

AAD Connect setup guide

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

Contents

Introduction	3
Step 1: Run the AAD Connect tool	4
Step 2: Select your setup type.....	5
Step 3: Install required components	6
Step 4: User Sign-in	7
Step 5: Connect to Azure AD.....	8
Step 6: Connect your directories.....	9
Step 7: AD Forest account.....	10
Step 8: Azure AD sign-in configuration	11
Step 9: Domain and OU filtering.....	12
Step 10: Uniquely identifying your users	13
Step 11: Filter users and devices	14
Step 12: Optional features	15
Step 13: AD FS farm	16
Step 14: AD FS servers.....	17
Step 15: Web Application Proxy servers	18
Step 16: Domain Administrator credentials.....	19
Step 17: AD FS service account	20
Step 18: Azure AD Domain	21
Step 19: Ready to configure	22
Step 20: Configuration Complete	23
Step 21: Verify federation configuration.....	24

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>

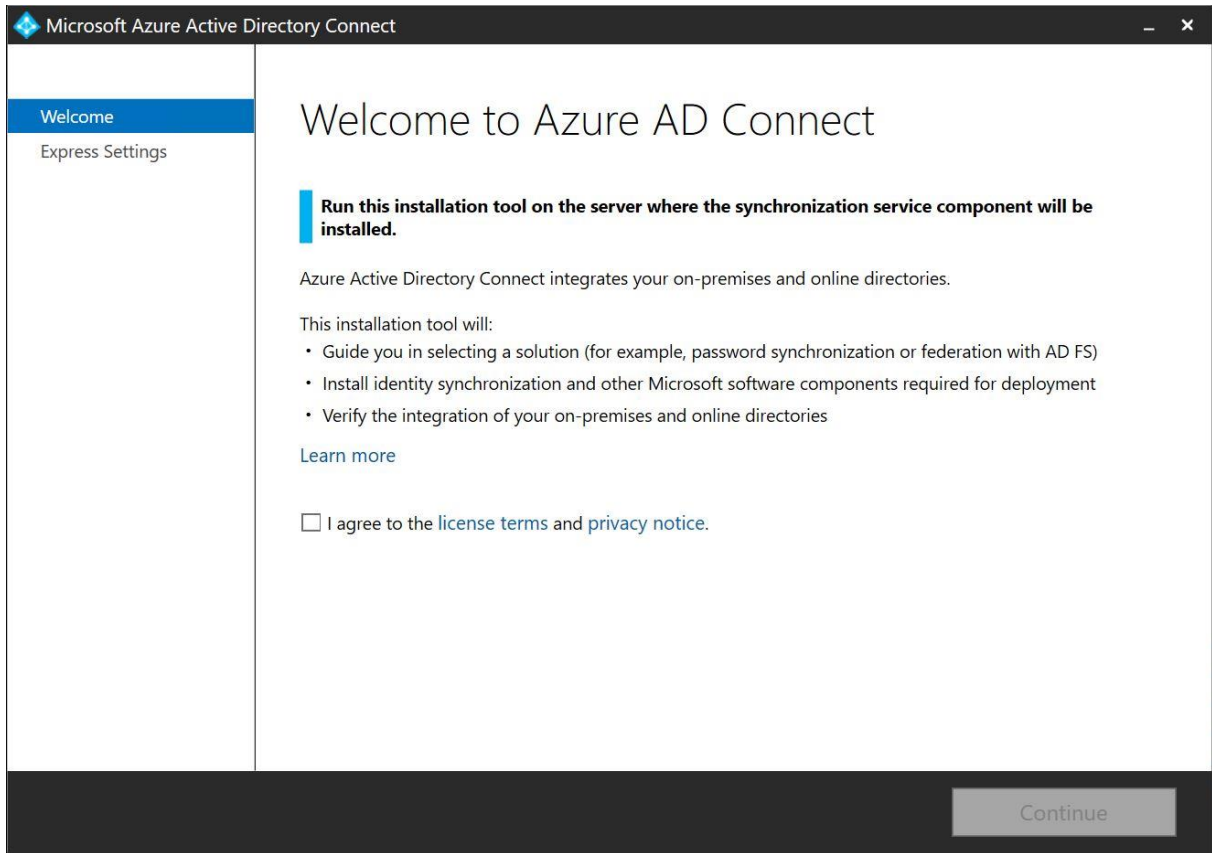
The set was created to help SURF institutions decide whether and how they can use SURFconext federated authentication (and related technology like SURFconext Strong Authentication) with Azure AD services, like Office 365.”

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>

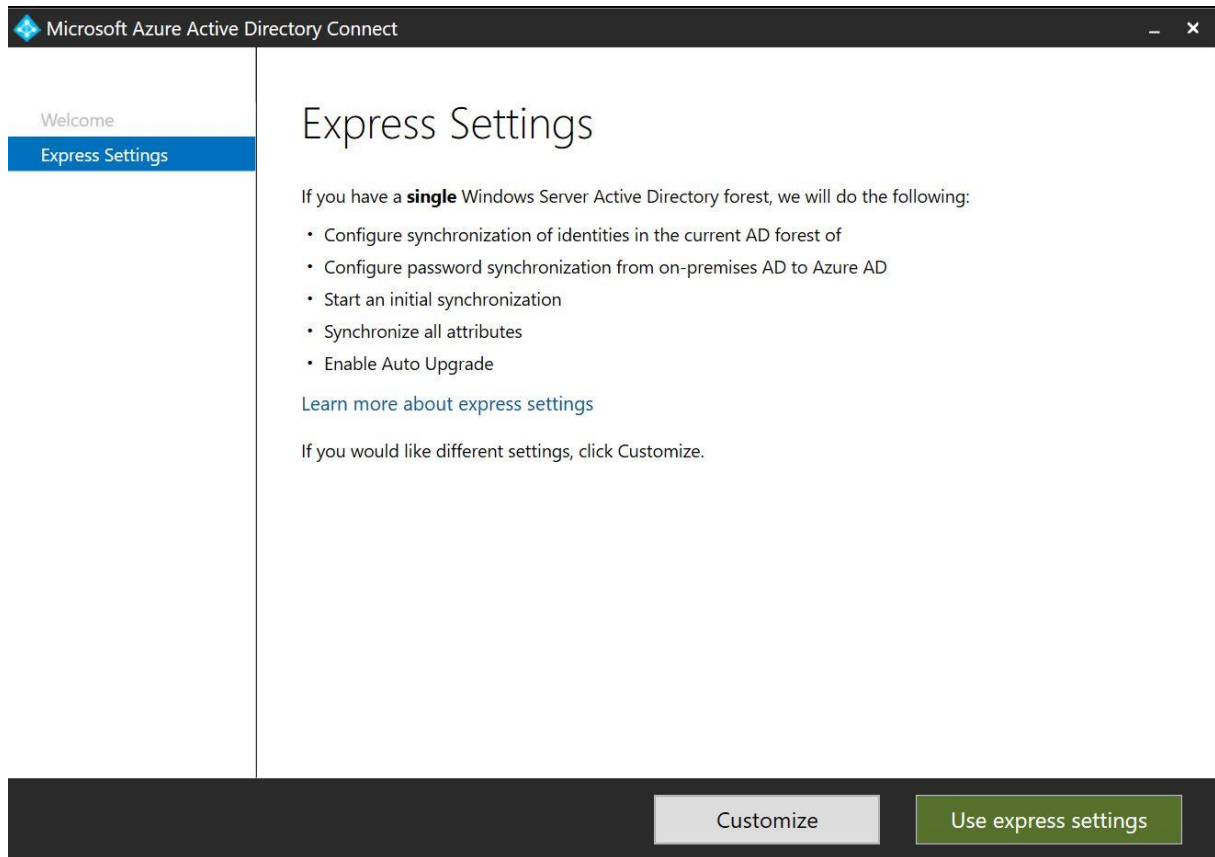
Step 1: Run the AAD Connect tool

Run the AAD Connect tool setup on a server in your domain. The AAD Connect tool can be found [here](#).



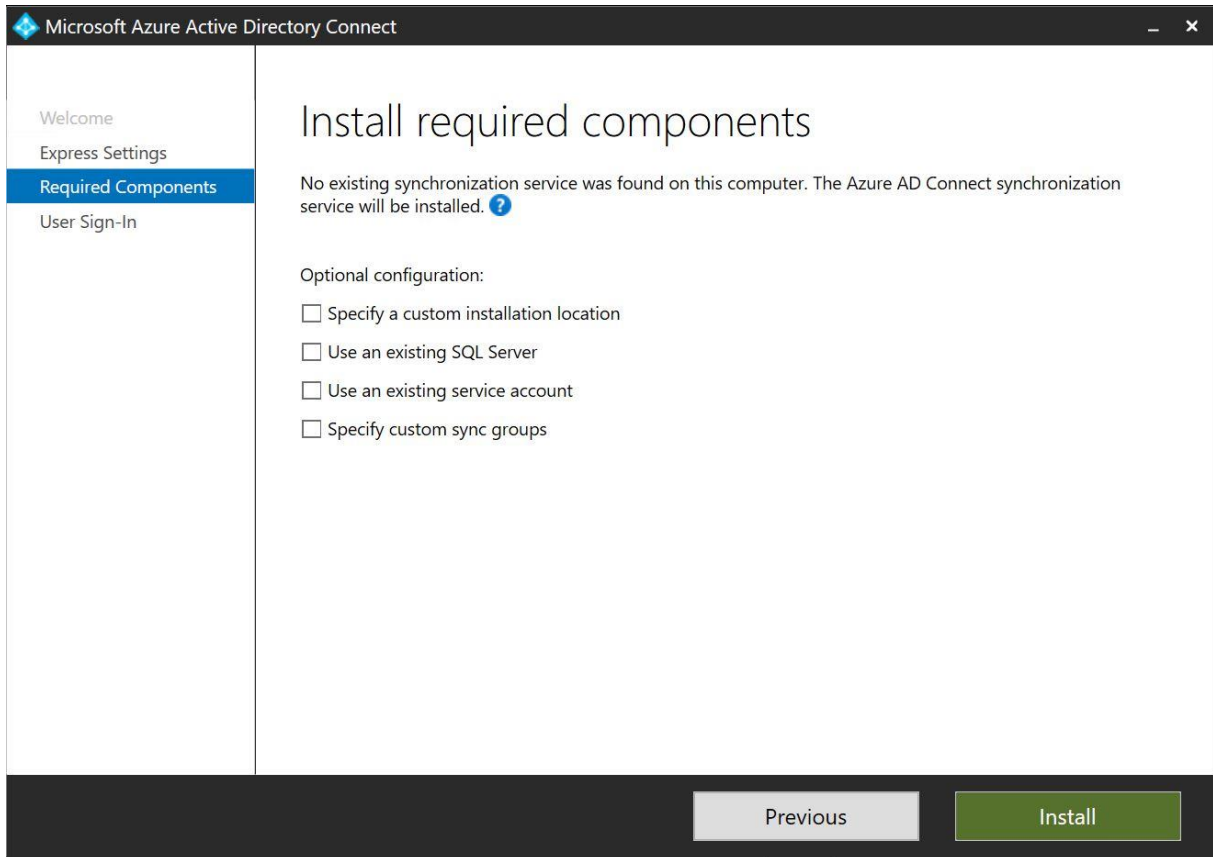
Step 2: Select your setup type

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



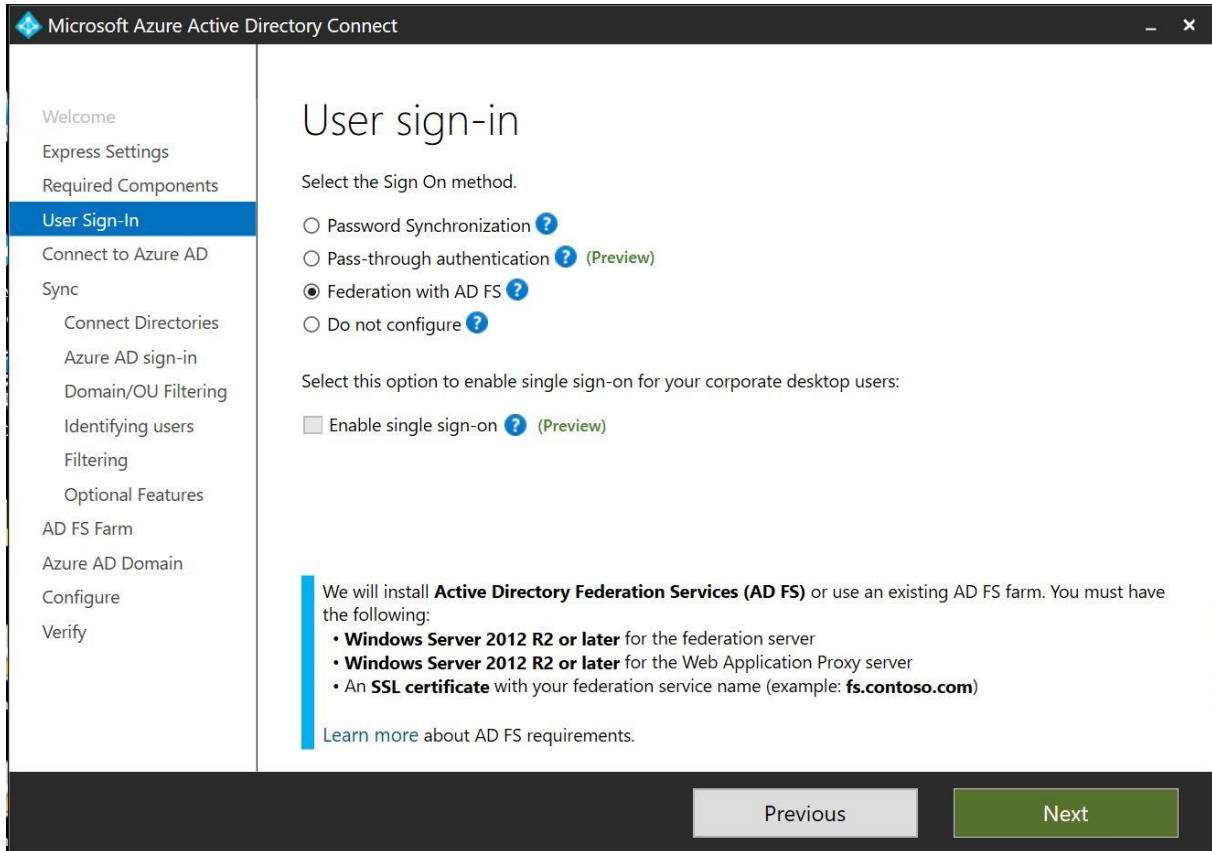
Step 3: Install required components

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.



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 'Federation with AD FS' option. When you select the 'Enable single sign-on' option, you will provide users with domain joined devices to use single sign on.



The screenshot shows the 'User sign-in' configuration window in Microsoft Azure Active Directory Connect. The window title is 'Microsoft Azure Active Directory Connect'. The left sidebar contains a navigation menu with the following items: Welcome, Express Settings, Required Components, User Sign-In (highlighted), 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, and Verify. The main content area is titled 'User sign-in' and contains the following text and options:

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)

We will install **Active Directory Federation Services (AD FS)** or use an existing AD FS farm. You must have the following:

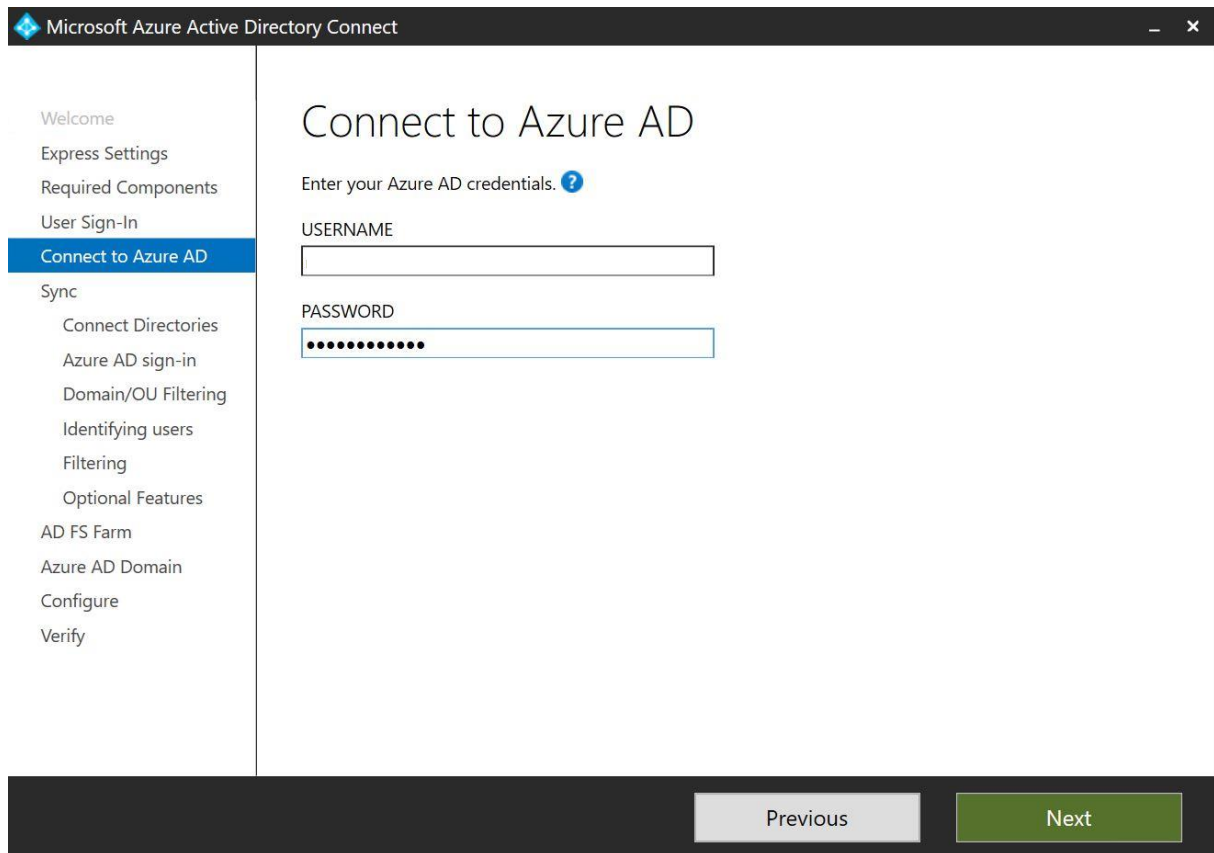
- **Windows Server 2012 R2 or later** for the federation server
- **Windows Server 2012 R2 or later** for the Web Application Proxy server
- An **SSL certificate** with your federation service name (example: **fs.contoso.com**)

[Learn more about AD FS requirements.](#)

At the bottom of the window, there are two buttons: 'Previous' (disabled) and 'Next' (active).

Step 5: Connect to Azure AD

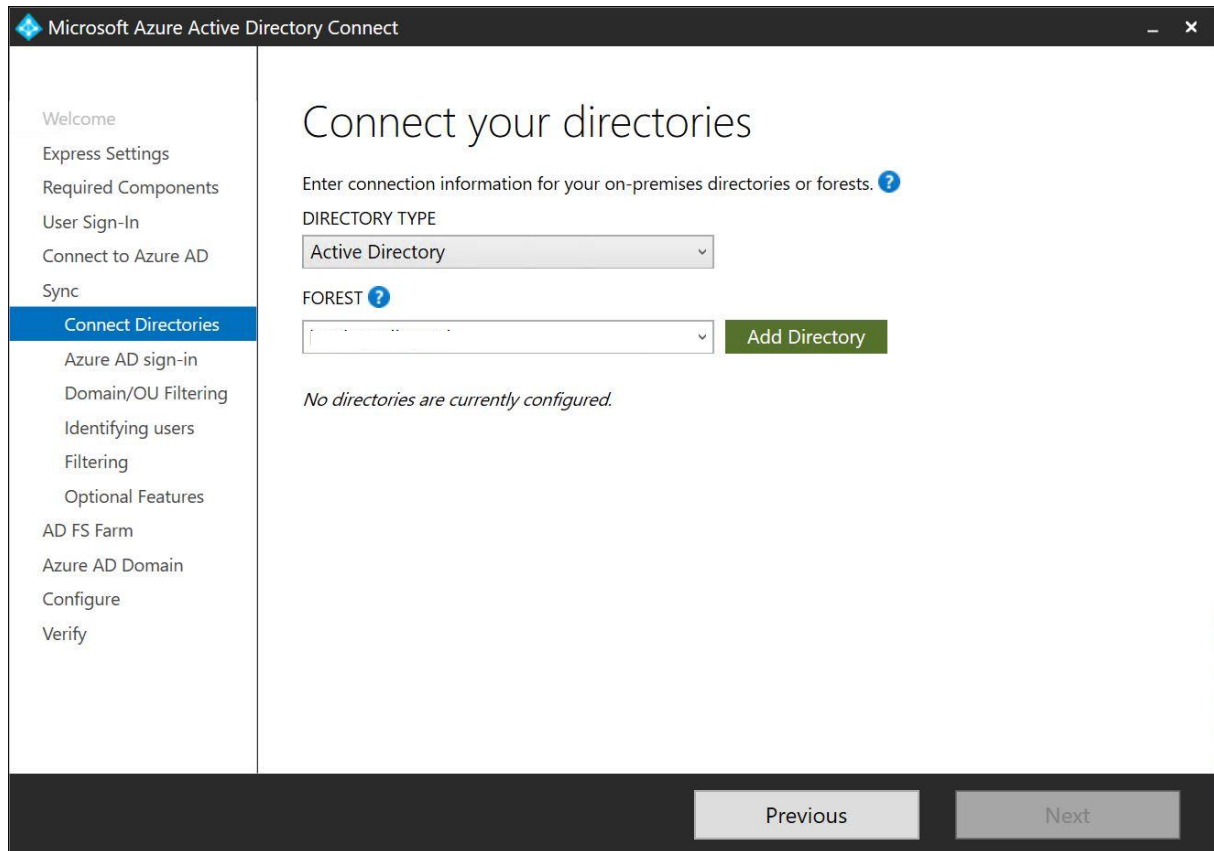
Fill in your Office 365 tenant admin password to connect to Azure AD



The screenshot shows the 'Microsoft Azure Active Directory Connect' application window. The title bar reads 'Microsoft Azure Active Directory Connect'. On the left is a navigation pane with the following items: Welcome, Express Settings, Required Components, User Sign-In, **Connect to Azure AD** (highlighted in blue), Sync, Connect Directories, Azure AD sign-in, Domain/OU Filtering, Identifying users, Filtering, Optional Features, AD FS Farm, Azure AD Domain, Configure, and Verify. The main content area is titled 'Connect to Azure AD' and contains the instruction 'Enter your Azure AD credentials. ?'. Below this are two input fields: 'USERNAME' and 'PASSWORD'. The 'PASSWORD' field is currently filled with ten black dots. At the bottom of the window, there are two buttons: 'Previous' (disabled) and 'Next' (active).

Step 6: Connect your directories

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



The screenshot shows the 'Microsoft Azure Active Directory Connect' application window. The title bar includes the Microsoft logo and the text 'Microsoft Azure Active Directory Connect'. On the left is a navigation pane with the following items: Welcome, Express Settings, Required Components, User Sign-In, Connect to Azure AD, Sync, **Connect Directories** (highlighted), Azure AD sign-in, Domain/OU Filtering, Identifying users, Filtering, Optional Features, AD FS Farm, Azure AD Domain, Configure, and Verify. The main content area is titled 'Connect your directories' and contains the instruction 'Enter connection information for your on-premises directories or forests. ?'. Below this, there are two dropdown menus: 'DIRECTORY TYPE' with 'Active Directory' selected, and 'FOREST ?' which is currently empty. To the right of the 'FOREST' dropdown is a green 'Add Directory' button. Below the dropdowns, the text 'No directories are currently configured.' is displayed. At the bottom of the window, there are two buttons: 'Previous' and 'Next'.

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

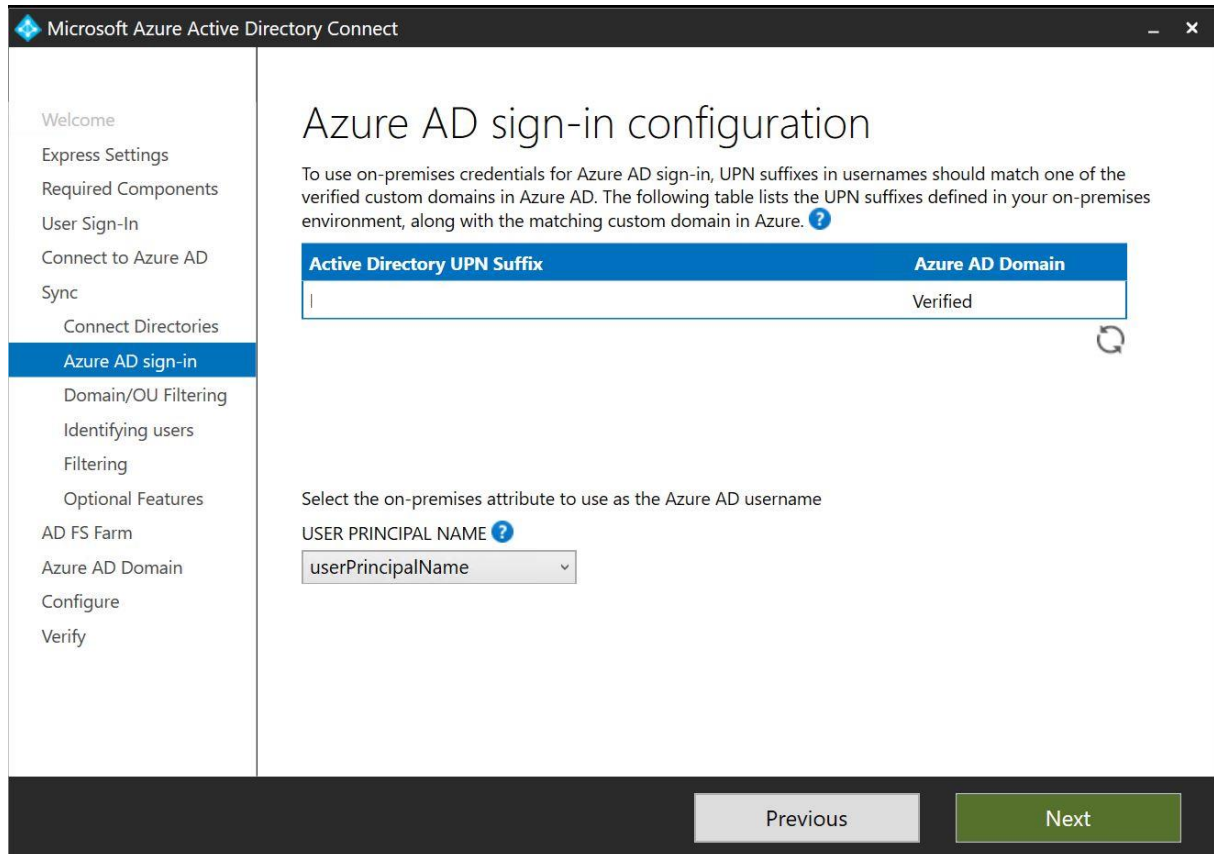
CONTOSO.COM\username

PASSWORD

OK Cancel

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.



Microsoft Azure Active Directory Connect

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

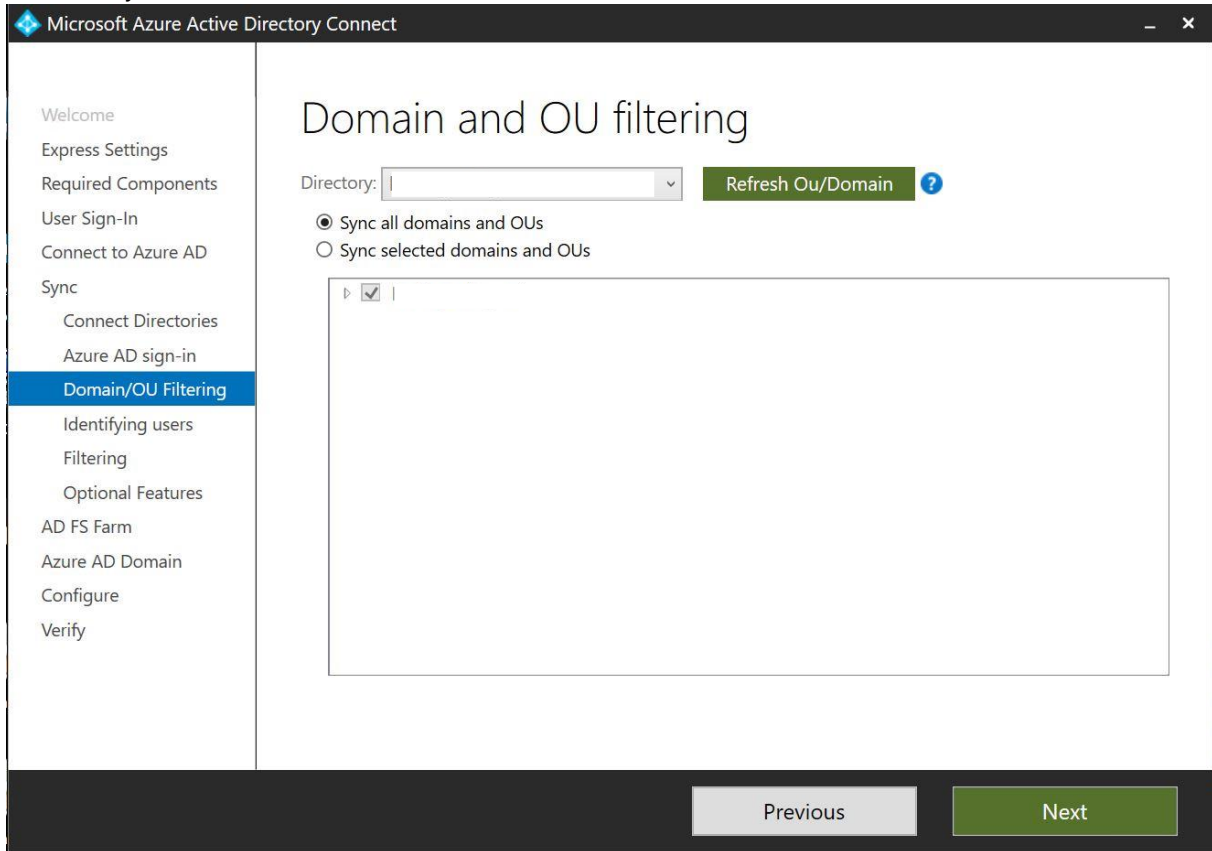
USER PRINCIPAL NAME ?

userPrincipalName

Previous Next

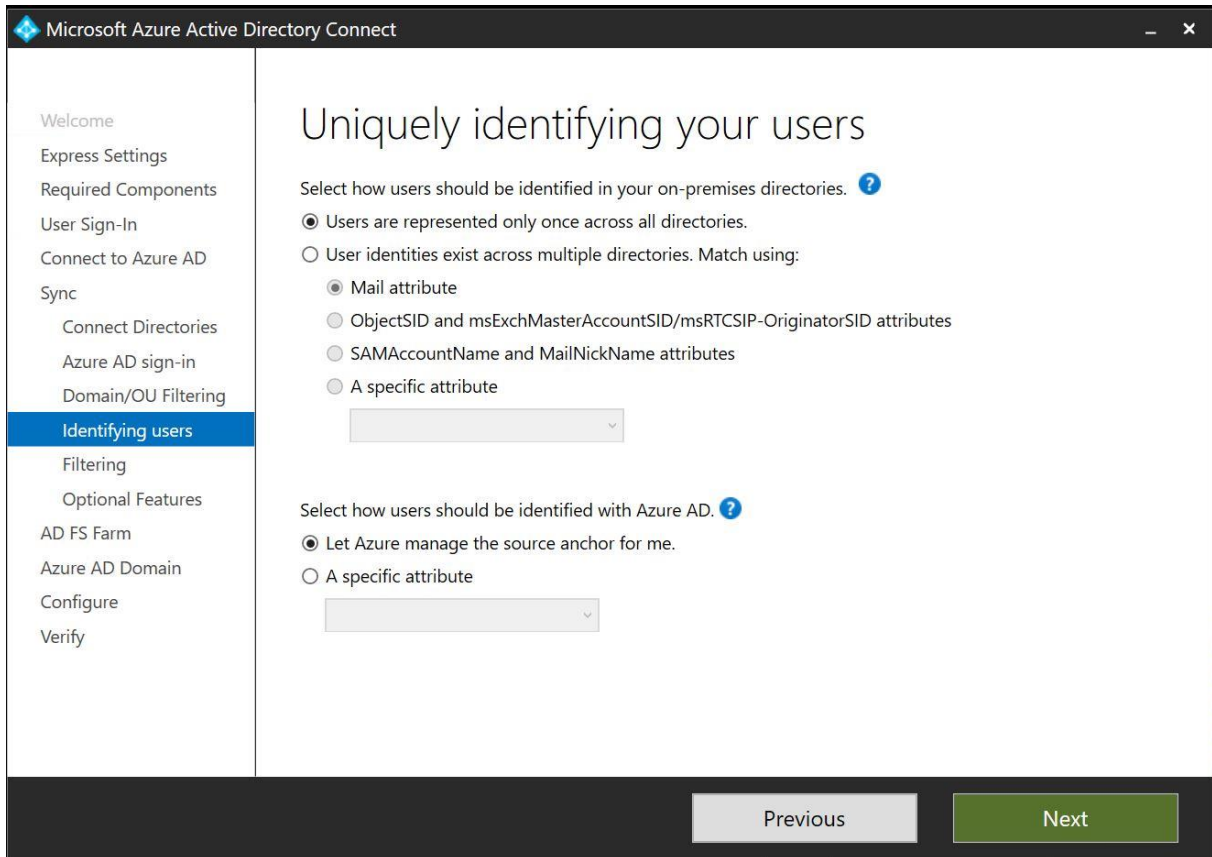
Step 9: Domain and OU filtering

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.



Step 10: Uniquely identifying your users

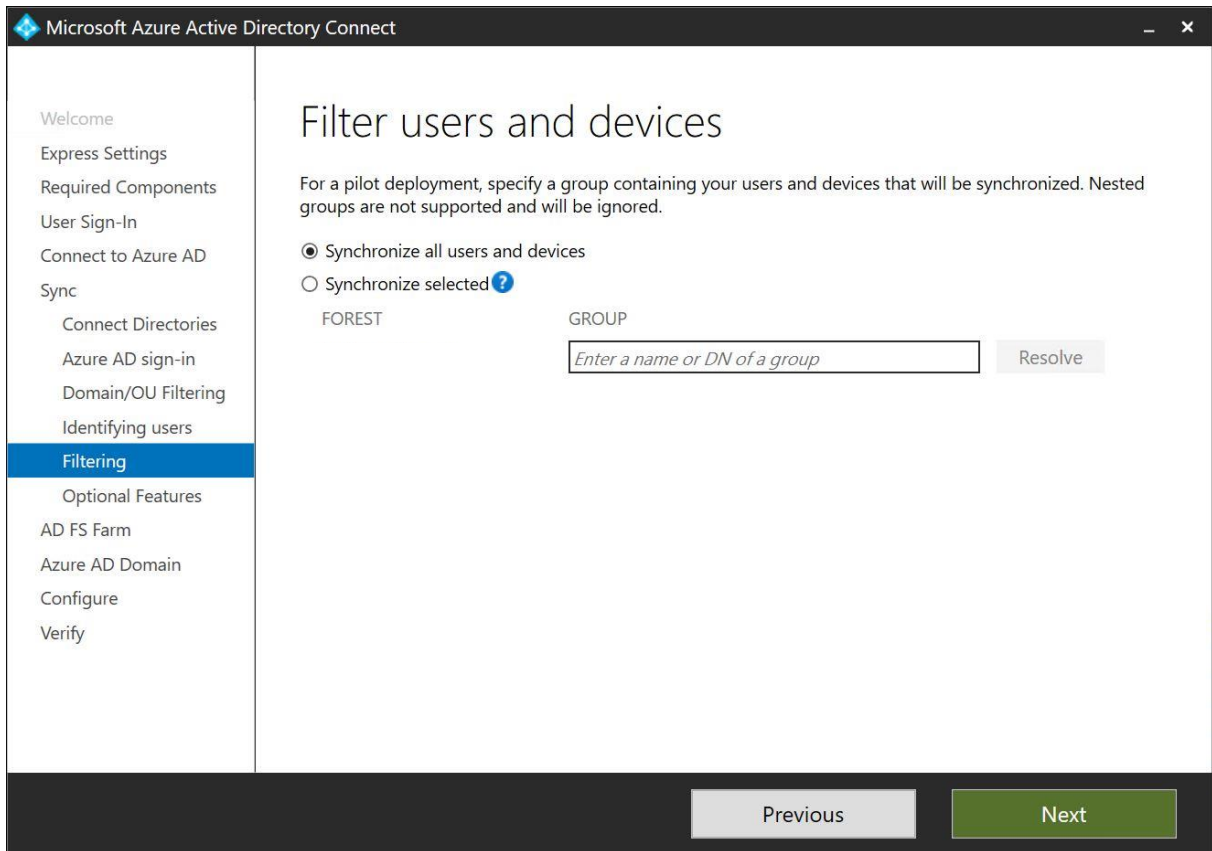
In this step, you can select if users are represented only once across all directories or not. If not, you are able to select an attribute by which the users are identified. You can also select the way users in Azure AD should be identified. You can only set this once for a user! ObjectGUID would be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



The screenshot shows the 'Uniquely identifying your users' configuration window in Microsoft Azure Active Directory Connect. The window title is 'Microsoft Azure Active Directory Connect'. 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** (highlighted), Filtering, Optional Features, AD FS Farm, Azure AD Domain, Configure, and Verify. The main content area is titled 'Uniquely identifying your users' and contains two sections. The first section is 'Select how users should be identified in your on-premises directories.' with a help icon. It has two radio button options: 'Users are represented only once across all directories.' (selected) and 'User identities exist across multiple directories. Match using:'. The second option has four sub-options: 'Mail attribute' (selected), 'ObjectSID and msExchMasterAccountSID/msRTCSIP-OriginatorSID attributes', 'SAMAccountName and MailNickName attributes', and 'A specific attribute'. Below these is a dropdown menu. The second section is 'Select how users should be identified with Azure AD.' with a help icon. It has two radio button options: 'Let Azure manage the source anchor for me.' (selected) and 'A specific attribute'. Below this is another dropdown menu. At the bottom of the window are two buttons: 'Previous' and 'Next'.

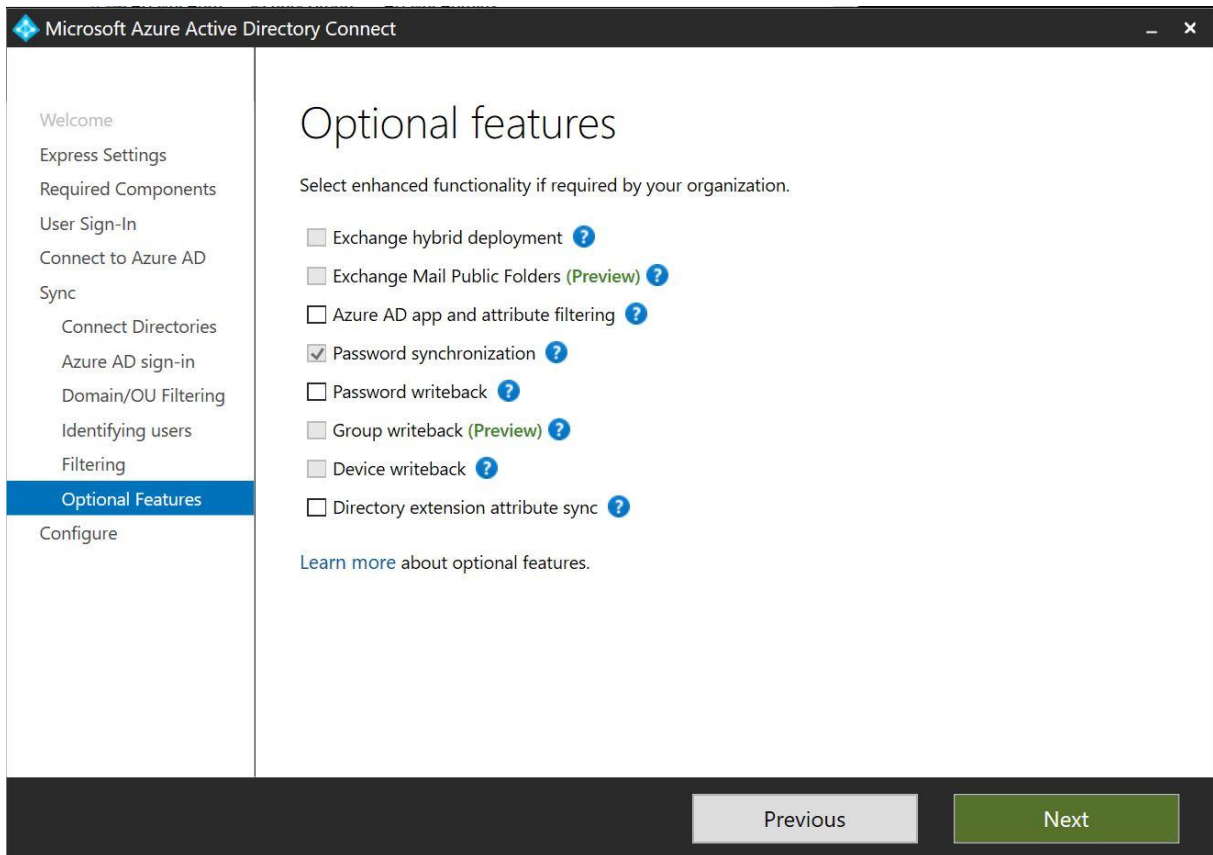
Step 11: Filter users and devices

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.



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.



The screenshot shows the 'Optional features' configuration window in Microsoft Azure Active Directory Connect. The window title is 'Microsoft Azure Active Directory Connect'. On the left, a navigation pane lists various steps: 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** (highlighted), and Configure. The main content area is titled 'Optional features' and contains the instruction: 'Select enhanced functionality if required by your organization.' Below this, there are seven checkboxes with corresponding feature names and help icons (question marks):

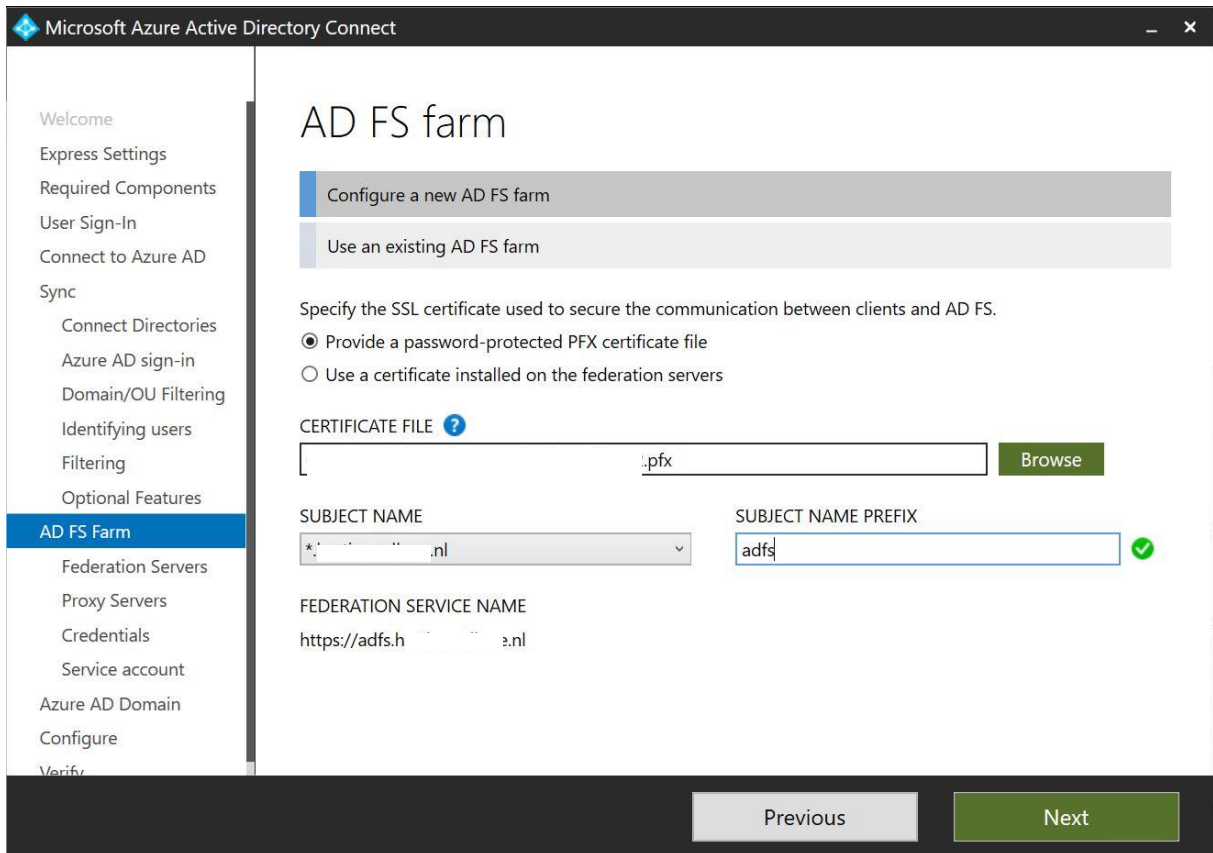
- Exchange hybrid deployment ?
- Exchange Mail Public Folders (Preview) ?
- Azure AD app and attribute filtering ?
- Password synchronization ?
- Password writeback ?
- Group writeback (Preview) ?
- Device writeback ?
- Directory extension attribute sync ?

At the bottom of the main content area, there is a link: [Learn more about optional features.](#)

At the bottom of the window, there are two buttons: 'Previous' (disabled) and 'Next' (active).

Step 13: AD FS farm

In this step, you can let AAD Connect configure your AD FS farm. You will need a certificate in *.pfx format and fill in the subject name prefix.

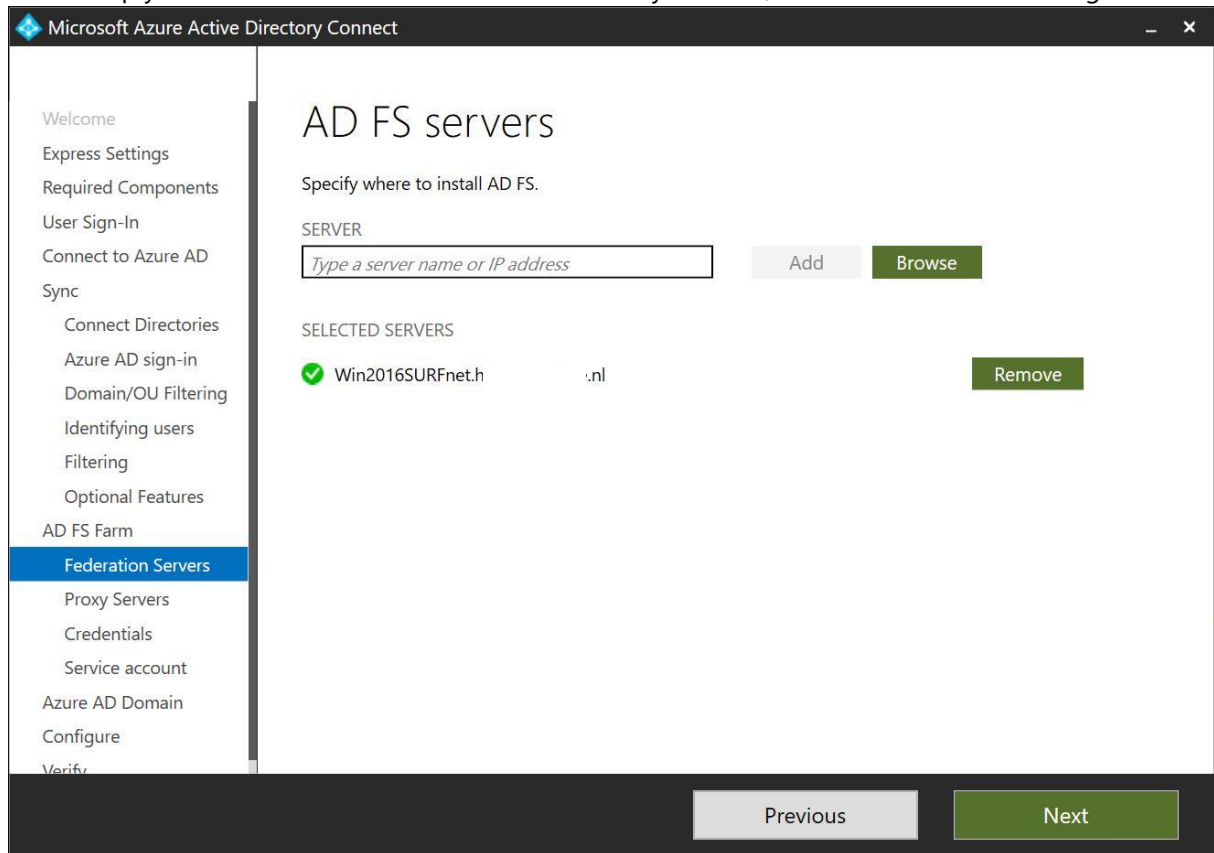


The screenshot shows the 'AD FS farm' configuration window in Microsoft Azure Active Directory Connect. The window title is 'Microsoft Azure Active Directory Connect'. The left sidebar contains a navigation menu with the following items: Welcome, Express Settings, Required Components, User Sign-In, Connect to Azure AD, Sync, Connect Directories, Azure AD sign-in, Domain/OU Filtering, Identifying users, Filtering, Optional Features, AD FS Farm (highlighted), Federation Servers, Proxy Servers, Credentials, Service account, Azure AD Domain, Configure, and Verify.

The main content area is titled 'AD FS farm' and contains two options: 'Configure a new AD FS farm' (selected) and 'Use an existing AD FS farm'. Below these options, there is a section for specifying the SSL certificate used to secure the communication between clients and AD FS. The options are: 'Provide a password-protected PFX certificate file' (selected) and 'Use a certificate installed on the federation servers'. The 'CERTIFICATE FILE' field is empty, with a 'Browse' button next to it. The 'SUBJECT NAME' field is a dropdown menu showing '*.nl'. The 'SUBJECT NAME PREFIX' field contains 'adfs' and has a green checkmark next to it. The 'FEDERATION SERVICE NAME' field contains 'https://adfs.h.nl'. At the bottom of the window, there are 'Previous' and 'Next' buttons.

Step 14: AD FS servers

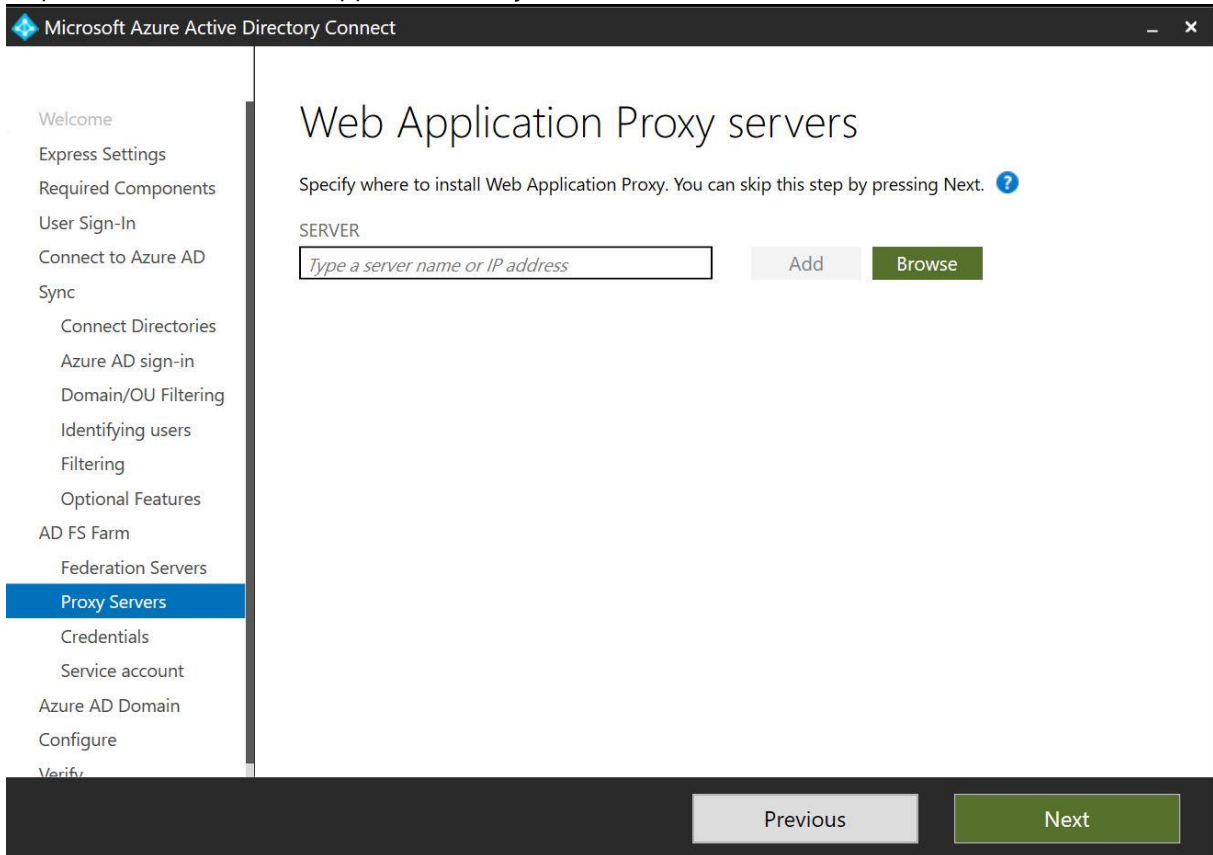
In this step you will have to select the AD FS servers in your farm, so AAD Connect can configure them.



The screenshot shows the 'AD FS servers' configuration window in Microsoft Azure Active Directory Connect. The window title is 'Microsoft Azure Active Directory Connect'. On the left is a navigation pane 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, AD FS Farm (expanded), Federation Servers (selected), Proxy Servers, Credentials, Service account, Azure AD Domain, Configure, and Verify. The main area is titled 'AD FS servers' and contains the instruction 'Specify where to install AD FS.' Below this is a 'SERVER' section with a text input field containing the placeholder 'Type a server name or IP address', an 'Add' button, and a 'Browse' button. Underneath is a 'SELECTED SERVERS' section with a table containing one entry: a green checkmark, 'Win2016SURFnet.h', and '.nl', with a 'Remove' button to its right. At the bottom of the window are 'Previous' and 'Next' buttons.

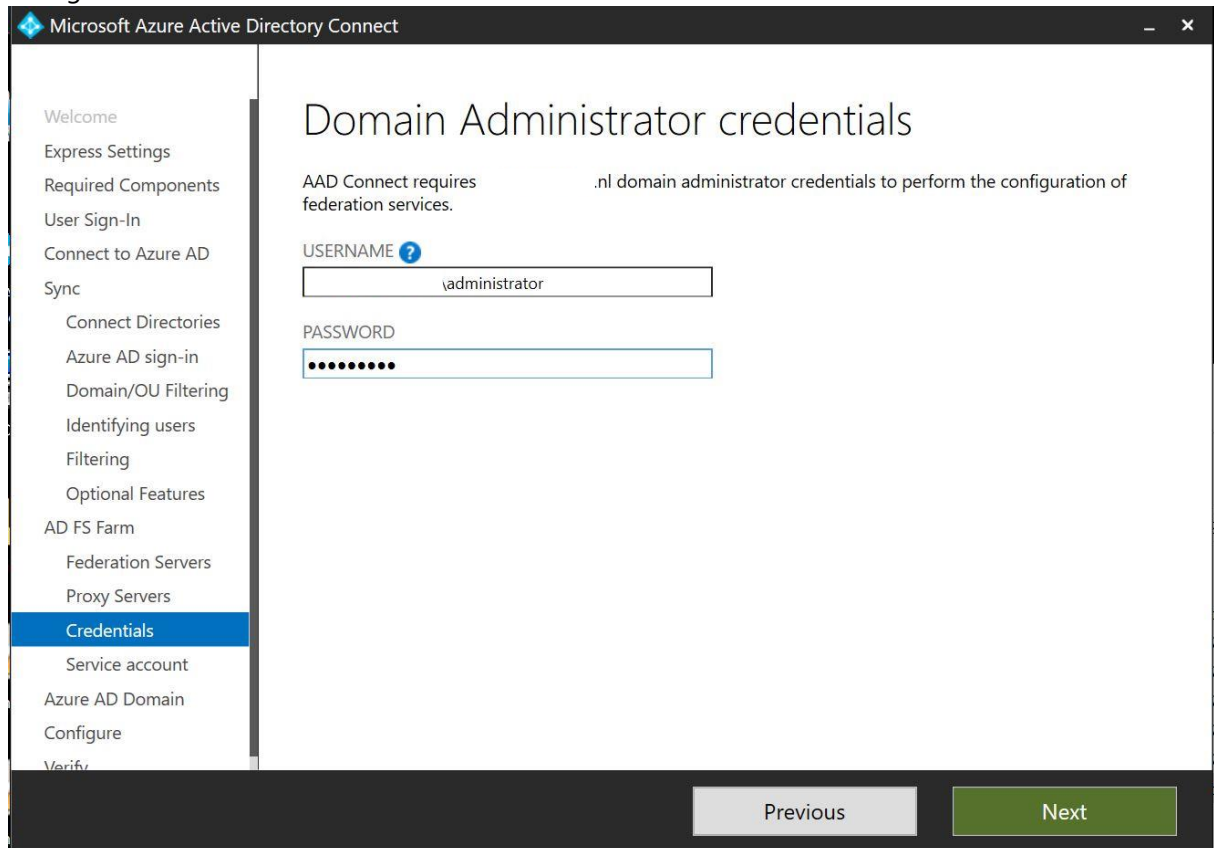
Step 15: Web Application Proxy servers

In this step, you will be able to select the Web Applications servers in your farm. This is an optional step. We didn't use a Web Application Proxy server.



Step 16: Domain Administrator credentials

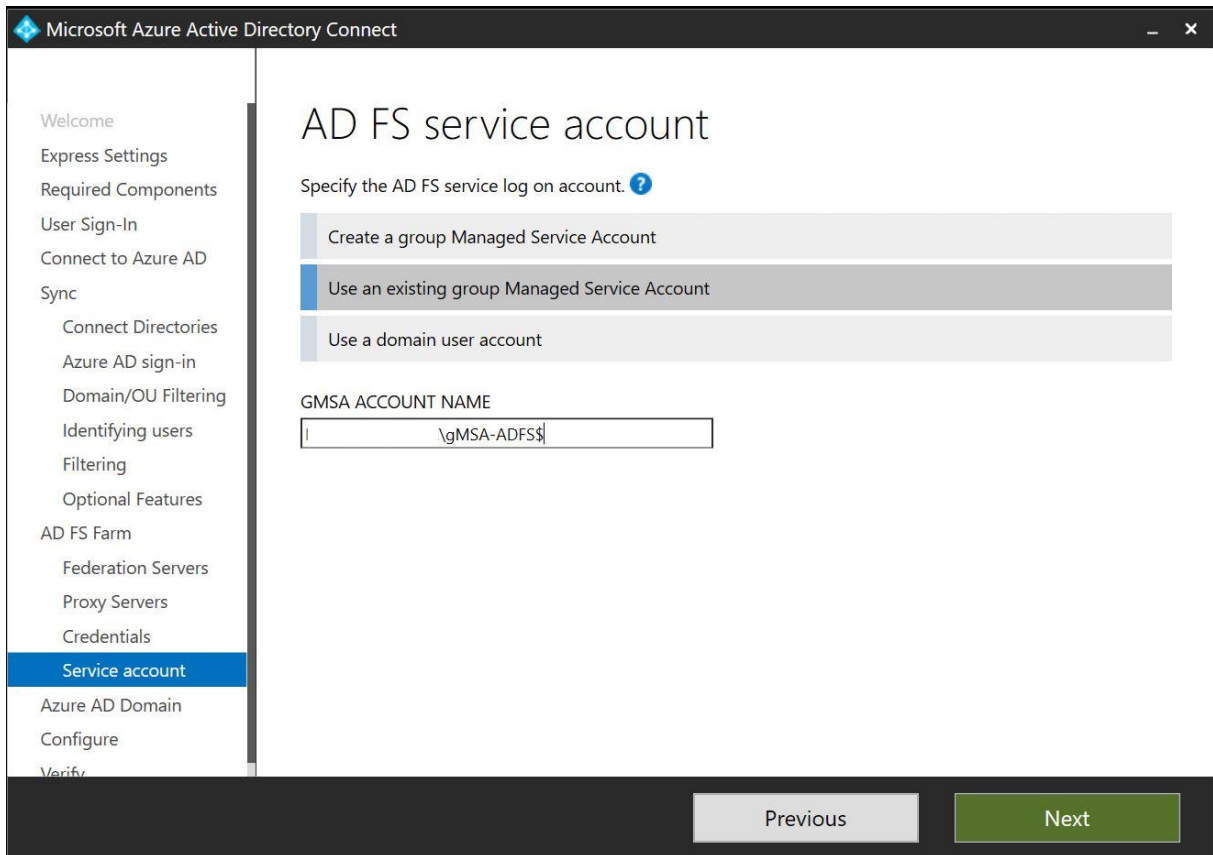
In this step, you will have to provide the domain administrator credentials to perform the AD FS configuration.



The screenshot shows the 'Microsoft Azure Active Directory Connect' application window. The title bar reads 'Microsoft Azure Active Directory Connect'. On the left is a navigation pane 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, AD FS Farm, Federation Servers, Proxy Servers, **Credentials** (highlighted), Service account, Azure AD Domain, Configure, and Verify. The main content area is titled 'Domain Administrator credentials'. Below the title, it states: 'AAD Connect requires .nl domain administrator credentials to perform the configuration of federation services.' There are two input fields: 'USERNAME' with a help icon and a question mark, containing the text '\administrator', and 'PASSWORD' which is masked with ten black dots. At the bottom of the window are two buttons: 'Previous' (disabled) and 'Next' (active).

Step 17: AD FS service account

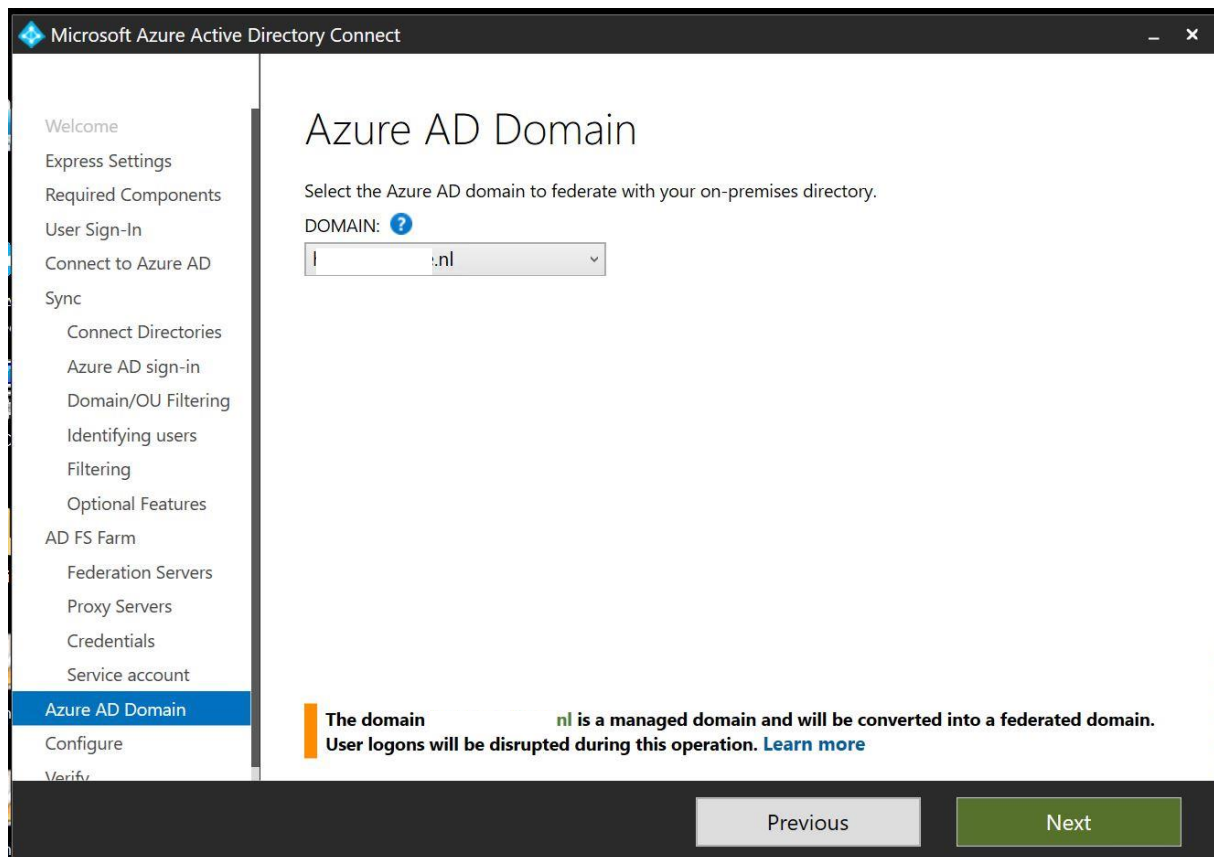
When you are going through the installation step on the [SURFnet wiki](#), you've just created a group Managed Service Account. You will have to enter an existing service account, or let AAD Connect create one.



The screenshot shows the 'Microsoft Azure Active Directory Connect' application window. The title bar reads 'Microsoft Azure Active Directory Connect'. On the left is a navigation pane 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, AD FS Farm, Federation Servers, Proxy Servers, Credentials, Service account (highlighted in blue), Azure AD Domain, Configure, and Verify. The main content area is titled 'AD FS service account' and contains the instruction 'Specify the AD FS service log on account. ?'. Below this are three radio button options: 'Create a group Managed Service Account', 'Use an existing group Managed Service Account' (which is selected), and 'Use a domain user account'. Underneath is a text box labeled 'GMSA ACCOUNT NAME' containing the text '\gMSA-ADFS\$'. At the bottom of the window are two buttons: 'Previous' and 'Next'.

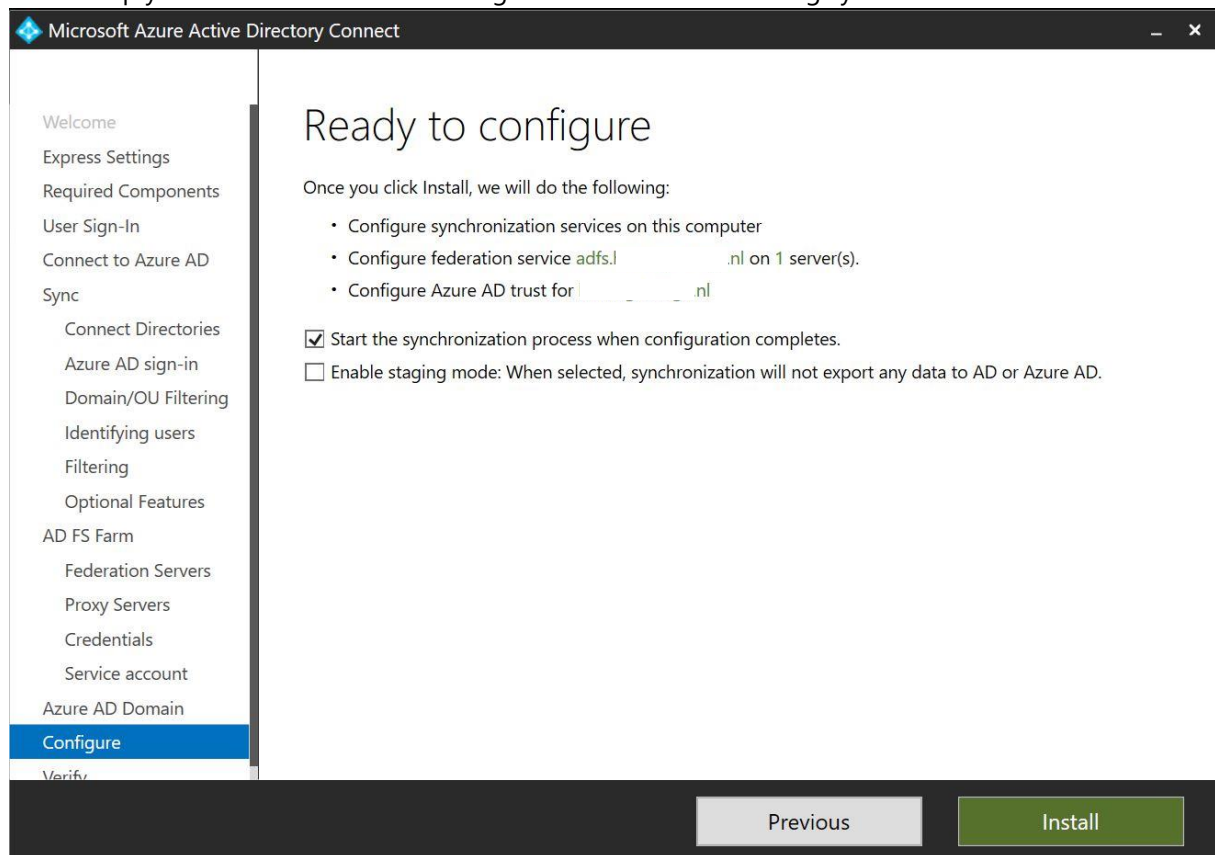
Step 18: Azure AD Domain

You can select the Azure AD Domain you want to federate with your (on-premises) directory. You have to run this step for all domains you want to federate.



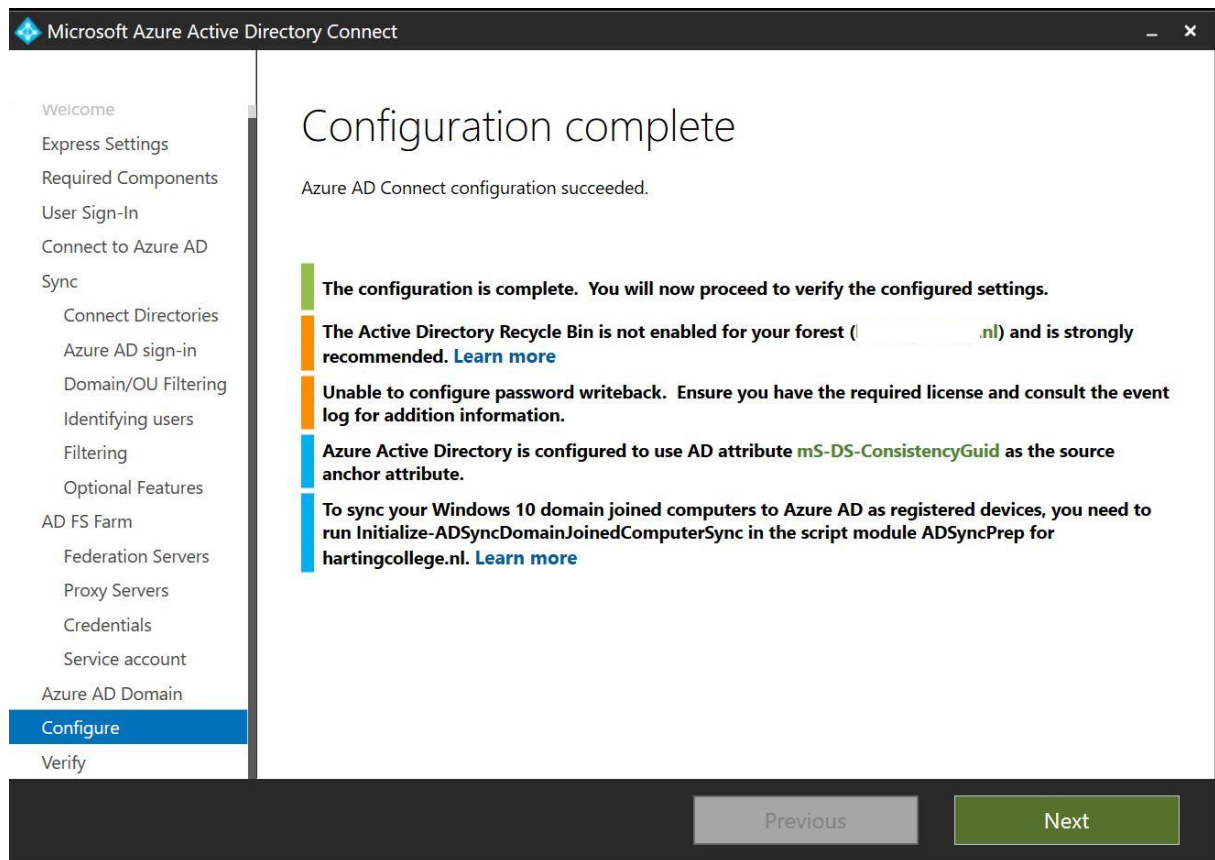
Step 19: Ready to configure

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



Step 20: 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.



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
 Federation Servers
 Proxy Servers
 Credentials
 Service account
Azure AD Domain
Configure
Verify

Configuration complete

Azure AD Connect configuration succeeded.

- The configuration is complete. You will now proceed to verify the configured settings.**
- The Active Directory Recycle Bin is not enabled for your forest (hartingcollege.nl) and is strongly recommended. [Learn more](#)**
- Unable to configure password writeback. Ensure you have the required license and consult the event log for addition information.**
- 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 [hartingcollege.nl](#). [Learn more](#)**

Previous Next

Step 21: Verify federation configuration

The last step is the verification step for AD FS. If you've created a DNS record for your AD FS server(s), you will be able to test your setup.

