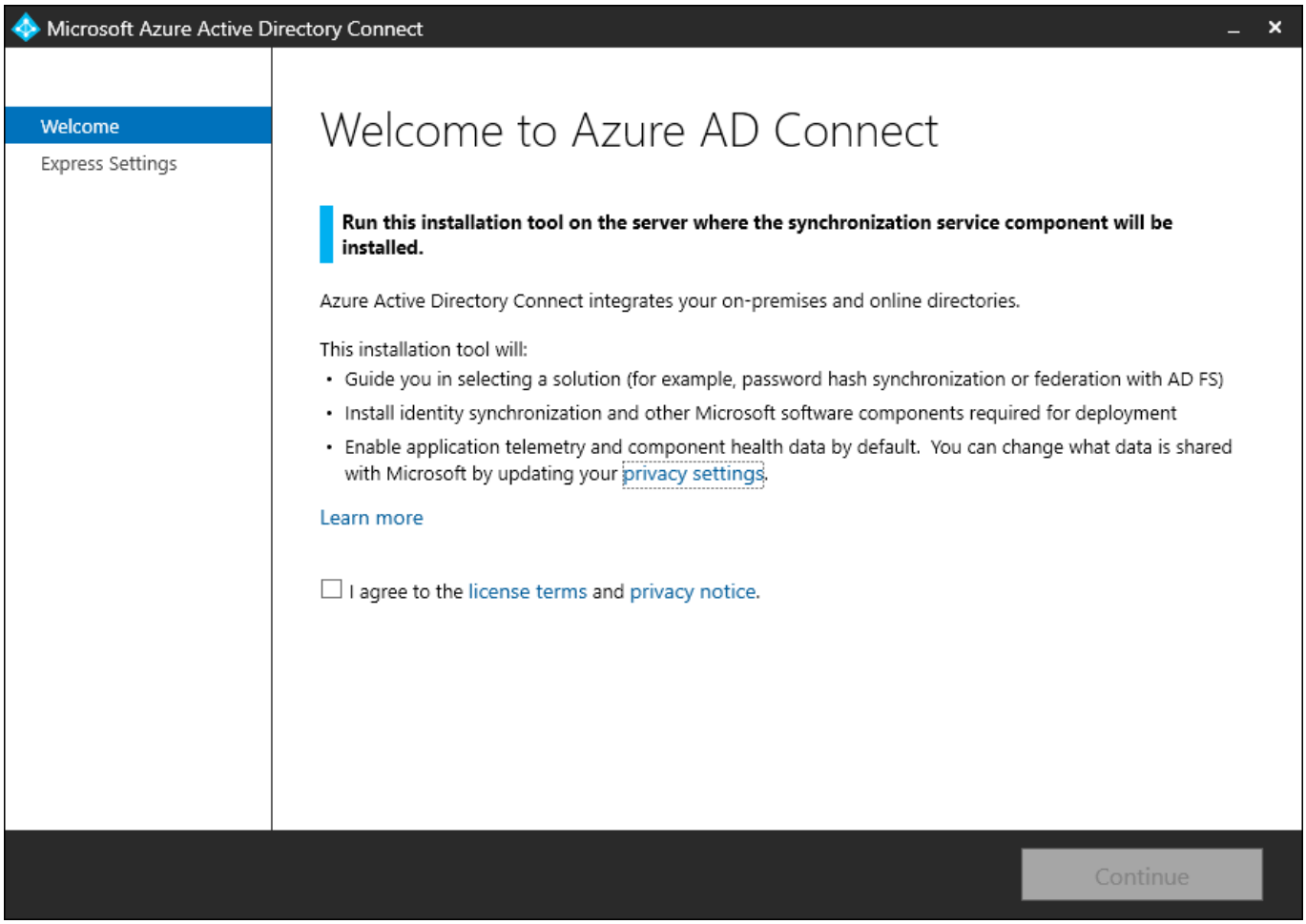
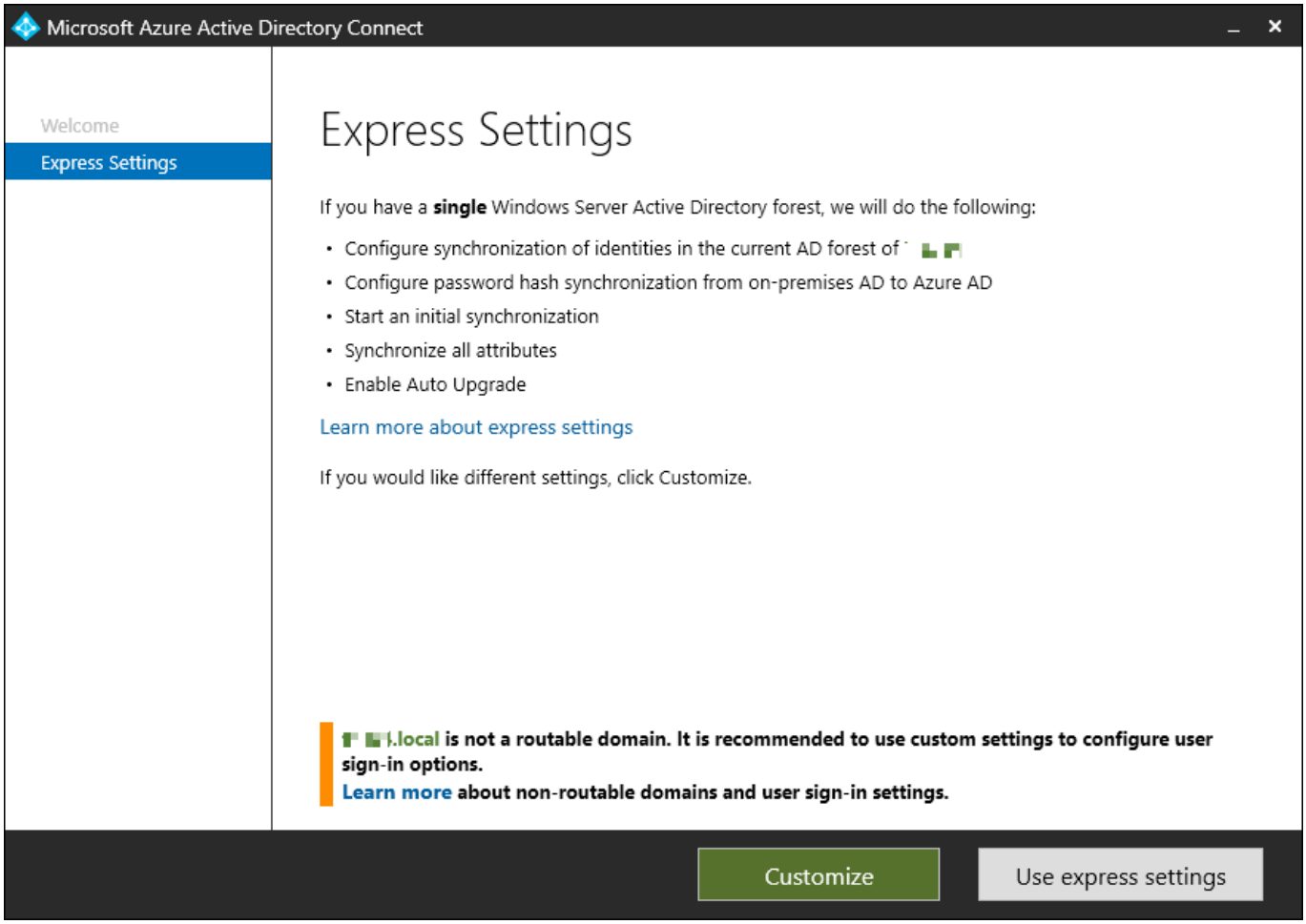
Azure-AD-Connect (AD-Hybridmodus)

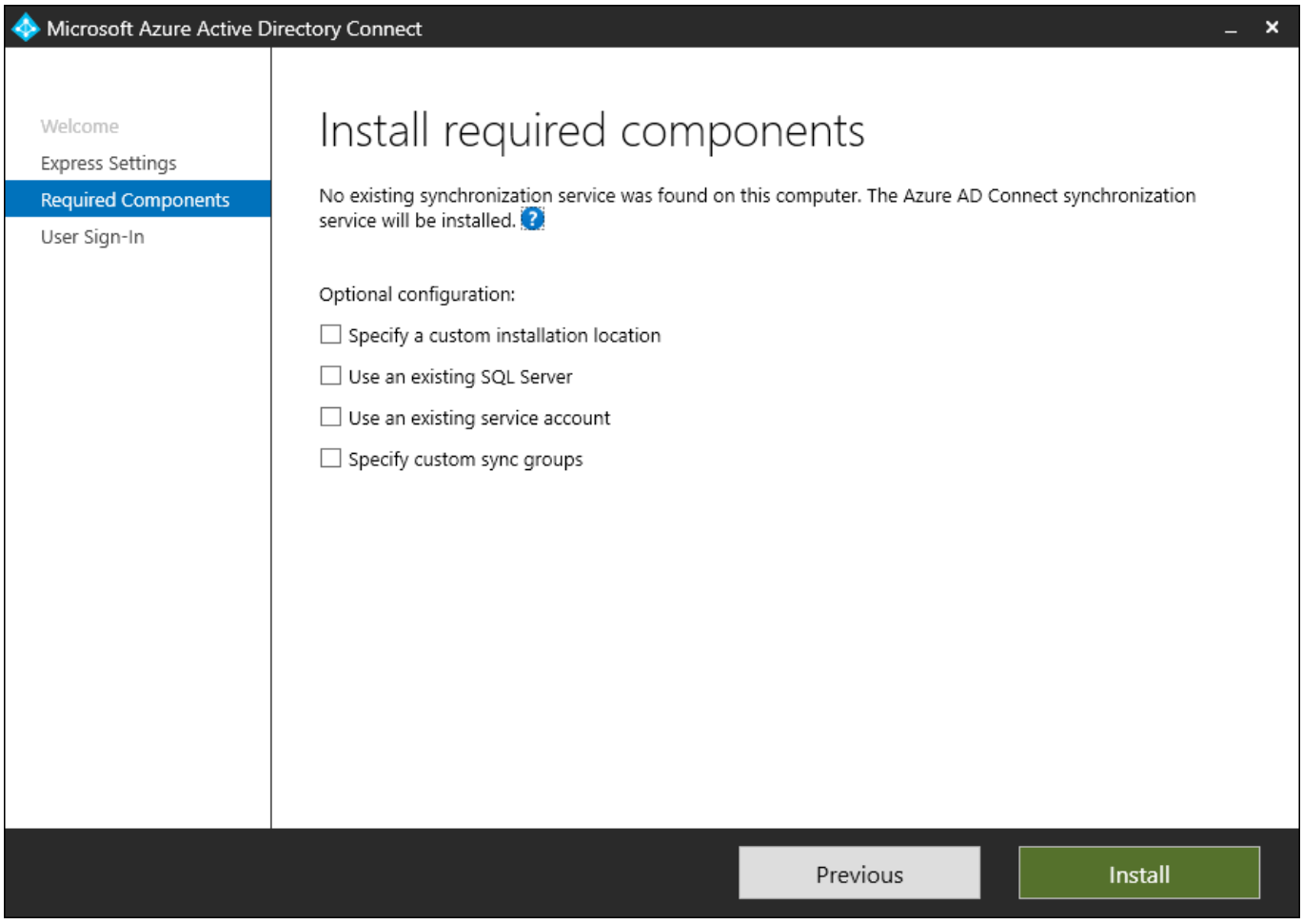
Vorbereitende Maßnahmen

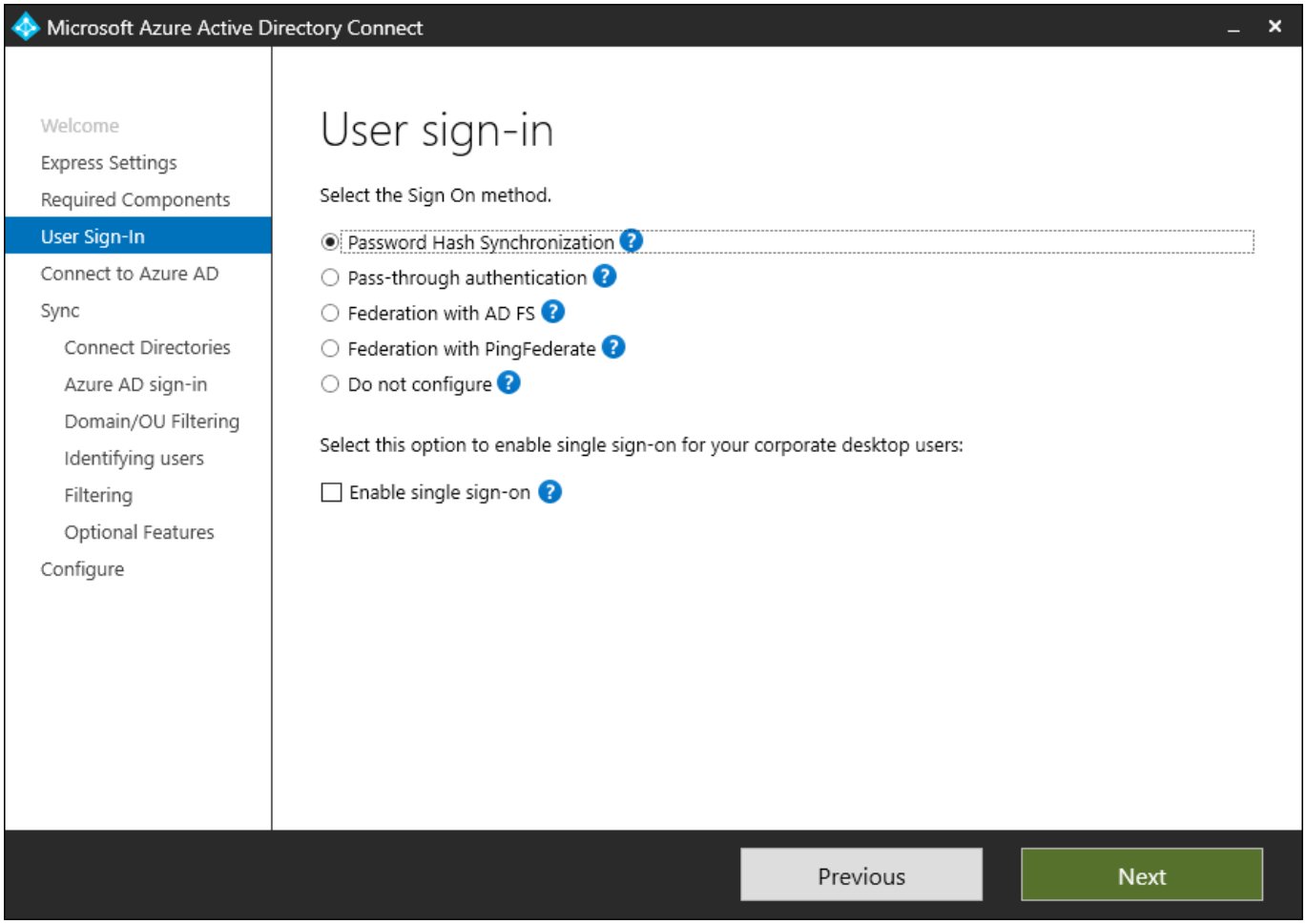
- Login-Domain mit Tenant verbinden und DNS-Einträge für alle zu nutzenden Dienste hinterlegen
- IDfix-Tool laufen lassen und empfohlene Maßnahmen durchführen
  https://github.com/microsoft/idfix/blob/master/publish/setup.exe

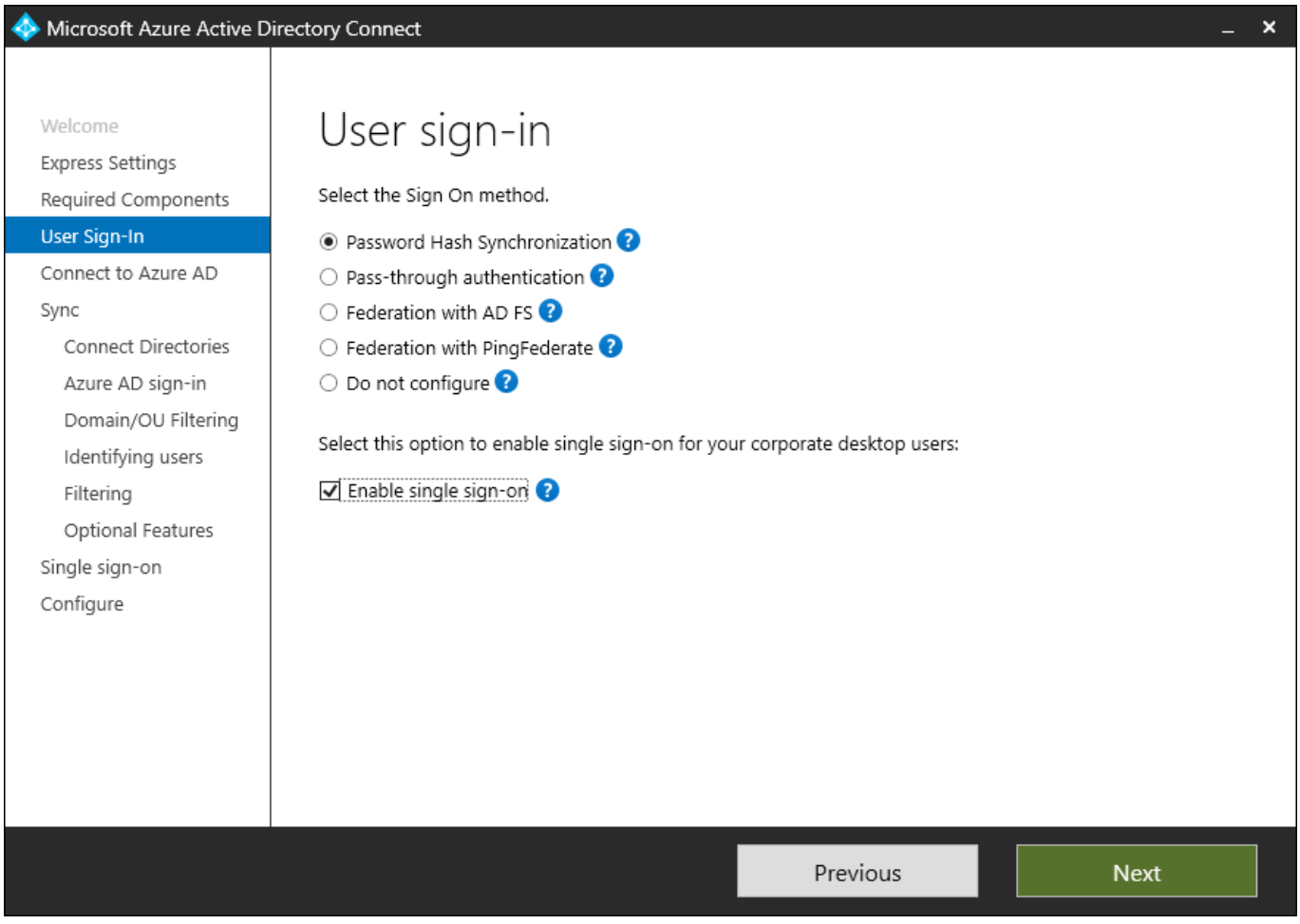
AAD-Connect Installation

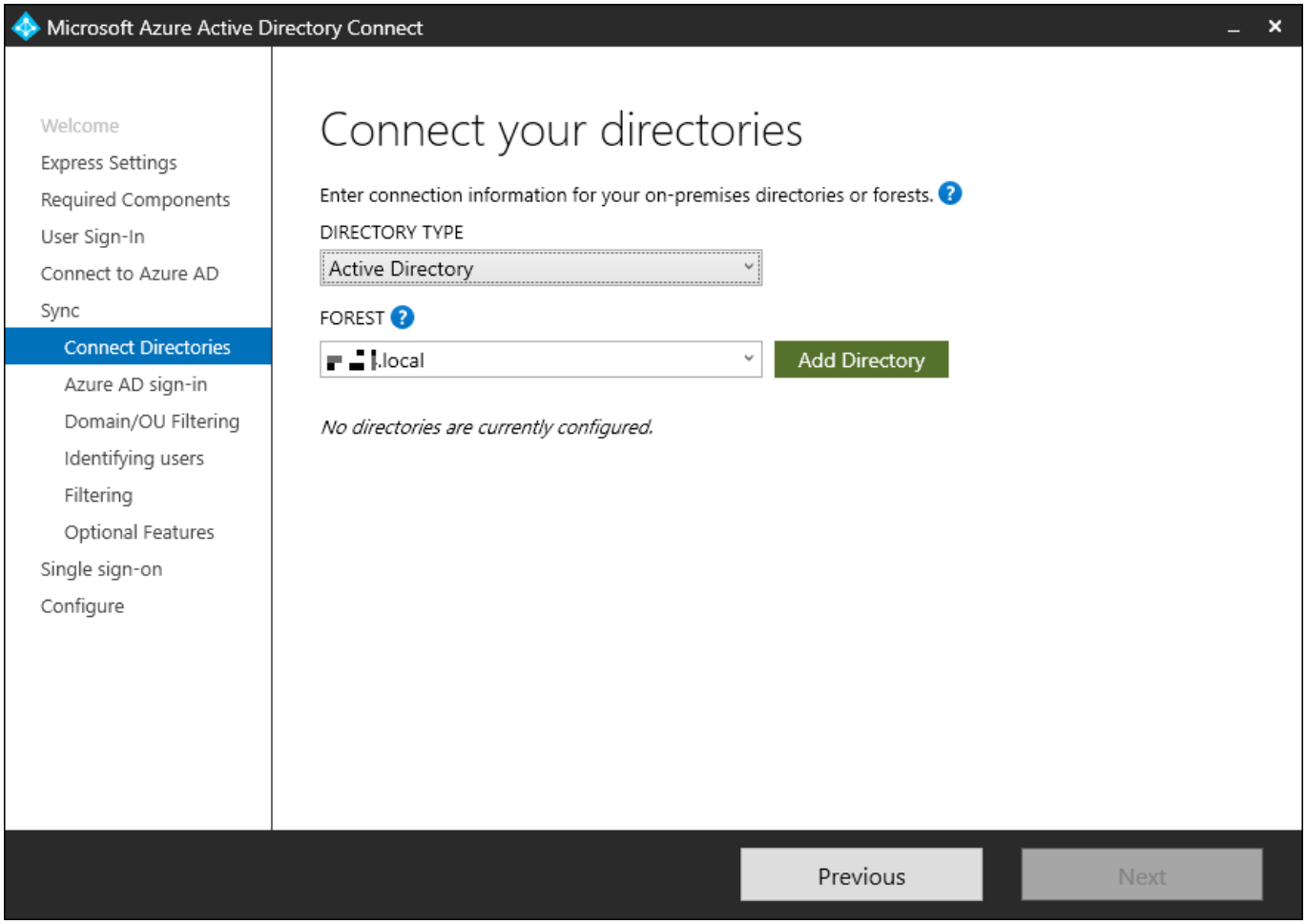


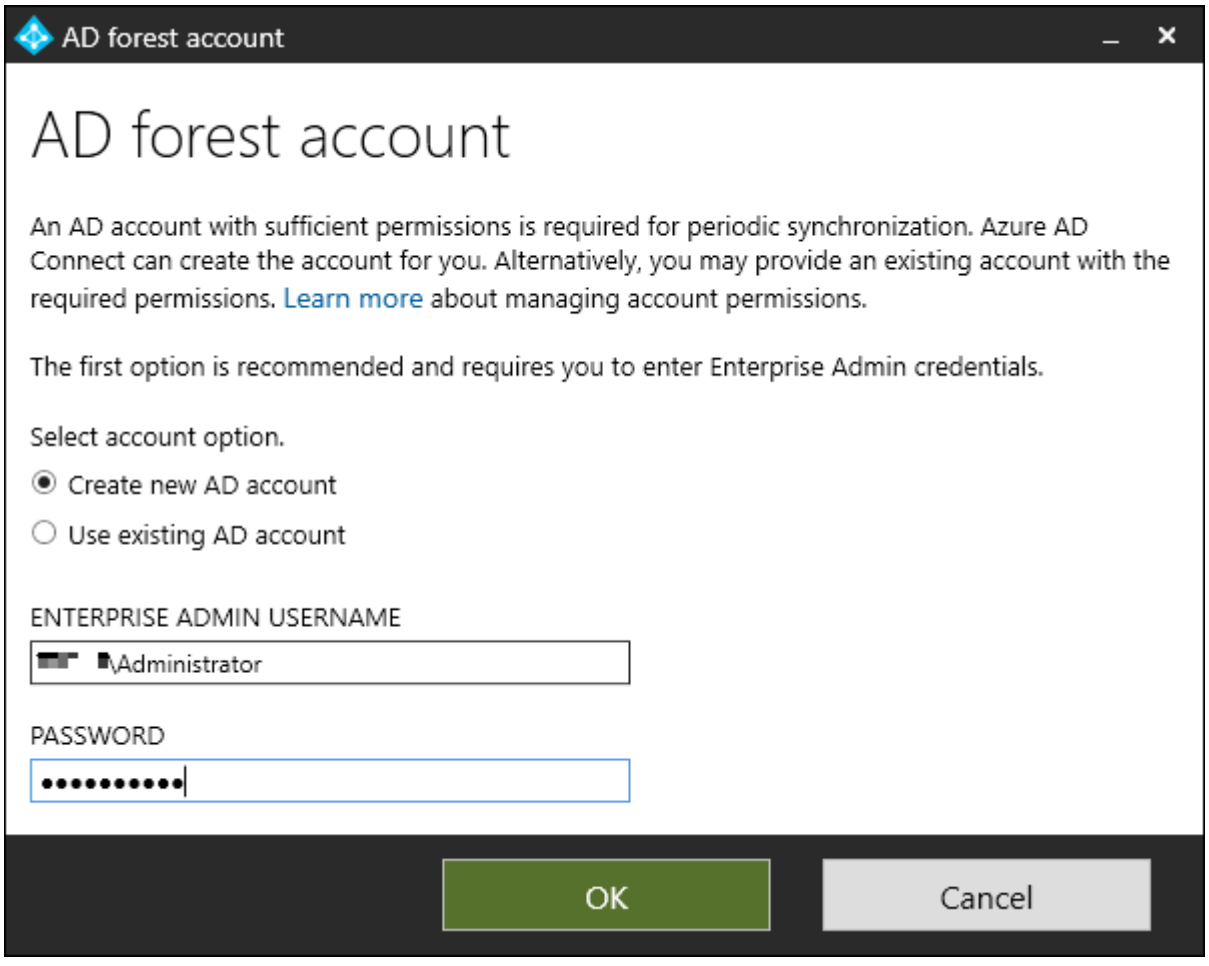

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Express Settings
If you have a single Windows Server Active Directory forest, we will do the following:
Configure synchronization of identities in the current AD forest of
Configure password hash synchronization from on-premises AD to 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.
.local is not a routable domain. It is recommended to use custom settings to configure user sign-in options.
Learn more about non-routable domains and user sign-in settings.
Customize
Use express settings

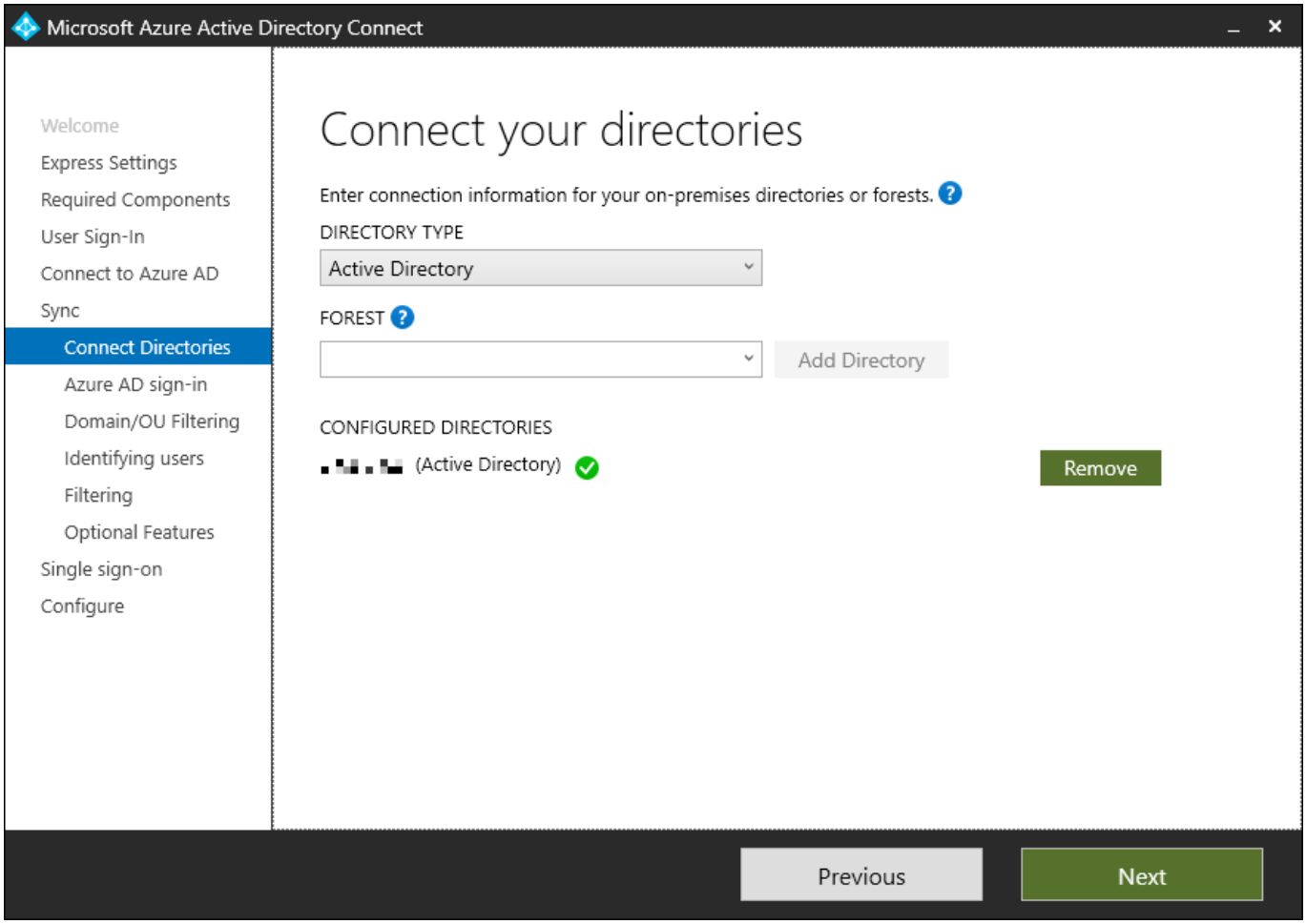

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Install required components
No existing synchronization service was found on this computer. The Azure AD Connect synchronization service will be installed.
Optional configuration:
Specify a custom installation location
Use an existing SQL Server
Use an existing service account
Specify custom sync groups
Previous
Install

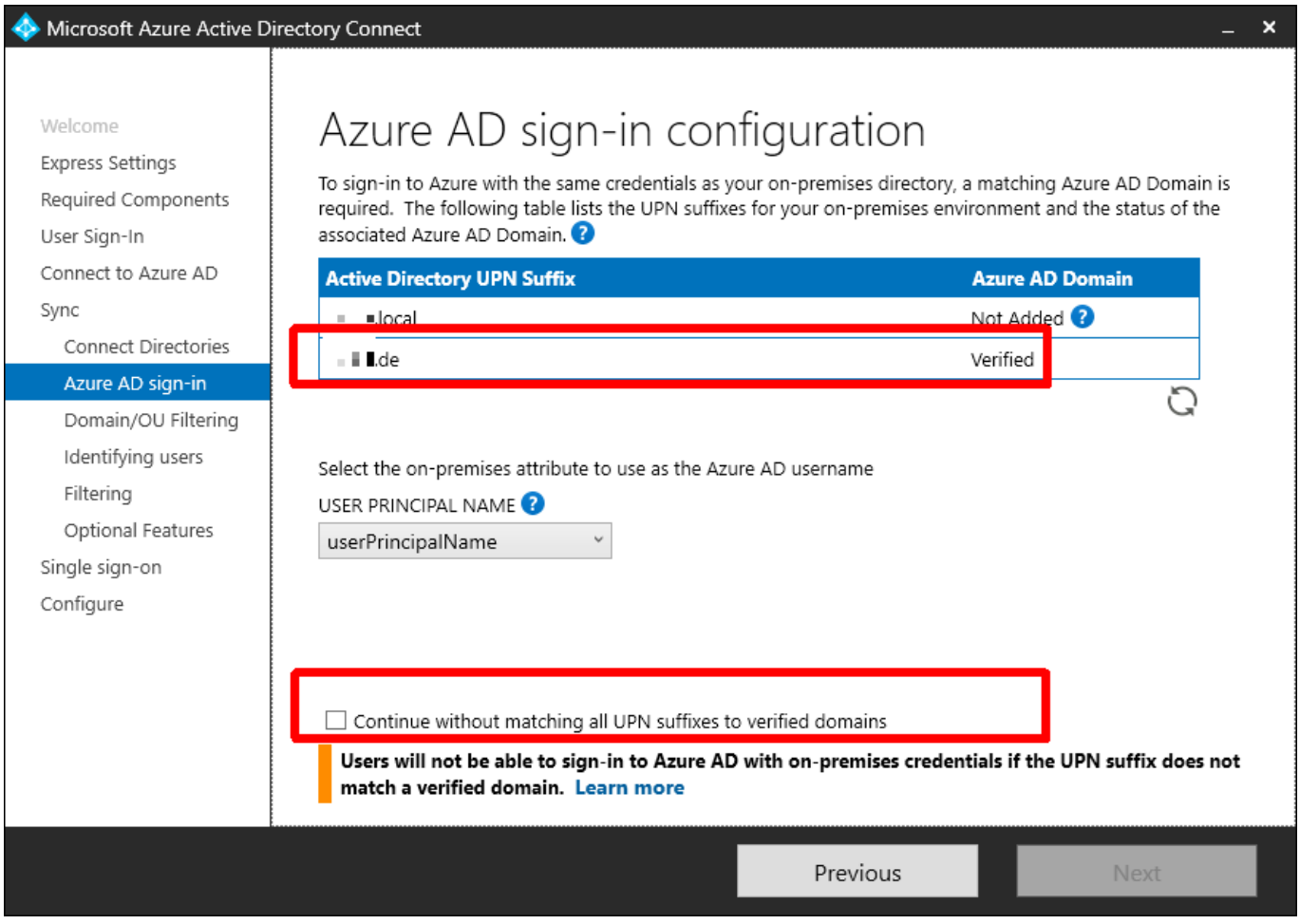

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Configure
User sign-in
Select the Sign On method.
Password Hash Synchronization
Pass-through authentication
Federation with AD FS
Federation with PingFederate
Do not configure
Select this option to enable single sign-on for your corporate desktop users:
Enable single sign-on
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
User sign-in
Select the Sign On method.
Password Hash Synchronization
Pass-through authentication
Federation with AD FS
Federation with PingFederate
Do not configure
Select this option to enable single sign-on for your corporate desktop users:
Enable single sign-on
Previous
Next

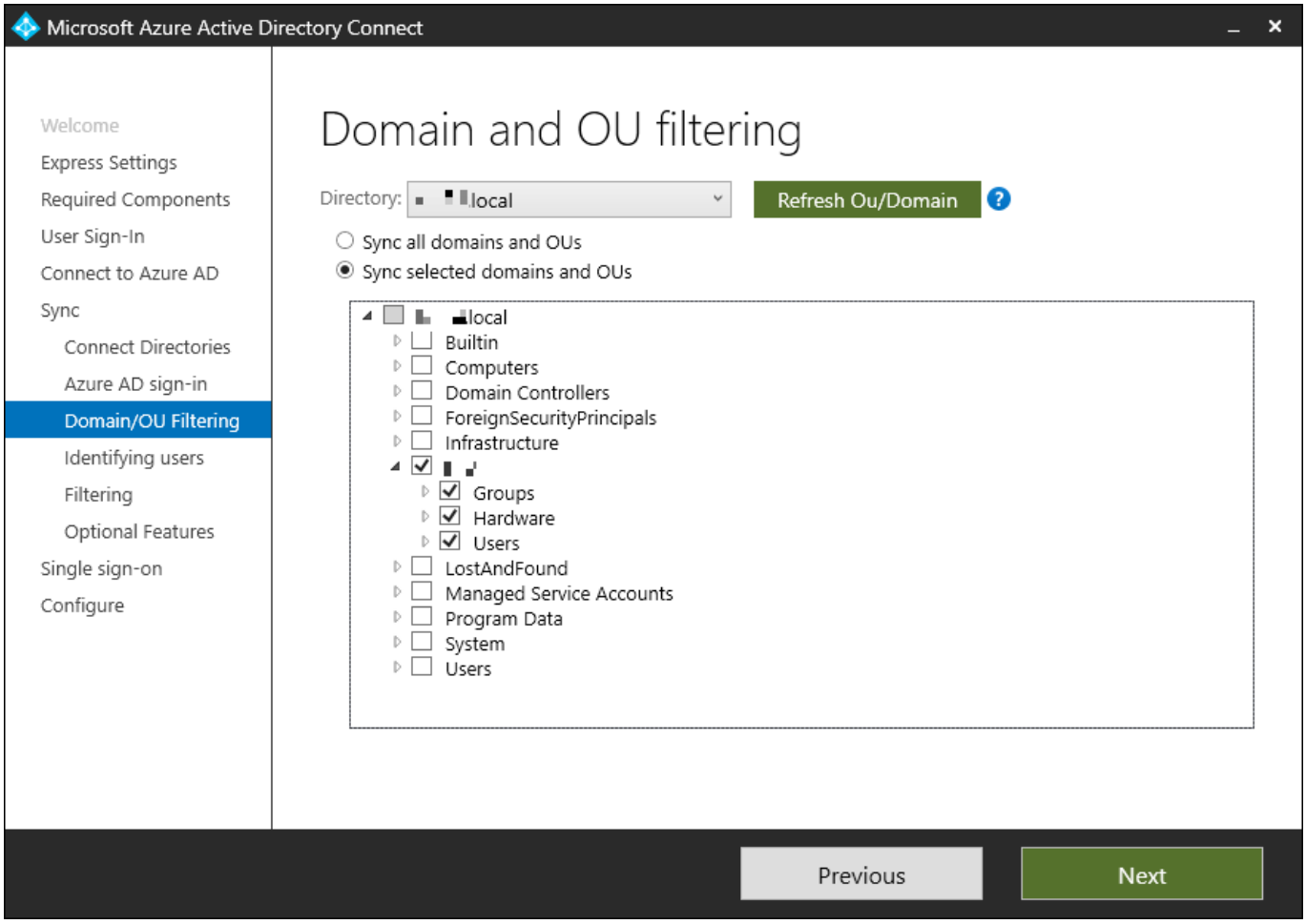

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Single sign-on
Configure
Connect your directories
Enter connection information for your on-premises directories or forests.
DIRECTORY TYPE
Active Directory
FOREST
.local
Add Directory
No directories are currently configured.
Previous
Next

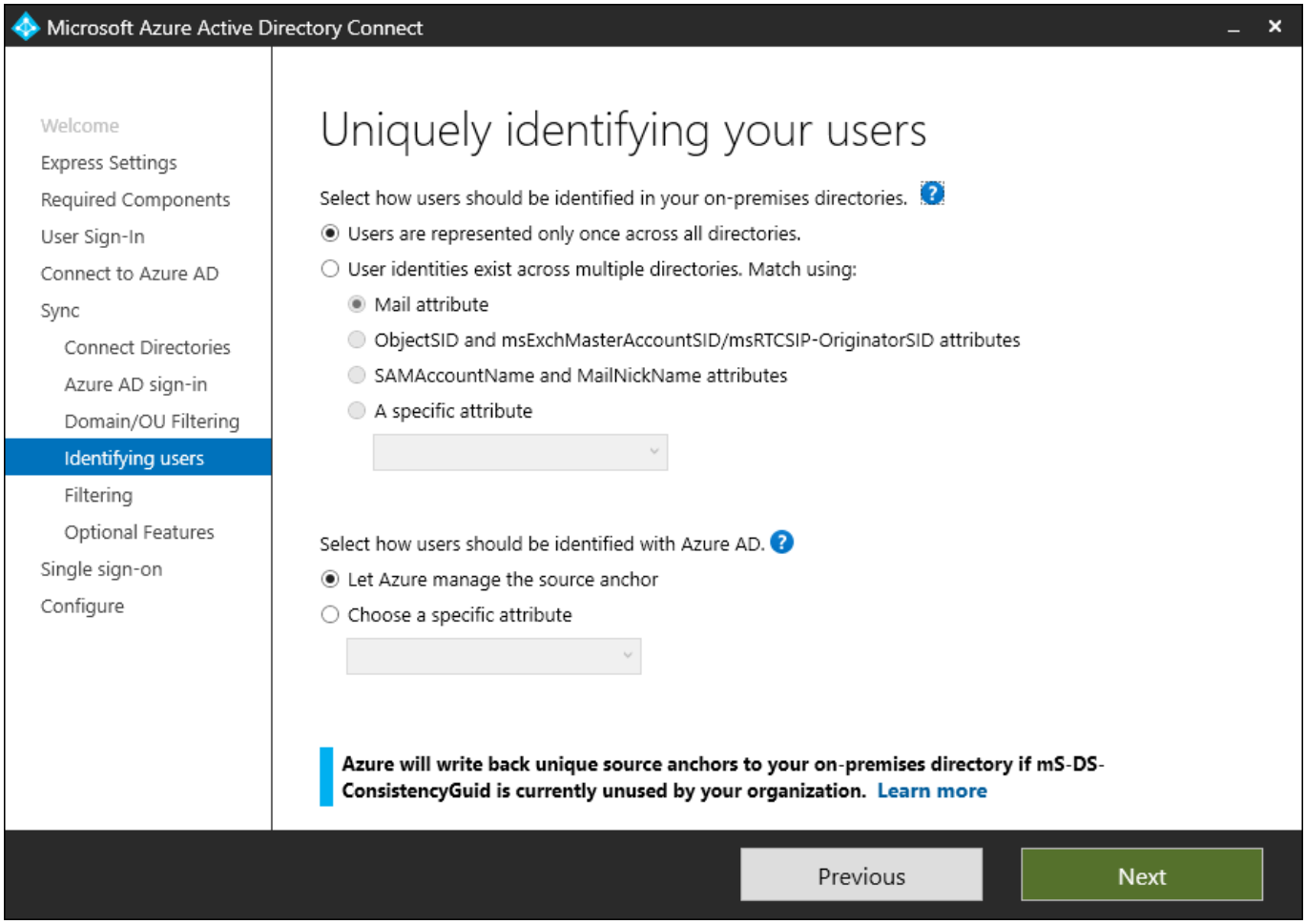

AD forest account
AD forest account
An AD account with sufficient permissions is required for periodic synchronization. Azure AD Connect can create the account for you. Alternatively, you may provide an existing account with the required permissions. Learn more about managing account permissions.
The 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
\Administrator
PASSWORD
OK
Cancel

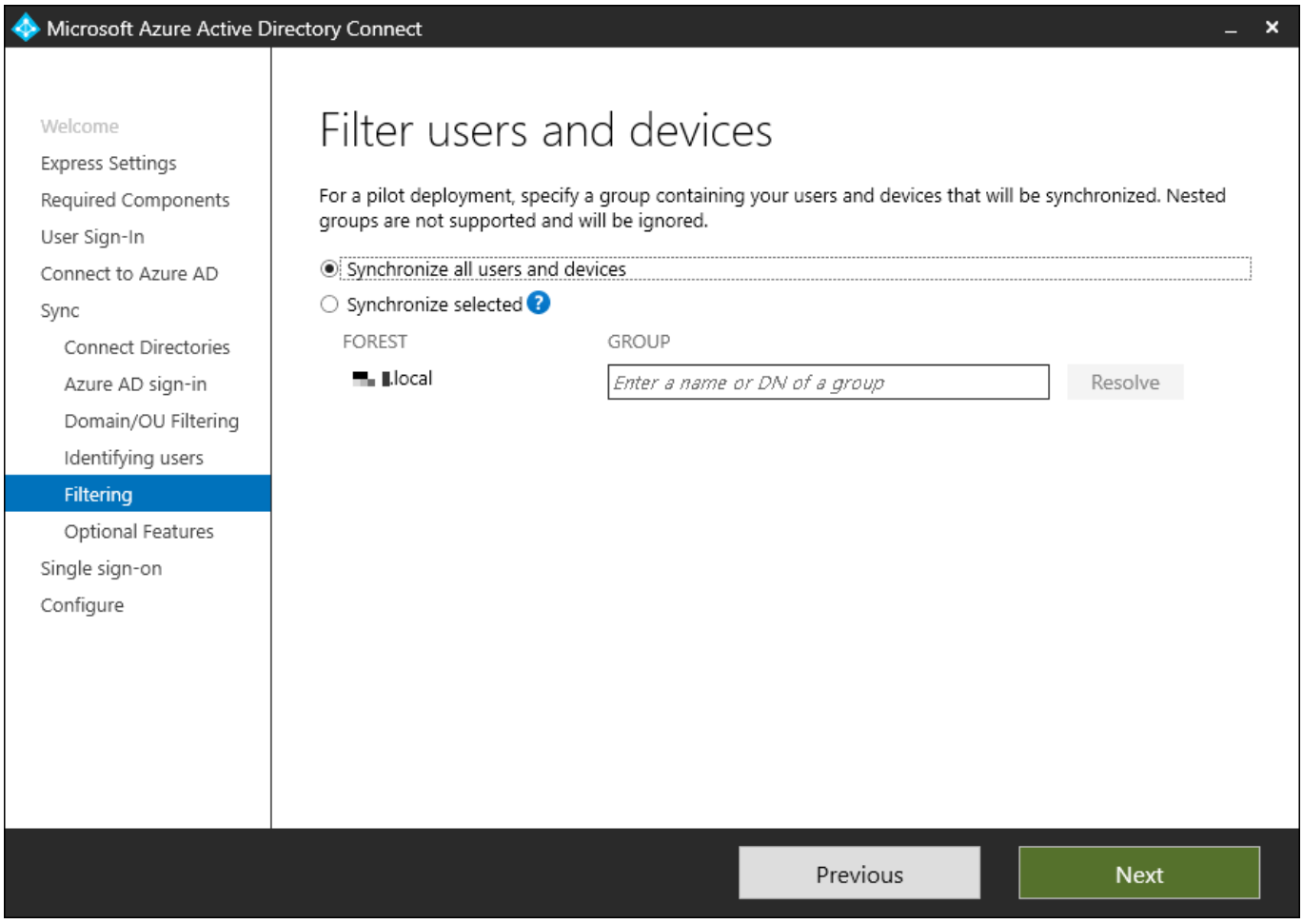

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Single sign-on
Configure
Connect your directories
Enter connection information for your on-premises directories or forests.
DIRECTORY TYPE
Active Directory
FOREST
Add Directory
CONFIGURED DIRECTORIES
(Active Directory)
Remove
Previous
Next

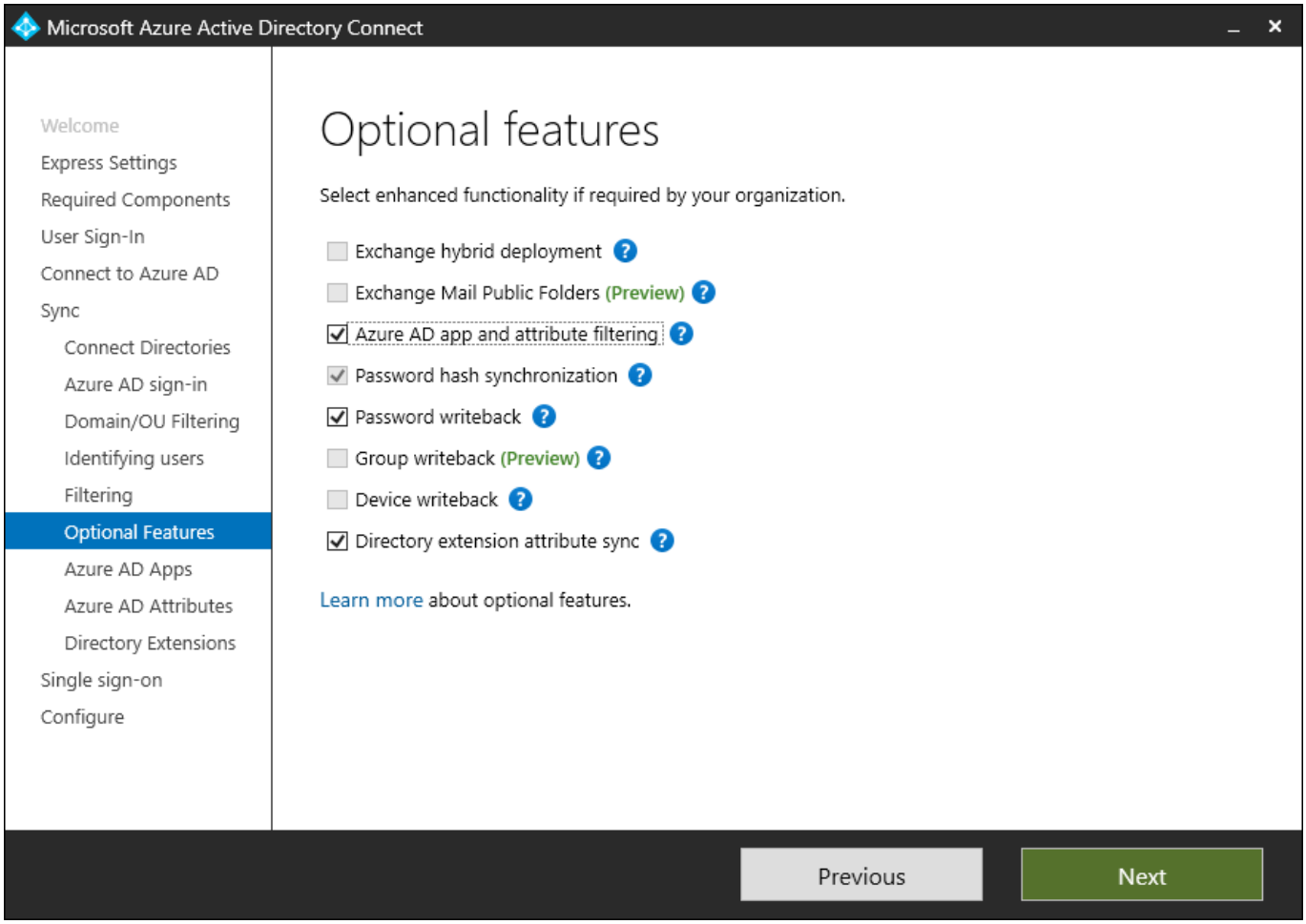

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Single sign-on
Configure
Azure AD sign-in configuration
To sign-in to Azure with the same credentials as your on-premises directory, a matching Azure AD Domain is required. The following table lists the UPN suffixes for your on-premises environment and the status of the associated Azure AD Domain.
Active Directory UPN Suffix
Azure AD Domain
.local
Not Added
.de
Verified
Select the on-premises attribute to use as the Azure AD username
USER PRINCIPAL NAME
userPrincipalName
Continue without matching all UPN suffixes to verified domains
Users will not be able to sign-in to Azure AD with on-premises credentials if the UPN suffix does not match a verified domain. Learn more
Previous
Next

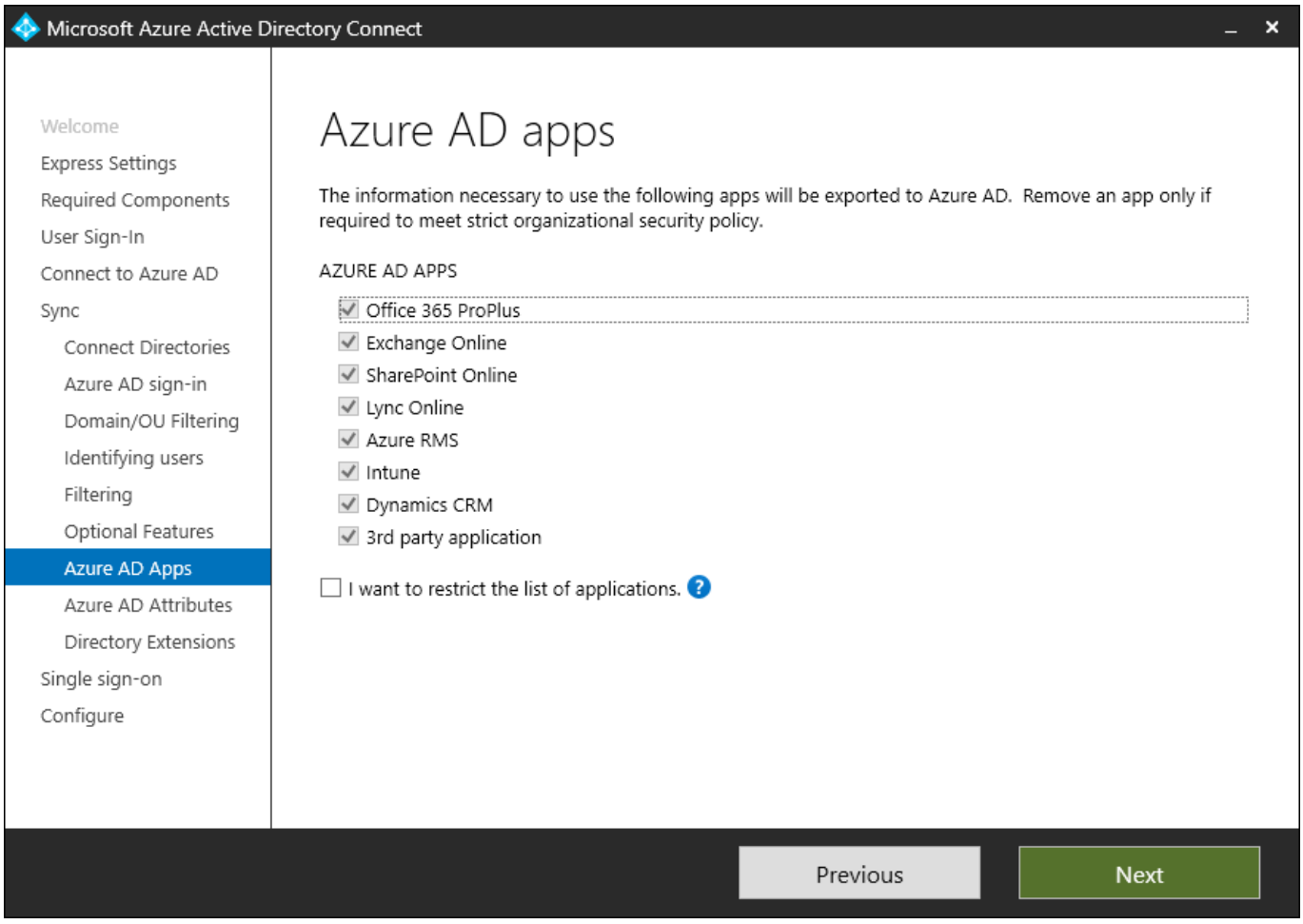
Hier wäre zu prüfen, ob ein Logon über die Mailadresse des Users sinnvoll wäre. Siehe https://docs.microsoft.com/de-de/azure/active-directory/hybrid/plan-connect-userprincipalname .

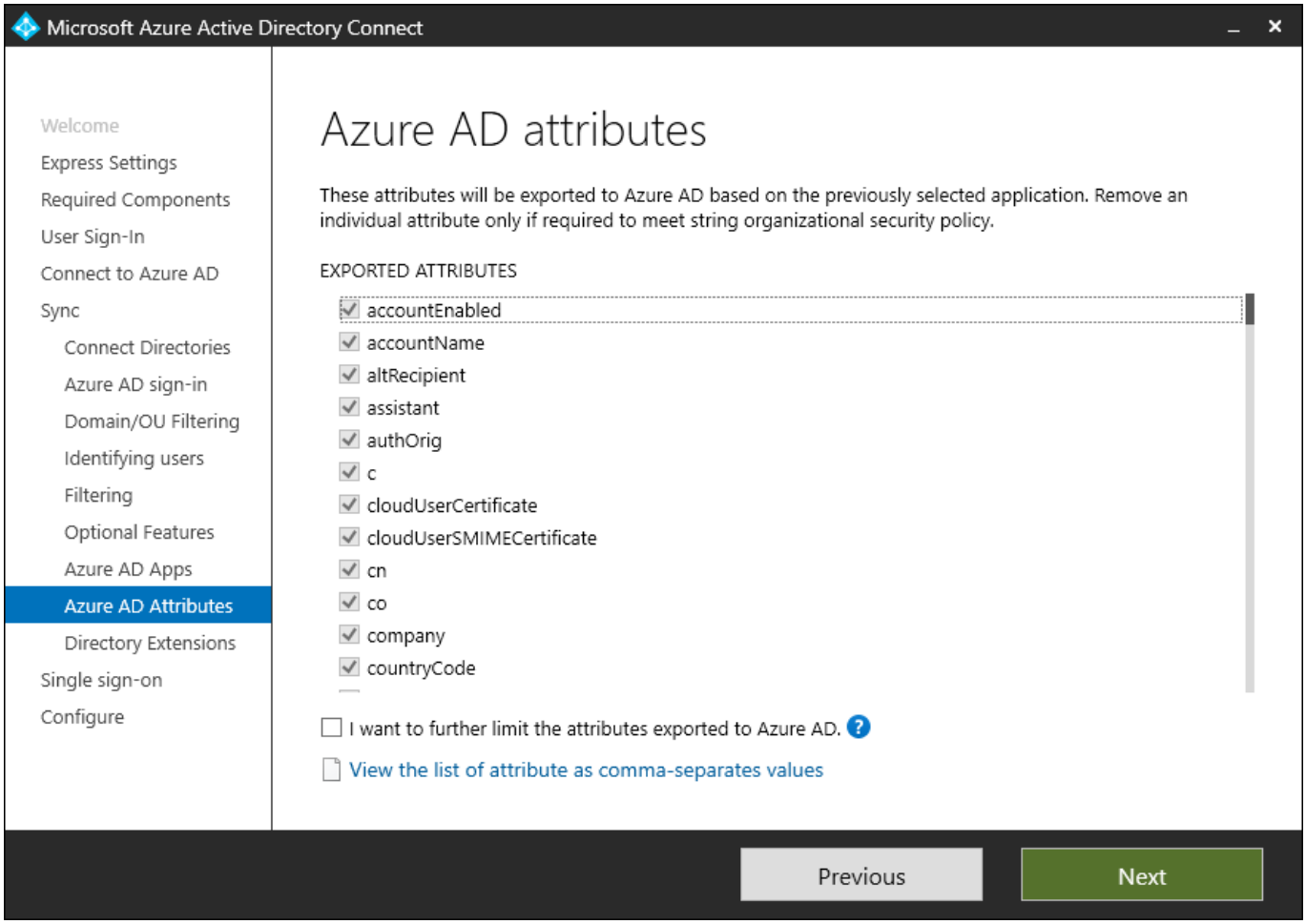


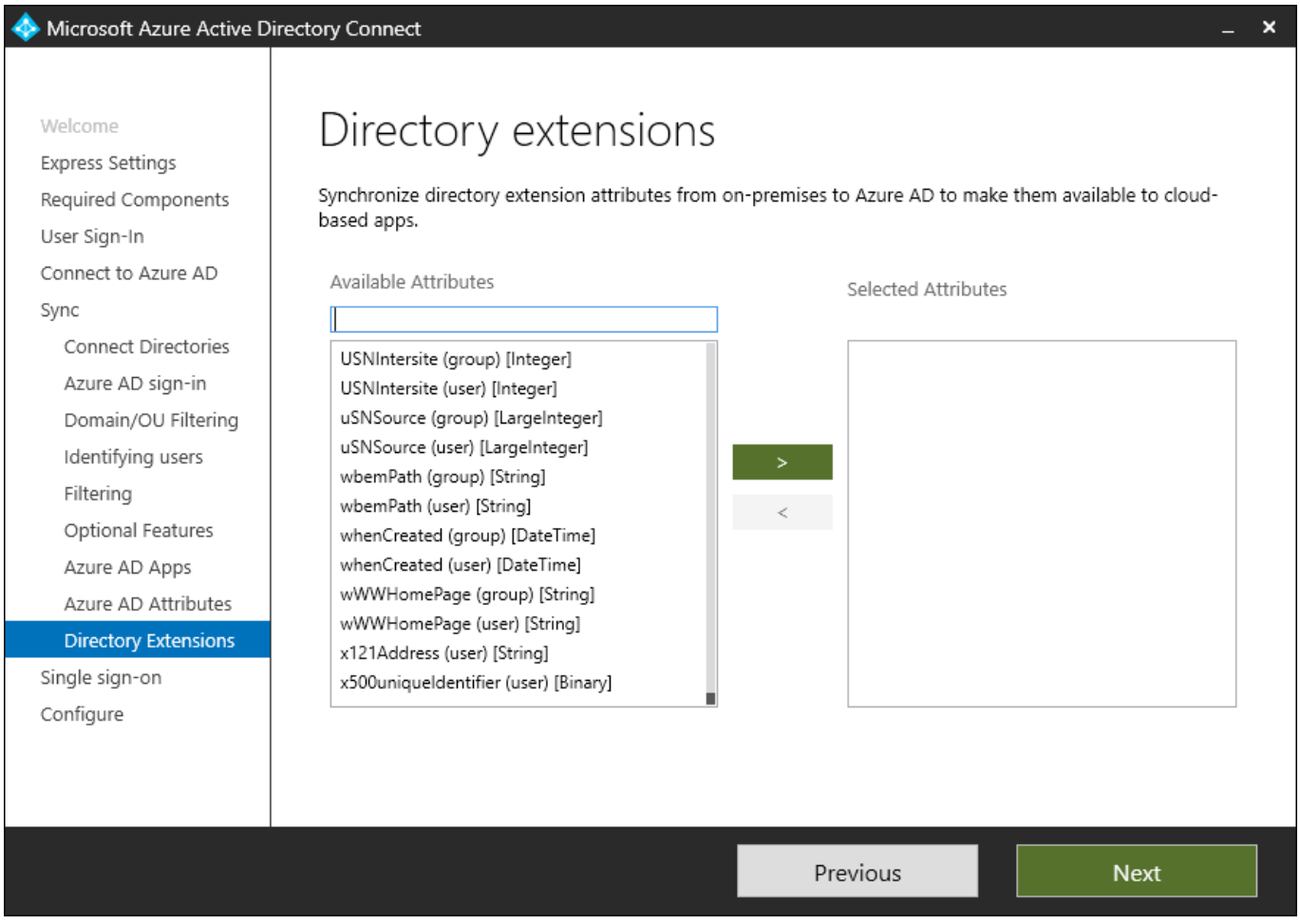

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Single sign-on
Configure
Uniquely identifying your users
Select how users 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
Choose a specific attribute
Azure will write back unique source anchors to your on-premises directory if mS-DS-ConsistencyGuid is currently unused by your organization. Learn more
Previous
Next

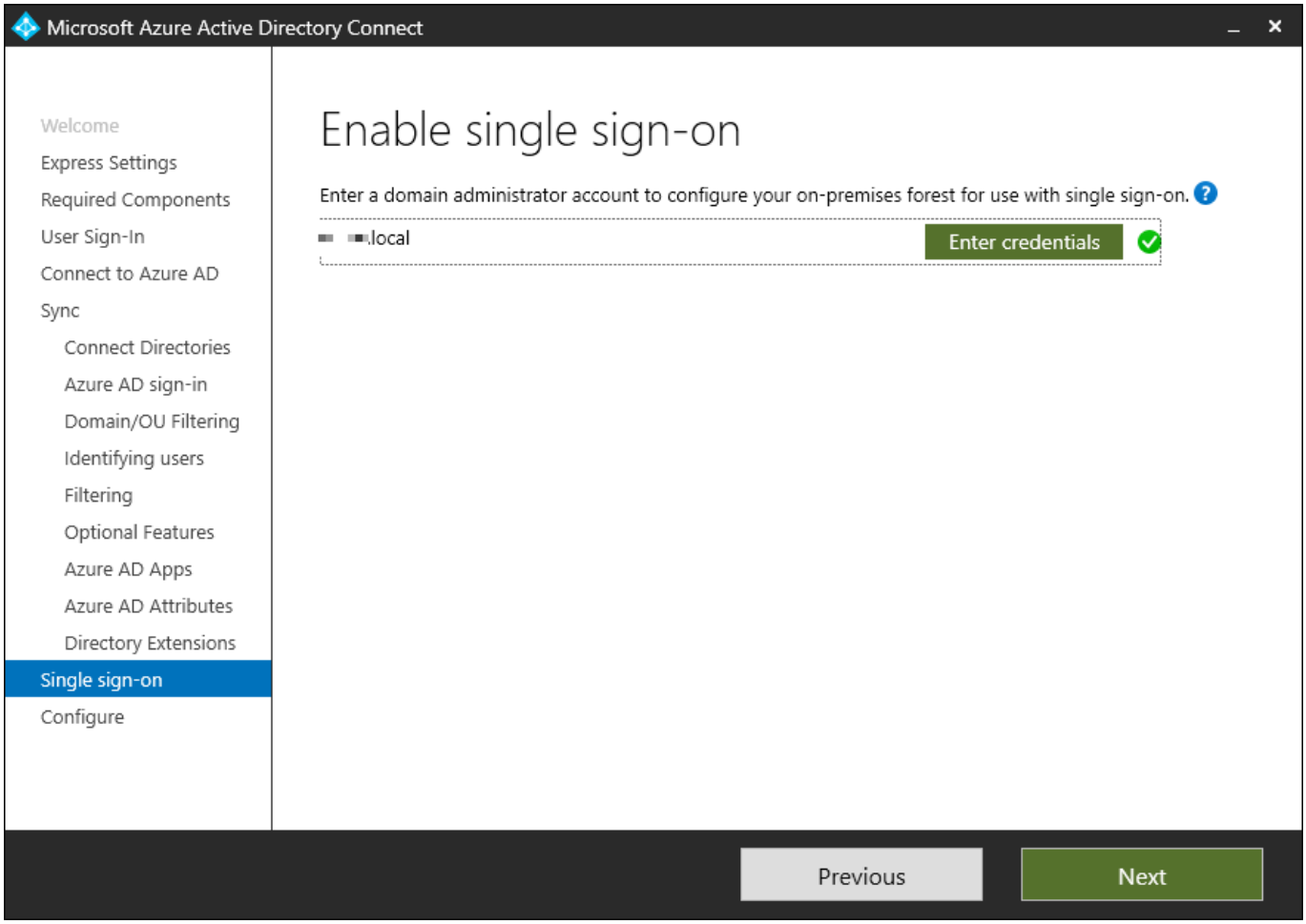

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Single sign-on
Configure
Filter users and devices
For a pilot deployment, 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
local
Enter a name or DN of a group
Resolve
Previous
Next

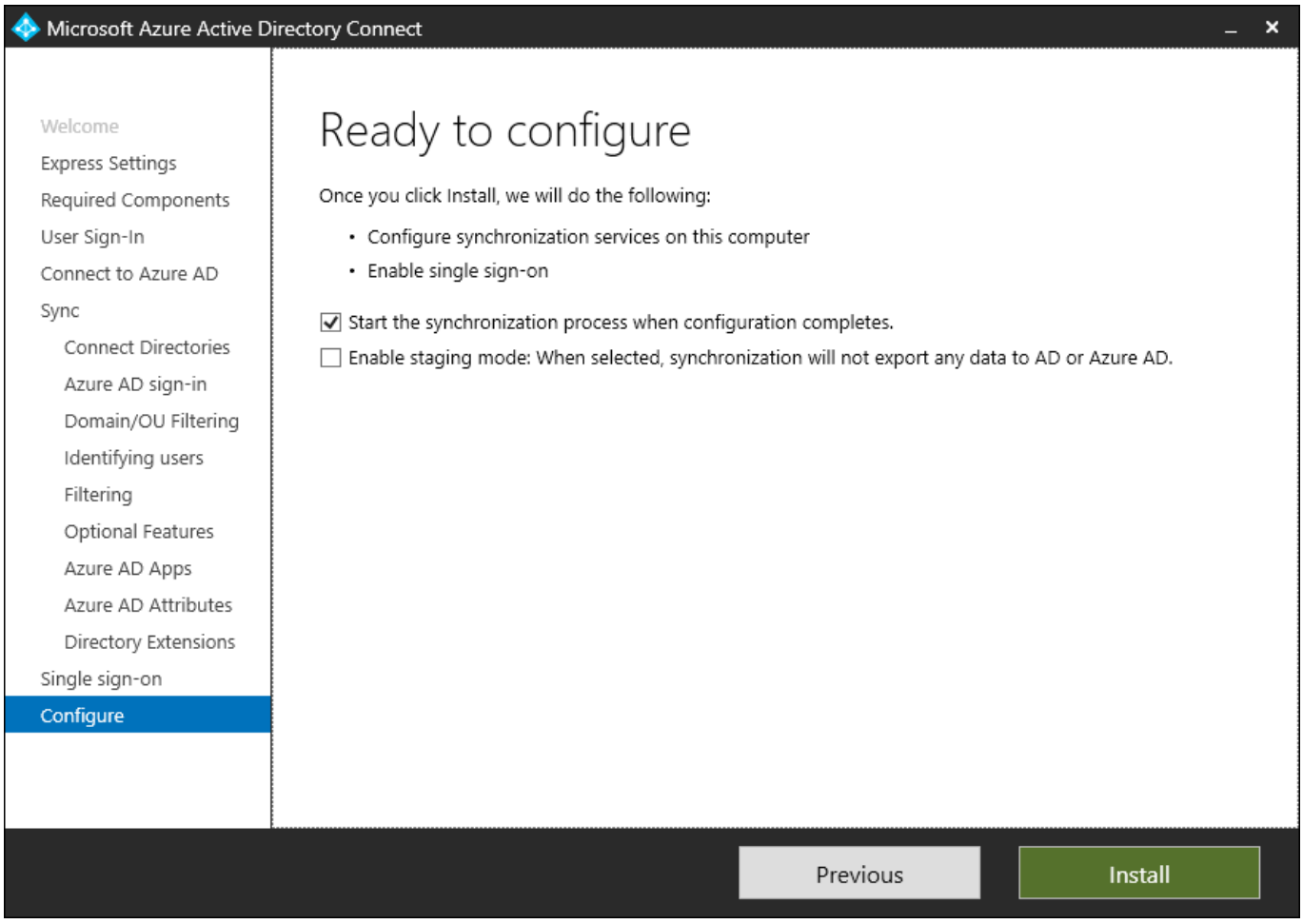

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Azure AD Apps
Azure AD Attributes
Directory Extensions
Single sign-on
Configure
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 hash synchronization
Password writeback
Group writeback (Preview)
Device writeback
Directory extension attribute sync
Learn more about optional features.
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
Azure AD Apps
Azure AD Attributes
Directory Extensions
Single sign-on
Configure
Azure AD apps
The information necessary to use the following apps will be exported to Azure AD. Remove an app only if required to meet strict organizational security policy.
AZURE AD APPS
Office 365 ProPlus
Exchange Online
SharePoint Online
Lync Online
Azure RMS
Intune
Dynamics CRM
3rd party application
I want to restrict the list of applications.
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
Azure AD Apps
Azure AD Attributes
Directory Extensions
Single sign-on
Configure
Azure AD attributes
These attributes will be exported to Azure AD based on the previously selected application. Remove an individual attribute only if required to meet string organizational security policy.
EXPORTED ATTRIBUTES
accountEnabled
accountName
altRecipient
assistant
authOrig
c
cloudUserCertificate
cloudUserSMIMECertificate
cn
co
company
countryCode
I want to further limit the attributes exported to Azure AD.
View the list of attribute as comma-separates values
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
Azure AD Apps
Azure AD Attributes
Directory Extensions
Single sign-on
Configure
Directory extensions
Synchronize directory extension attributes from on-premises to Azure AD to make them available to cloud-based apps.
Available Attributes
Selected Attributes
USNIntersite (group) [Integer]
USNIntersite (user) [Integer]
uSNSource (group) [LargeInteger]
uSNSource (user) [LargeInteger]
wbemPath (group) [String]
wbemPath (user) [String]
whenCreated (group) [DateTime]
whenCreated (user) [DateTime]
wWWHomePage (group) [String]
wWWHomePage (user) [String]
x121Address (user) [String]
x500uniqueIdentifier (user) [Binary]
>
<
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
Azure AD Apps
Azure AD Attributes
Directory Extensions
Single sign-on
Configure
Enable single sign-on
Enter a domain administrator account to configure your on-premises forest for use with single sign-on.
local
Enter credentials
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
Azure AD Apps
Azure AD Attributes
Directory Extensions
Single sign-on
Configure
Ready to configure
Once you click Install, we will do the following:
Configure synchronization services on this computer
Enable single sign-on
Start the synchronization process when configuration completes.
Enable staging mode: When selected, synchronization will not export any data to AD or Azure AD.
Previous
Install