

Windows¹⁸

Technology



Office 365 SSO Lako i jednostavno

Vladimir Stefanović
Superadmins - Belgrade

Technology

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

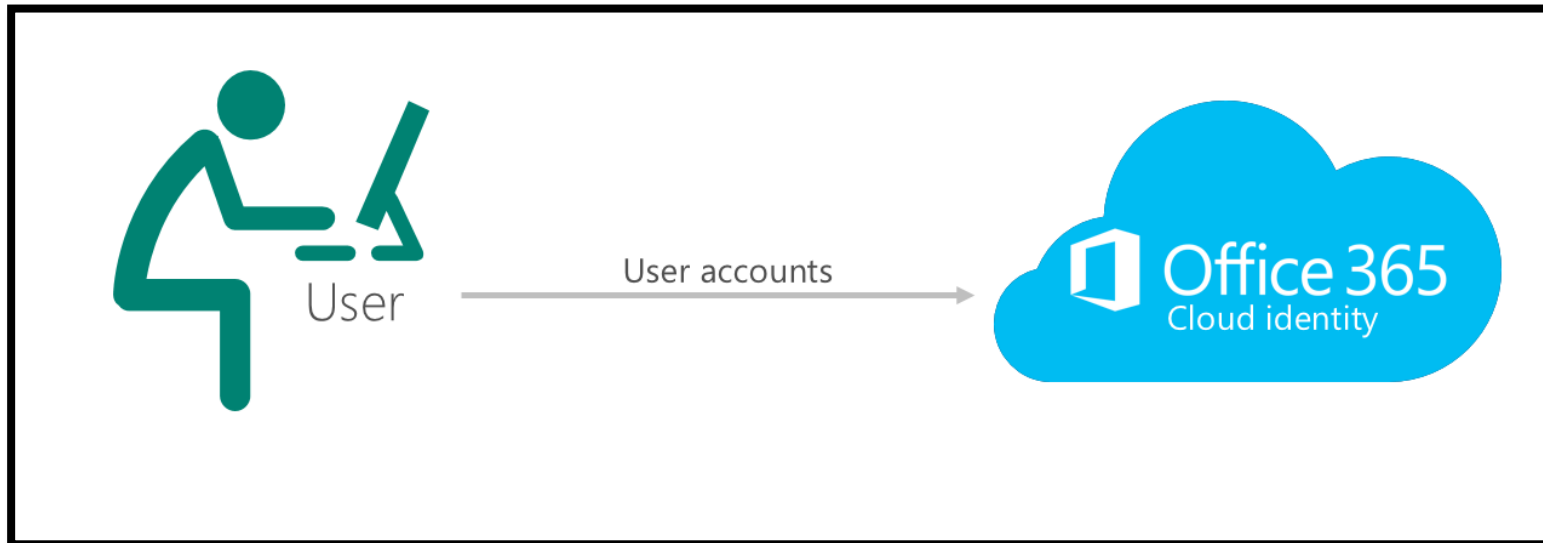
The right half of the slide features a blue background with a geometric, low-poly pattern of various shades of blue. The word "Technology" is written in a white, sans-serif font. The letter "o" is replaced by a 3D cube icon that is white on the outside and blue on the inside, with a grey shadow beneath it.

Technology

Identity models

Cloud identity

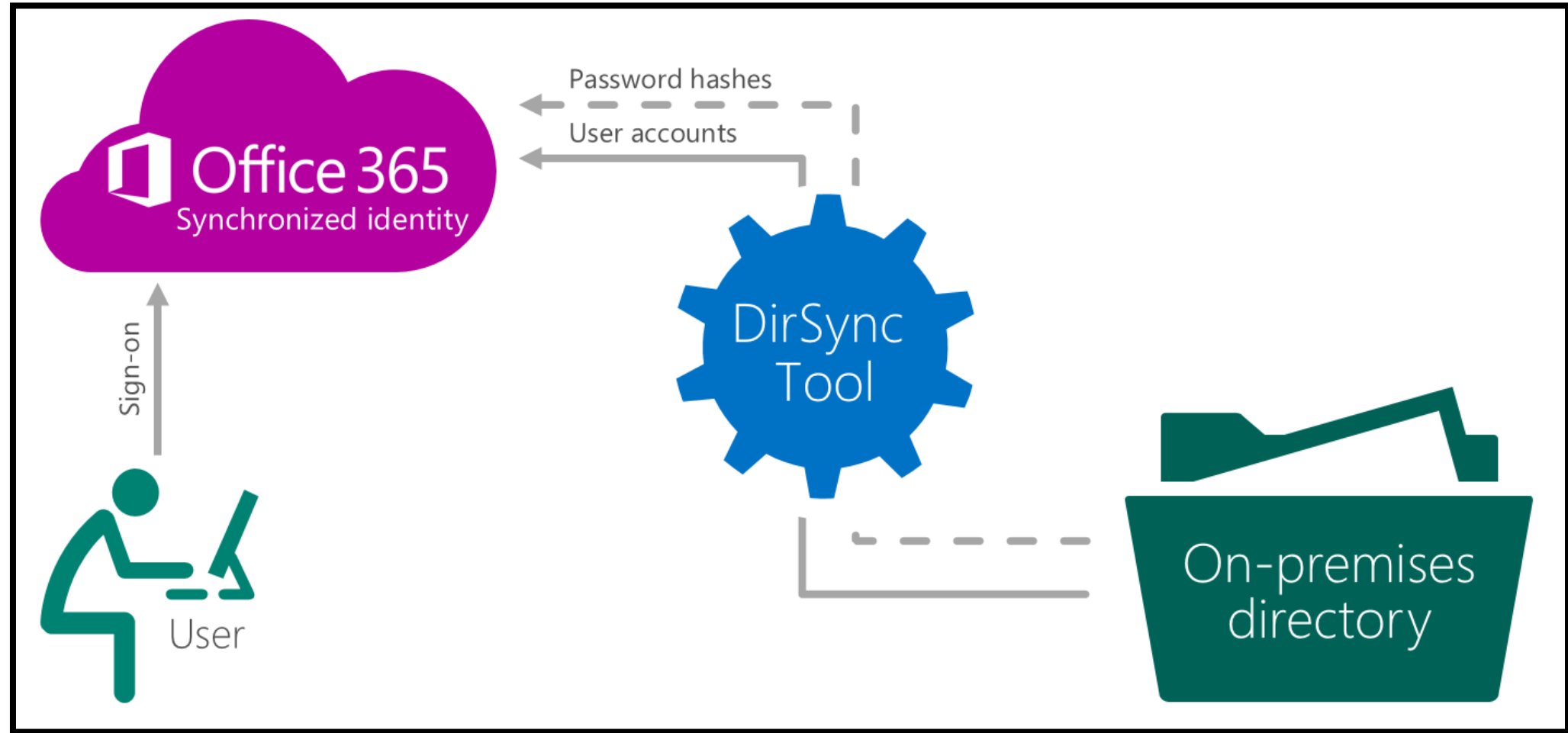
- User is created and managed in Office 365 and stored in Azure Active Directory
- Identity is verified by Azure AD
- There is no equivalent user account on-premises



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

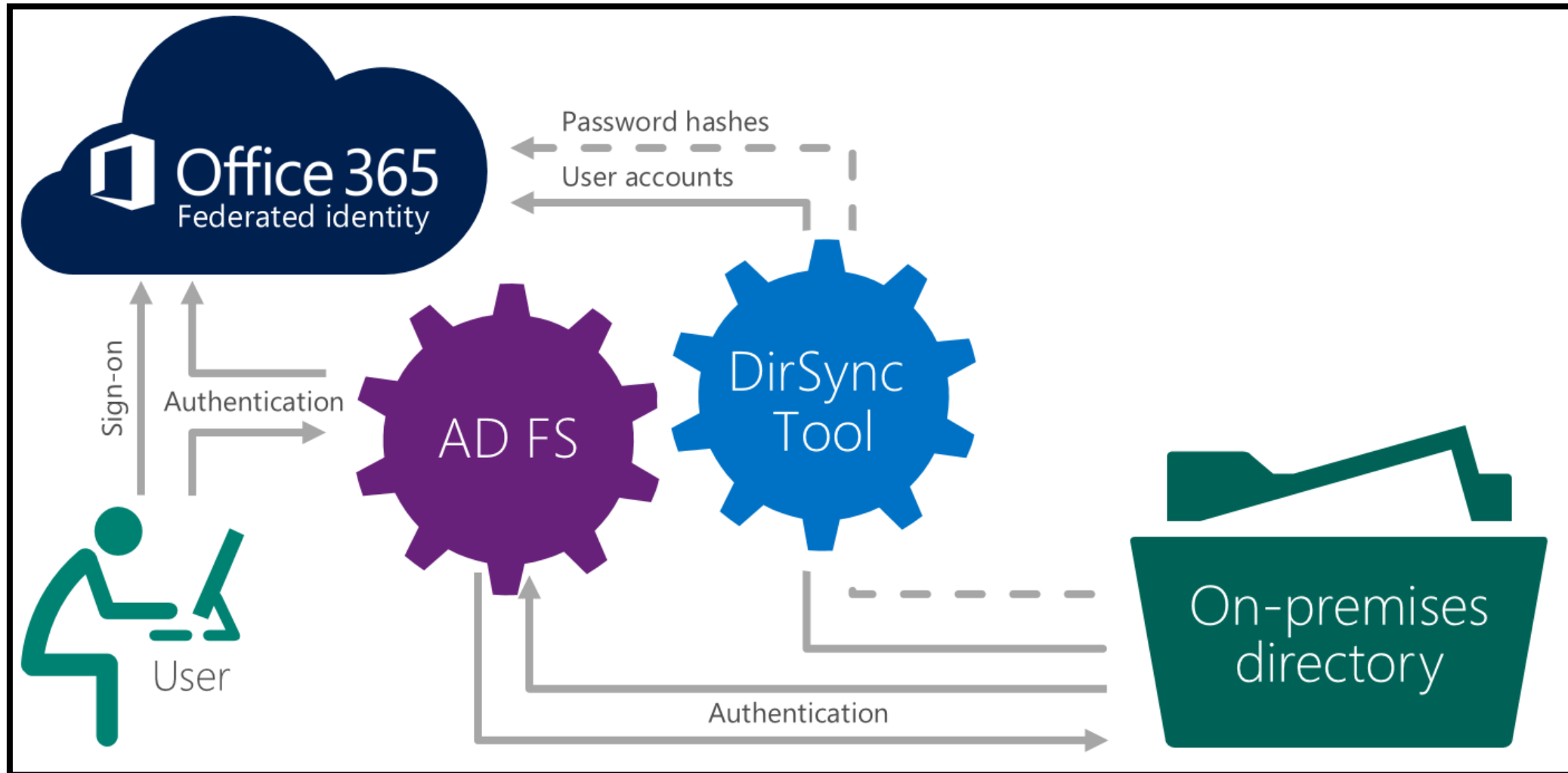
Synchronized Identity - PHS & PTA



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

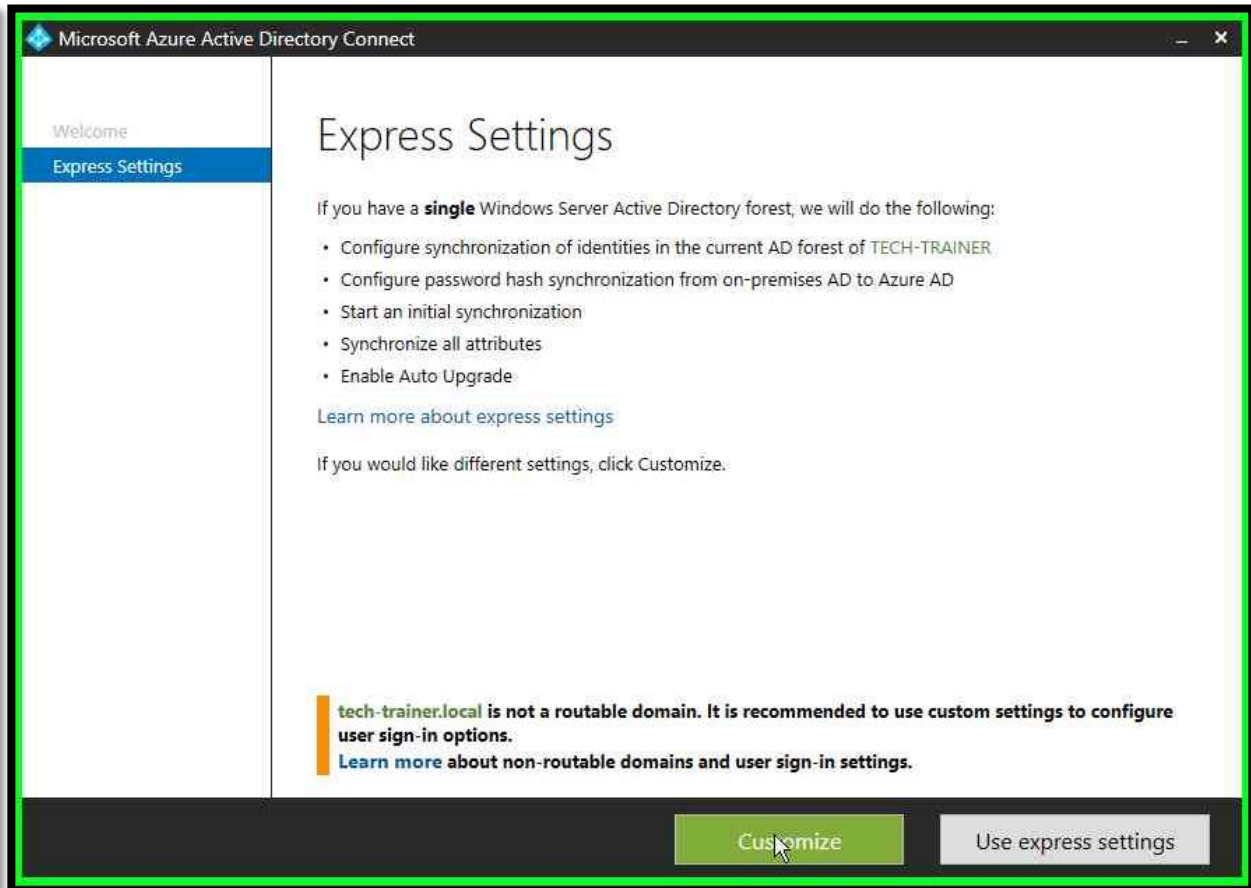
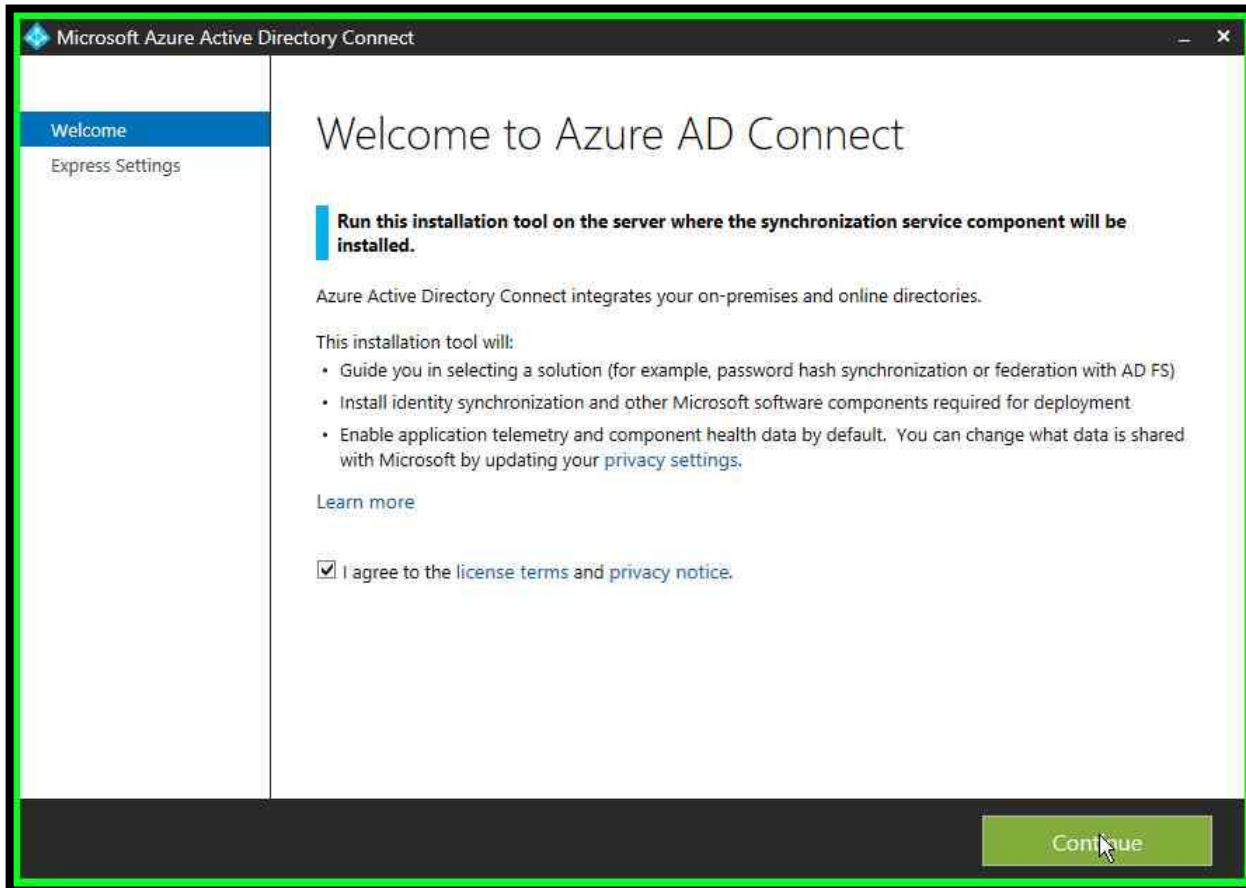
Do not forget

- 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>

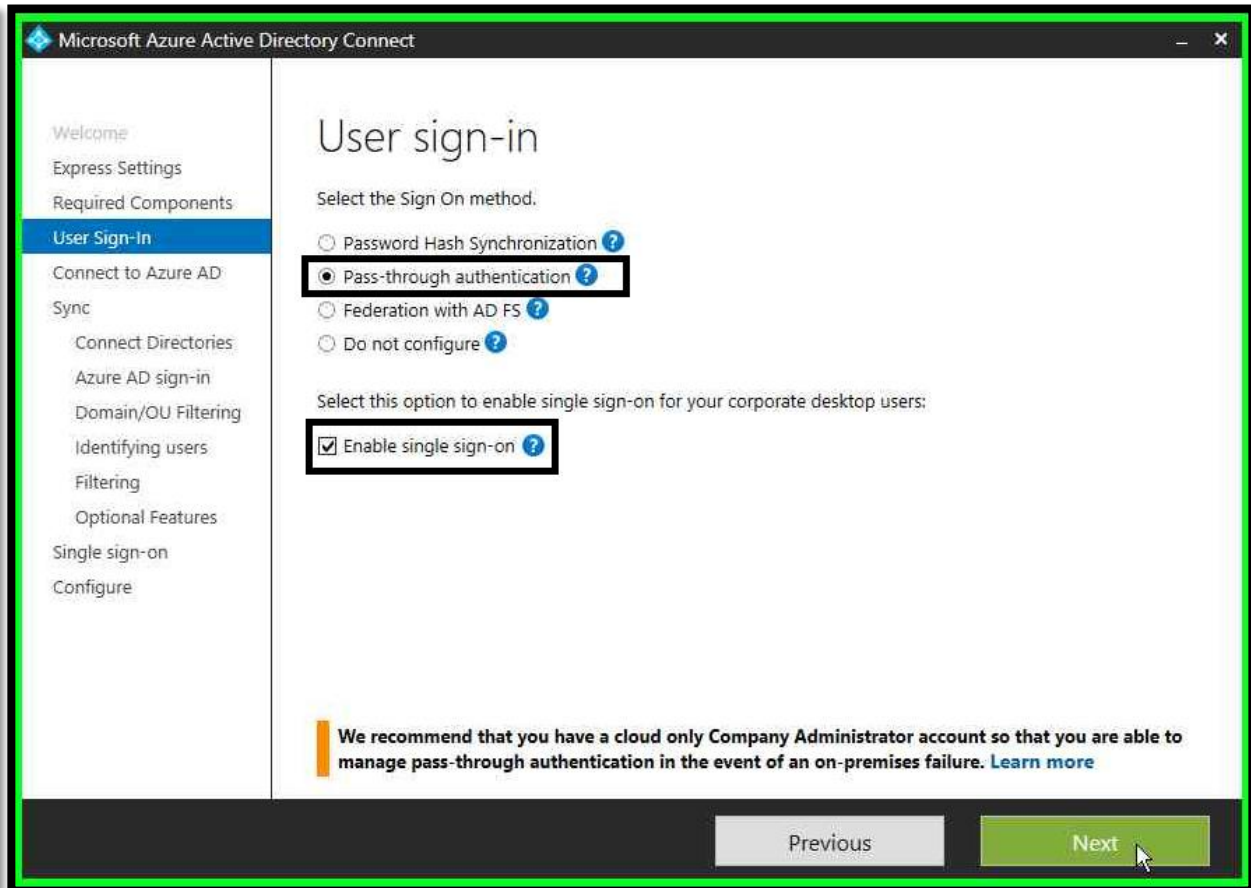
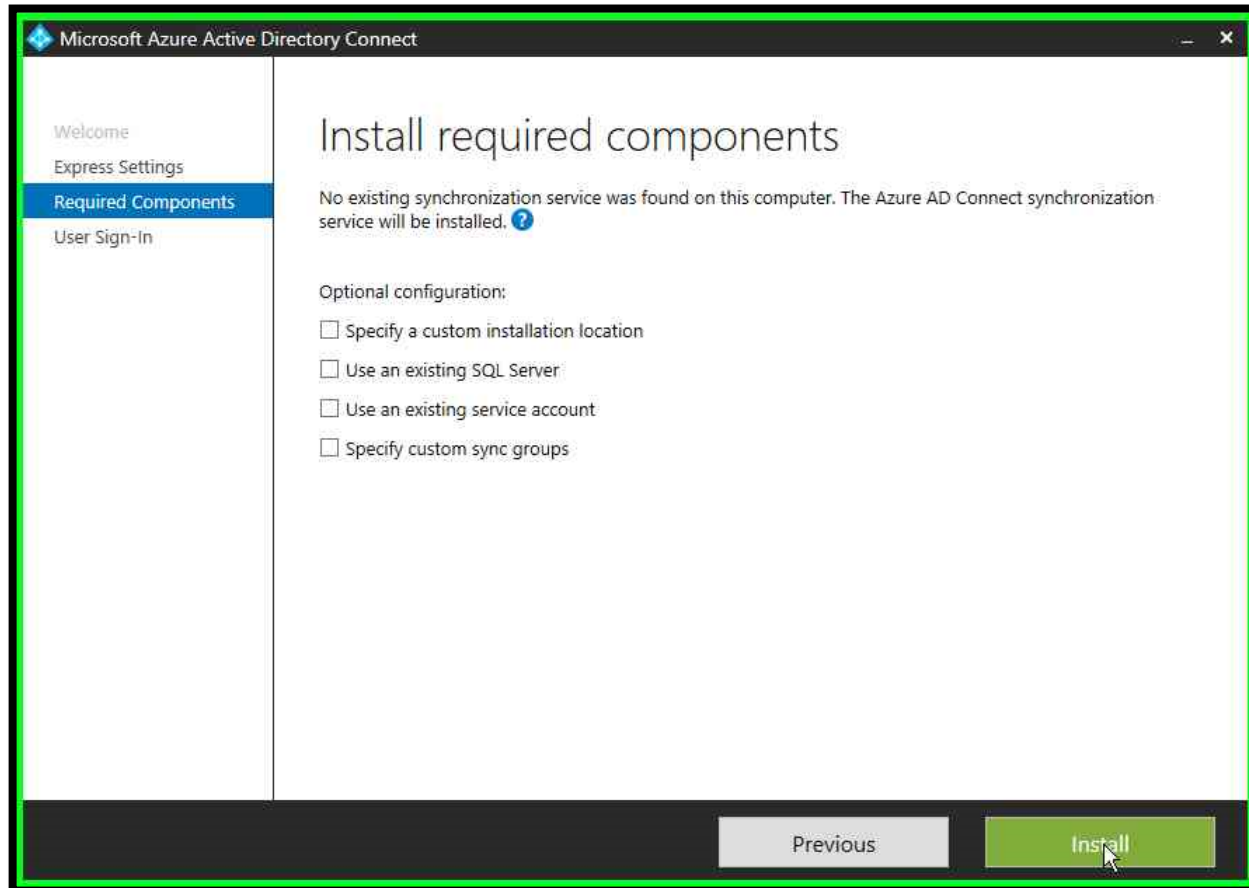
Demo - ADFS

Demo (*Slideshow*) – PTA

PTA - Step-by-step



PTA - Step-by-step



PTA - Step-by-step

The screenshot shows the 'Connect to Azure AD' step of the Microsoft Azure Active Directory Connect wizard. The left sidebar contains a navigation menu with the following items: 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, and Configure. The main content area is titled 'Connect to Azure AD' and includes the instruction 'Enter your Azure AD global administrator credentials. ?'. Below this, there are two input fields: 'USERNAME' with the value 'admin@wladinho.onmicrosoft.com' and 'PASSWORD' with masked characters. At the bottom, there are 'Previous' and 'Next' buttons, with the 'Next' button highlighted in green.

The screenshot shows the 'Connect your directories' step of the Microsoft Azure Active Directory Connect wizard. The left sidebar contains a navigation menu with the following items: 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, and Configure. The main content area is titled 'Connect your directories' and includes the instruction 'Enter connection information for your on-premises directories or forests. ?'. Below this, there are two dropdown menus: 'DIRECTORY TYPE' set to 'Active Directory' and 'FOREST ?' set to 'tech-trainer.local'. To the right of the 'FOREST' dropdown is a blue 'Add directory' button. Below these fields, the text 'No directories are currently configured.' is displayed. At the bottom, there are 'Previous' and 'Next' buttons, both of which are disabled.

PTA - Step-by-step

This screenshot shows the 'AD forest account' dialog box in the Microsoft Azure Active Directory Connect application. The dialog is titled 'AD forest account' and contains the following text: '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.' Below this, it states 'The first option is recommended and requires you to enter Enterprise Admin credentials.' Under 'Select account option.', the 'Create new AD account' radio button is selected. The 'Use existing AD account' option is also visible. There are input fields for 'ENTERPRISE ADMIN USERNAME' (containing 'CONTOSO.COM\username') and 'PASSWORD' (containing 'CONTOSO.COM\username'). At the bottom are 'OK' and 'Cancel' buttons.

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

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

CONTOSO.COM\username

PASSWORD

CONTOSO.COM\username

OK

Cancel

Previous

Next

This screenshot shows the 'Connect your directories' screen in the Microsoft Azure Active Directory Connect application. The screen is titled 'Connect your directories' and contains the following text: 'Enter connection information for your on-premises directories or forests. ?' Below this, there is a 'DIRECTORY TYPE' dropdown menu set to 'Active Directory'. There is also a 'FOREST ?' dropdown menu and an 'Add Directory' button. A 'CONFIGURED DIRECTORIES' section shows 'tech-trainer.local (Active Directory)' with a green checkmark. A 'Remove' button is next to it. At the bottom are 'Previous' and 'Next' buttons.

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

Connect your directories

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

DIRECTORY TYPE

Active Directory

FOREST ?

Add Directory

CONFIGURED DIRECTORIES

tech-trainer.local (Active Directory) ✓

Remove

Previous

Next

PTA - Step-by-step

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

Azure AD sign-in configuration

To use on-premises credentials for Azure AD sign-in, UPN suffixes in usernames should match one of the verified custom domains in Azure AD. The following table lists the UPN suffixes defined in your on-premises environment, along with the matching custom domain in Azure. ?

Active Directory UPN Suffix	Azure AD Domain
tech-trainer.local	Not Added ?
tech-trainer.info	Verified

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

USER PRINCIPAL NAME ?

userPrincipalName

Users will not be able to sign-in Azure AD using their on-premises credentials.
[Learn more](#)

Previous Next

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: tech-trainer.local Refresh Ou/Domain ?

☐ Sync all domains and OUs

☒ Sync selected domains and OUs

- ☐ tech-trainer.local
 - ☐ BuiltIn
 - ☐ Computers
 - ☐ Domain Controllers
 - ☐ ForeignSecurityPrincipals
 - ☐ Infrastructure
 - ☐ LostAndFound
 - ☐ Managed Service Accounts
 - ☐ Program Data
 - ☐ System
 - ☒ TECH TRAINER
 - ☐ Users
 - ☐ Configuration

Previous Next

PTA - Step-by-step

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 for me.

☐ A specific attribute

Previous Next

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

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 ?

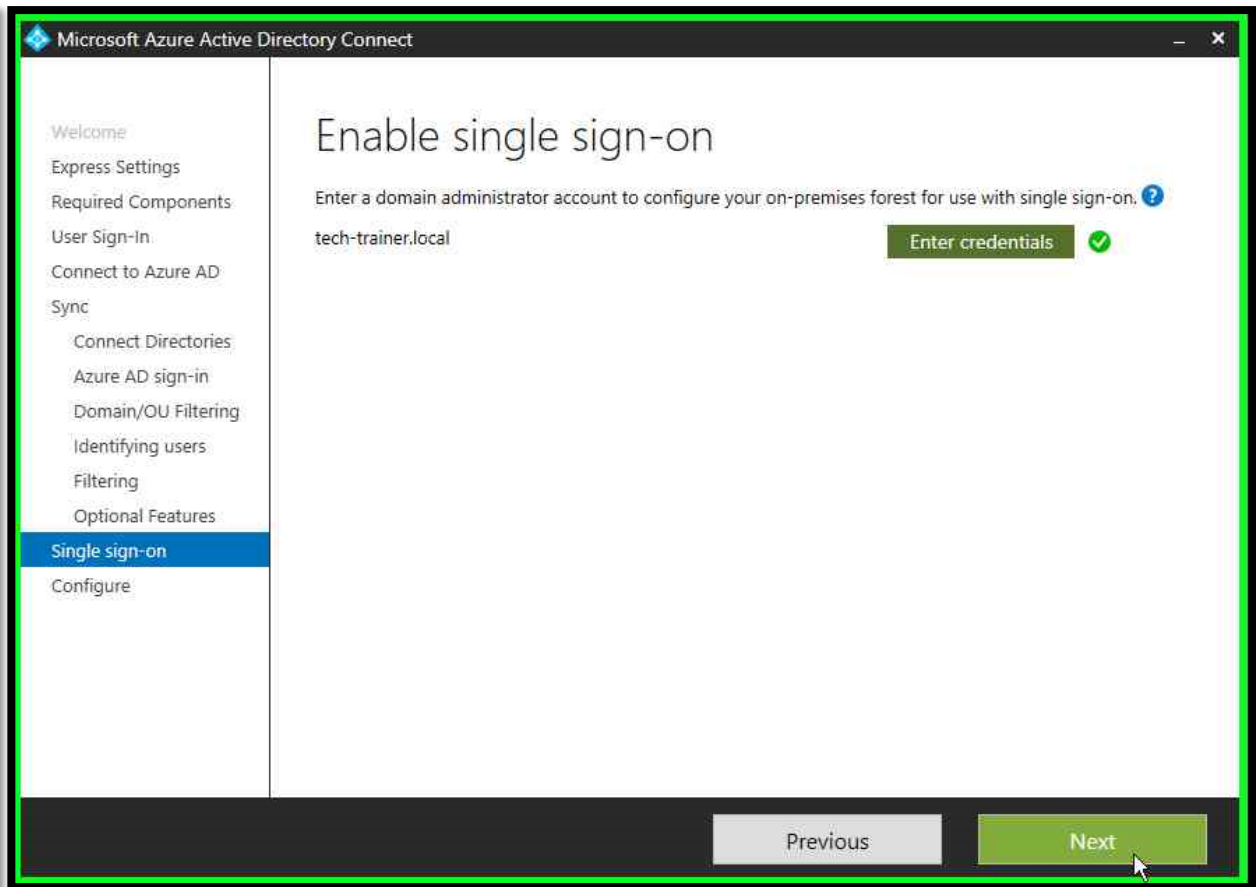
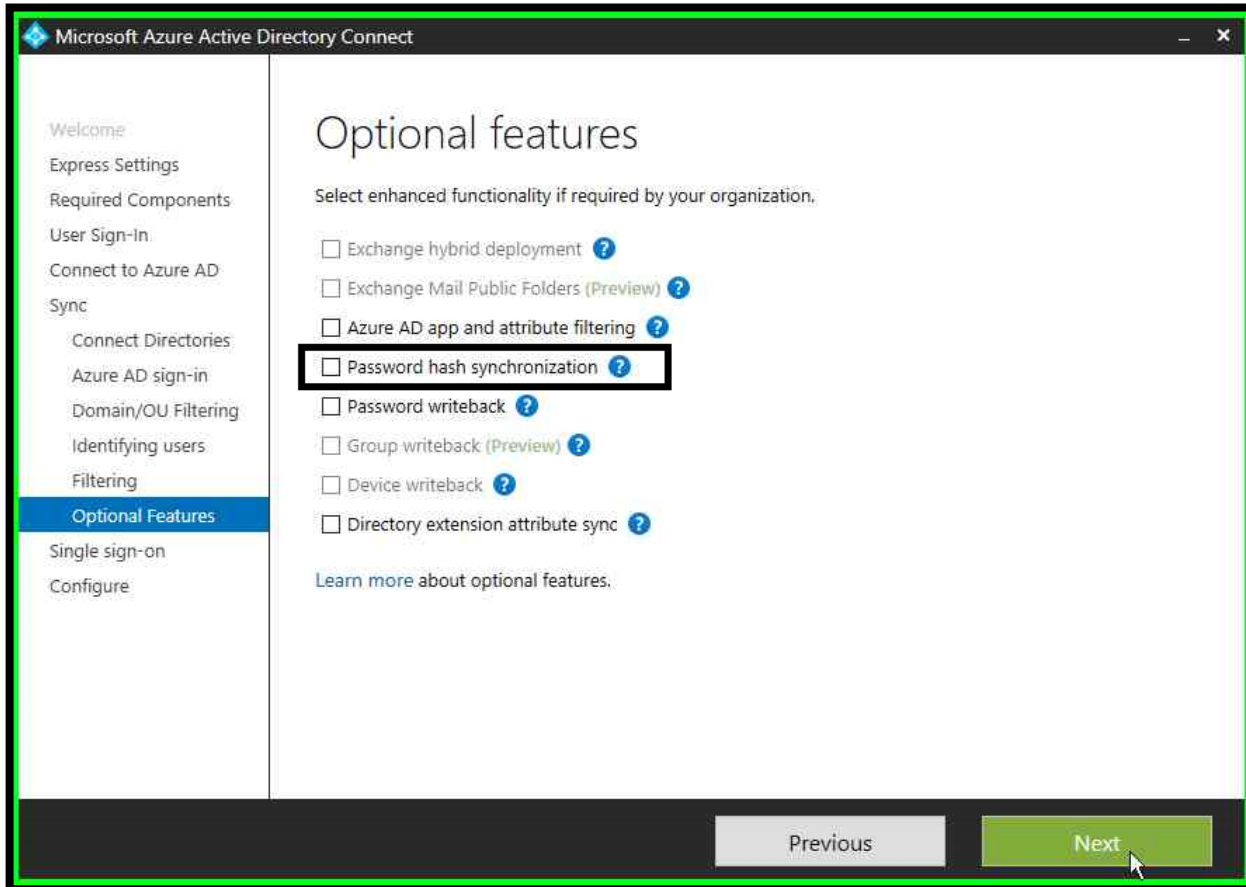
FOREST: tech-trainer.local

GROUP:

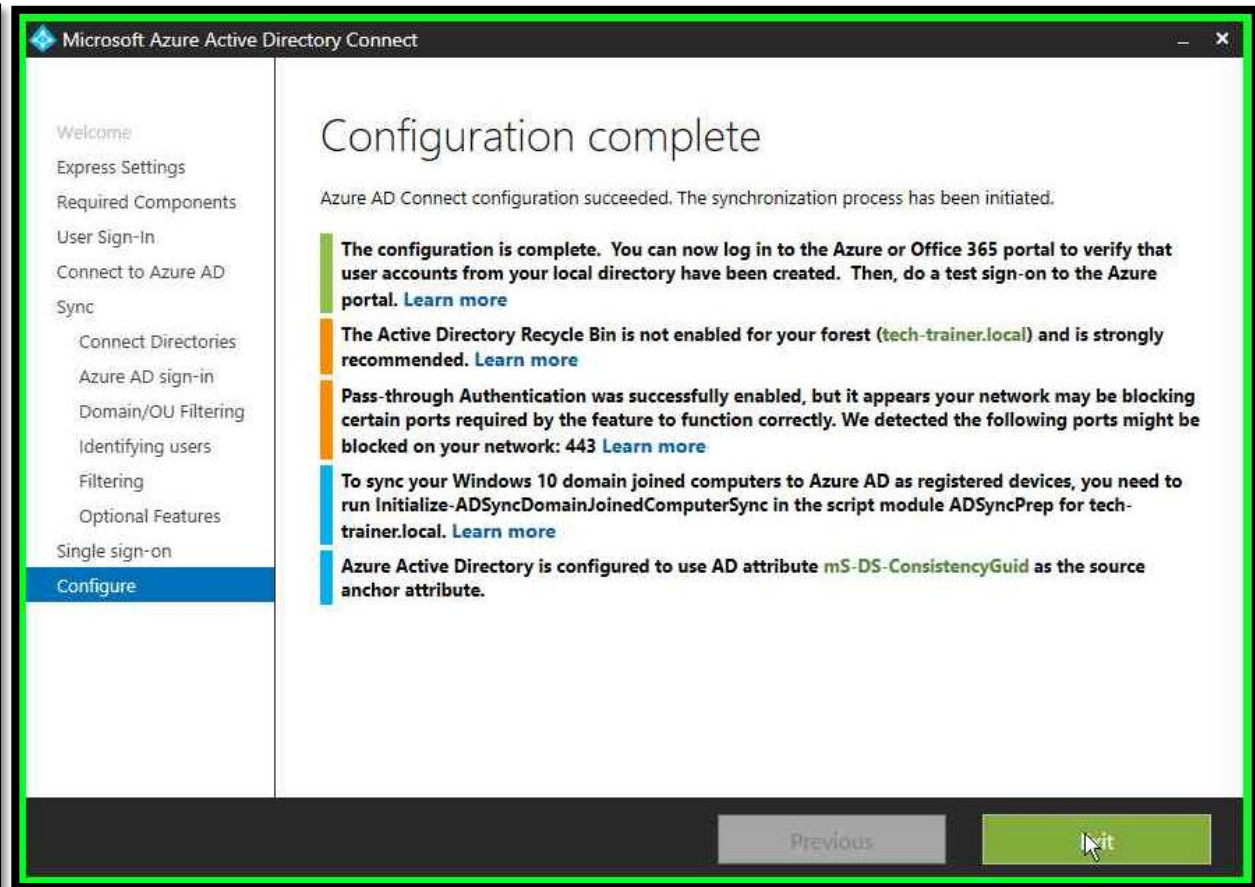
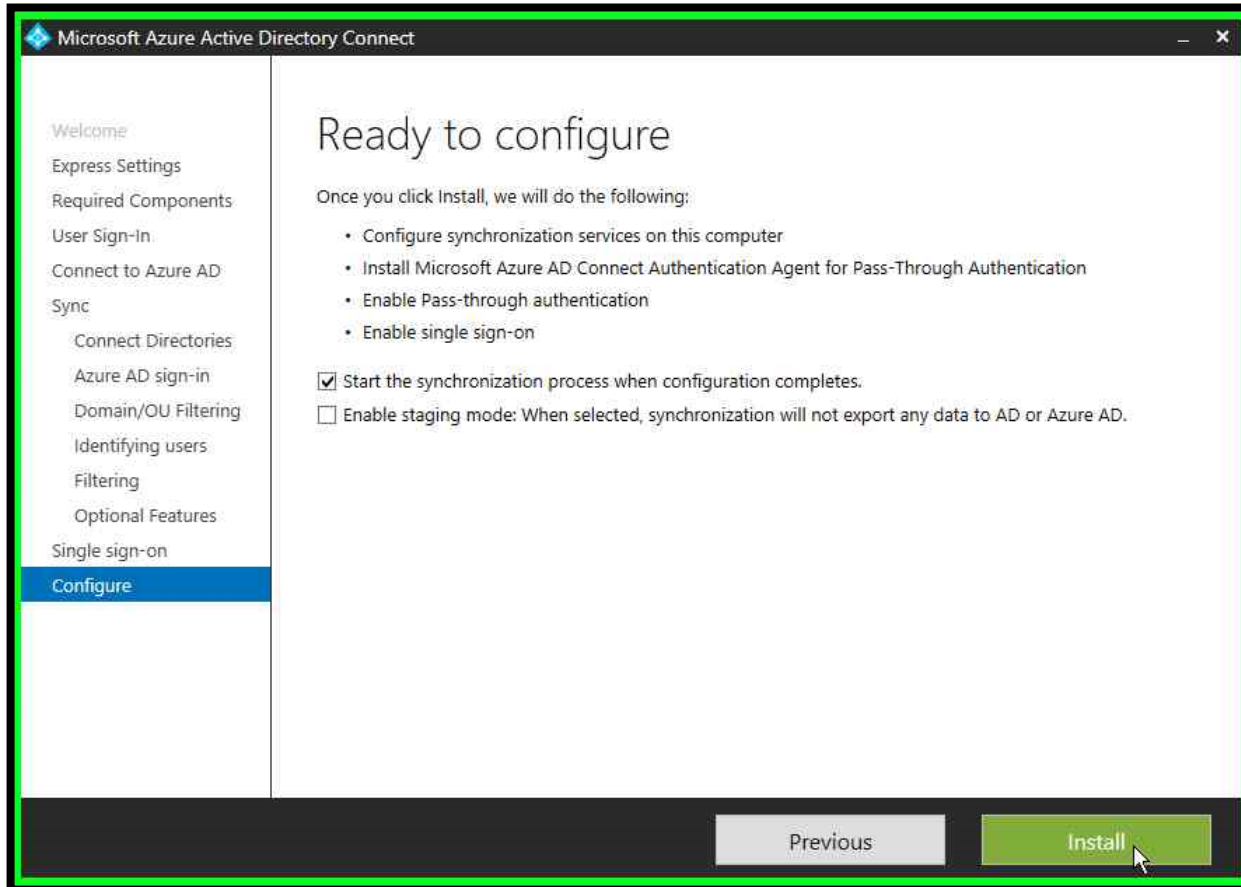
Resolve

Previous Next

PTA - Step-by-step



PTA - Step-by-step



PTA - Step-by-step

FAVORITES

- Dashboard
- Azure Active Directory
- Users
- Enterprise applications

MANAGE

- Users
- Groups
- Enterprise applications
- Devices
- App registrations
- Application proxy
- Licenses
- Azure AD Connect
- Custom domain names
- Mobility (MDM and MAM)
- Password reset
- Company branding
- User settings
- Properties
- Notifications settings

SECURITY

- Conditional access

SYNC STATUS

Sync Status	Enabled
Last Sync	Less than 1 hour ago
Password Sync	Disabled

USER SIGN-IN

Federation	Disabled	0 domains
Seamless single sign-on	Enabled	1 domain
Pass-through authentication	Enabled	1 agent

ON-PREMISES APPLICATIONS

Looking to configure remote access for on-premises applications? [Head to Application Proxy](#)

HEALTH AND ANALYTICS

Monitor your on-premises identity infrastructure and synchronization services in the cloud. [Azure AD Connect Health](#)

Seamless single sign-on

ON-PREMISES DOMAIN NAME **KEY CREATION DATE (UTC)** **STATUS**

tech-trainer.local	4/23/2018	✓
--------------------	-----------	---

Pass-through authentication

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

Windows¹⁸

Technology