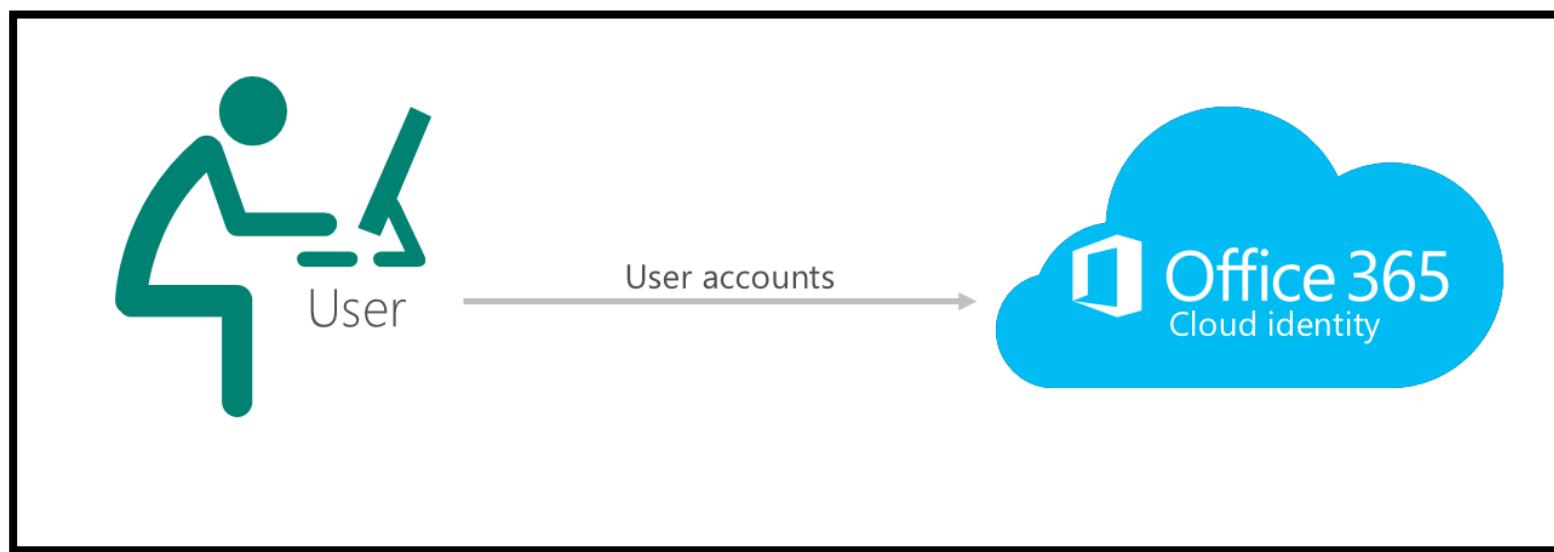
Technology

A large, stylized white word "Technology" is positioned in the upper right quadrant of the slide. The letter "y" is unique, designed as a 3D cube with a blue top face and a grey bottom edge, casting a shadow. The background features a dynamic, geometric pattern of blue and light blue triangles and polygons that radiate from behind the text.

Identity models

Cloud identity

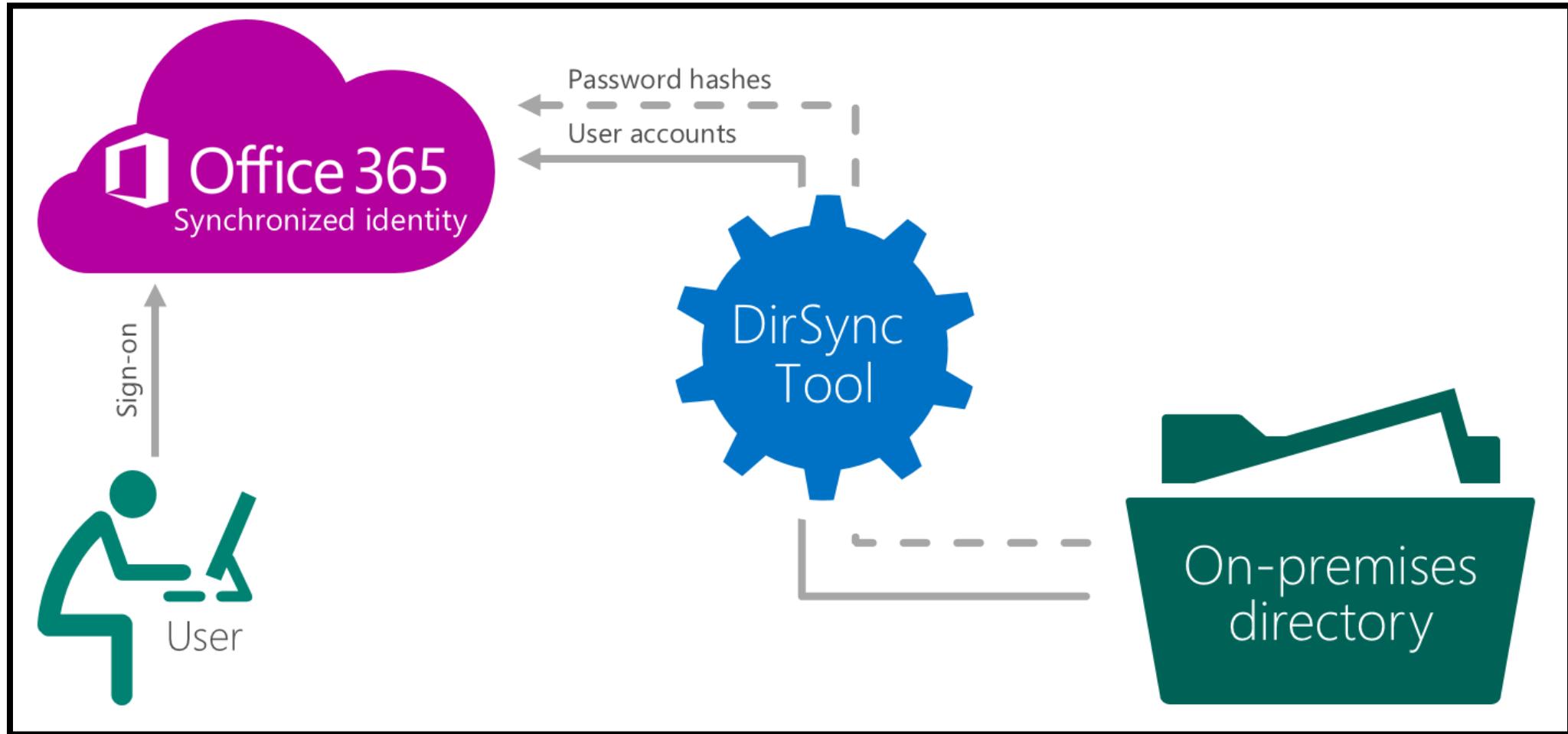
- User is created and managed in Office 365 and stored in Azure Active Directory
- Identity is verified by Azure AD
- There is no equivalent user account on-premises



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

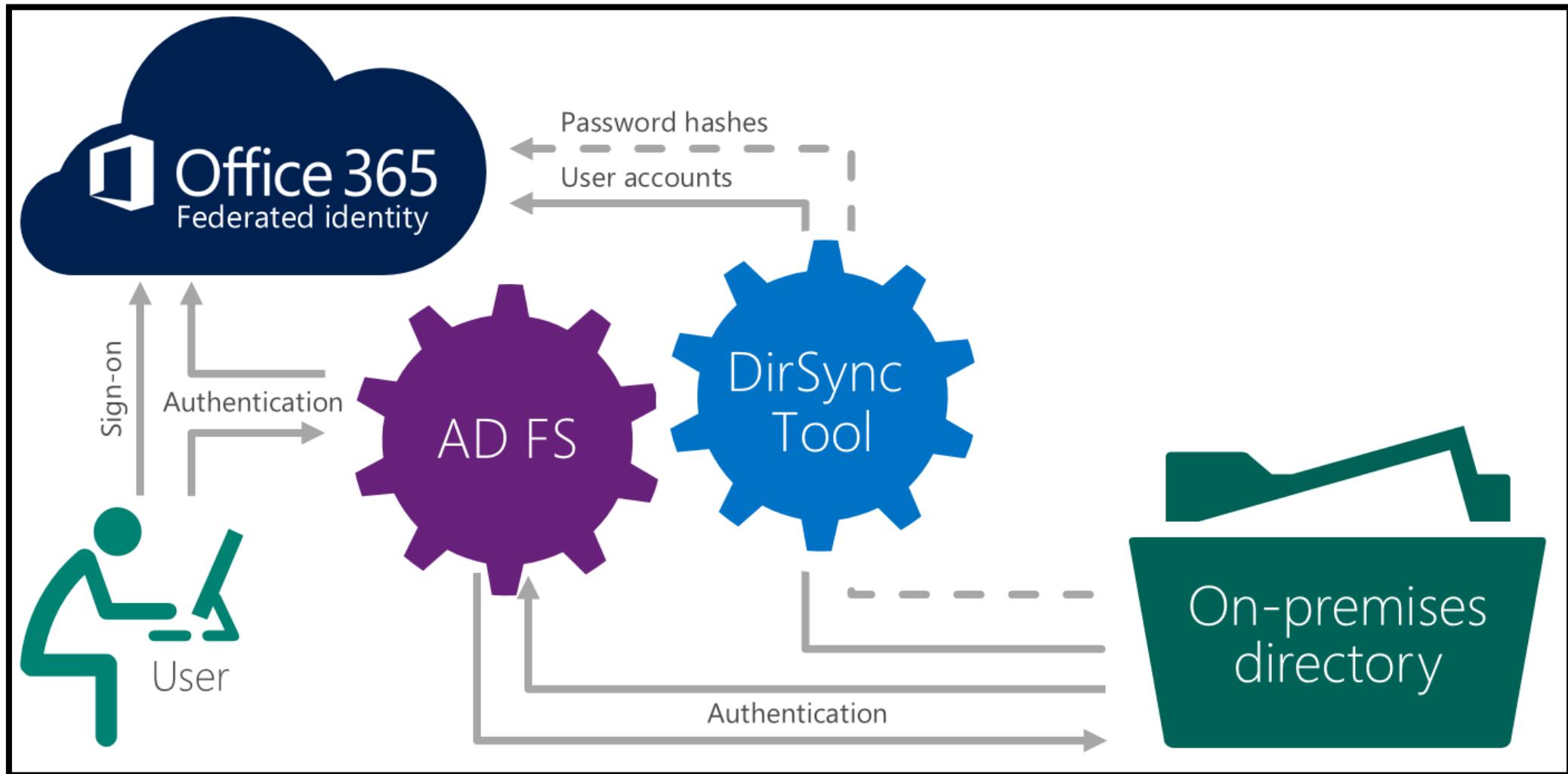
Synchronized Identity - PHS & PTA



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

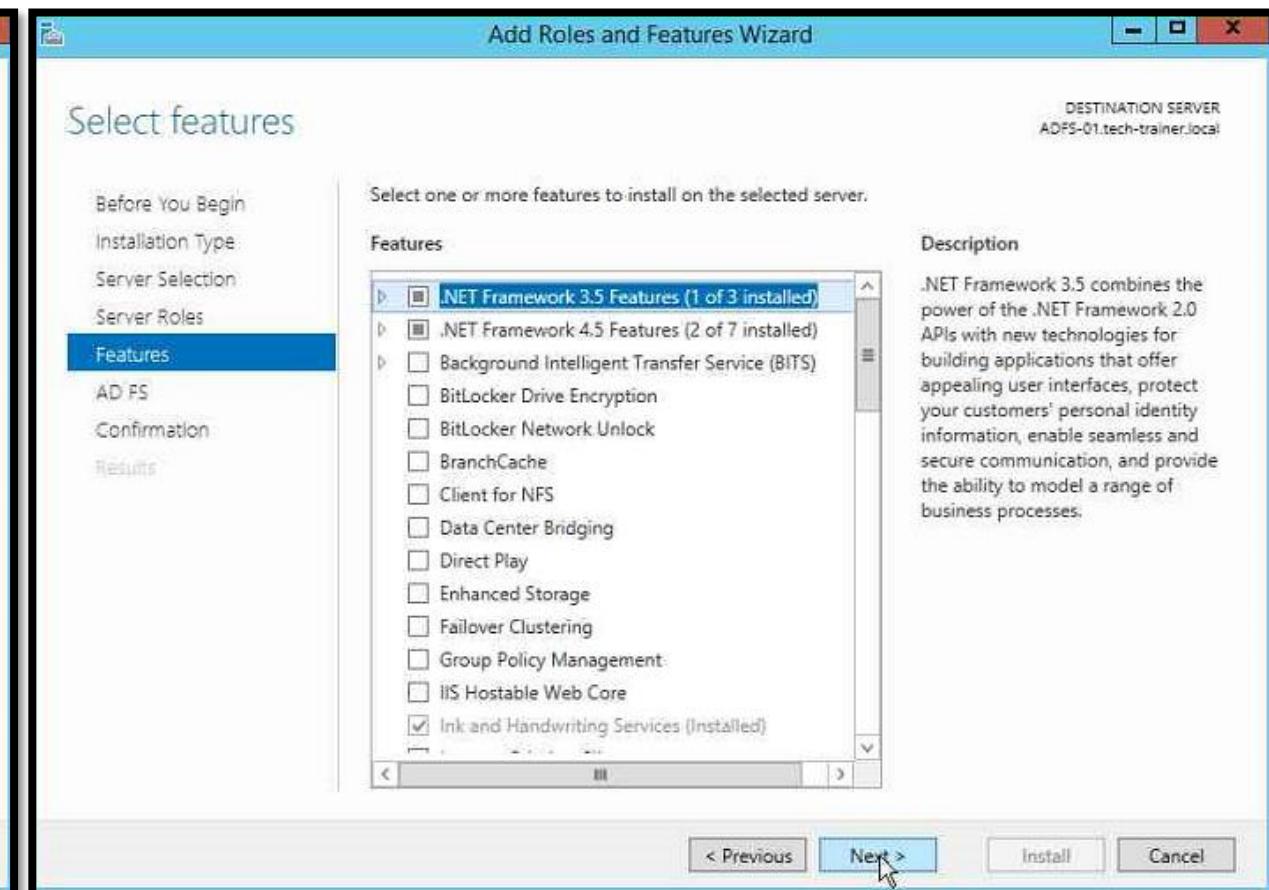
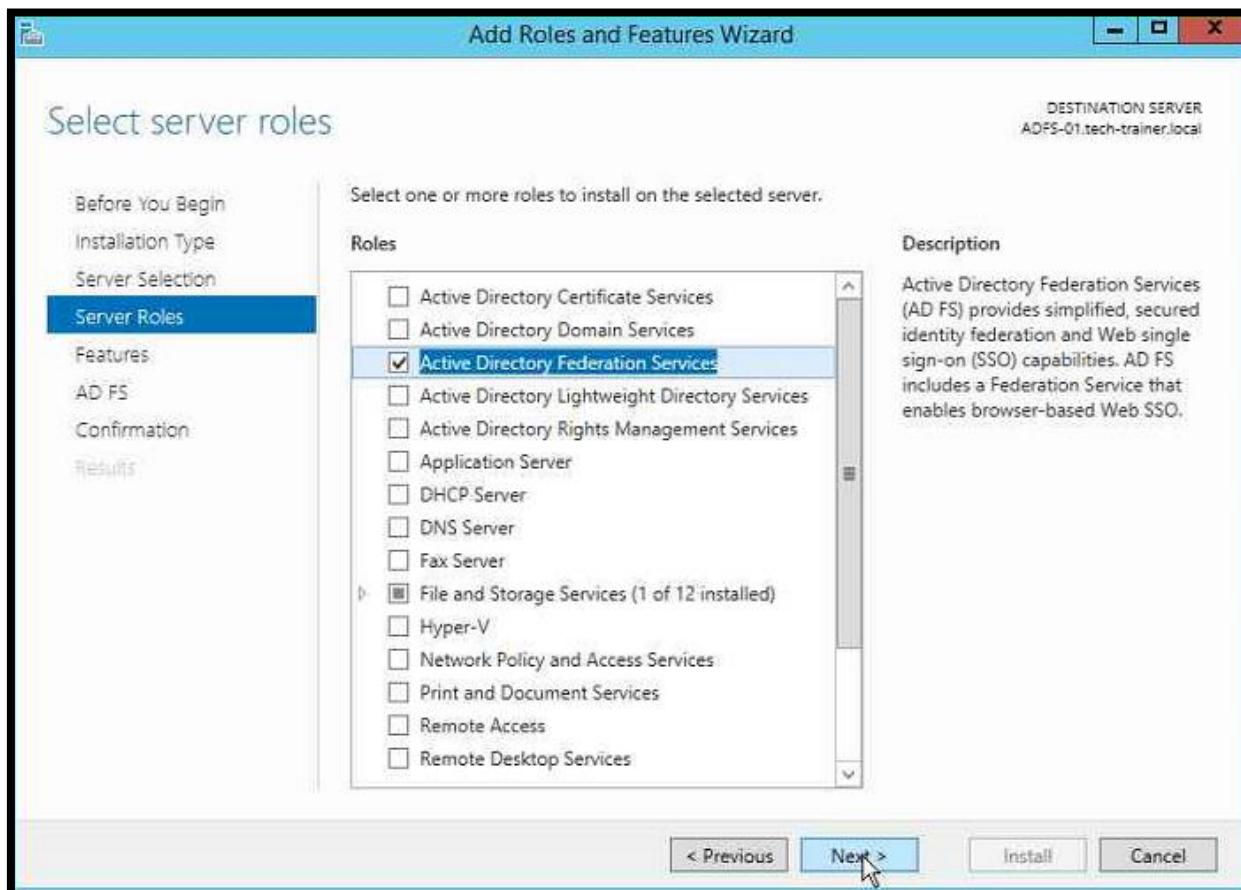
- Great user experience
 - *Users are automatically signed into on-premises and cloud-based apps*
 - *Users don't have to enter their passwords*
- Easy to deploy & administer
 - *No additional components needed on-premises*
 - *Works with Password Hash Synchronization or Pass-through Authentication*
 - *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

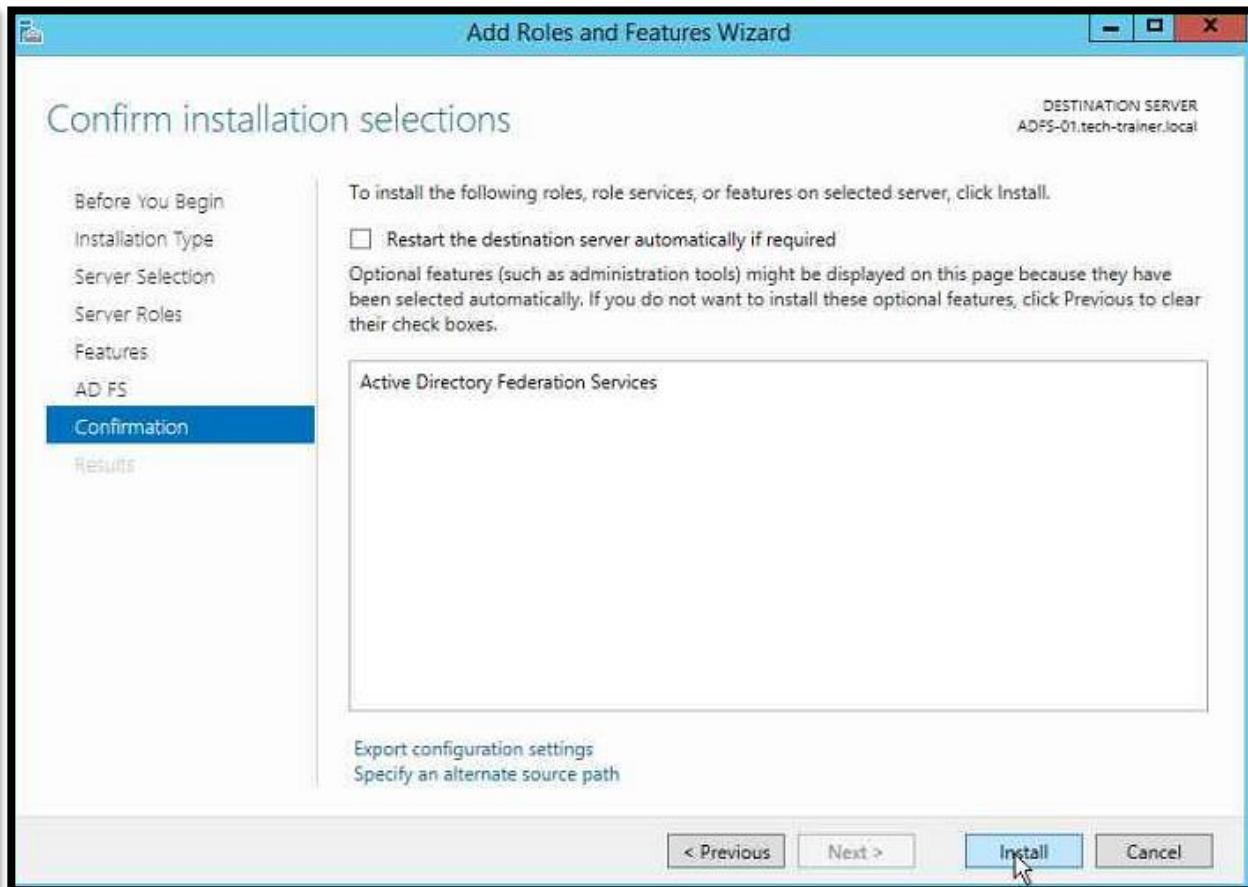
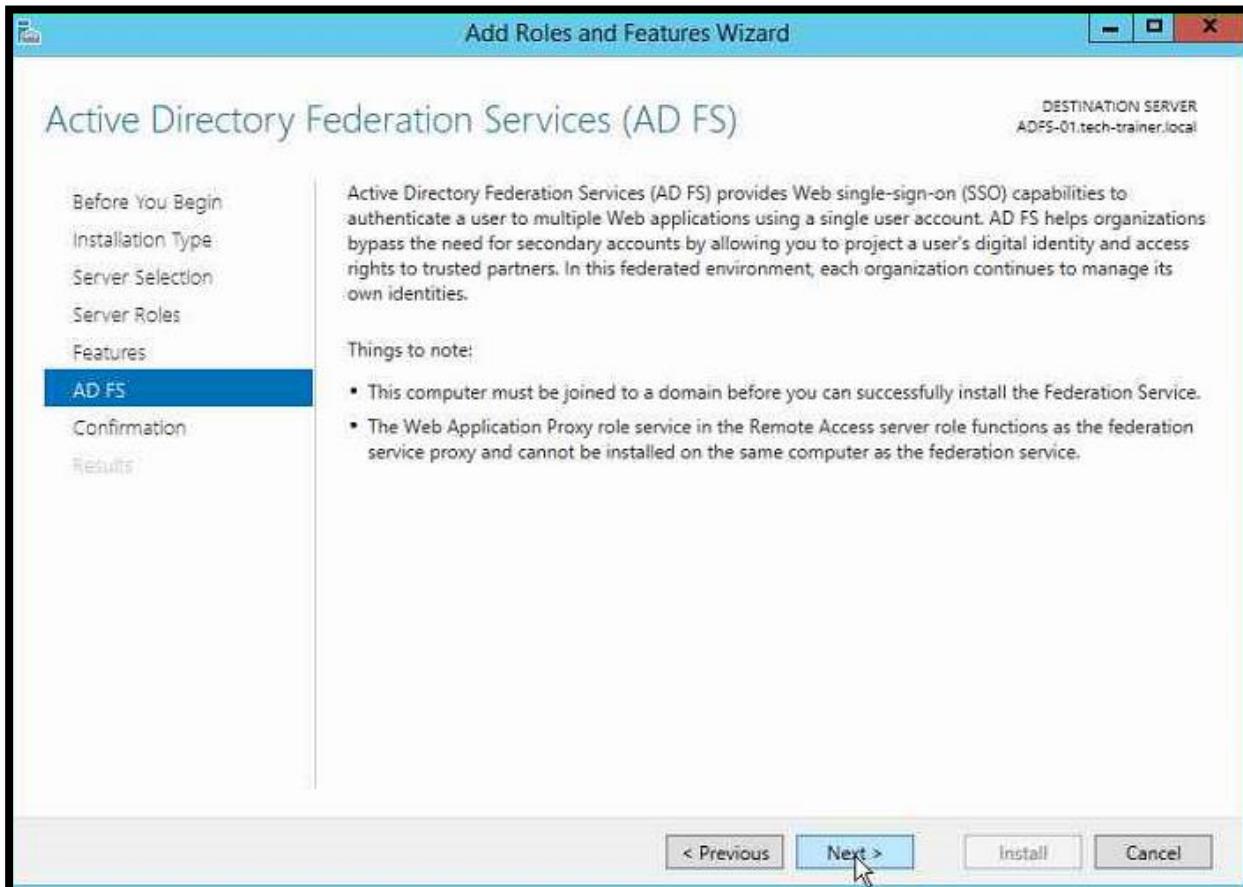
- Add the following Azure AD URL to the users *Intranet zone settings* by using GPO
 - <https://autologon.microsoftazuread-sso.com>
 - <https://aadg.windows.net.nsatc.net>

Demo - ADFS

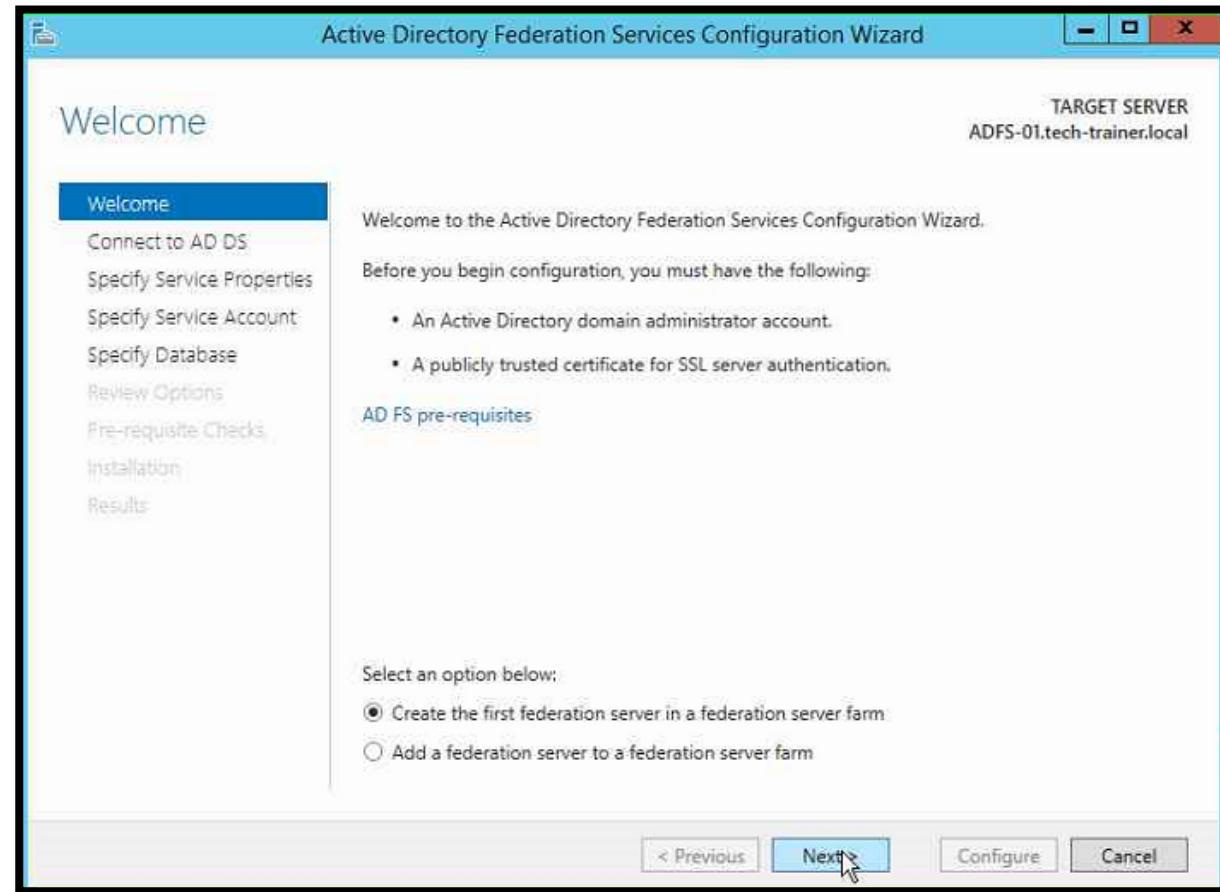
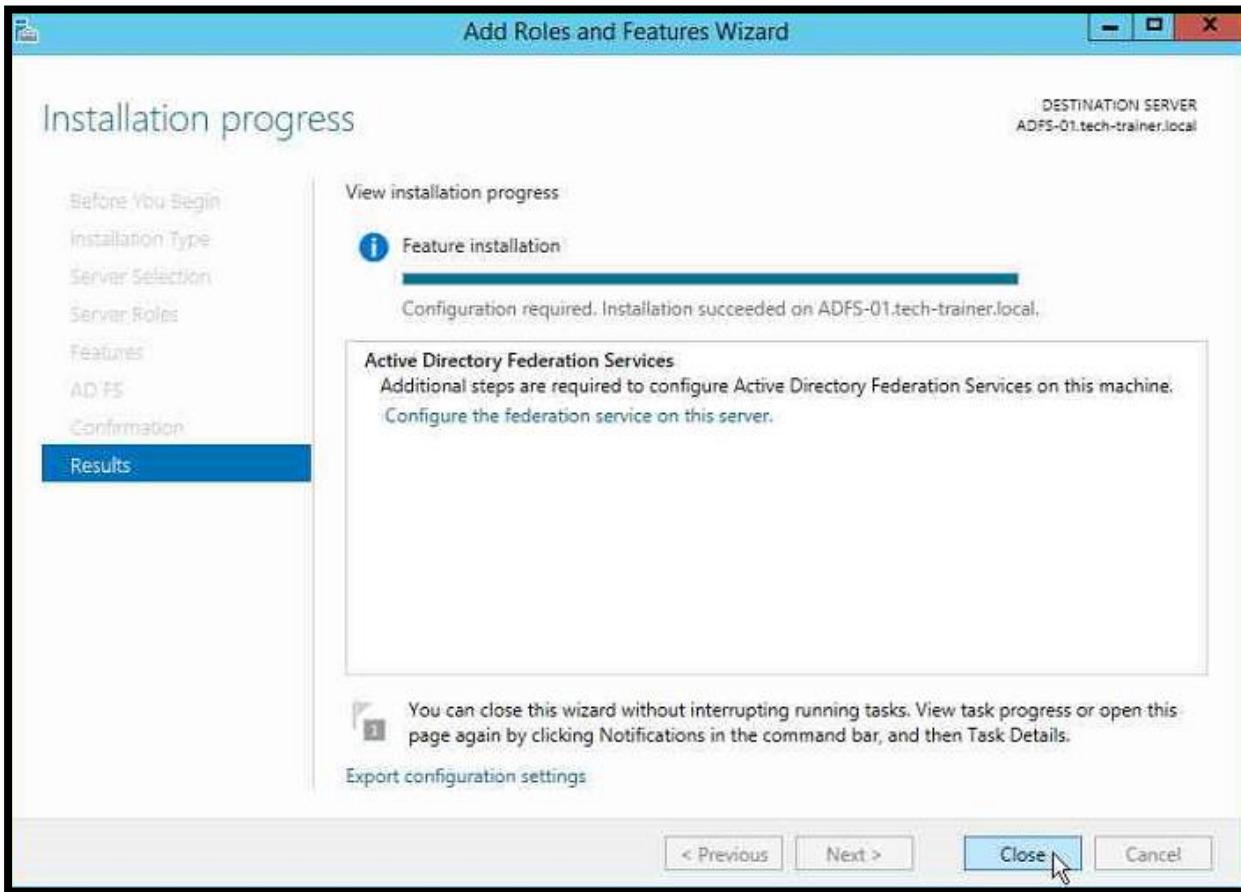
ADFS - Step-by-step



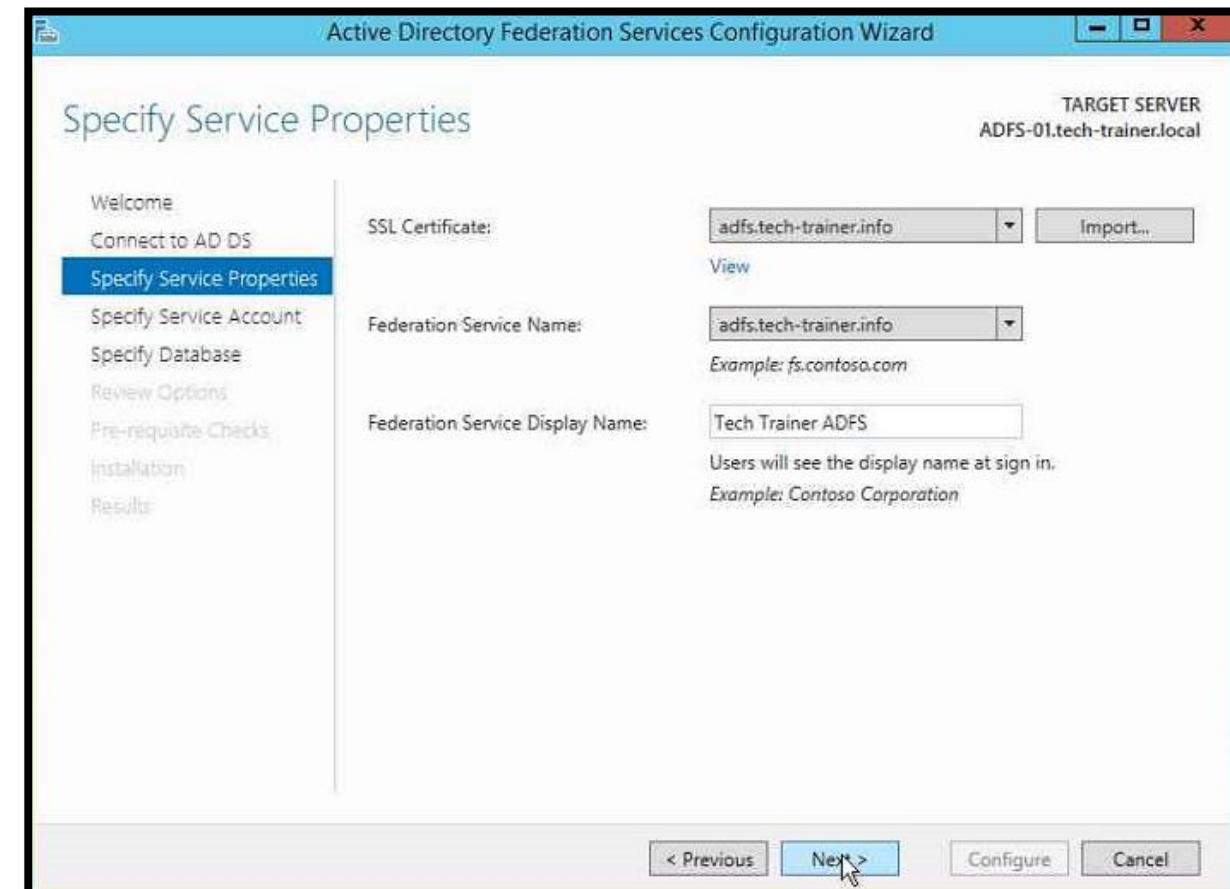
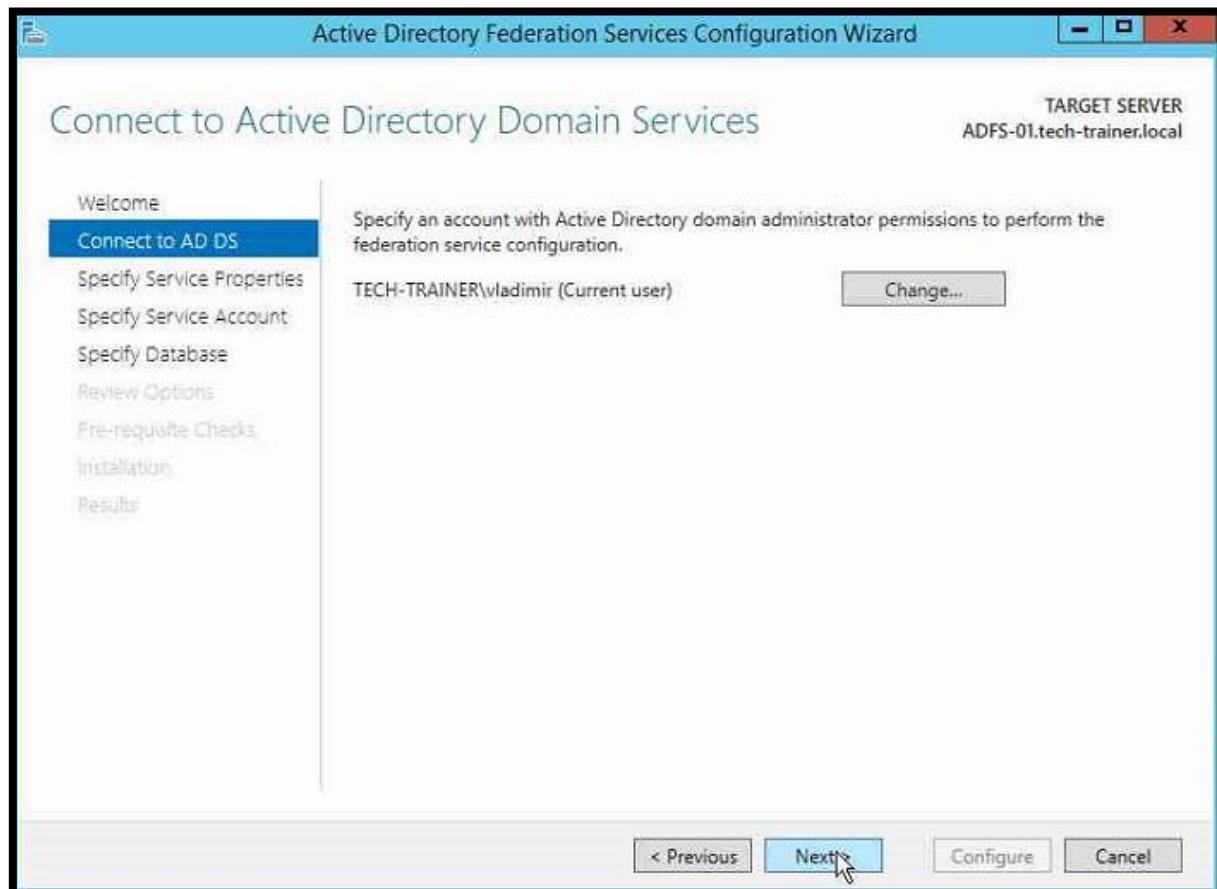
ADFS - Step-by-step



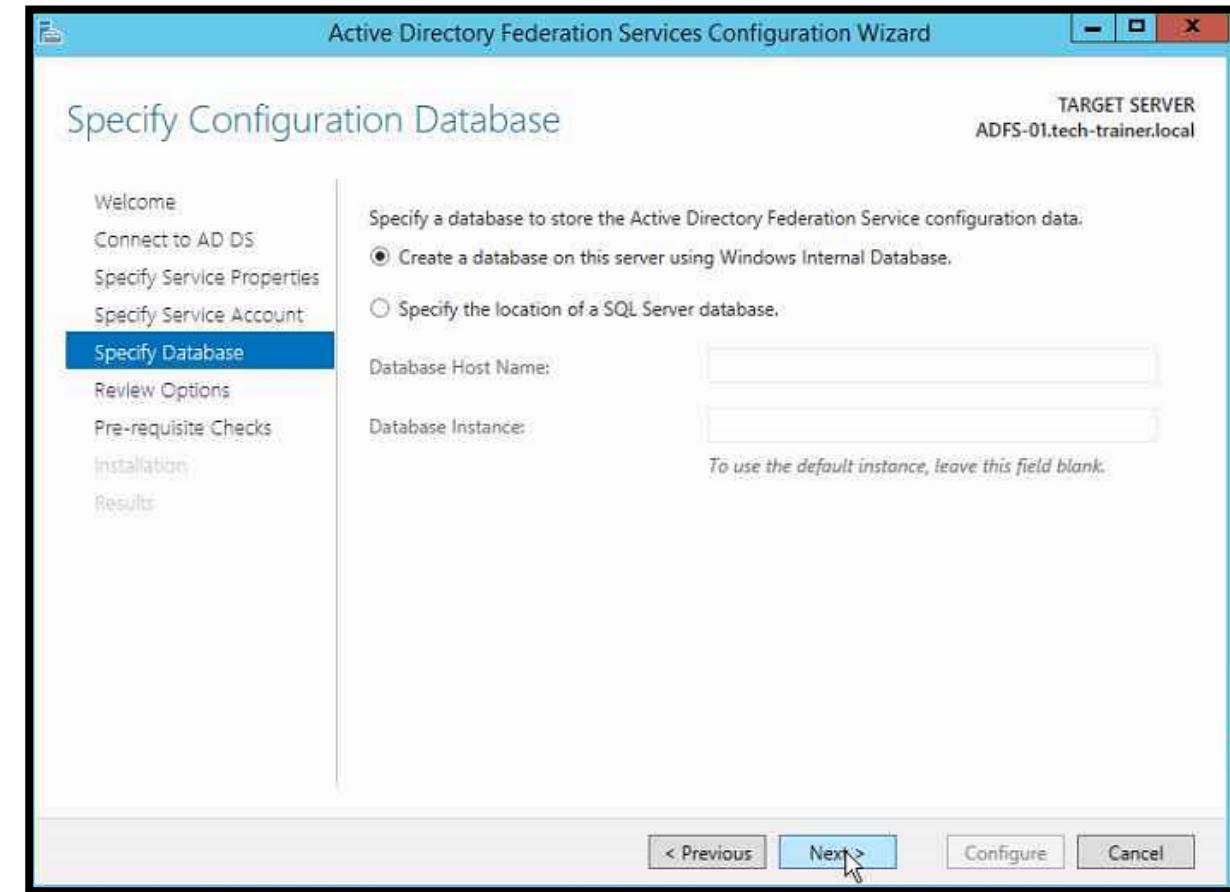
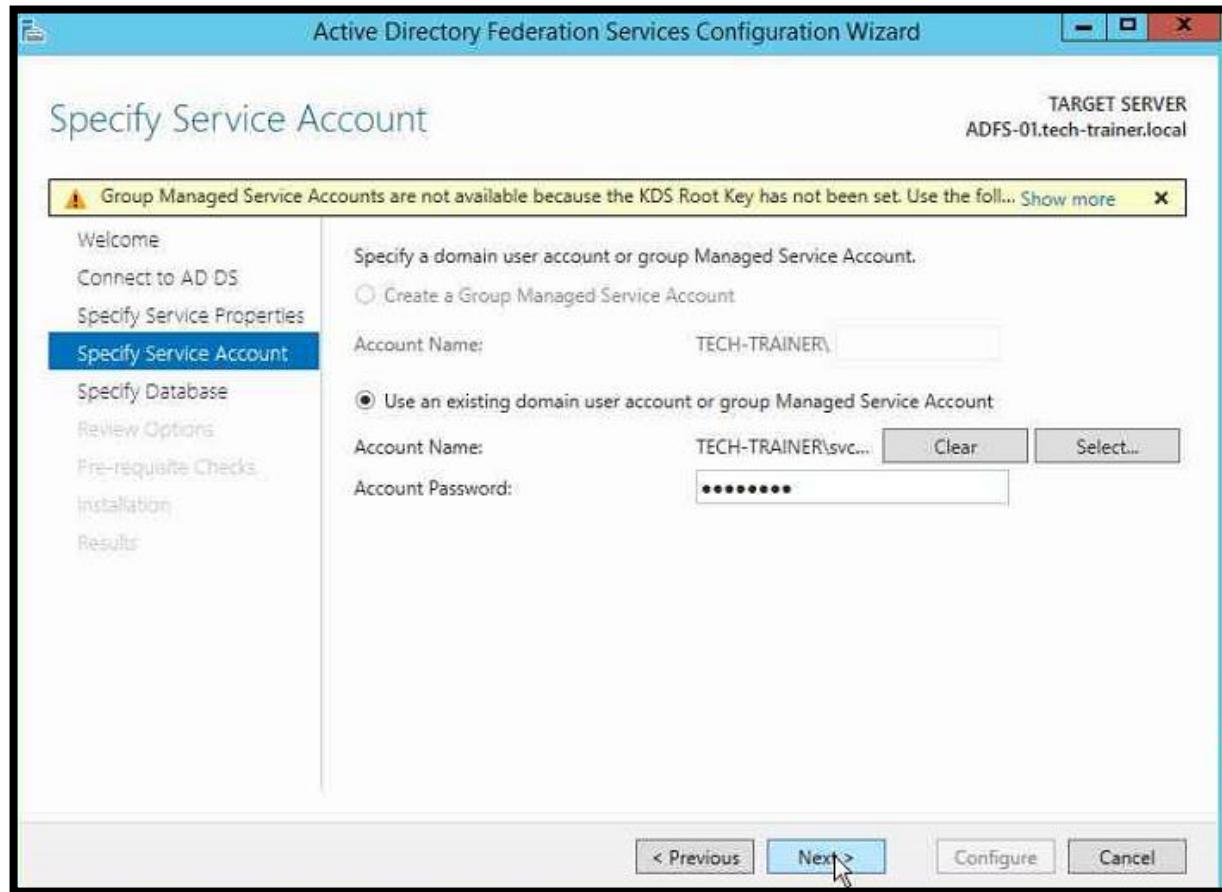
ADFS - Step-by-step



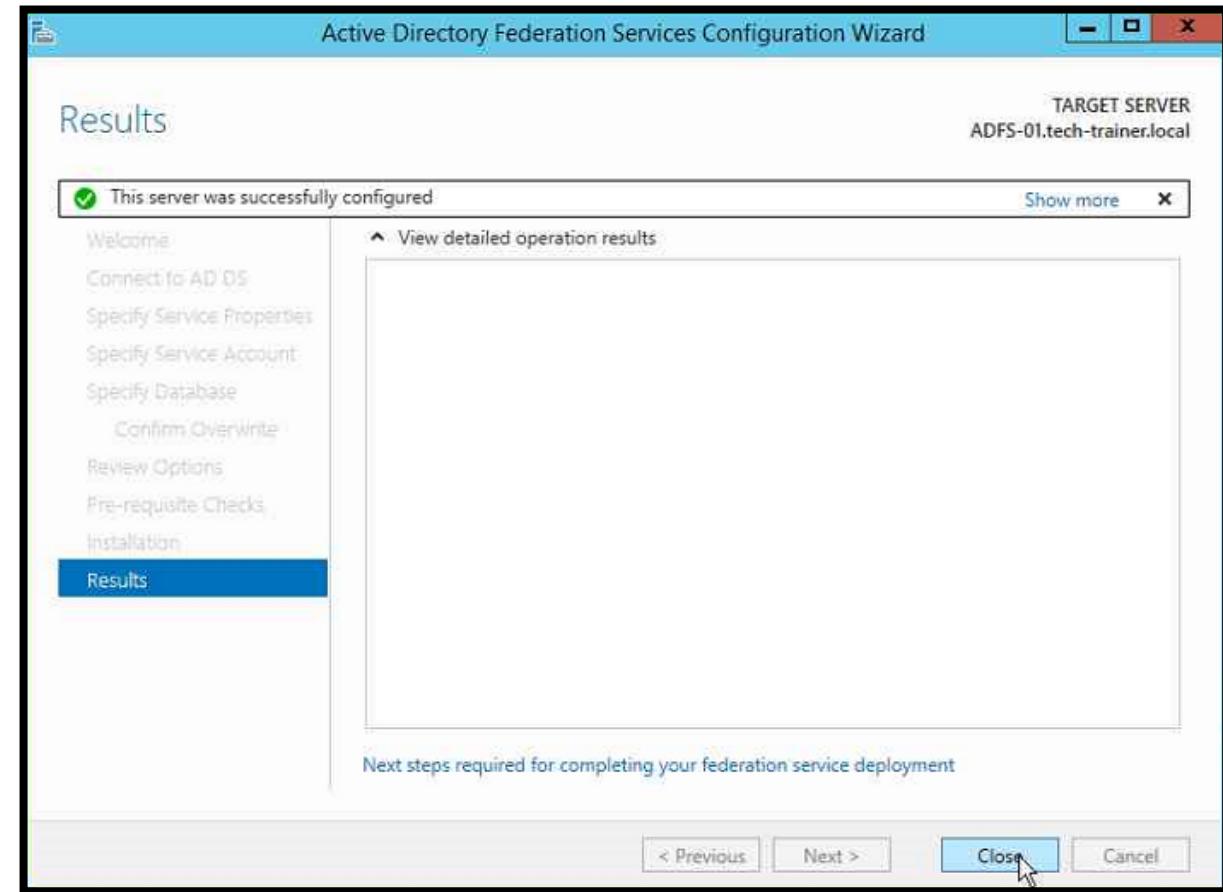
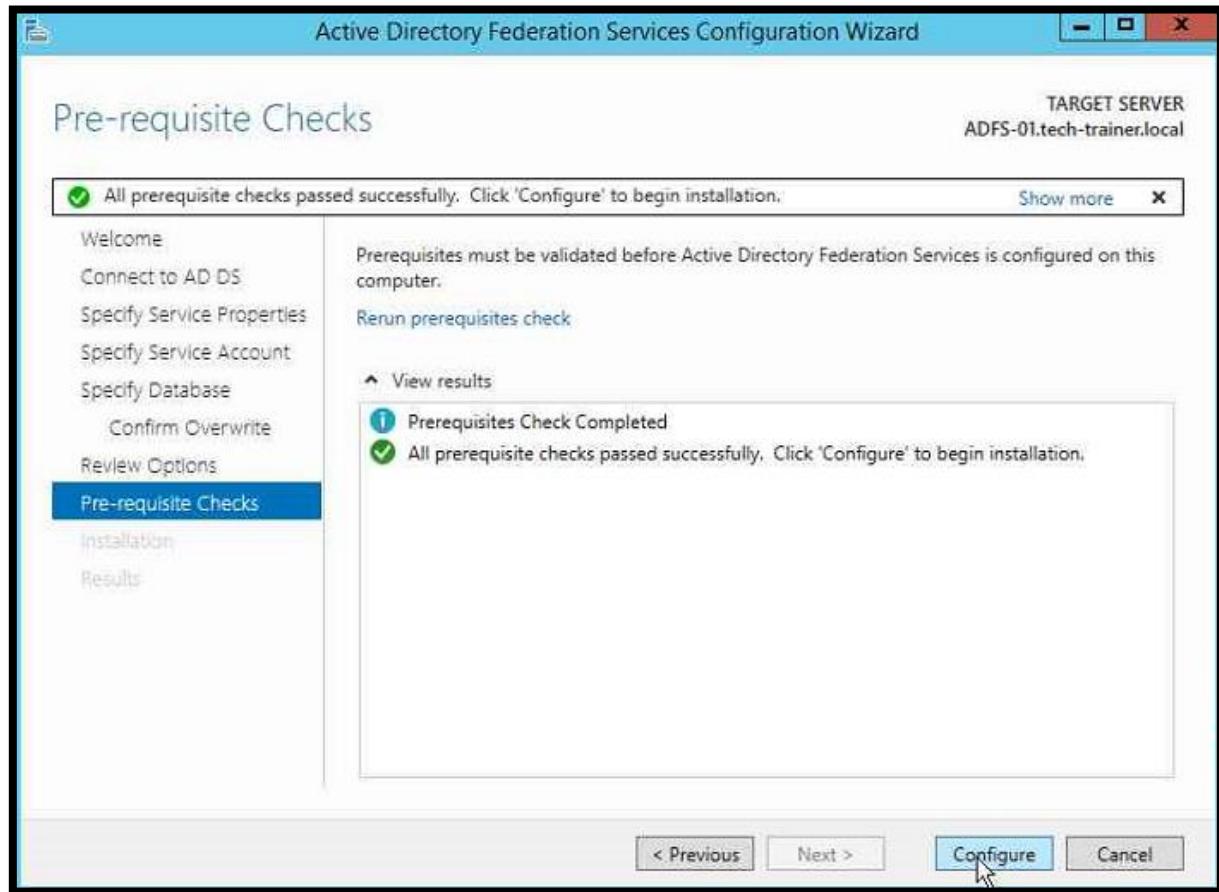
ADFS - Step-by-step



ADFS - Step-by-step



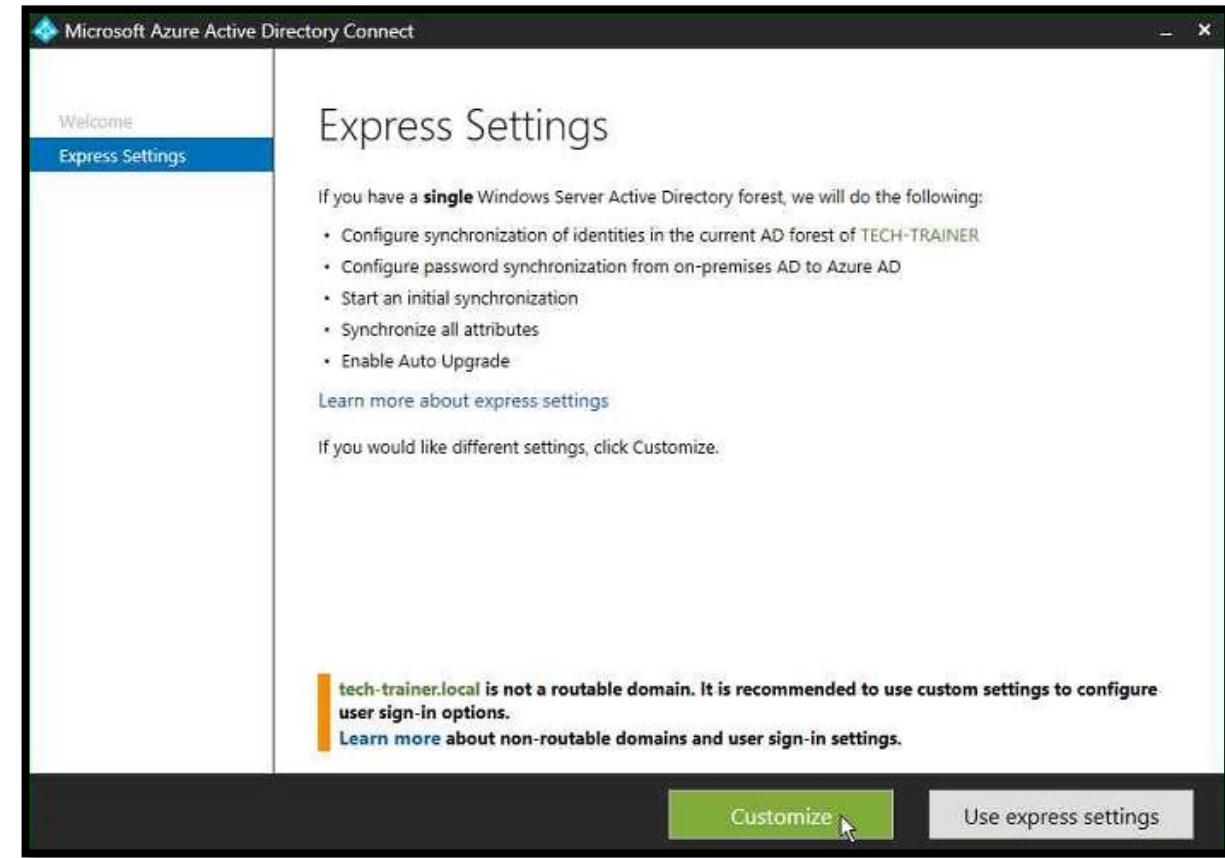
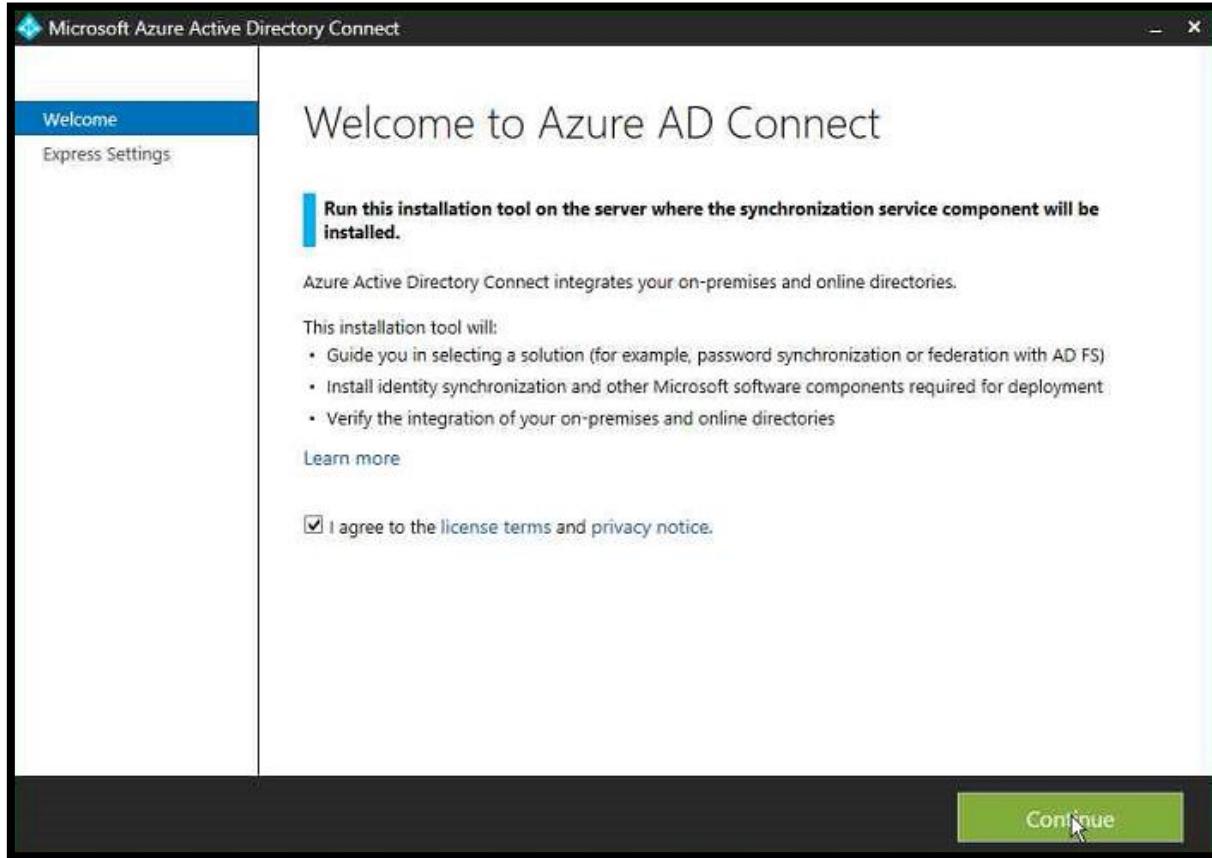
ADFS - Step-by-step



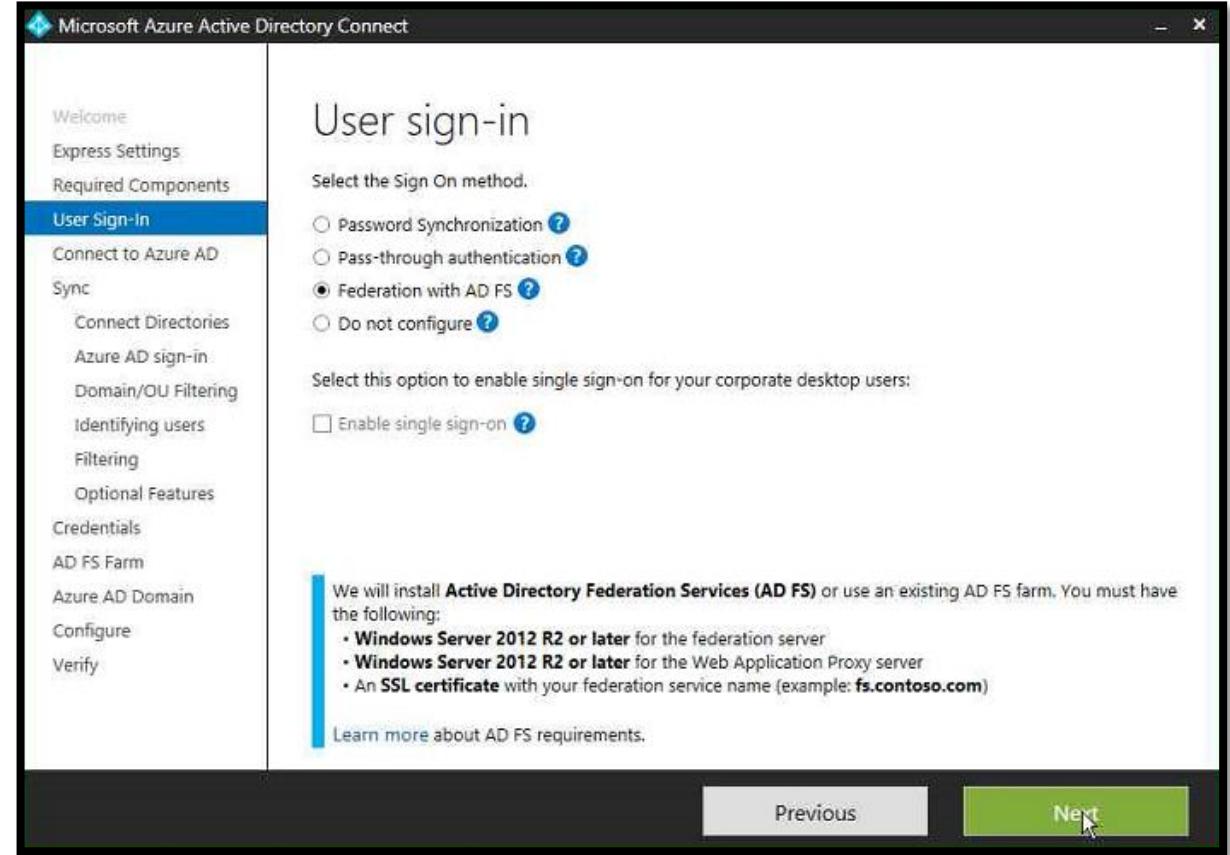
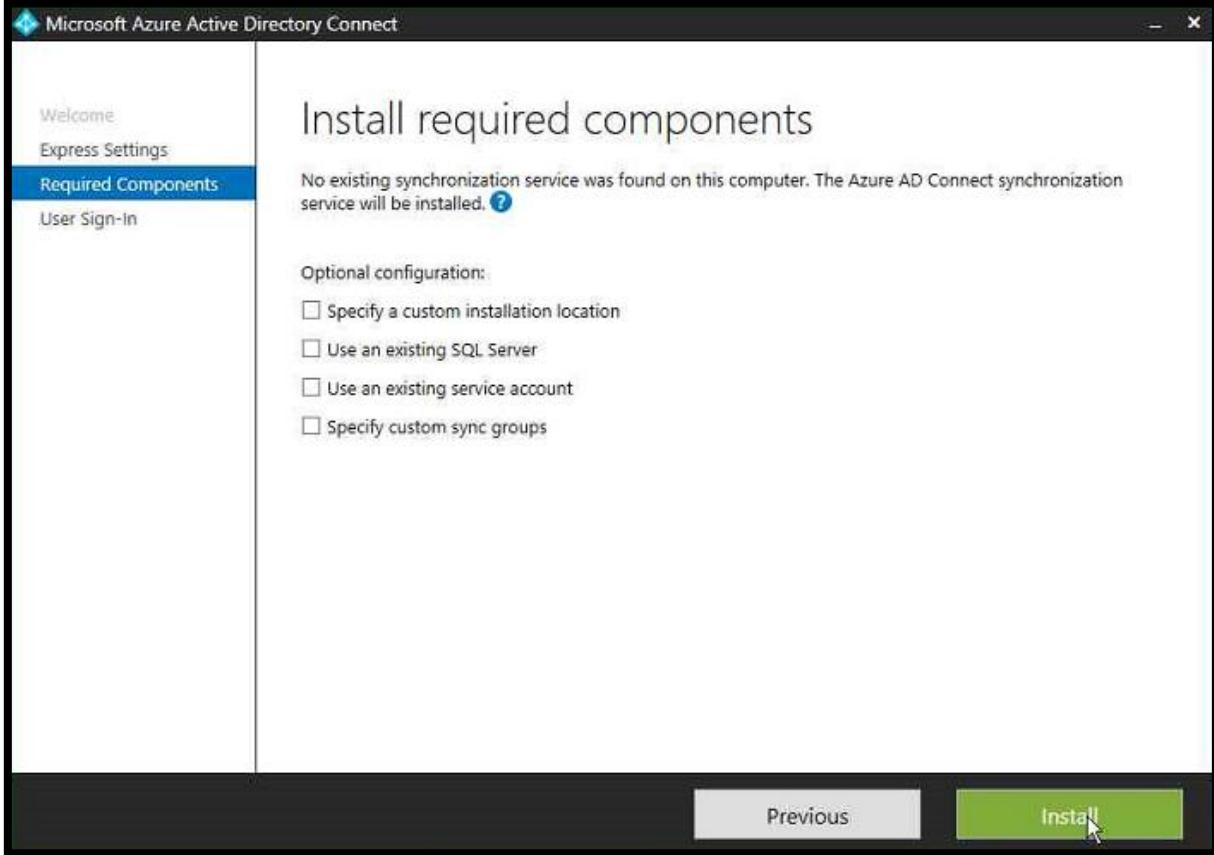
ADFS - Step-by-step

- 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"`

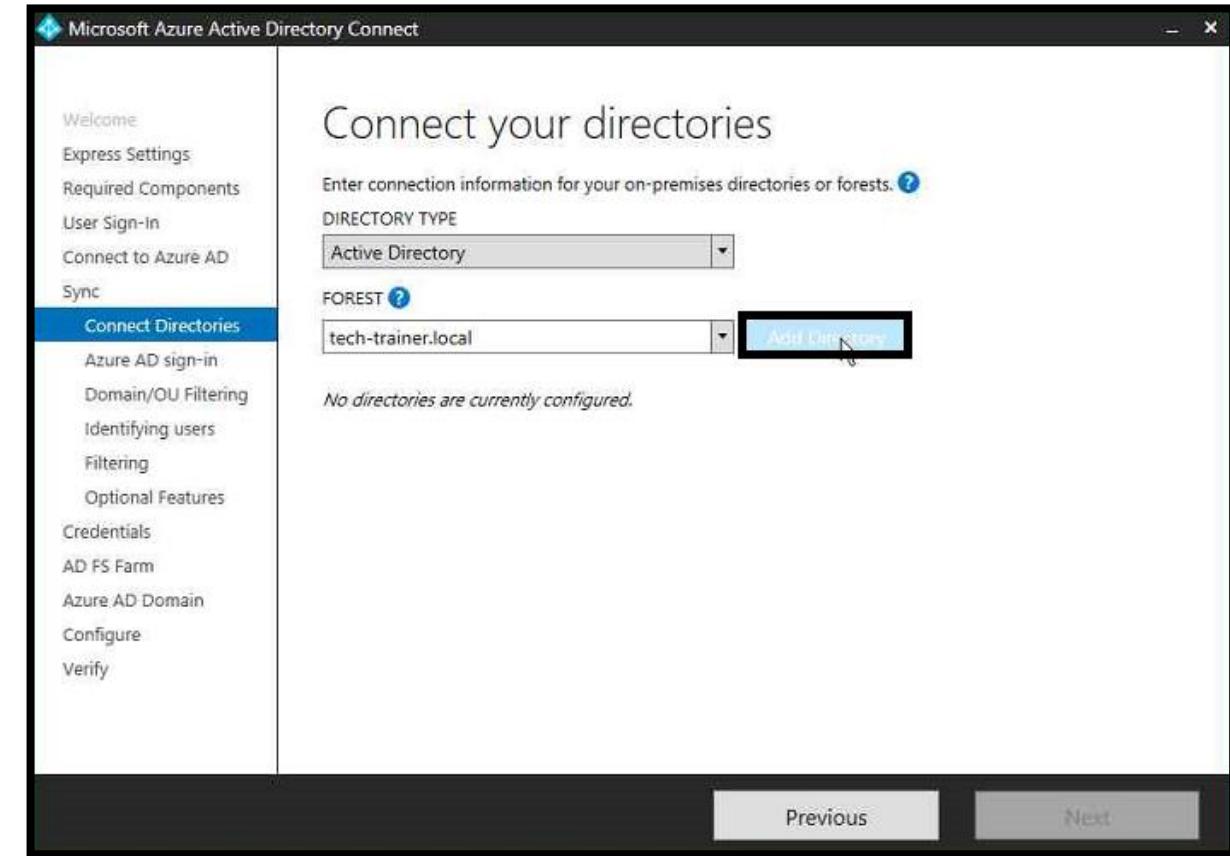
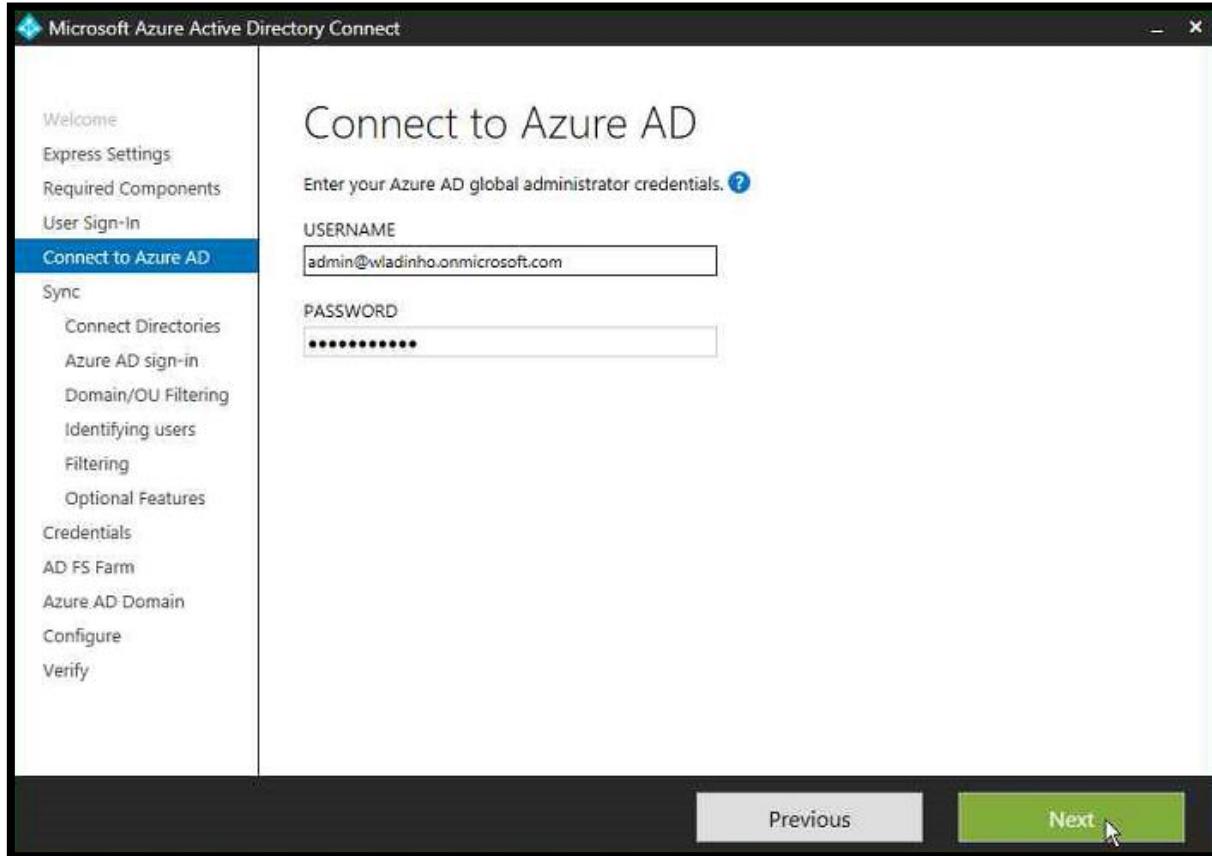
ADFS - Step-by-step



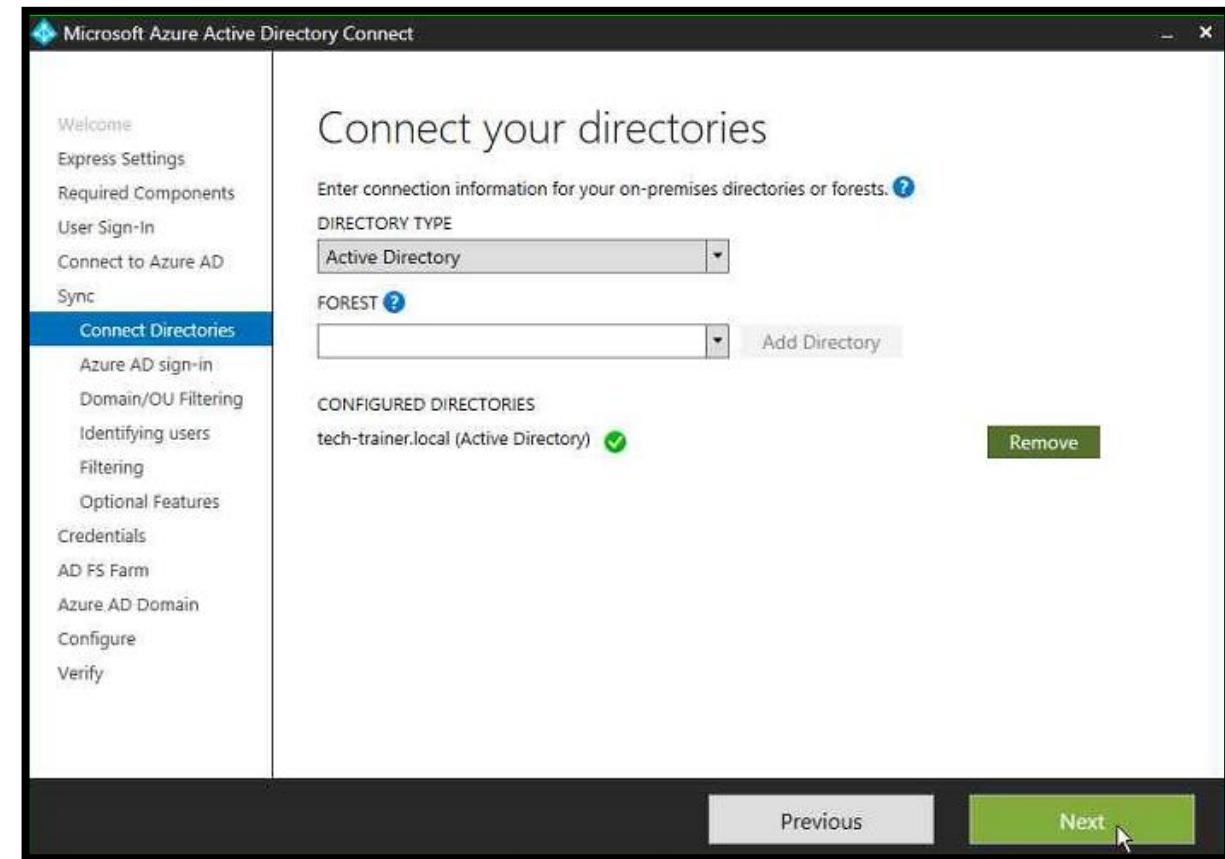
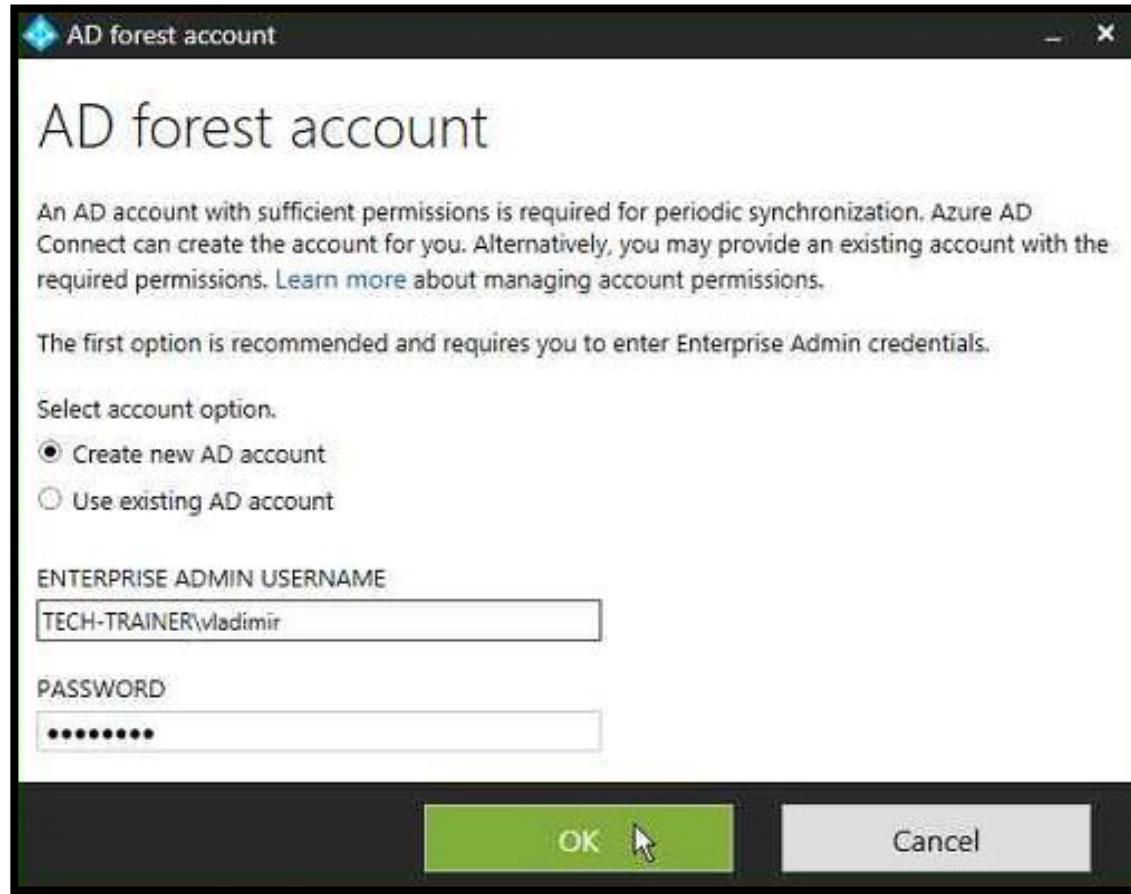
ADFS - Step-by-step



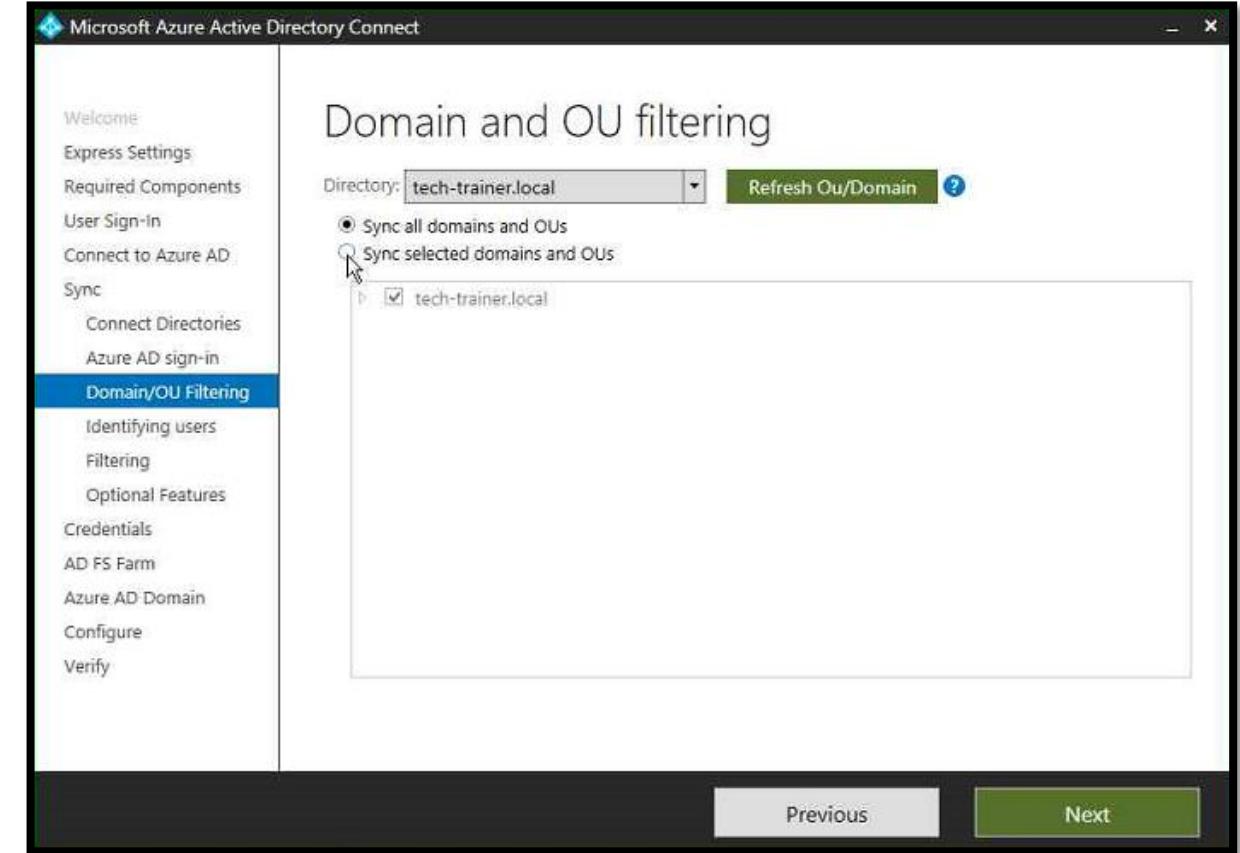
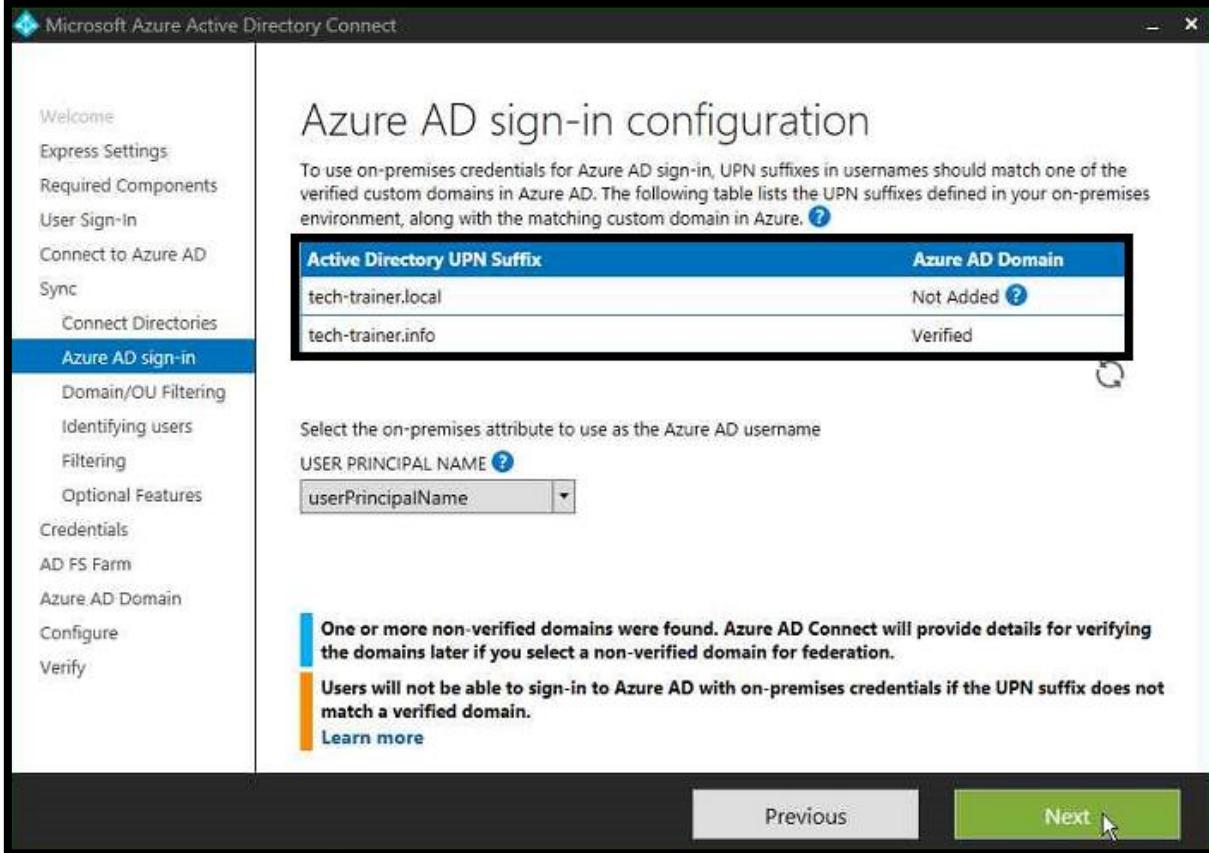
ADFS - Step-by-step



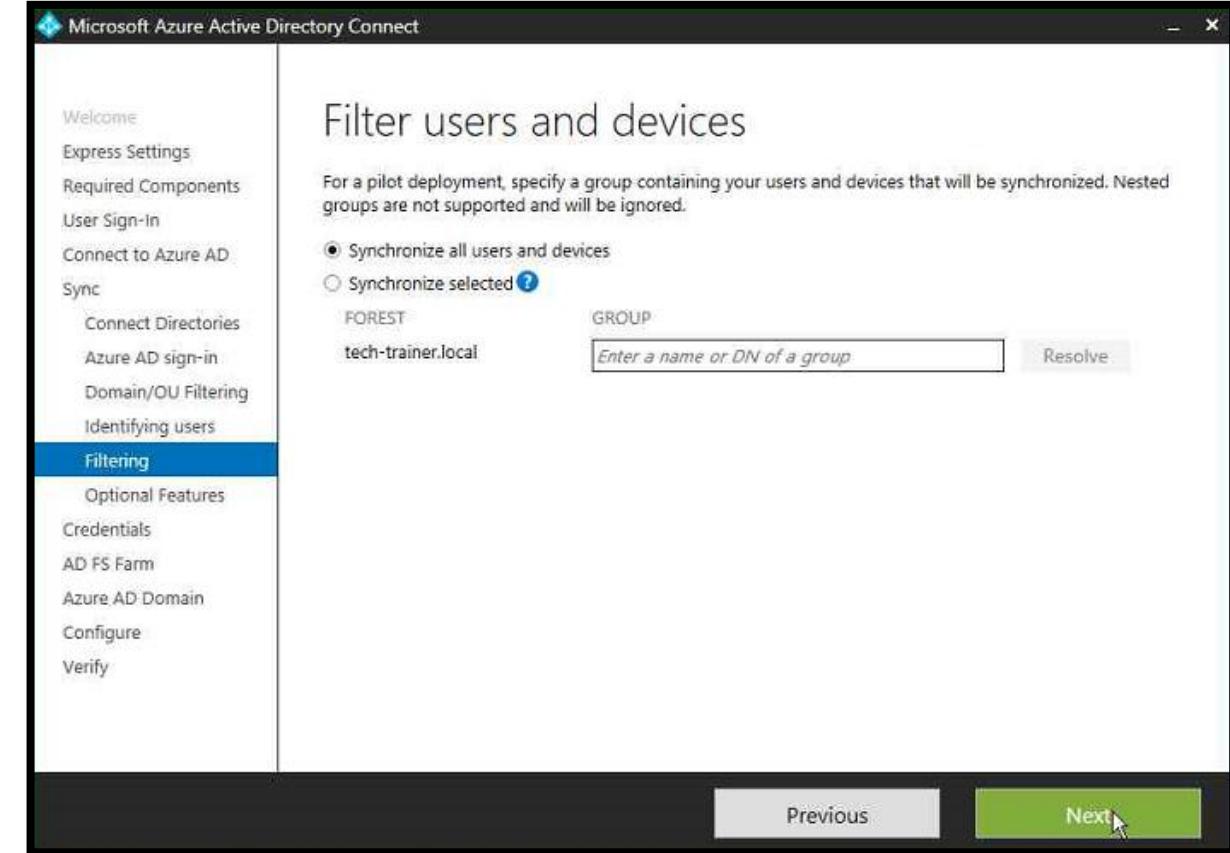
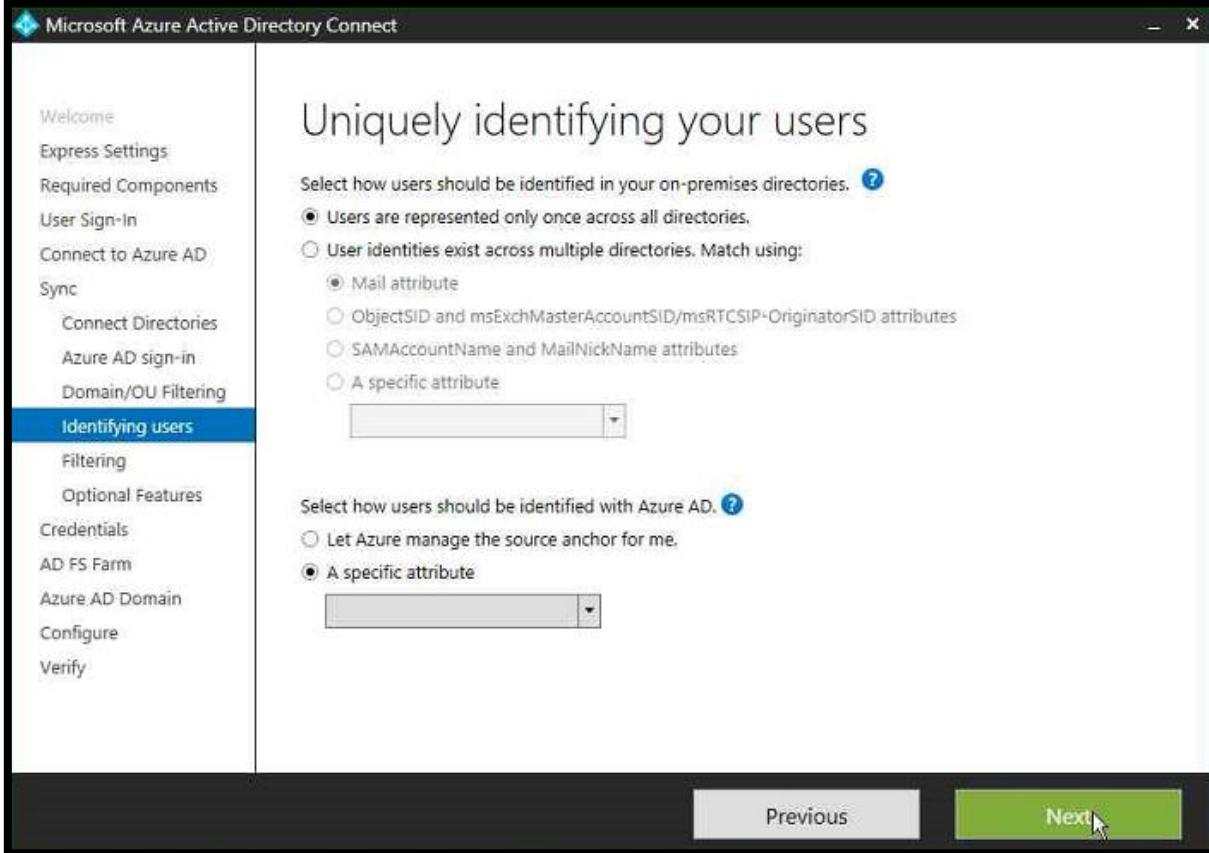
ADFS - Step-by-step



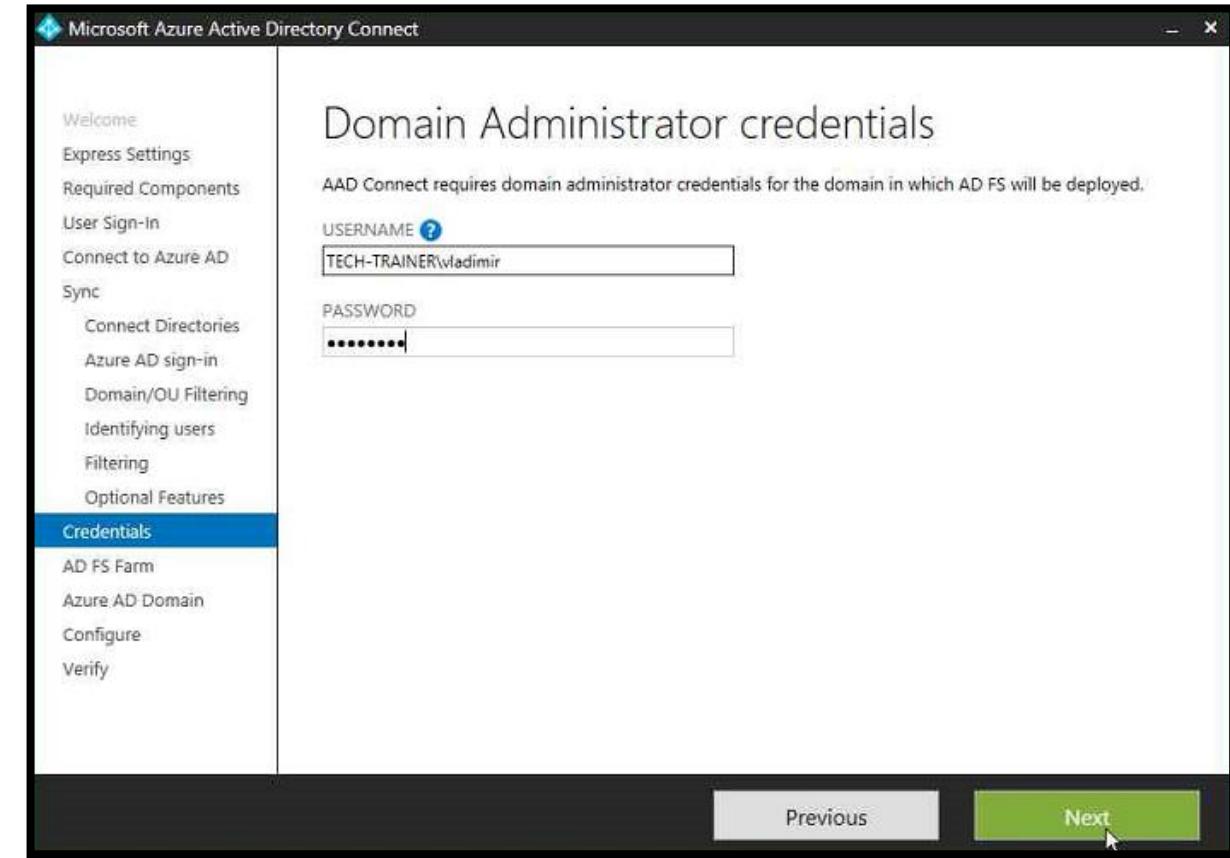
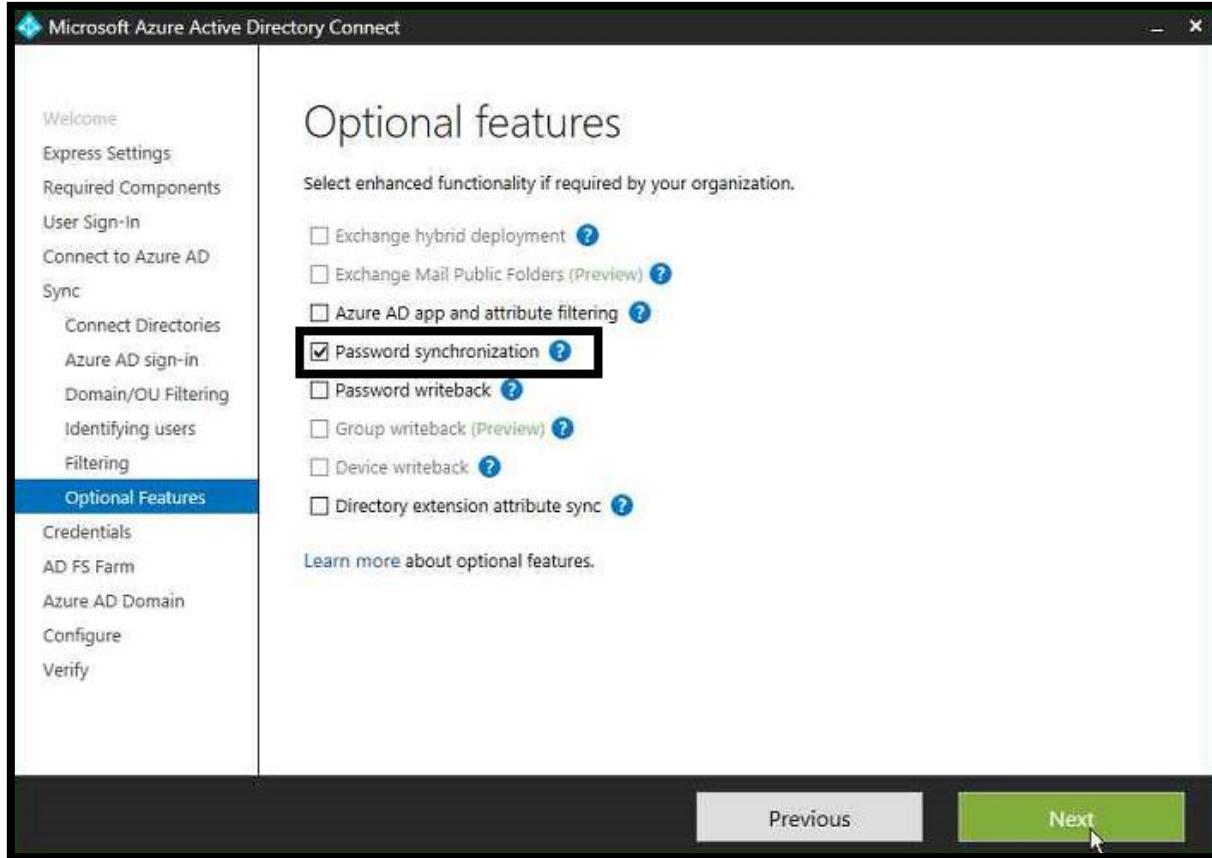
ADFS - Step-by-step



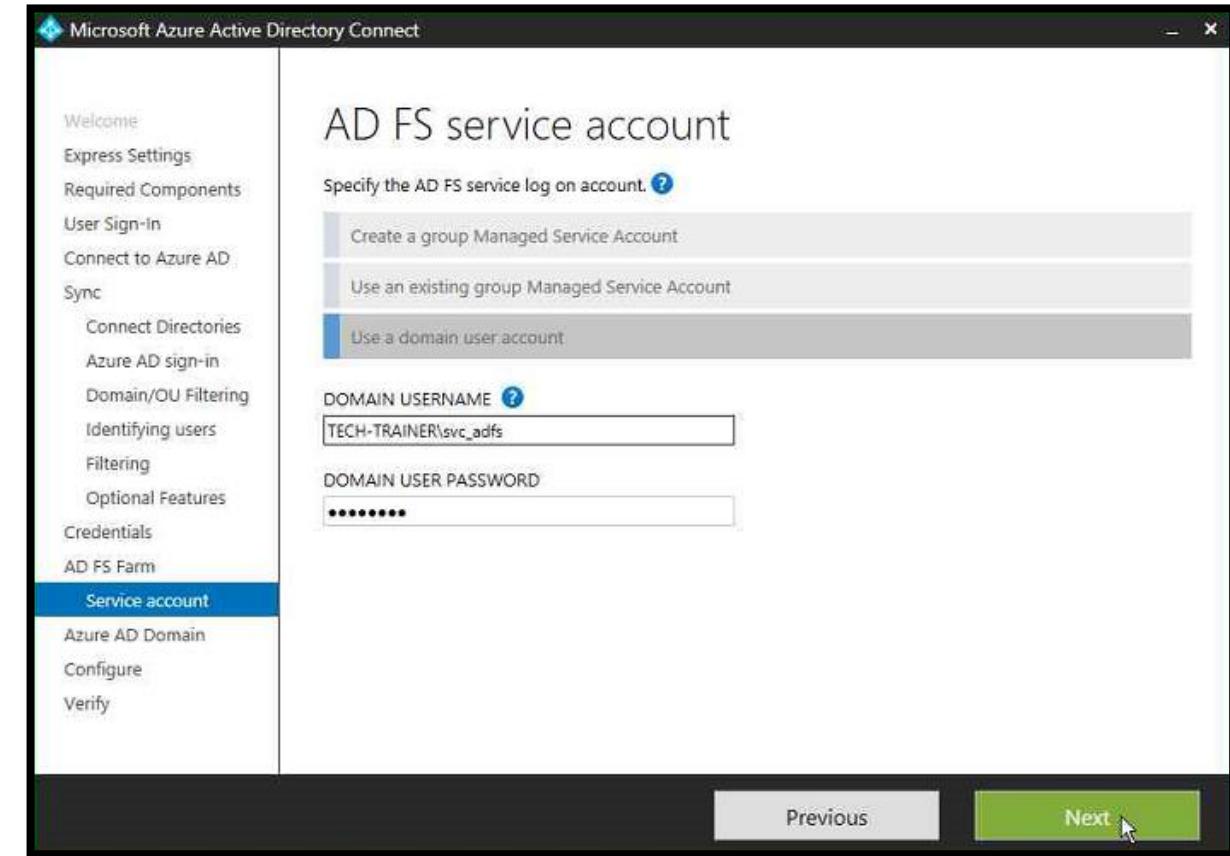
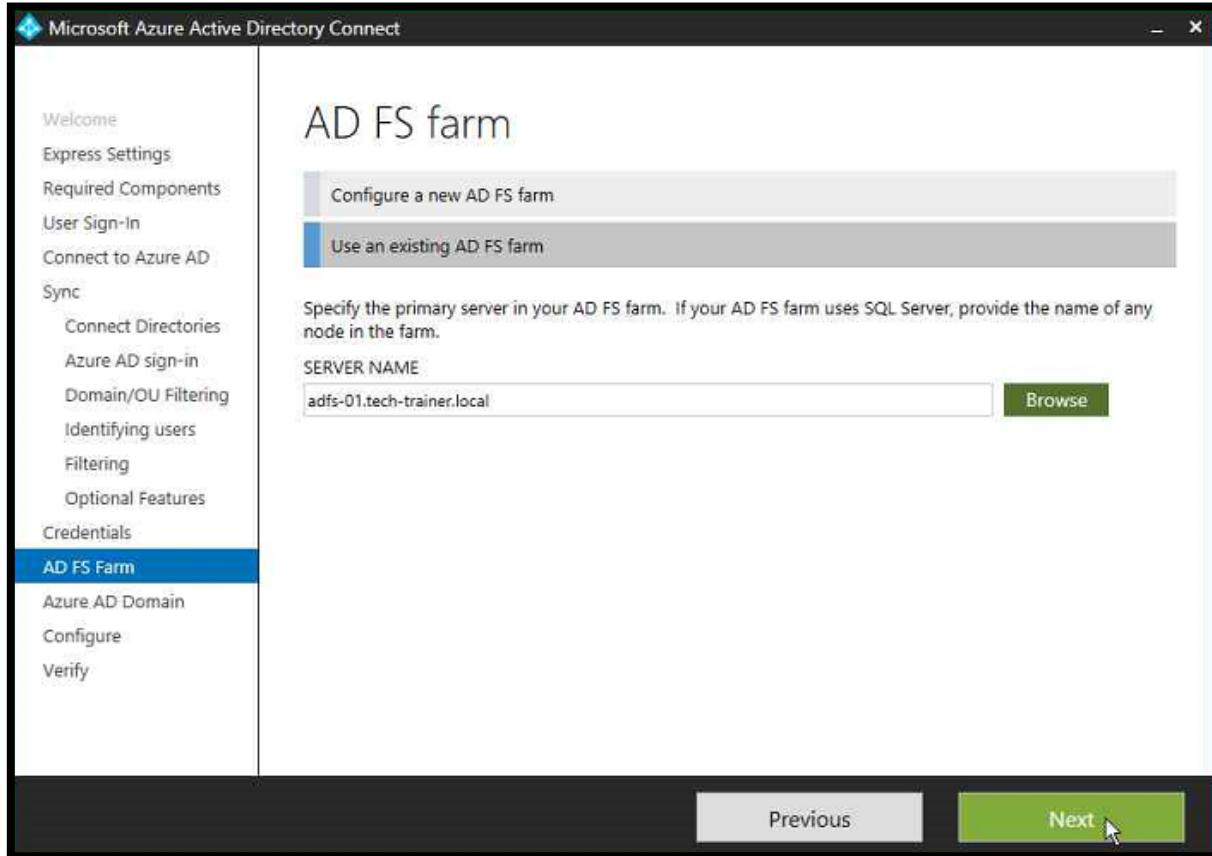
ADFS - Step-by-step



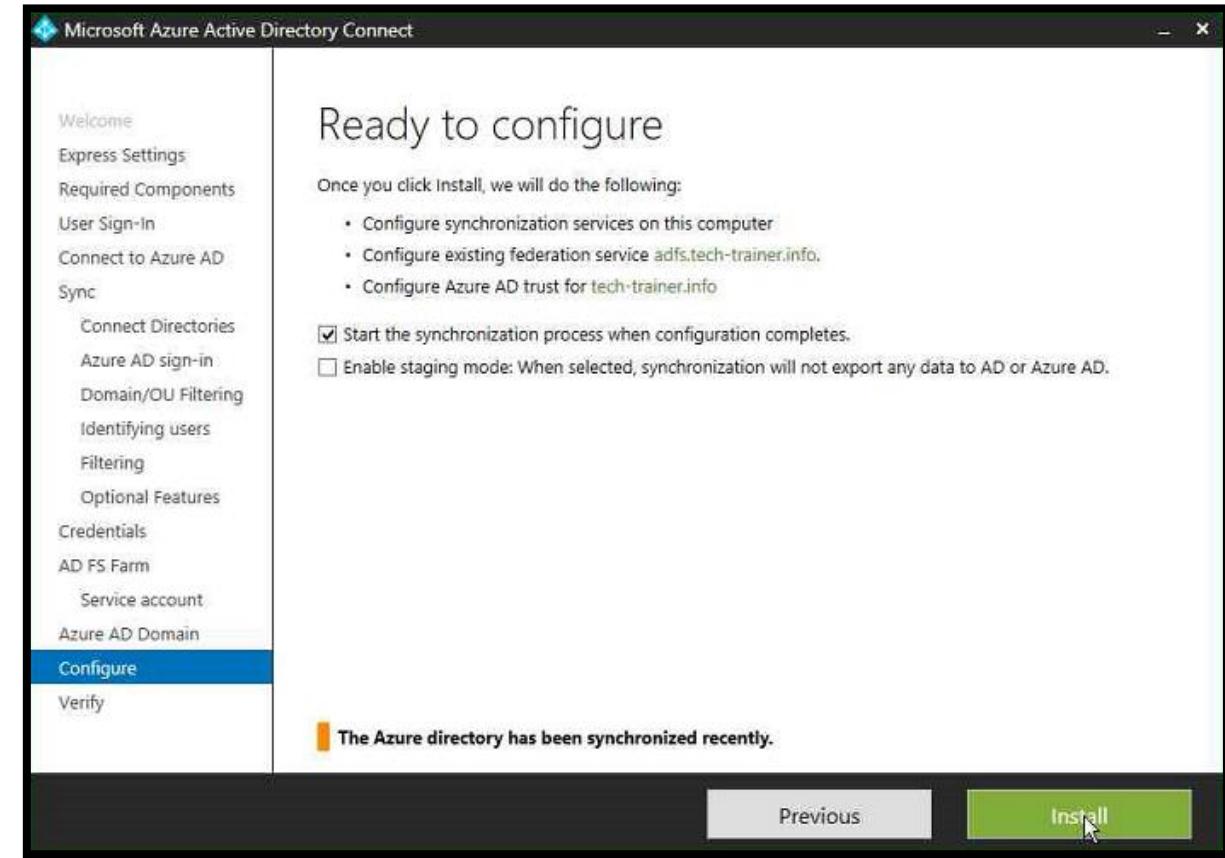
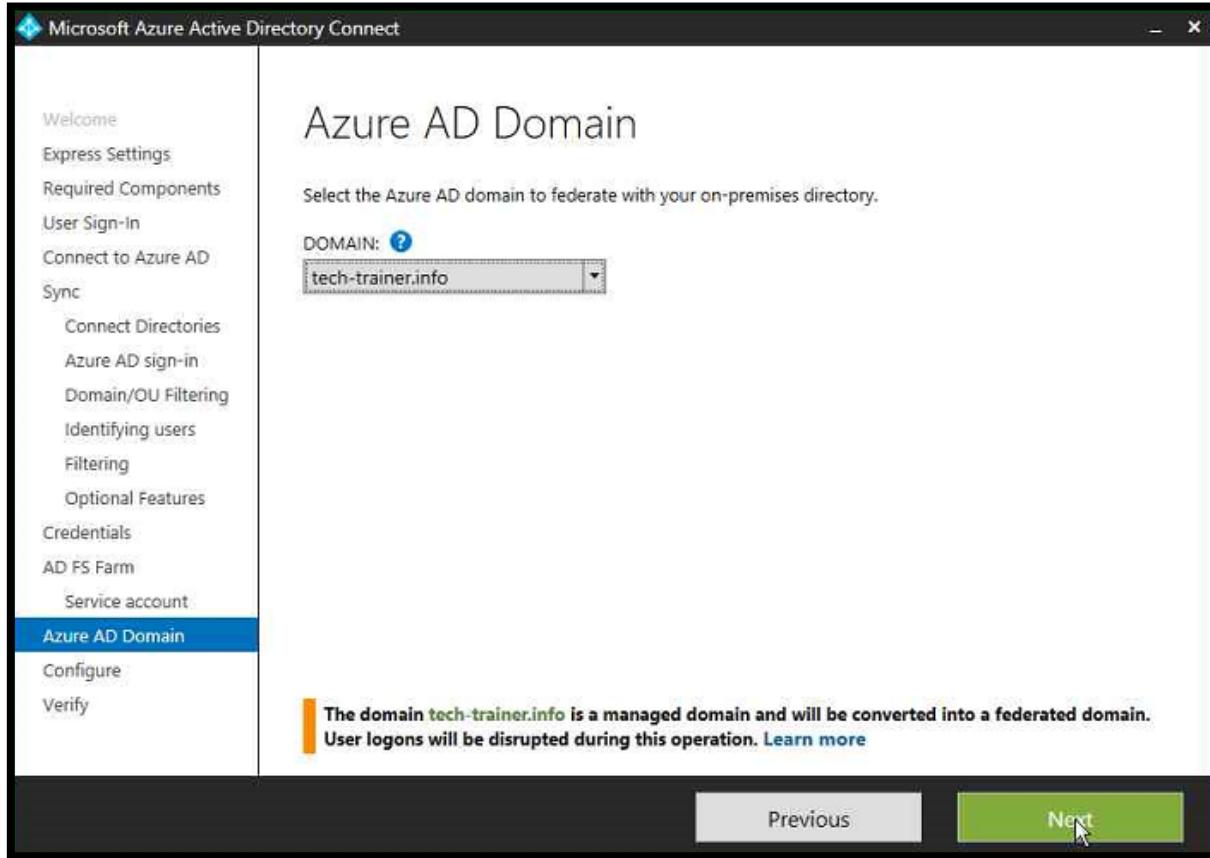
ADFS - Step-by-step



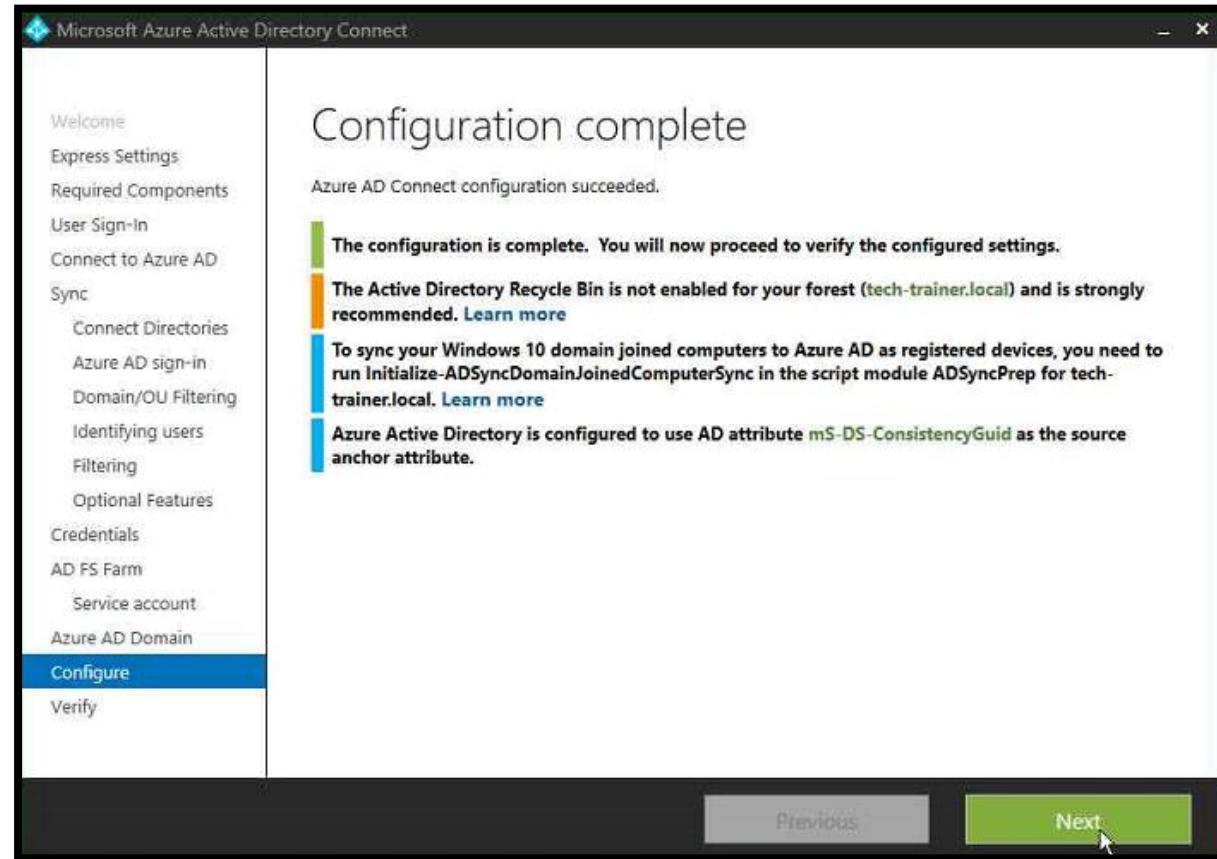
ADFS - Step-by-step



ADFS - Step-by-step

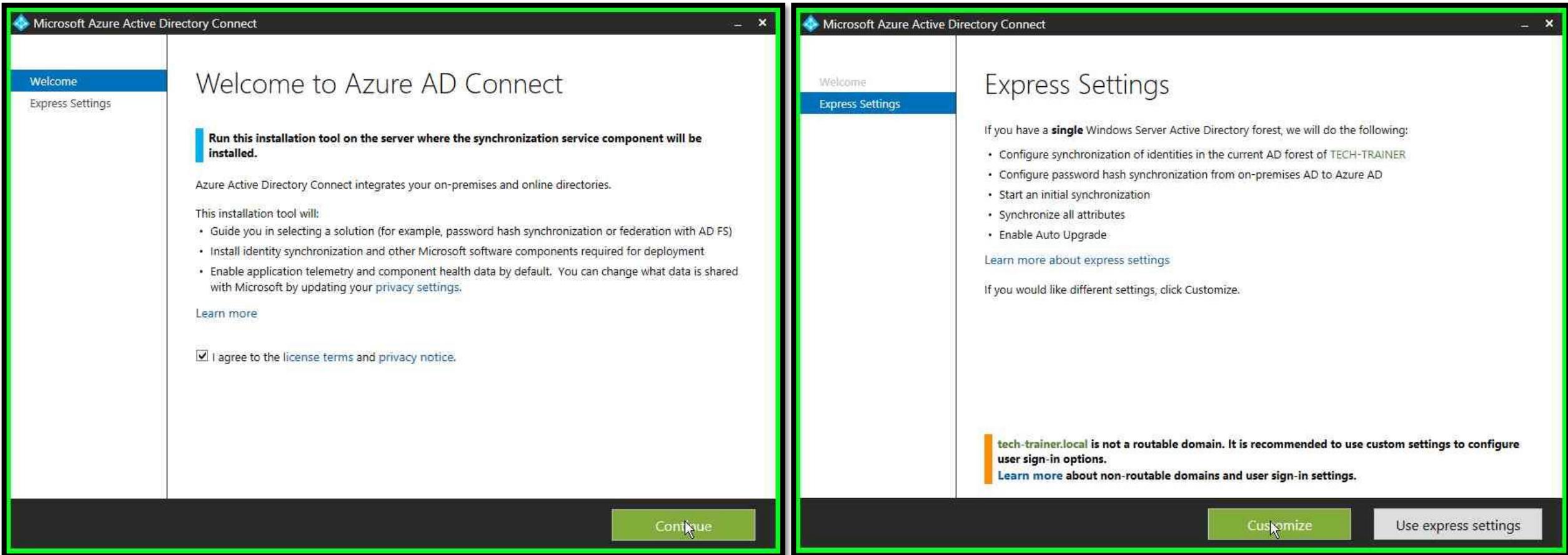


ADFS - Step-by-step

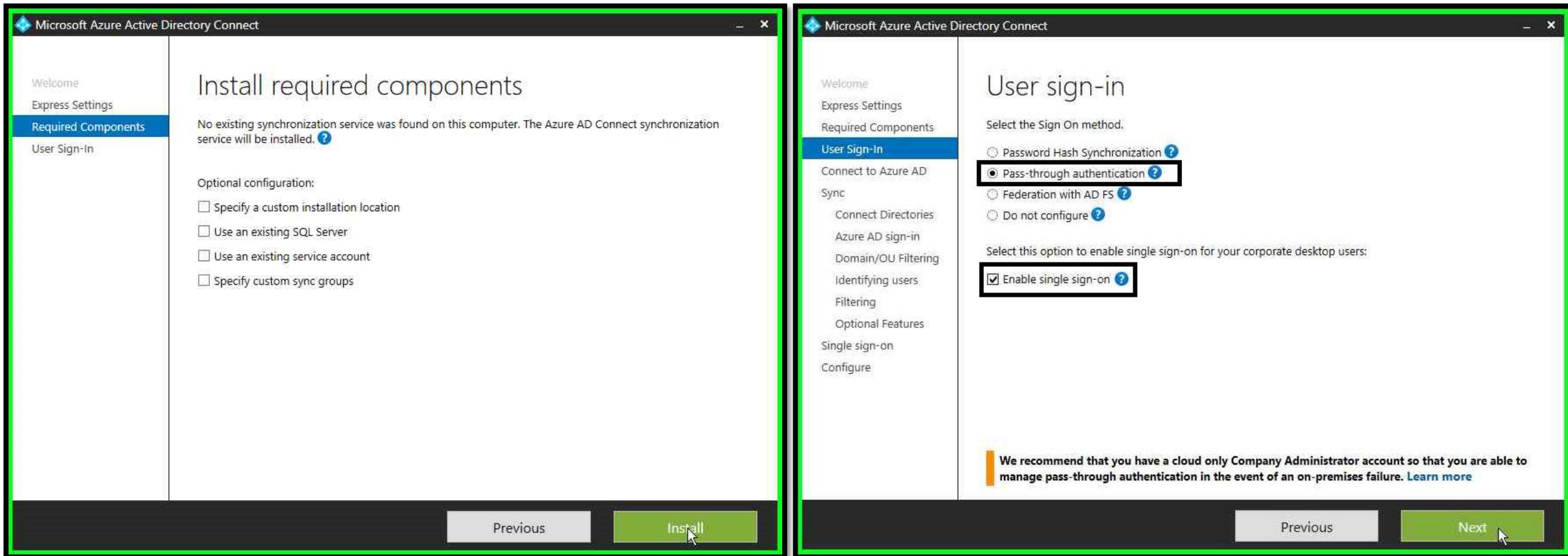


Demo (*Slideshow*) - PTA

PTA - Step-by-step



PTA - Step-by-step



PTA - Step-by-step

The image displays two side-by-side windows of the Microsoft Azure Active Directory Connect setup wizard, both framed by a thick green border.

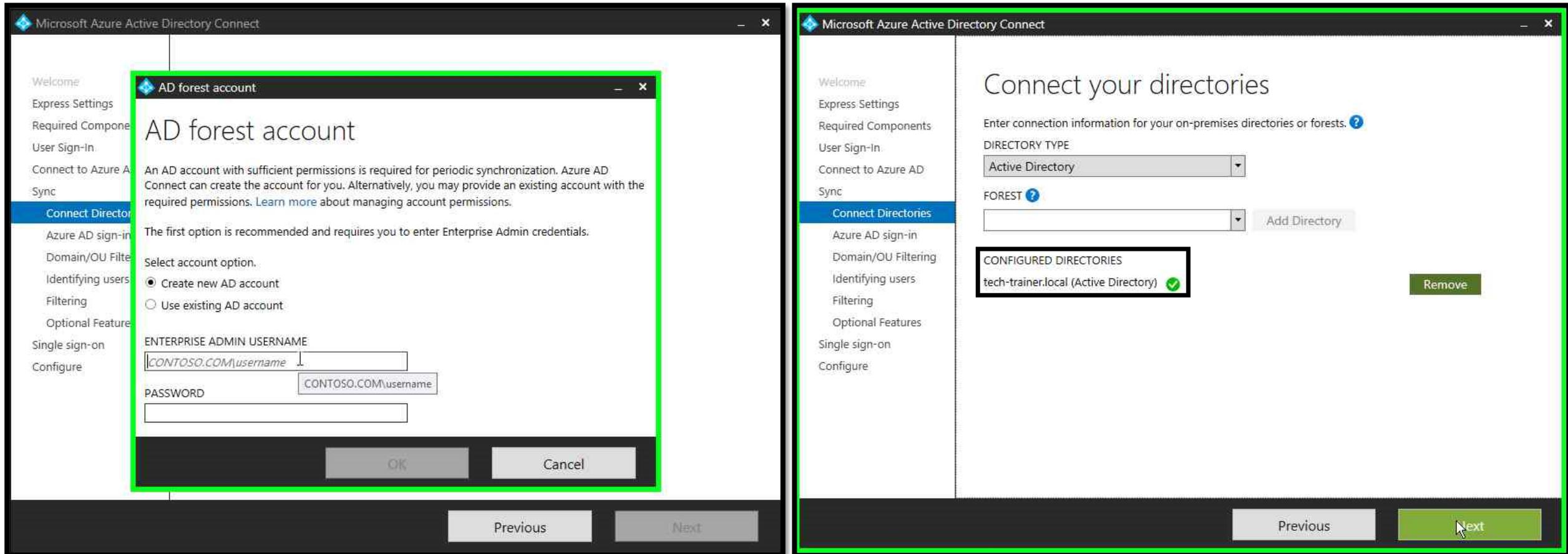
Left Window (Connect to Azure AD):

- Header:** Microsoft Azure Active Directory Connect
- Left sidebar:** Welcome, Express Settings, Required Components, User Sign-In, **Connect to Azure AD** (selected), Sync, Connect Directories, Azure AD sign-in, Domain/OU Filtering, Identifying users, Filtering, Optional Features, Single sign-on, Configure.
- Main area:** Connect to Azure AD. Enter your Azure AD global administrator credentials. ?
USERNAME: admin@wladinho.onmicrosoft.com
PASSWORD: [REDACTED]
- Buttons at the bottom:** Previous, **Next** (highlighted with a cursor).

Right Window (Connect your directories):

- Header:** Microsoft Azure Active Directory Connect
- Left sidebar:** Welcome, Express Settings, Required Components, User Sign-In, Connect to Azure AD, Sync, **Connect Directories** (selected), Azure AD sign-in, Domain/OU Filtering, Identifying users, Filtering, Optional Features, Single sign-on, Configure.
- Main area:** Connect your directories. Enter connection information for your on-premises directories or forests. ?
DIRECTORY TYPE: Active Directory
FOREST ?
tech-trainer.local
[Add Directory] (highlighted with a cursor)
No directories are currently configured.
- Buttons at the bottom:** Previous, Next.

PTA - Step-by-step



PTA - Step-by-step

The image displays two side-by-side screenshots of the Microsoft Azure Active Directory Connect wizard, both highlighted with a thick green border.

Screenshot 1: Azure AD sign-in configuration

- Left Panel:** A navigation menu with items: Welcome, Express Settings, Required Components, User Sign-In, Connect to Azure AD, Sync, Connect Directories, **Azure AD sign-in** (selected), Domain/OU Filtering, Identifying users, Filtering, Optional Features, Single sign-on, Configure.
- Center Content:** A table titled "Active Directory UPN Suffix" showing two entries:

Active Directory UPN Suffix	Azure AD Domain
tech-trainer.local	Not Added ?
tech-trainer.info	Verified
- Bottom Content:** A note: "Select the on-premises attribute to use as the Azure AD username" followed by a dropdown menu set to "USER PRINCIPAL NAME [?](#)" with the value "userPrincipalName". A warning message at the bottom states: "Users will not be able to sign-in Azure AD using their on-premises credentials." with a "Learn more" link.
- Footer:** Buttons for "Previous" and "Next" (highlighted with a mouse cursor).

Screenshot 2: Domain and OU filtering

- Left Panel:** Same navigation menu as the first screenshot.
- Center Content:** A "Directory" dropdown set to "tech-trainer.local" with a "Refresh Ou/Domain" button and a help icon. Two radio buttons are shown: "Sync all domains and OUs" (unchecked) and "Sync selected domains and OUs" (checked). A tree view shows the domain structure with several objects expanded, including "TECH TRAINER" which has a checked checkbox next to it.
- Footer:** Buttons for "Previous" and "Next" (highlighted with a mouse cursor).

PTA - Step-by-step

Microsoft Azure Active Directory Connect

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 for me.

A specific attribute

Microsoft Azure Active Directory Connect

Filter users and devices

For a pilot deployment, specify a group containing your users and devices that will be synchronized. Nested groups are not supported and will be ignored.

Synchronize all users and devices

Synchronize selected [?](#)

FOREST GROUP
tech-trainer.local

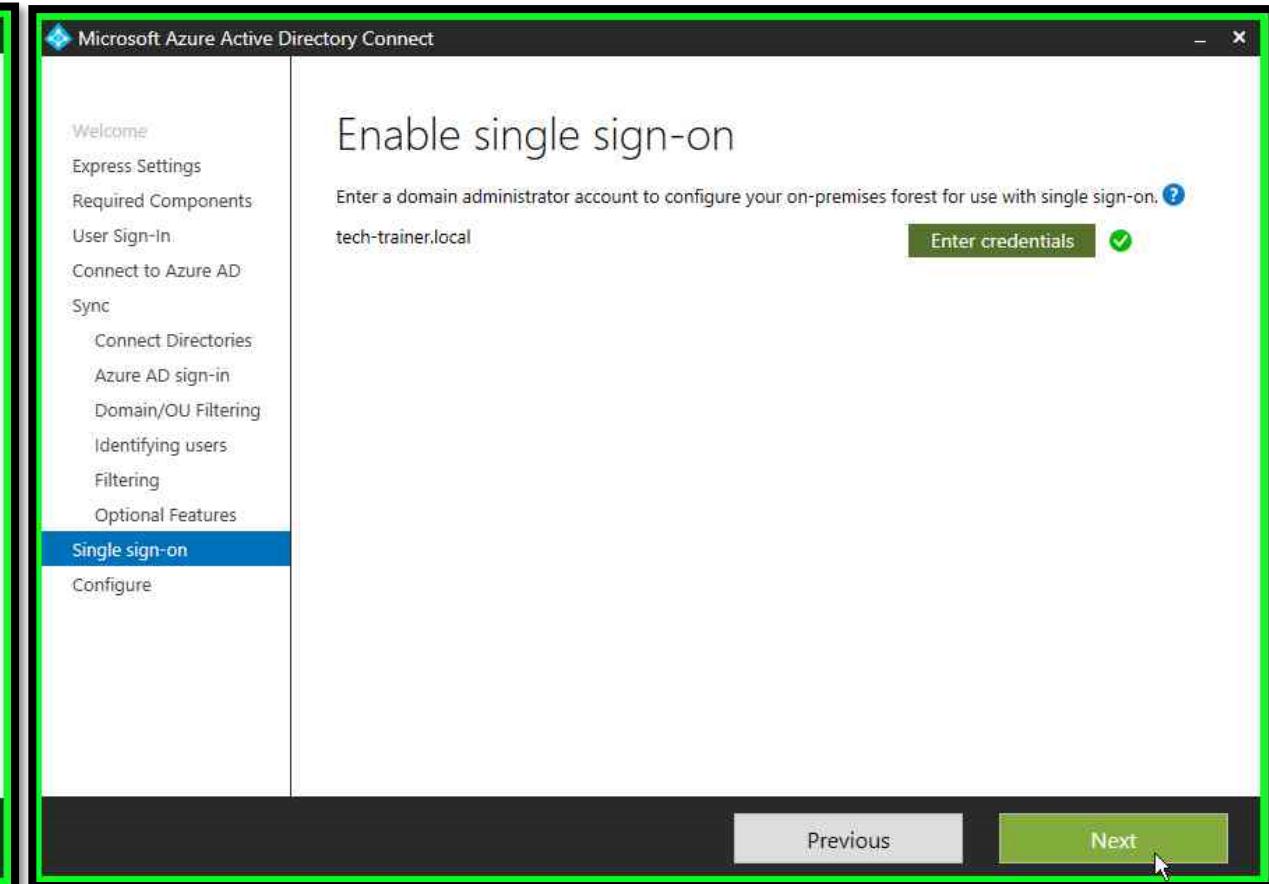
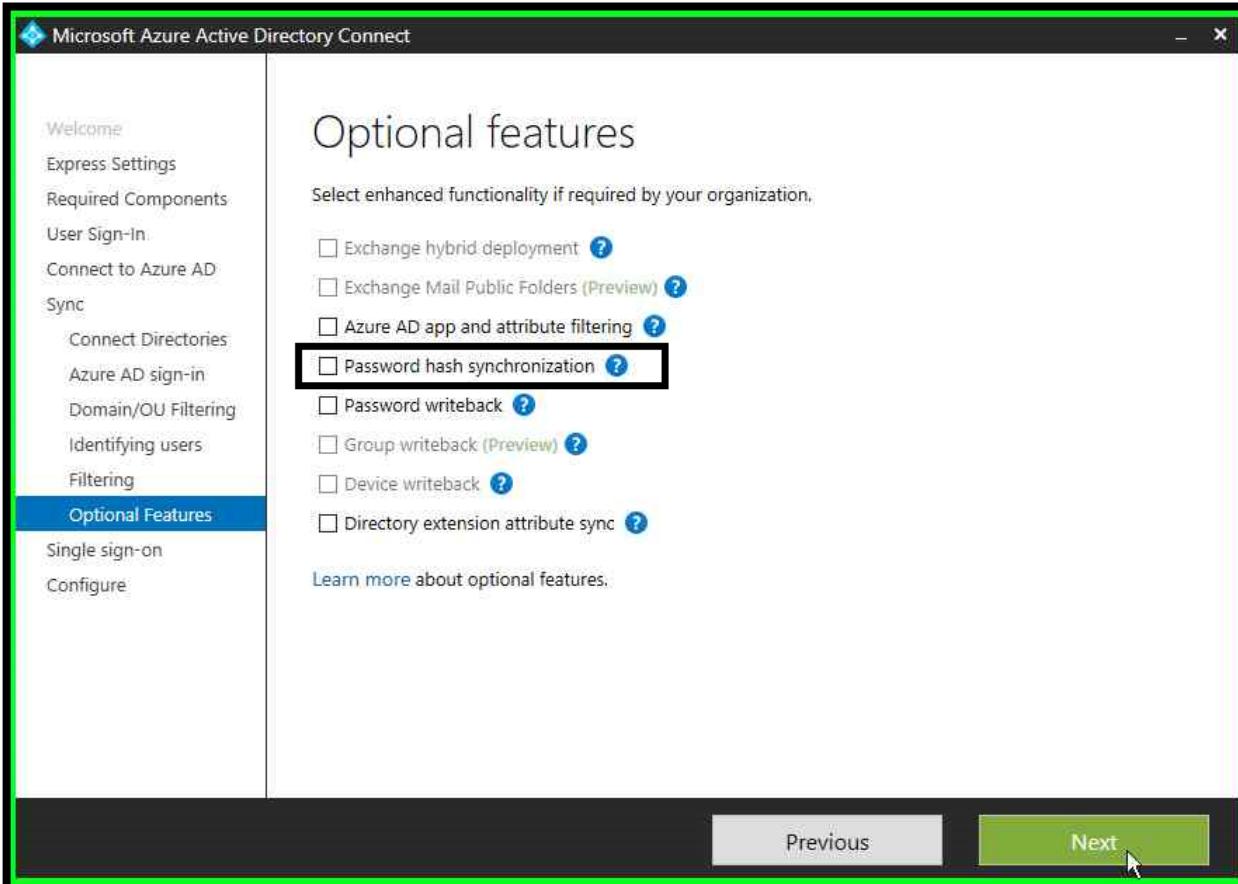
Enter a name or DN of a group

Resolve

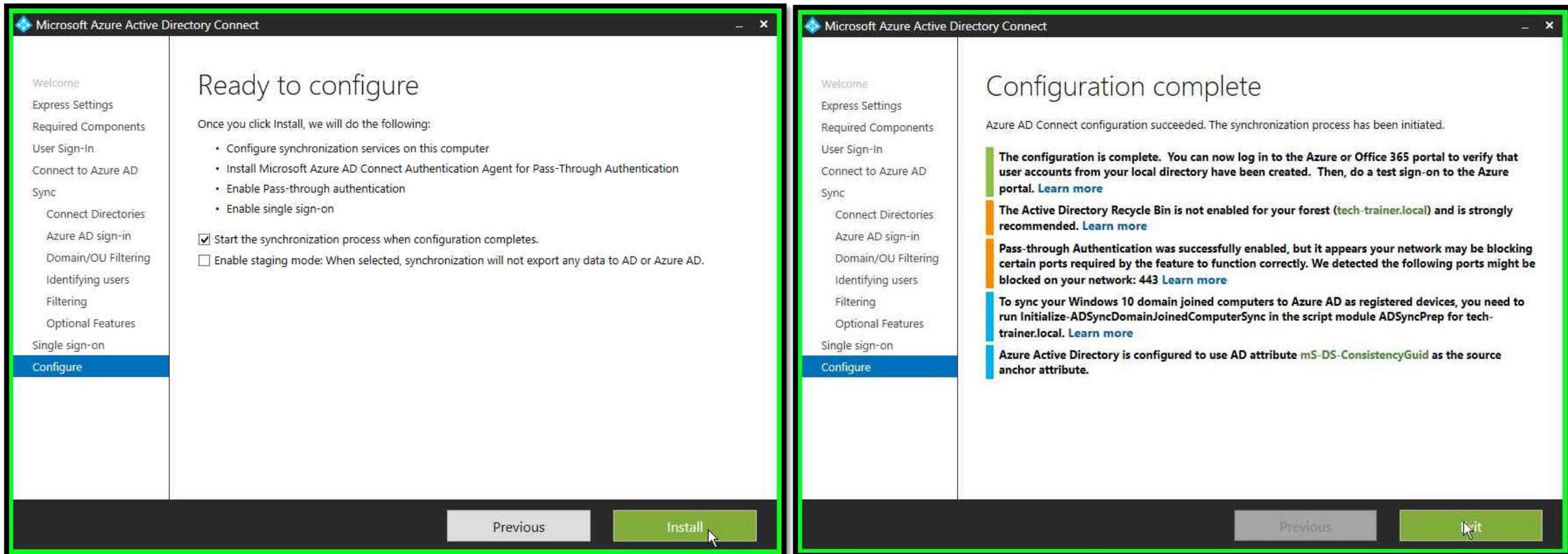
Previous **Next**

Previous **Next**

PTA - Step-by-step



PTA - Step-by-step



PTA - Step-by-step

The diagram illustrates a step-by-step configuration process for Azure AD Connect, shown through four sequential screenshots:

- Screenshot 1: Azure Active Directory Overview**
 - The left sidebar shows "Azure Active Directory" selected.
 - The main area displays "SYNC STATUS" with "Sync Status" set to "Enabled" (last sync "Less than 1 hour ago") and "Password Sync" set to "Disabled".
 - "USER SIGN-IN" section shows "Federation" as "Disabled", "Seamless single sign-on" as "Enabled" (with 1 domain), and "Pass-through authentication" as "Enabled" (with 1 agent).
 - "ON-PREMISES APPLICATIONS" section includes a link to "Head to Application Proxy".
 - "HEALTH AND ANALYTICS" section includes a link to "AD Connect Health".
- Screenshot 2: Seamless single sign-on**
 - The title bar shows the path: Home > technical trainer - Azure AD Connect > Seamless single sign-on.
 - The main area displays a table with one row:

ON-PREMISES DOMAIN NAME	KEY CREATION DATE (UTC)	STATUS
tech-trainer.local	4/23/2018	✓
- Screenshot 3: Pass-through authentication**
 - The title bar shows the path: Home > technical trainer - Azure AD Connect > Pass-through authentication.
 - The main area displays a table with one row:

AUTHENTICATION AGENT	IP	STATUS
Default group for Pass-through Authentication DC01.tech-trainer.local	40.91.219.143	Active

Q & A

Thank you for your attention

Windays¹⁸

Technology