AAD Connect setup guide

Version 1.0 (11-07-2017)
Nick Boszhard (2AT)

Contents

Introduction

In this guide you will find a customized configuration of AAD Connect. This setup is done with mostly default and Microsoft recommended settings. This document is part of a set of information about Office 365/Azure AD and SURFnet SURFconext. More information about this can be found on https://wiki.surfnet.nl/display/services/Office+365+Reference+environments

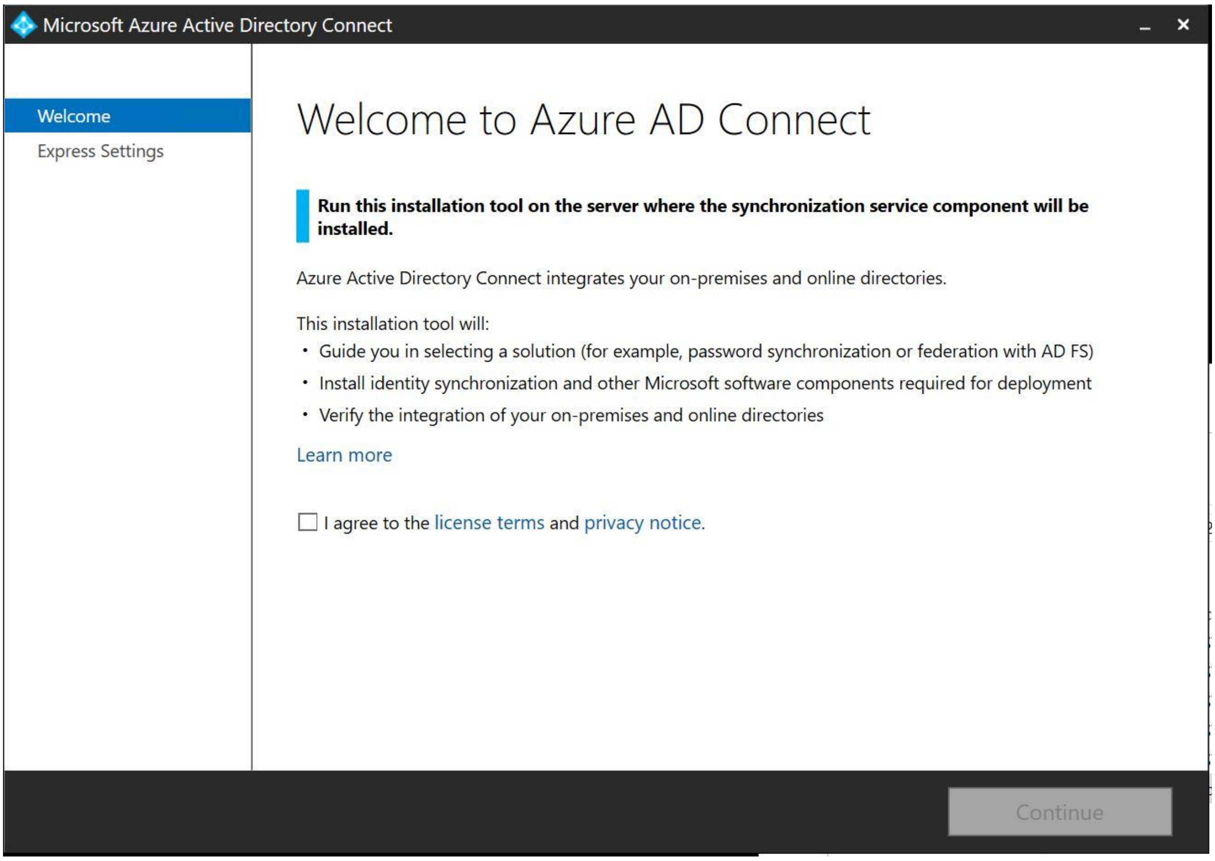
The set was created to help SURF institutions decide whether and how they can use SURFconext federated authentication (and related technology like SURFconext Strong Authentication) with Azure AD services, like Office 365."

We have tested this working setup in our own environment and if you have any questions or you need help, feel free to contact us via support@surfconext.nl

This document is created on 11-07-2017 based on the components that are current at this date. The most up-to-date version can be found on https://wiki.surfnet.nl/display/services/Microsoft+Office+365

Step 1: Run the AAD Connect tool

Run the AAD Connect tool setup on a server in your domain. The AAD Connect tool can be found here.



Microsoft Azure Active Directory Connect

Welcome to Azure AD Connect

Run this installation tool on the server where the synchronization service component will be installed.

Azure Active Directory Connect integrates your on-premises and online directories.

This installation tool will:

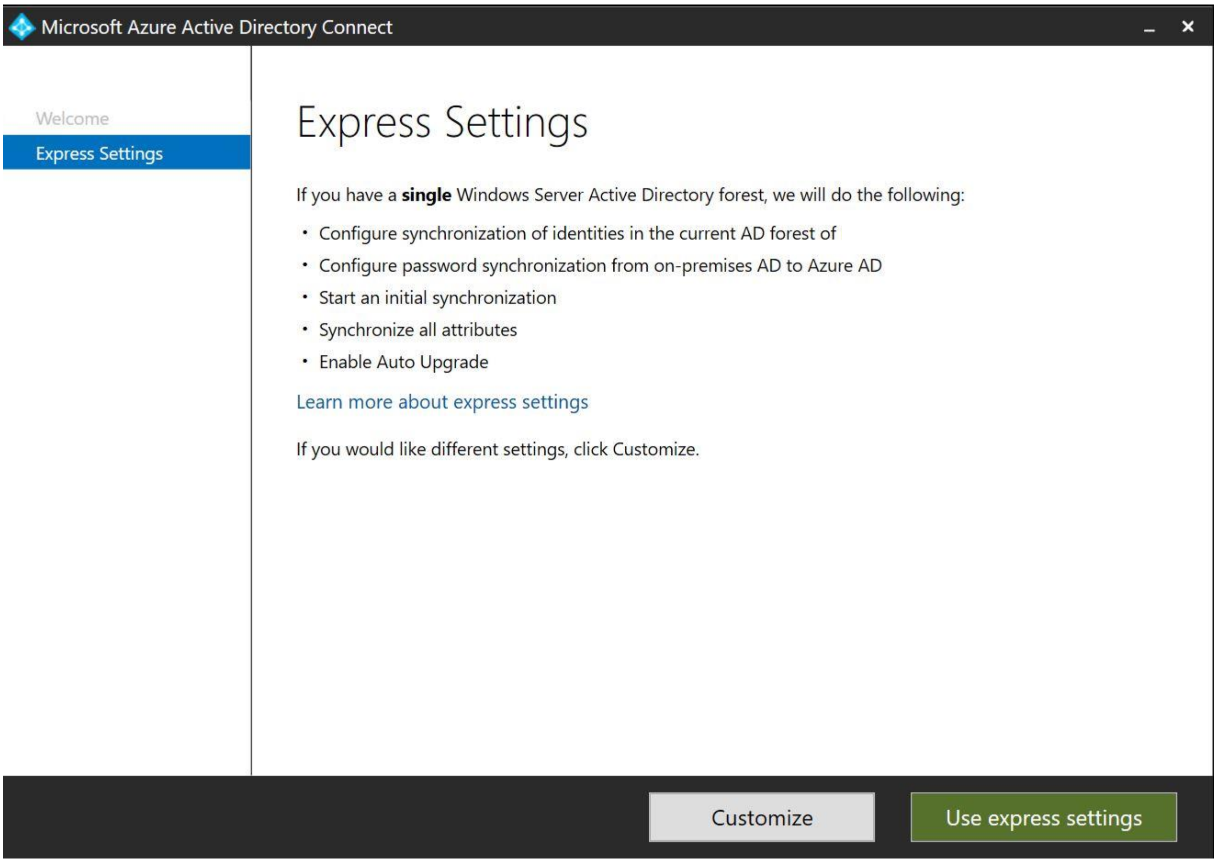
- Guide you in selecting a solution (for example, password synchronization or federation with AD FS)
- Install identity synchronization and other Microsoft software components required for deployment
- Verify the integration of your on-premises and online directories

Learn more

□ I agree to the license terms and privacy notice.

Step 2: Select your setup type

You can choose the express settings or to customize your settings. This guide will show you a customized setup.



Express Settings

If you have a **single** Windows Server Active Directory forest, we will do the following:

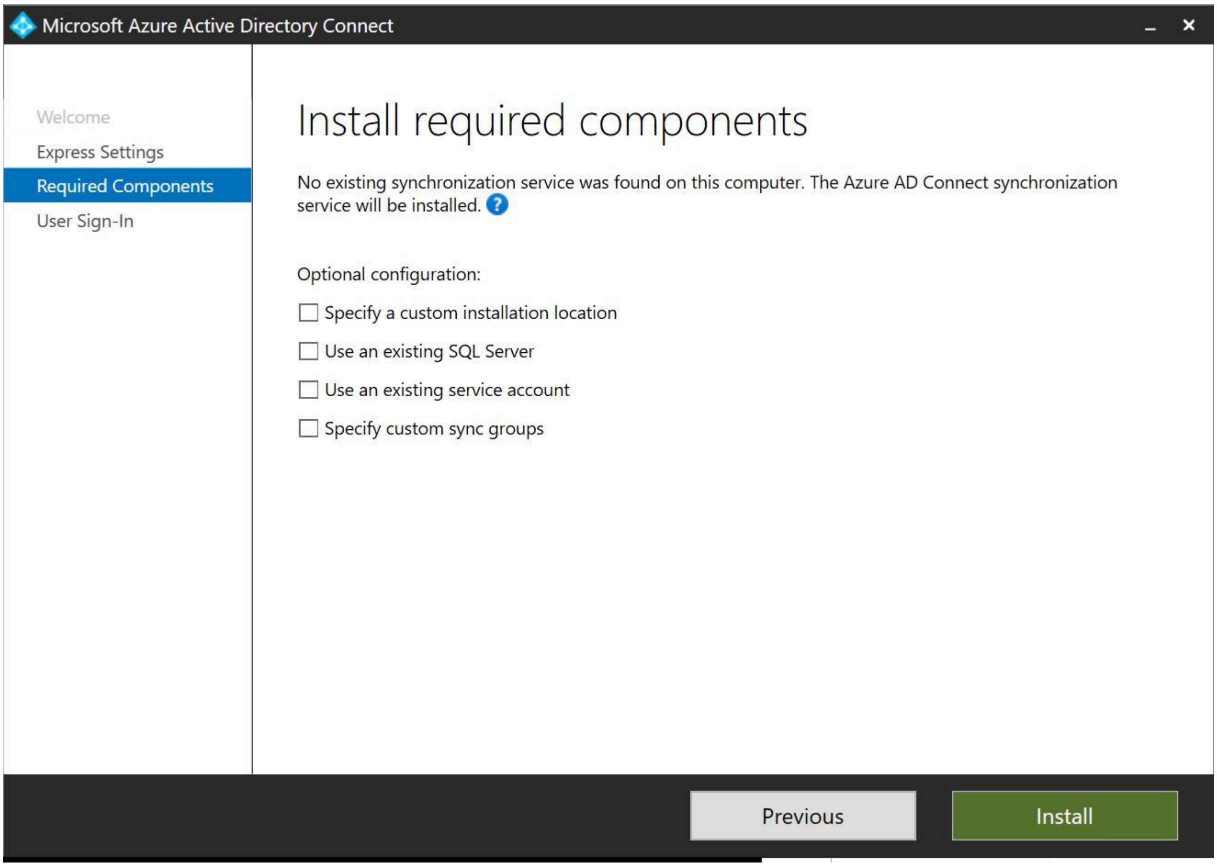
- Configure synchronization of identities in the current AD forest of
- Configure password synchronization from on-premises AD to Azure AD
- Start an initial synchronization
- Synchronize all attributes
- Enable Auto Upgrade

Learn more about express settings

If you would like different settings, click Customize.

Step 3: Install required components

You can choose your own components in this screen. When you don't select a component, AAD Connect will create them for you. In case you don't use a SQL Server installation, AAD Connect will install SQL Express. When you are working with big numbers of users, then SQL Express is not recommended. We did not add any optional configurations.



Microsoft Azure Active Directory Connect

Install required components

No existing synchronization service was found on this computer. The Azure AD Connect synchronization service will be installed.

Optional configuration:

□ Specify a custom installation location

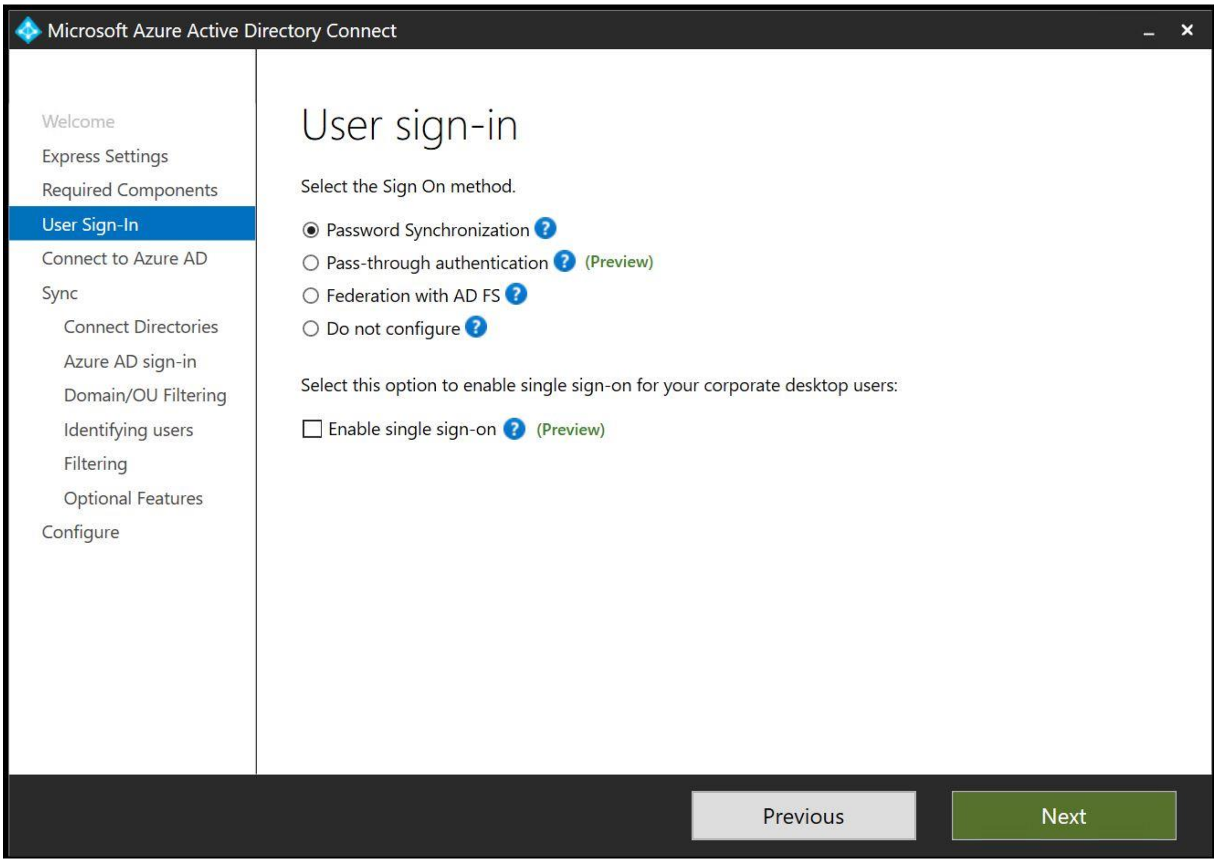
□ Use an existing SQL Server

□ Use an existing service account

□ Specify custom sync groups

Step 4: User Sign-in

In this step you can choose the way users are going to sign in. In this case we are going to choose the 'Password Synchronisaztion' option. When you select the 'Enable single sign-on' option, you will provide users with domain joined devices to use single sign on.



User sign-in

Select the Sign On method.

● Password Synchronization ?

○ Pass-through authentication ? (Preview)

○ Federation with AD FS ?

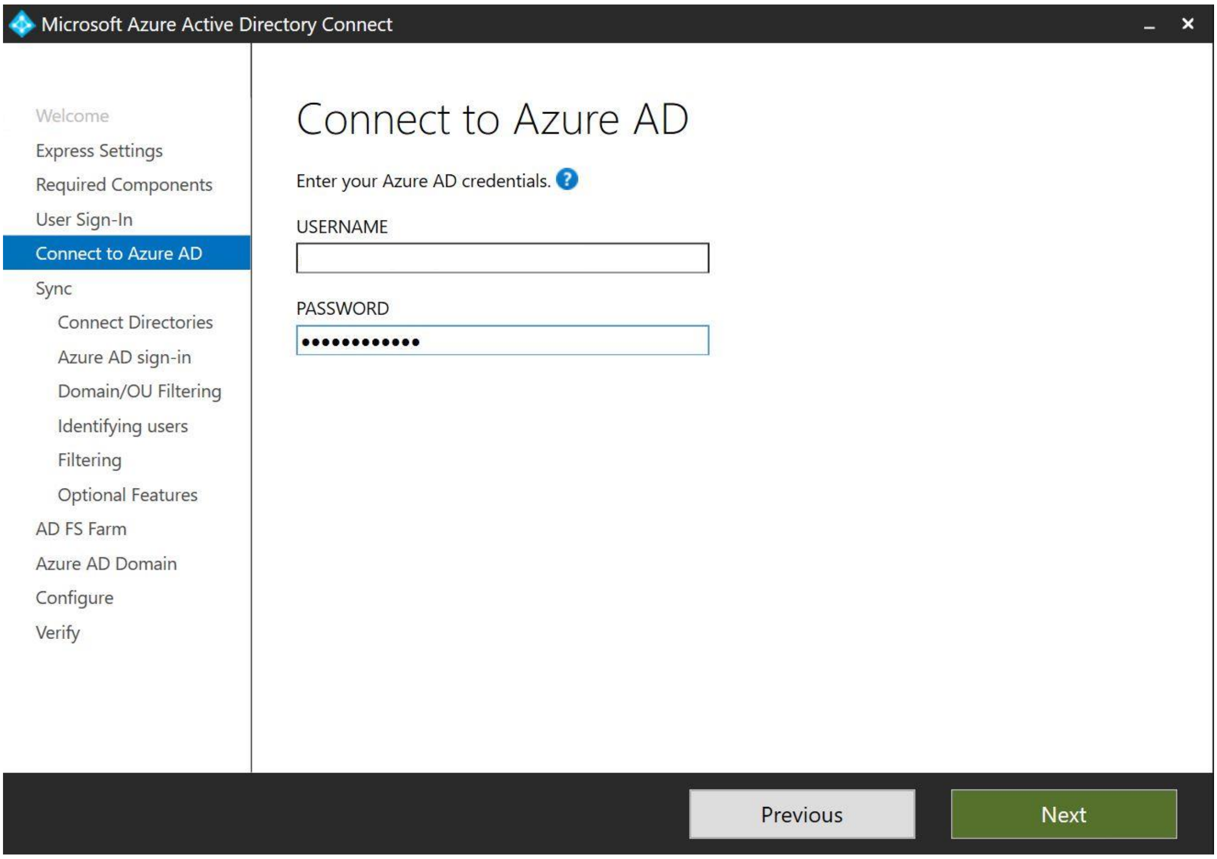
○ Do not configure ?

Select this option to enable single sign-on for your corporate desktop users:

□ Enable single sign-on ? (Preview)

Step 5: Connect to Azure AD

Fill in your Office 365 tenant admin password to connect to Azure AD



Connect to Azure AD

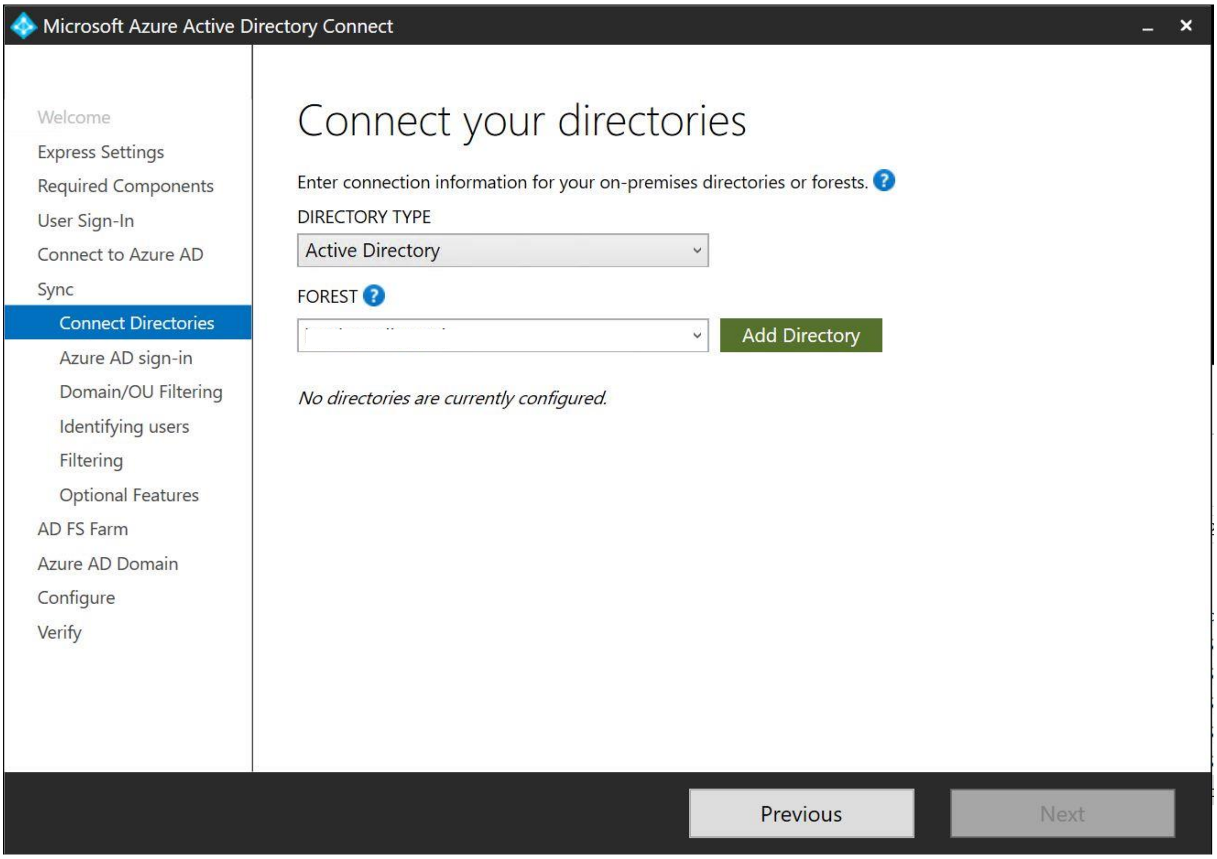
Enter your Azure AD credentials.

USERNAME

PASSWORD ●●●●●●●●●●●●●

Step 6: Connect your directories

Azure AD Connect will need the forest name to connect with your AD domain services



Microsoft Azure Active Directory Connect

Connect your directories

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

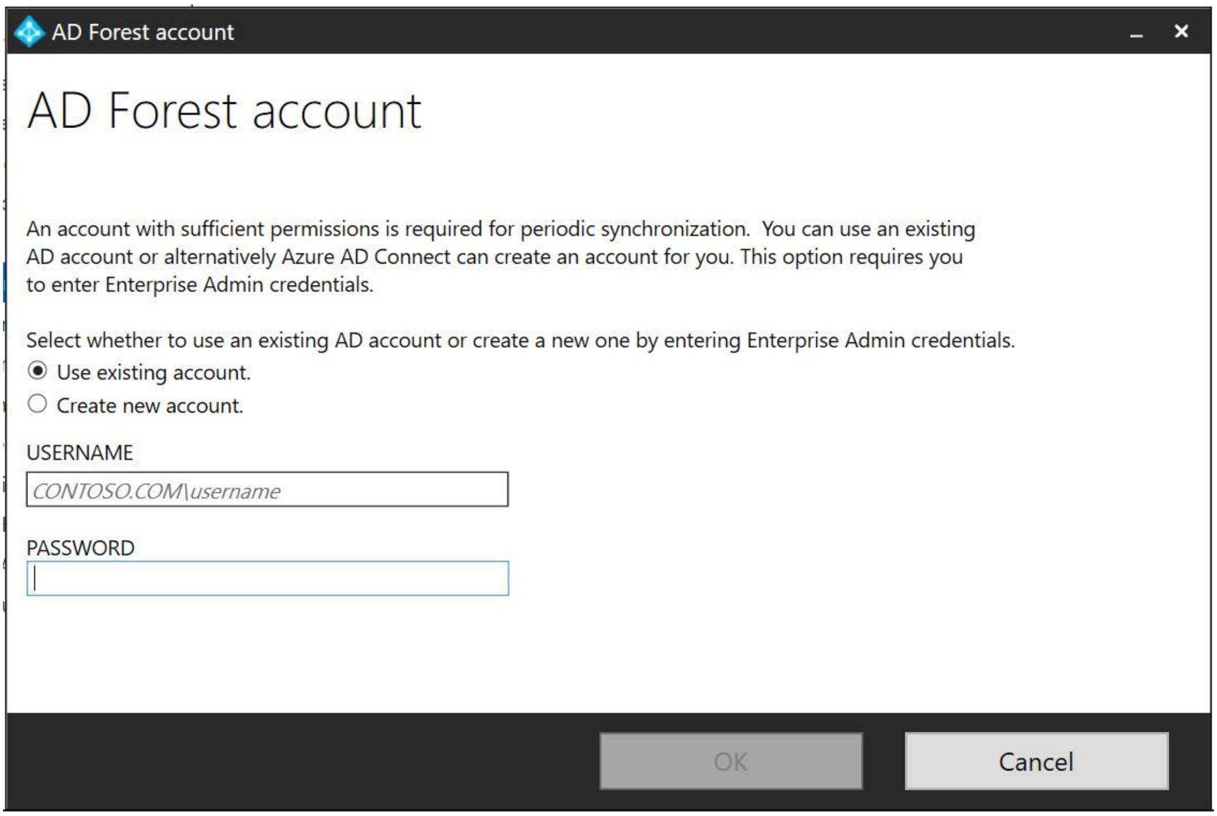
DIRECTORY TYPE: Active Directory

FOREST

No directories are currently configured.

Step 7: AD Forest account

Azure AD Connect will need an AD Forest account to connect with your AD domain services. If you don’t have one, you could let AD connect create one for you.



AD Forest account

AD Forest account

An account with sufficient permissions is required for periodic synchronization. You can use an existing AD account or alternatively Azure AD Connect can create an account for you. This option requires you to enter Enterprise Admin credentials.

Select whether to use an existing AD account or create a new one by entering Enterprise Admin credentials.

● Use existing account.

○ Create new account.

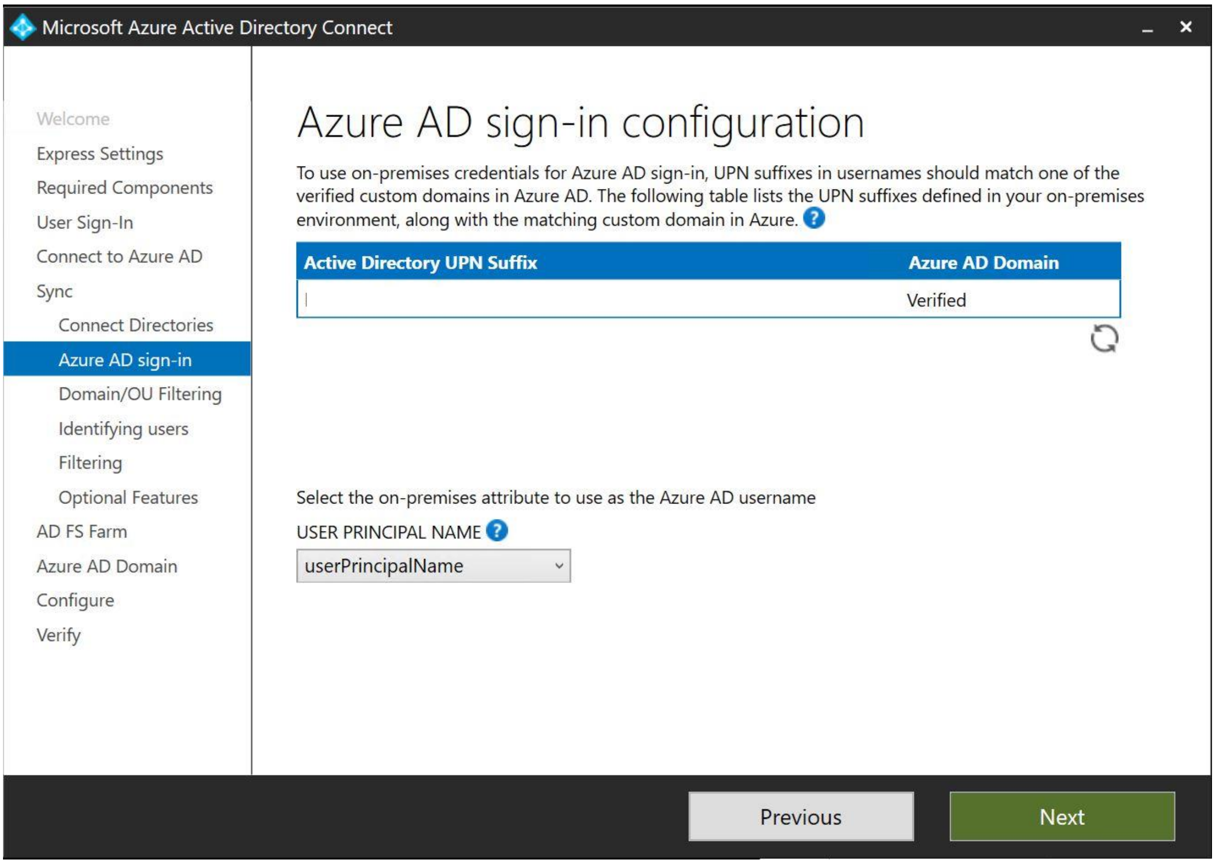
USERNAME

CONTOSO.COM\username

PASSWORD

Step 8: Azure AD sign-in configuration

On this page your Office 365 domains will be visible. The verification status will also be visible. In this step, you can choose what AD attribute will be used as User Principal Name. The use of an alternative UPN (such as email), is not supported by every Office 365 application.



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.

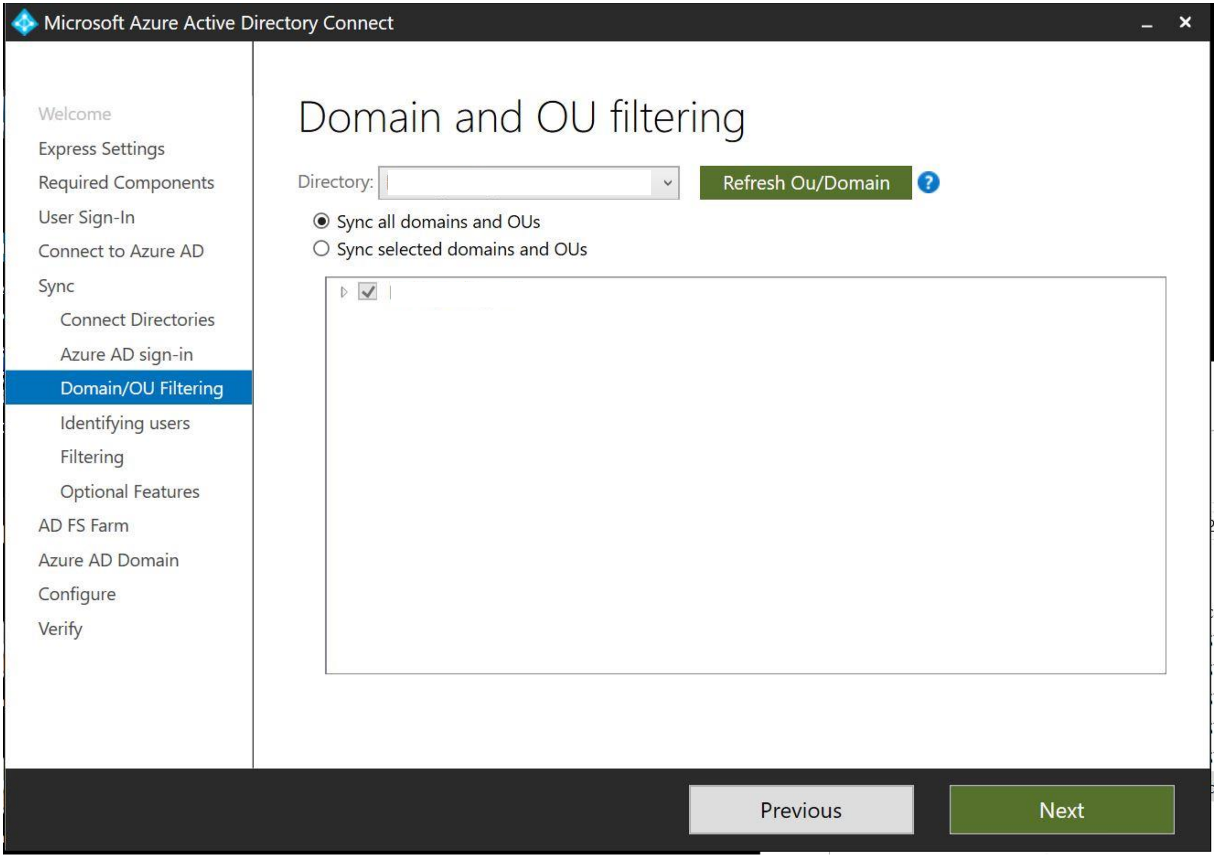
Active Directory UPN Suffix	Azure AD Domain
	Verified

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

USER PRINCIPAL NAME: userPrincipalName

Step 9: Domain and OU filtering

In this step you can select the domains and OU's you would want to sync. By default all domains and OU's are synced.



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
- AD FS Farm
- Azure AD Domain
- Configure
- Verify

Domain and OU filtering

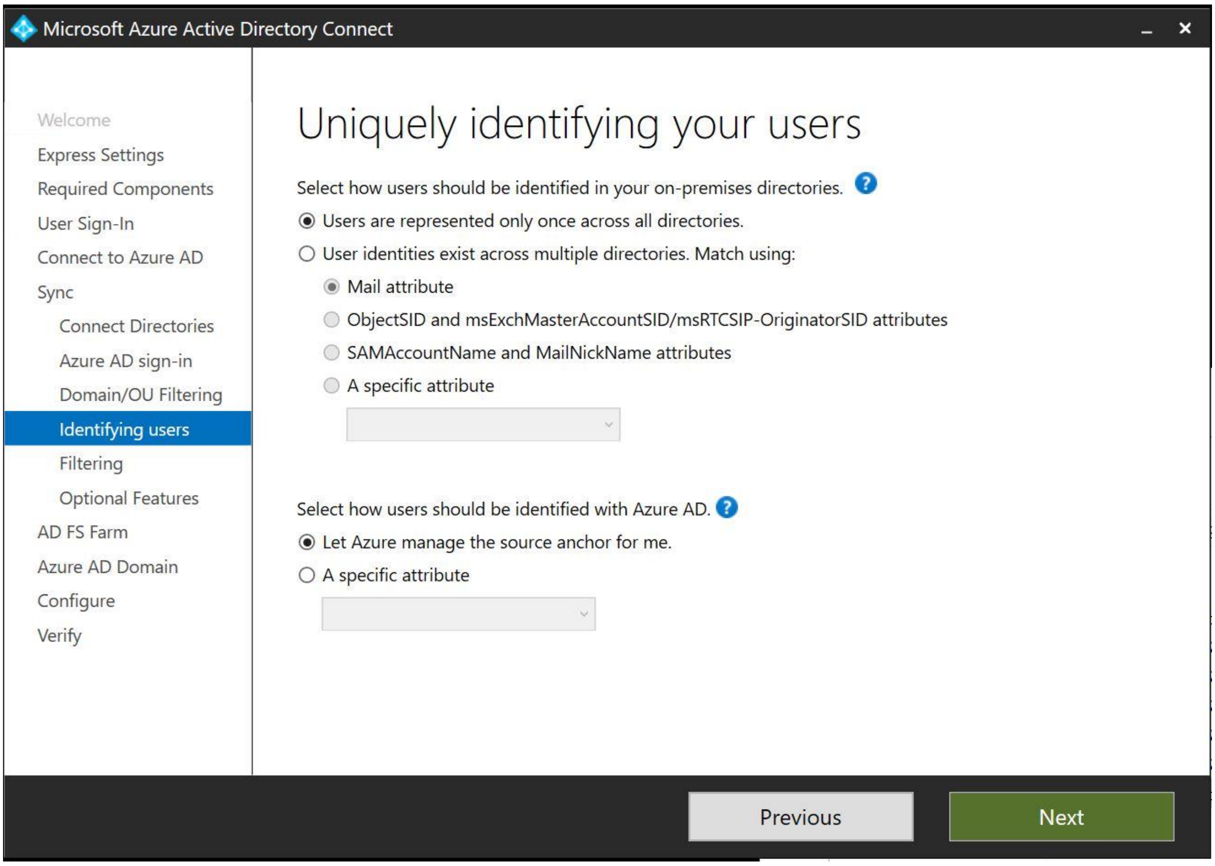
Directory:

● Sync all domains and OUs
○ Sync selected domains and OUs

☑

Step 10: Uniquely identifying your users

In this step, you can select if users are represented only once across all directories or not. If not, you are able to select an attribute by which the users are identified. You can also select the way users in Azure AD should be identified. You can only set this once for a user! ObjectGUID would be a good attribute to use, or you could just let Azure choose the source anchor for you.



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

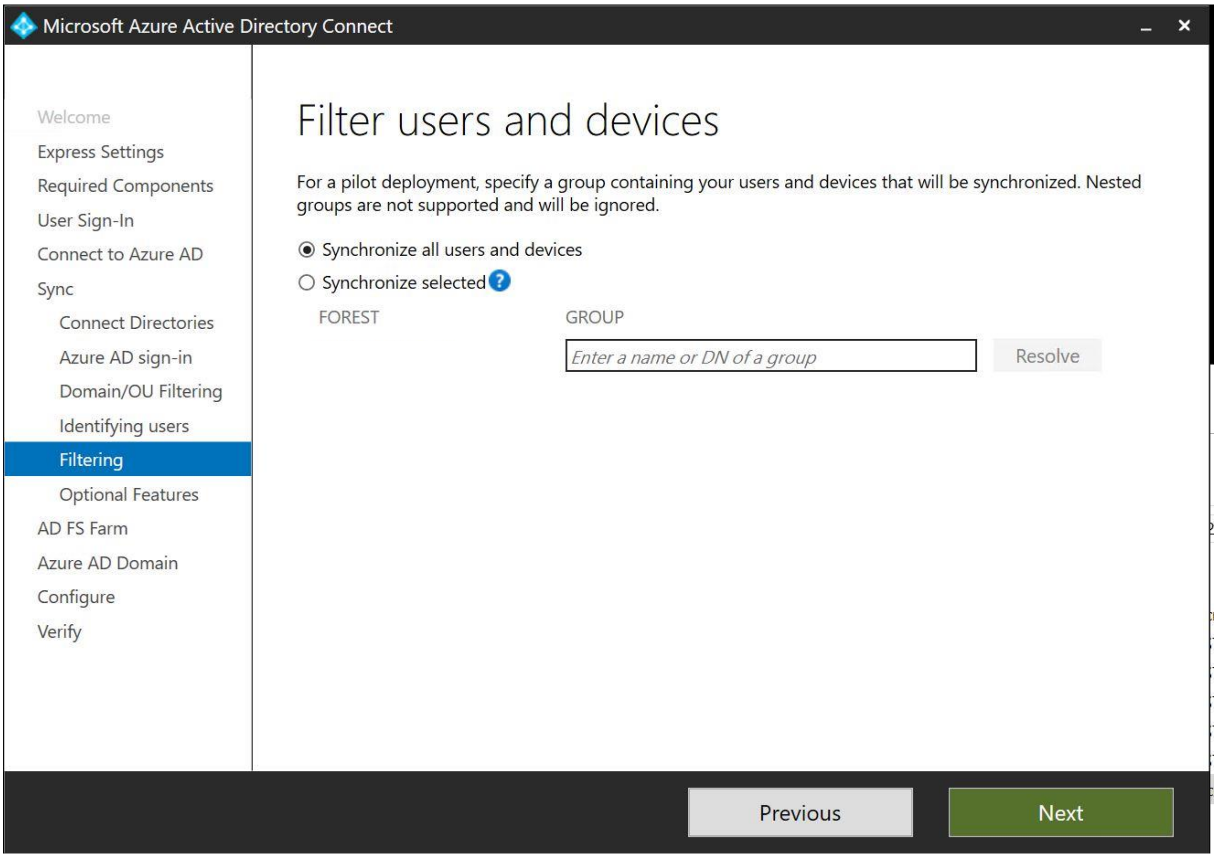
Select how users should be identified with Azure AD.

● Let Azure manage the source anchor for me.

○ A specific attribute

Step 11: Filter users and devices

In this step, you are able to select users and devices that should or should not be synchronized. By default all users and devices are being synced.



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

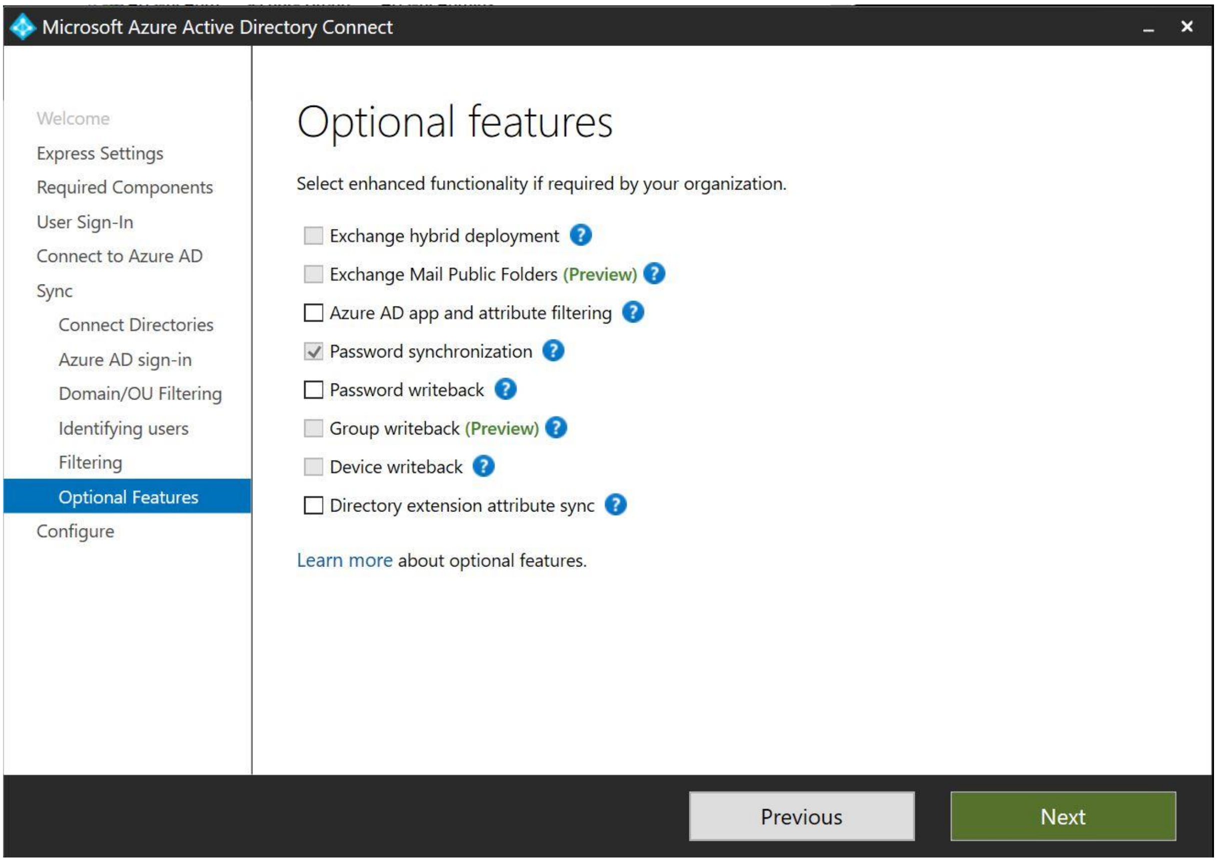
FOREST

GROUP

Enter a name or DN of a group

Step 12: Optional features

In this step you can select optional features based on your situation. We are using the Password synchronization, but NOT the password writeback because this is not recommended by Microsoft.



Optional features

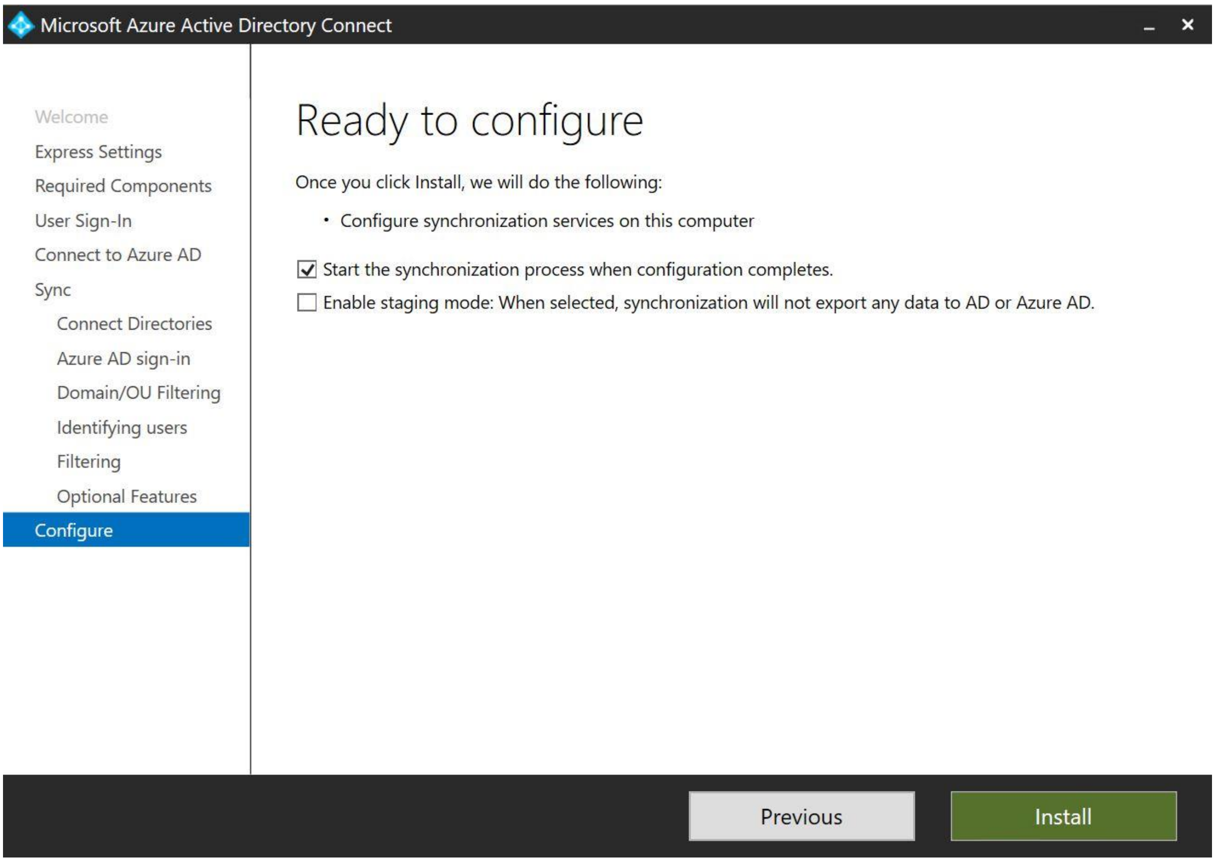
Select enhanced functionality if required by your organization.

- □ Exchange hybrid deployment
- □ Exchange Mail Public Folders (Preview)
- □ Azure AD app and attribute filtering
- ☑ Password synchronization
- □ Password writeback
- □ Group writeback (Preview)
- □ Device writeback
- □ Directory extension attribute sync

Learn more about optional features.

Step 13: Ready to configure

In this step you are able to start the configuration of all of the settings you've selected.



Ready to configure

Once you click Install, we will do the following:

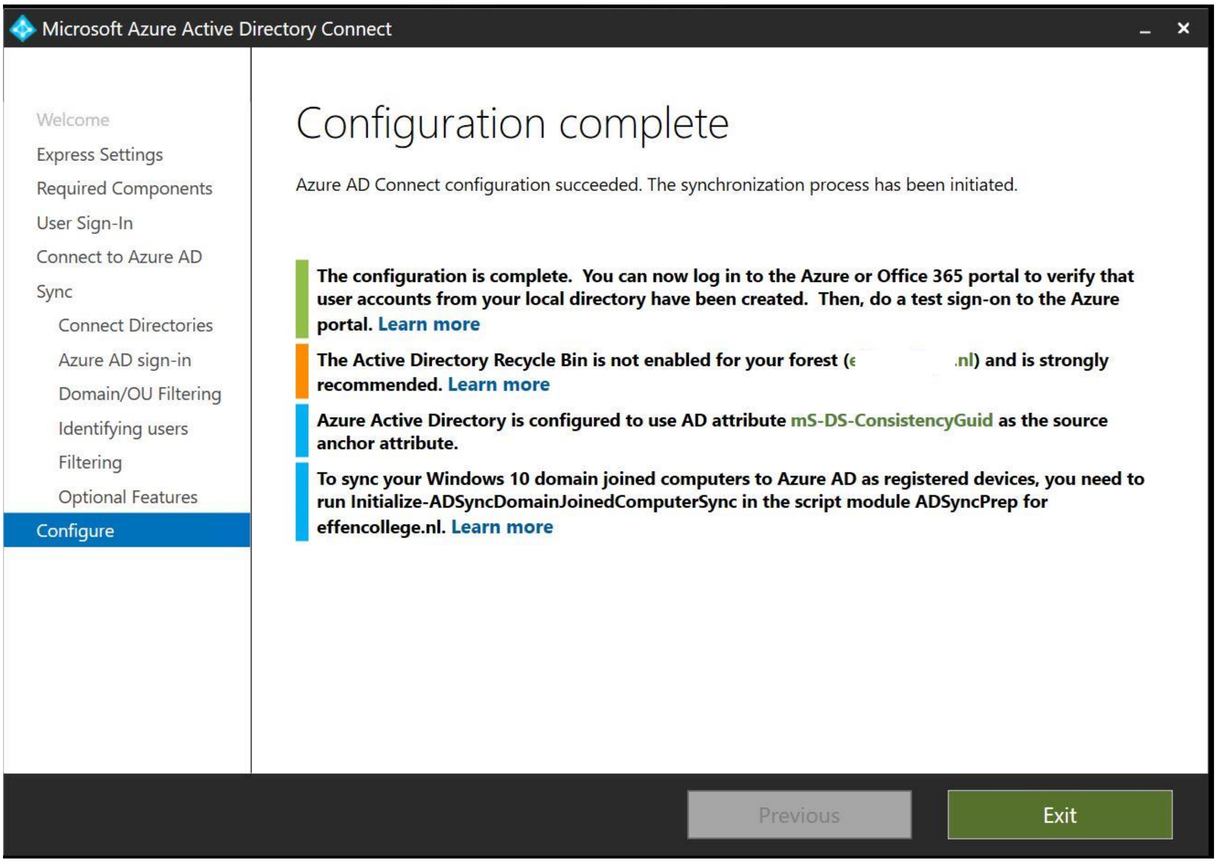
- Configure synchronization services on this computer

☑ Start the synchronization process when configuration completes.

□ Enable staging mode: When selected, synchronization will not export any data to AD or Azure AD.

Step 14: Configuration Complete

In this step you will see a summary of completed steps, warnings and errors. In this case it is recommended to enable the AD recycle bin.



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**

The Active Directory Recycle Bin is not enabled for your forest ([redacted].nl) and is strongly recommended. **Learn more**

Azure Active Directory is configured to use AD attribute mS-DS-ConsistencyGuid as the source anchor attribute.

To sync your Windows 10 domain joined computers to Azure AD as registered devices, you need to run Initialize-ADSyncDomainJoinedComputerSync in the script module ADSyncPrep for effencollege.nl. **Learn more**