Enterprise Identity

Hybrid Identity & Device Synchronization

Technical Guide

Waheed Anjum

Microsoft Certified Trainer
Azure Solutions Architect
O365 Architect

How to Setup Domain Controller!

To install Active Directory Domain Services (ADDS) on a Windows Server 2022, follow these steps:

1. Log in to your Windows Server 2022 as an administrator.
2. Open the Server Manager by clicking on the Server Manager icon on the taskbar, or by typing "Server Manager" in the Start menu.
3. In the Server Manager, click on the "Add roles and features" option in the dashboard.
4. In the "Add Roles and Features Wizard," click "Next" on the Before You Begin page.
5. On the "Installation Type" page, select "Role-based or feature-based installation," and click "Next."
6. On the "Server Selection" page, select the server you want to install ADDS on, and click "Next."
7. On the "Server Roles" page, select "Active Directory Domain Services," and click "Add Features" when prompted to add required features.
8. On the "Features" page, click "Next" without selecting any additional features.
9. On the "AD DS" page, review the information, and click "Next."
10. On the "Confirmation" page, review your selections, and click "Install" to start the installation.
11. Wait for the installation to complete, and then click "Close" on the "Results" page.
12. After the installation completes, you will see a notification to complete the AD DS Configuration Wizard. Click on "Promote this server to a domain controller" link to open the wizard.
13. In the wizard, select "Add a new forest" and enter the root domain name, and follow the prompts to configure the domain and the directory services.
14. When the configuration is complete, click "Finish" to close the wizard.
15. Reboot your server to complete the installation.

You have now successfully installed ADDS on your Windows Server 2022.

How to Setup Remote Server Administration Tools on **Staging Server!**

12th Page Last Slide > ***Enable Staging Mode*** (Uncheck First Option – Do not check both Options)

To install Remote Server Administration Tools (RSAT) on a member server, follow these steps:

1. Log in to your Windows Server 2022 as an administrator.
2. Join your Staging Server to existing domain.
3. Restart your server after joining the domain and login with Domain Admin account.
4. Open PowerShell as an administrator.
5. Run the following command to install the RSAT tools for Active Directory Domain Services:

```
Install-WindowsFeature RSAT-ADDS -IncludemanagementTools
```

6. Install Azure AD Connect Agent on this server https://www.microsoft.com/en-us/download/details.aspx?id=104056

7. Follow the steps from Microsoft official documentation https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-express

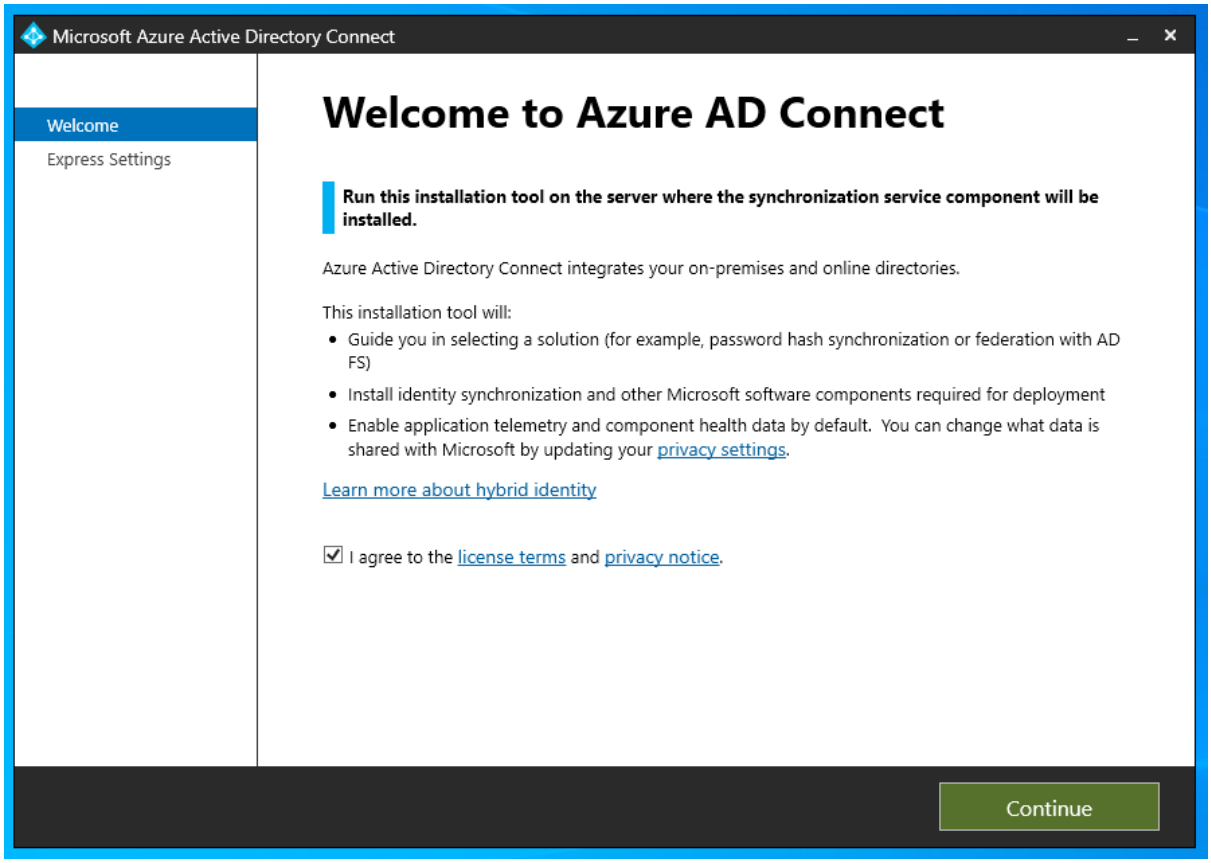
How to Setup Remote Server Administration Tools on Sync Server!

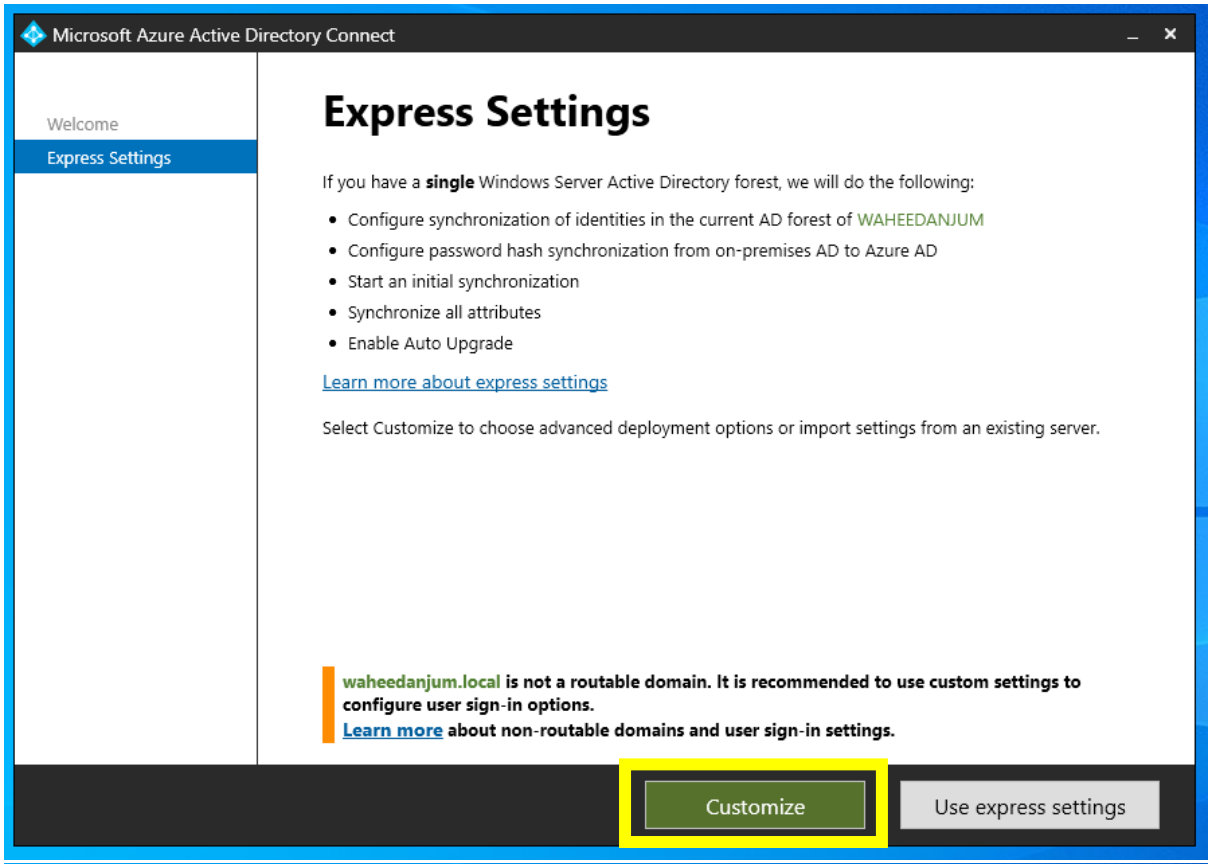
To install Remote Server Administration Tools (RSAT) on a member server, follow these steps:

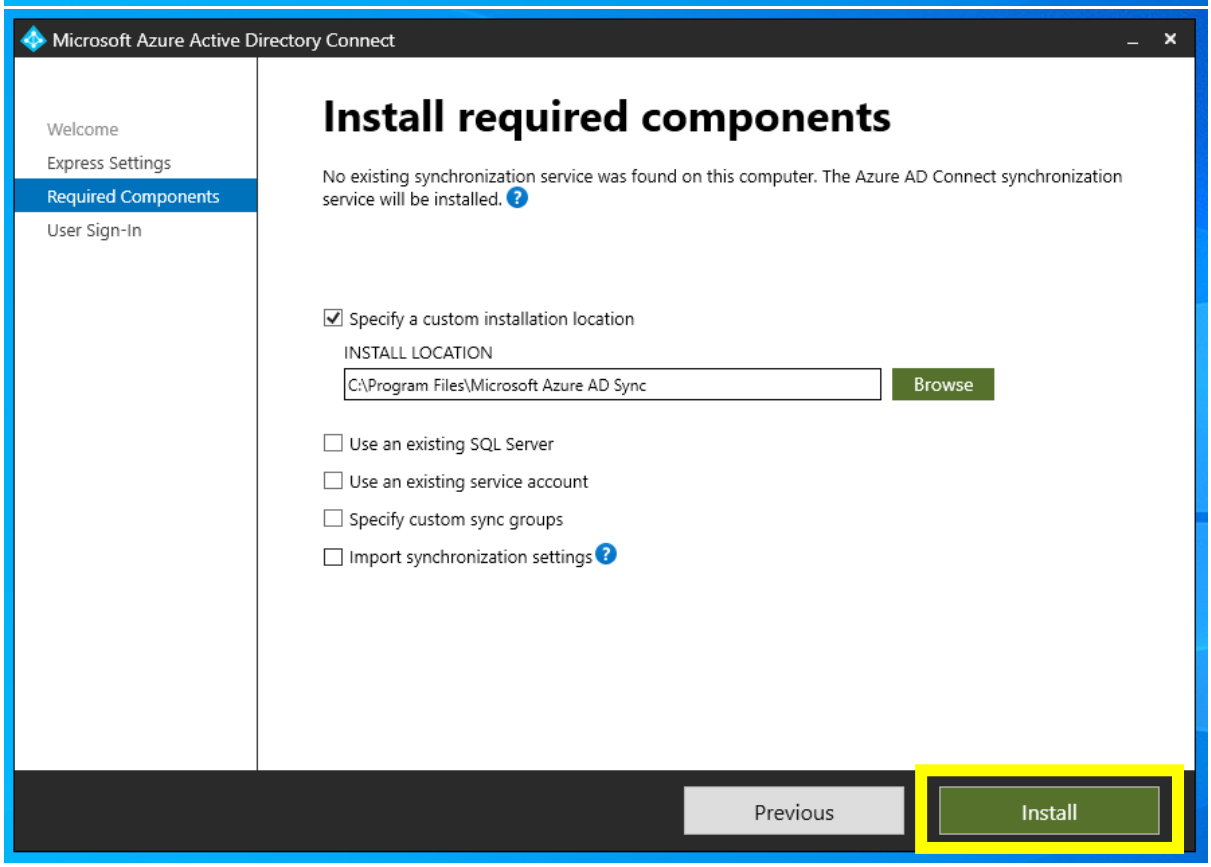
1. Log in to your Windows Server 2022 as an administrator.
2. Join your Staging Server to existing domain.
3. Restart your server after joining the domain and login with Domain Admin account.
4. Open PowerShell as an administrator.
5. Run the following command to install the RSAT tools for Active Directory Domain Services:

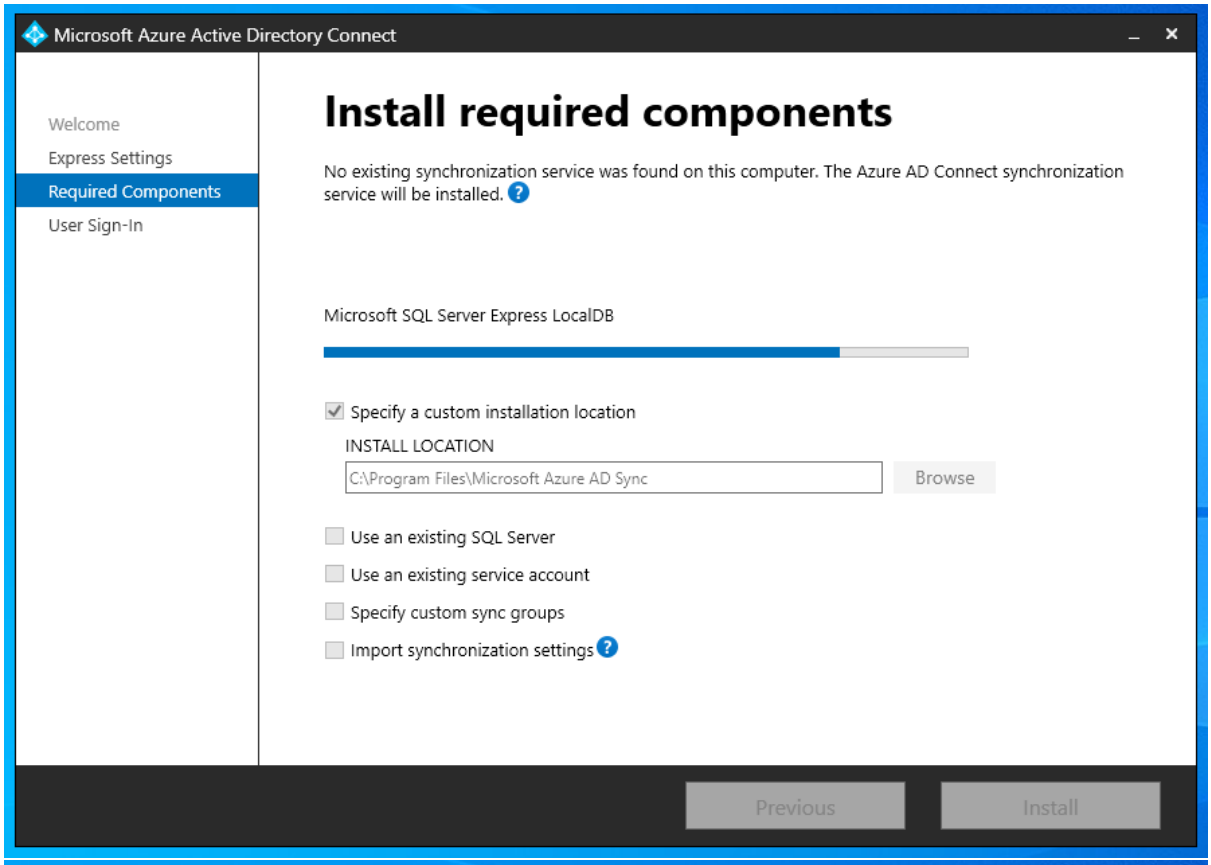
```
Install-WindowsFeature RSAT-ADDS -IncludemanagementTools
```

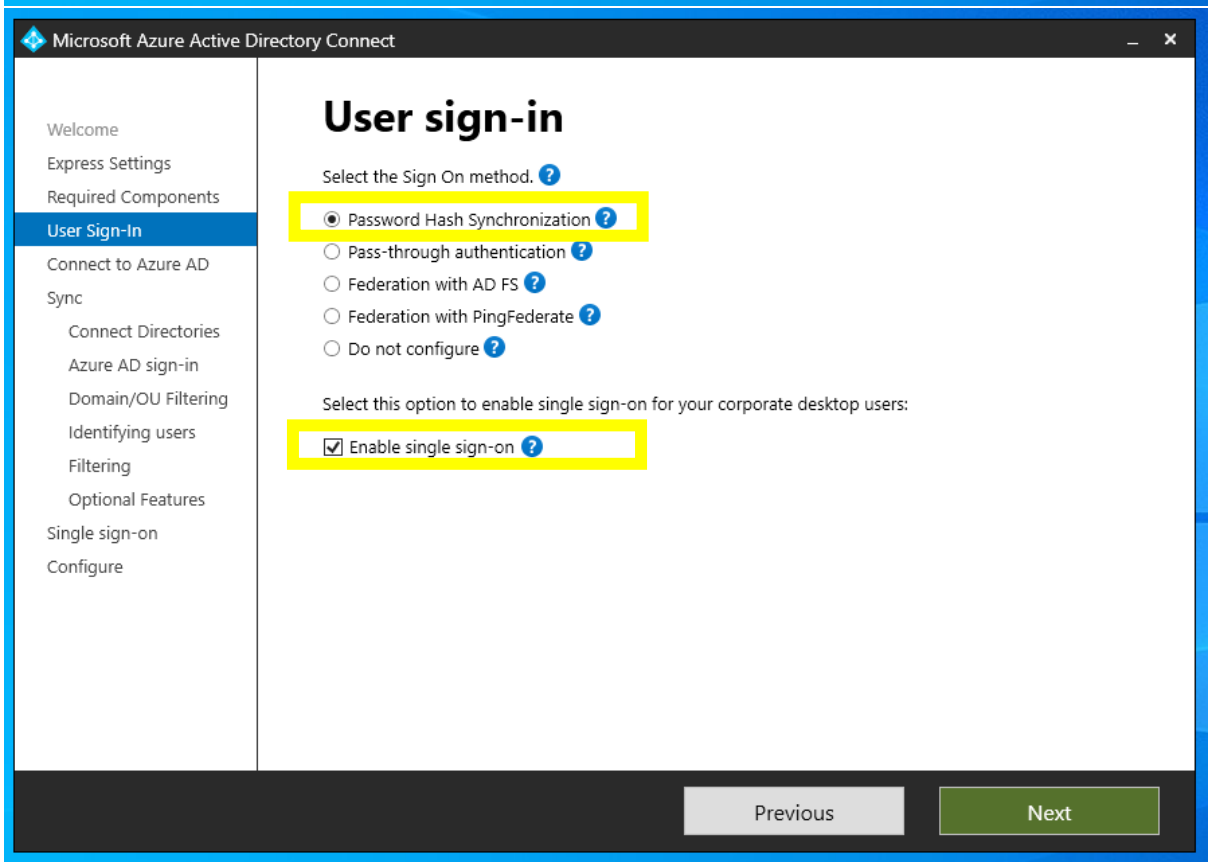
6. Install Azure AD Connect Agent on this server https://www.microsoft.com/en-us/download/details.aspx?id=104056
7. Follow the steps from Microsoft official documentation https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-express

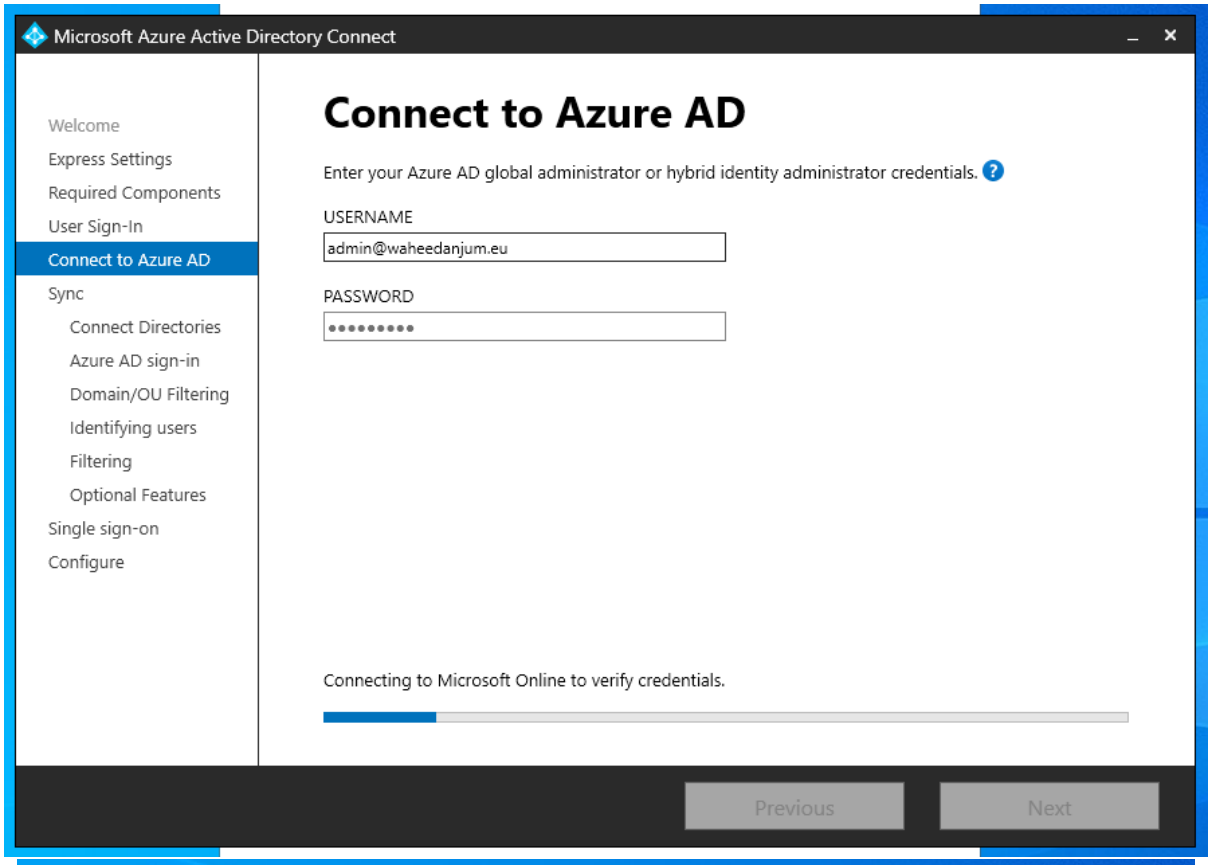


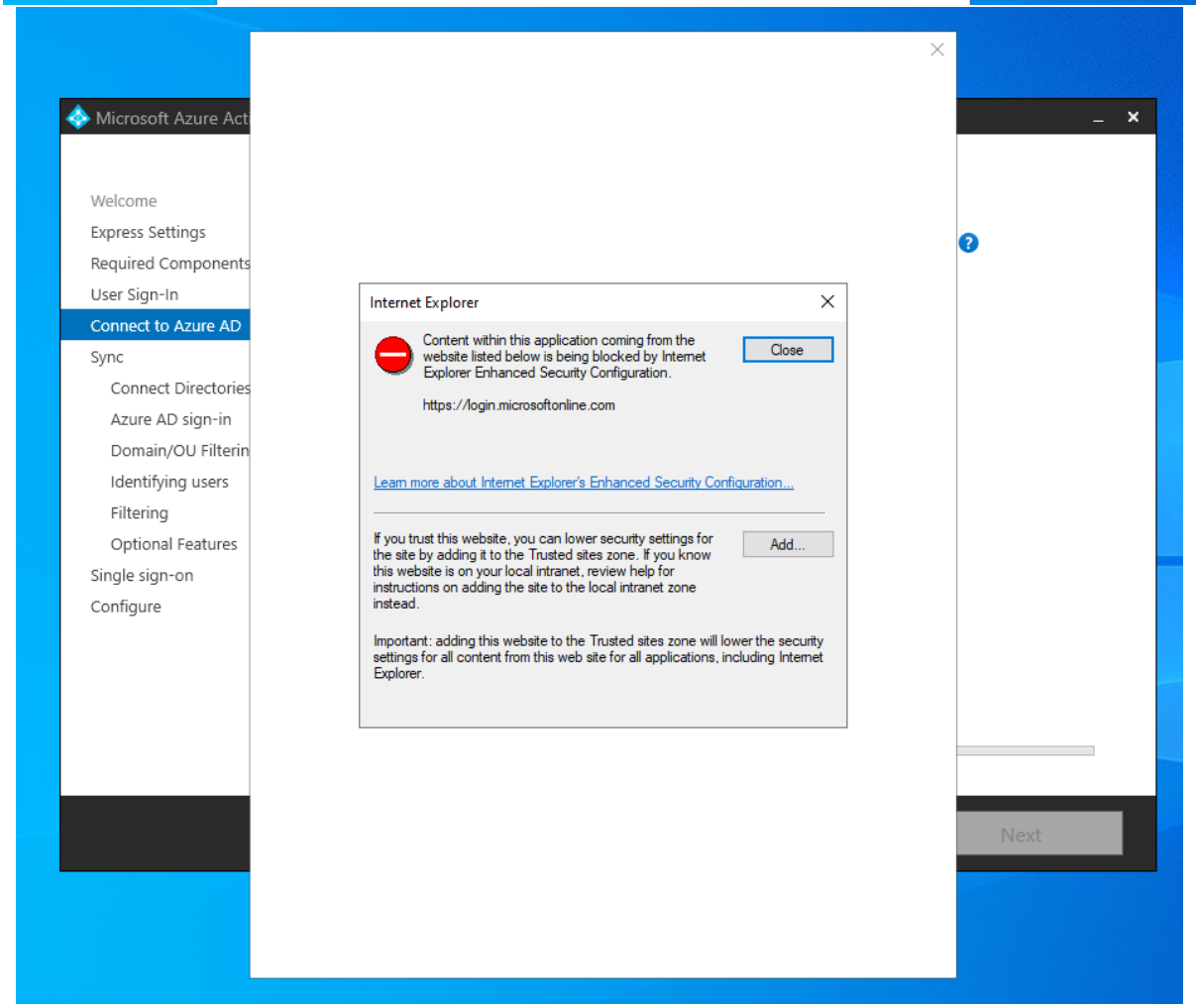

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Express Settings
If you have a single Windows Server Active Directory forest, we will do the following:
Configure synchronization of identities in the current AD forest of WAHEEDANJUM
Configure password hash synchronization from on-premises AD to Azure AD
Start an initial synchronization
Synchronize all attributes
Enable Auto Upgrade
Learn more about express settings
Select Customize to choose advanced deployment options or import settings from an existing server.
waheedanjum.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

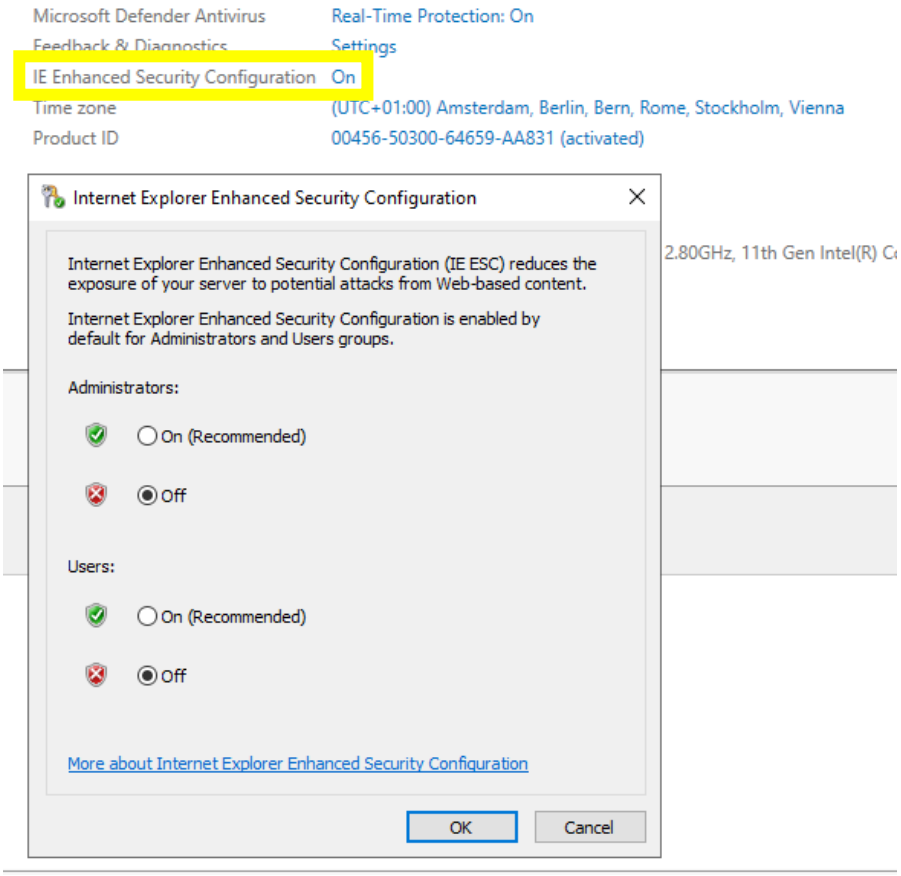

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Install required components
No existing synchronization service was found on this computer. The Azure AD Connect synchronization service will be installed.
Specify a custom installation location
INSTALL LOCATION
C:\Program Files\Microsoft Azure AD Sync
Browse
Use an existing SQL Server
Use an existing service account
Specify custom sync groups
Import synchronization settings
Previous
Install

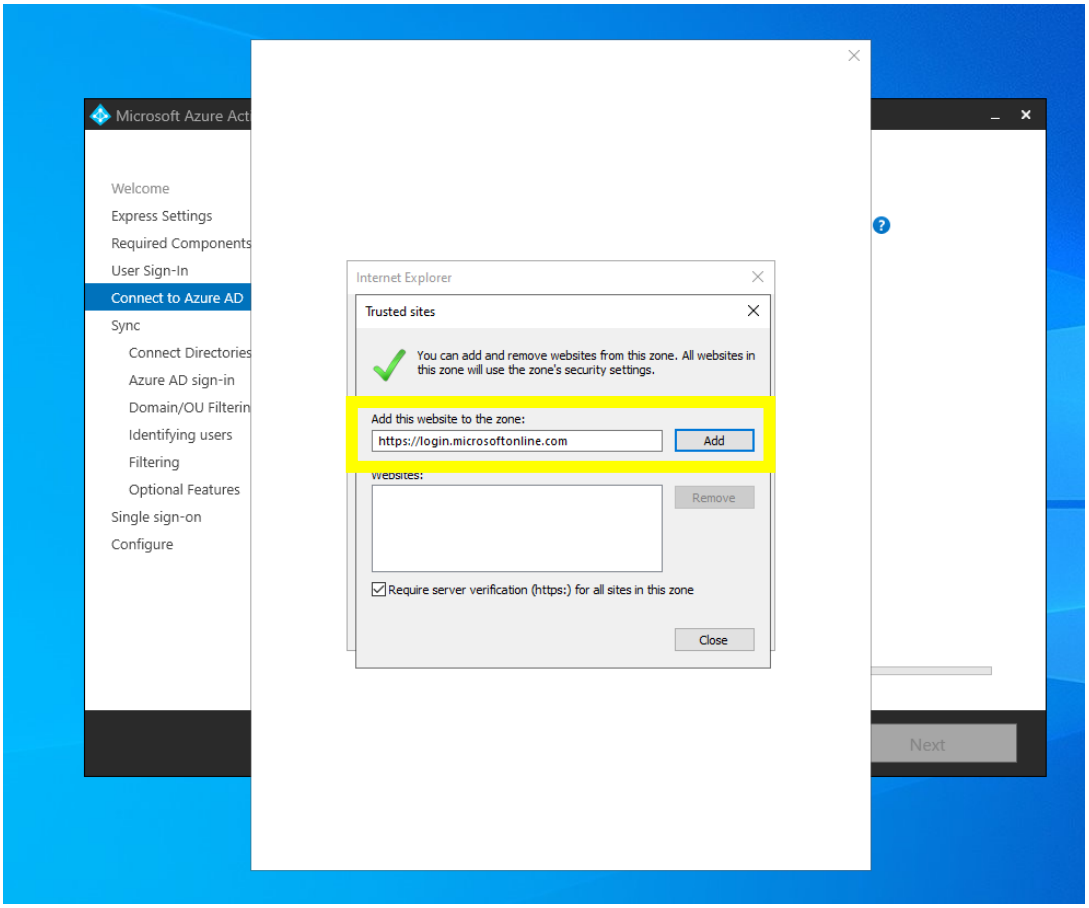

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Install required components
No existing synchronization service was found on this computer. The Azure AD Connect synchronization service will be installed.
Microsoft SQL Server Express LocalDB
Specify a custom installation location
INSTALL LOCATION
C:\Program Files\Microsoft Azure AD Sync
Browse
Use an existing SQL Server
Use an existing service account
Specify custom sync groups
Import synchronization settings
Previous
Install

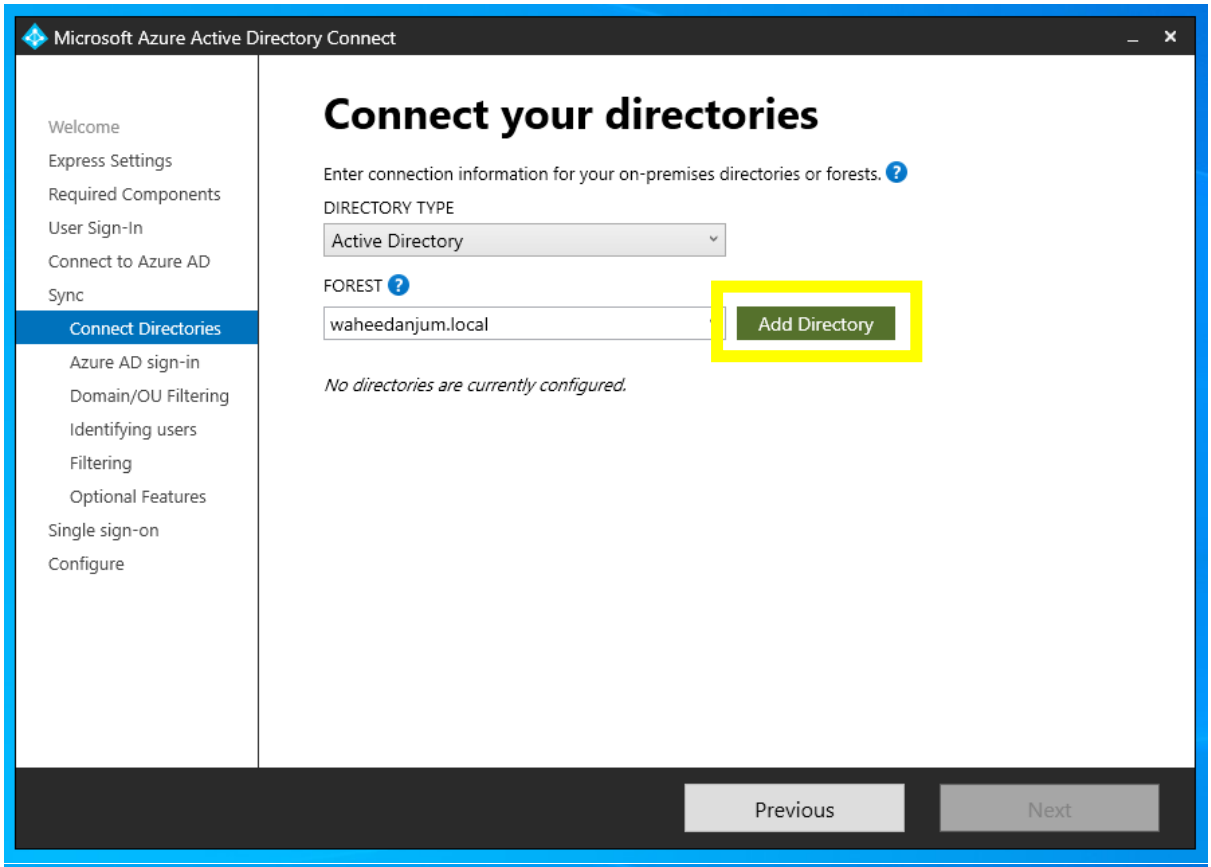

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Single sign-on
Configure
User sign-in
Select the Sign On method.
Password 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

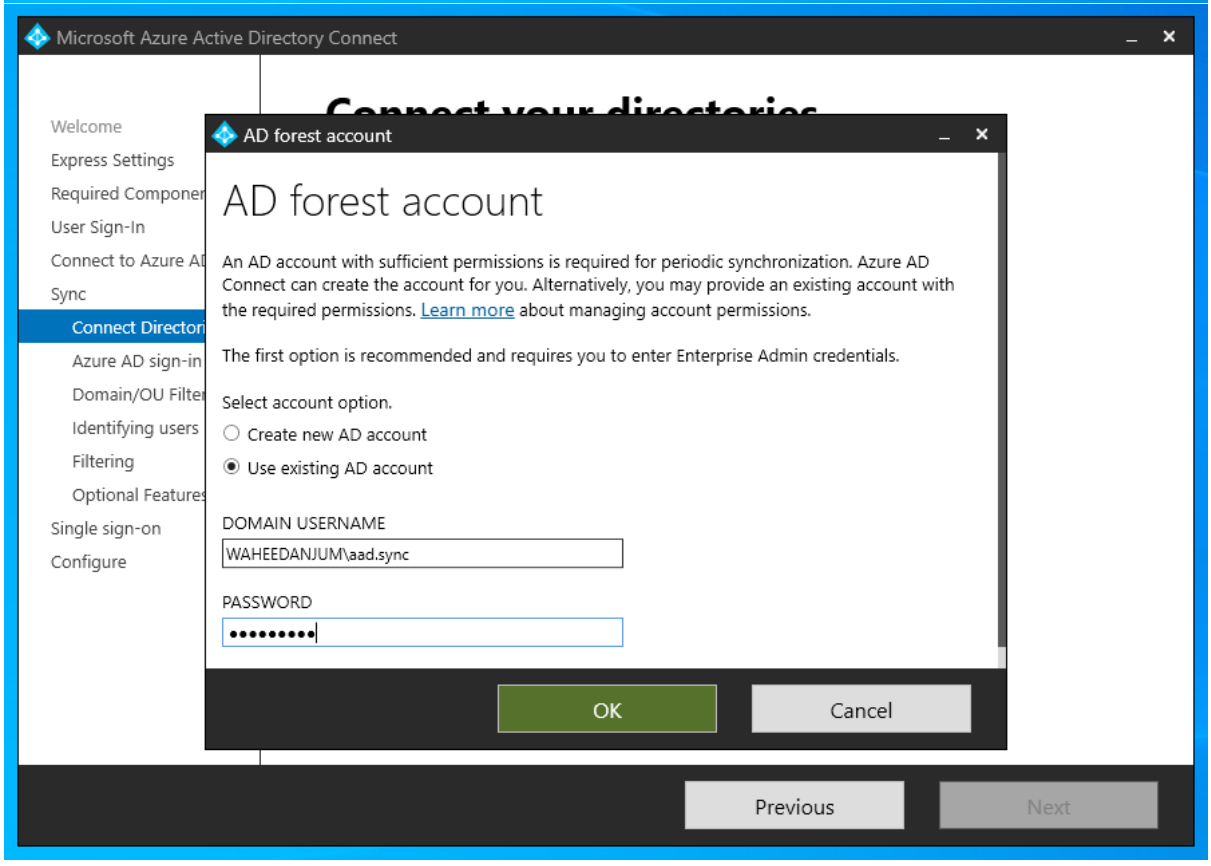

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Single sign-on
Configure
Connect to Azure AD
Enter your Azure AD global administrator or hybrid identity administrator credentials.
USERNAME
admin@waheedanjum.eu
PASSWORD
Connecting to Microsoft Online to verify credentials.
Previous
Next

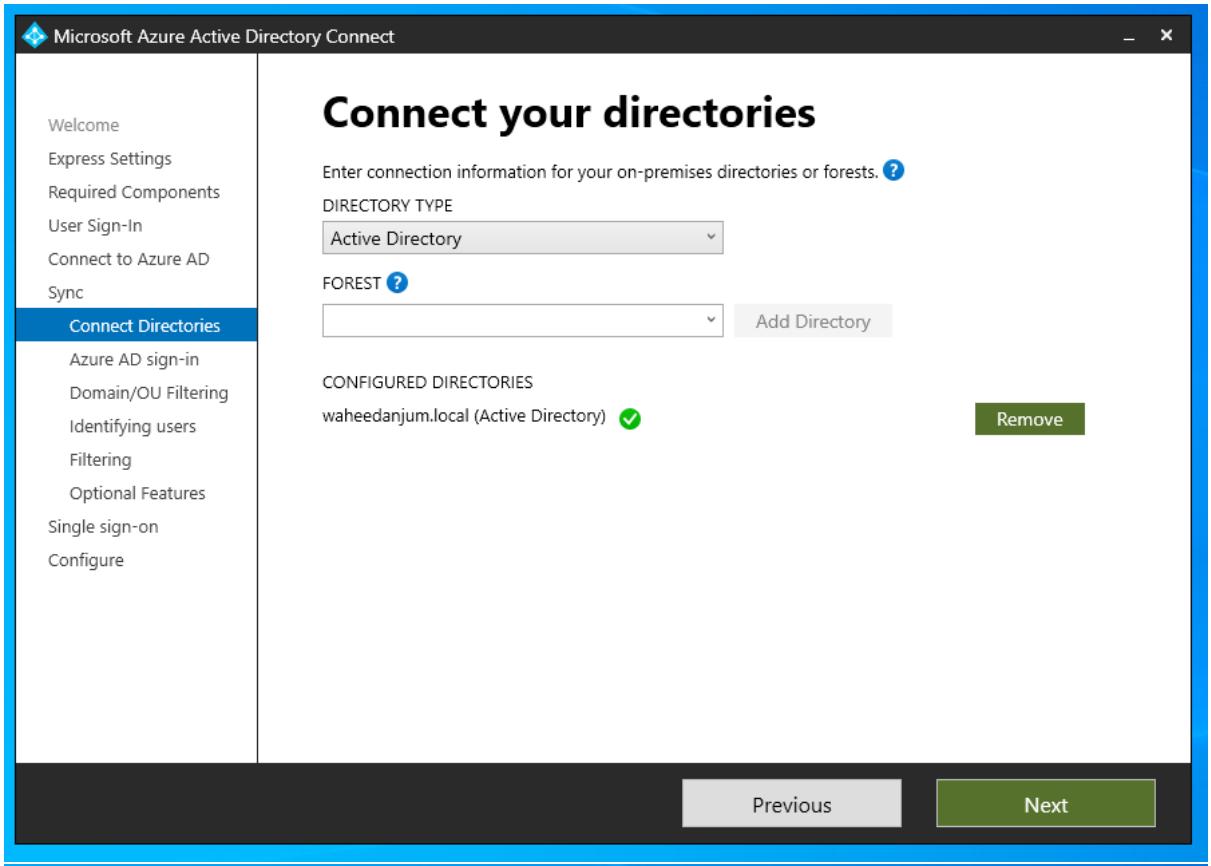

Microsoft Azure Act
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filterin
Identifying users
Filtering
Optional Features
Single sign-on
Configure
Next
Internet Explorer
Content within this application coming from the website listed below is being blocked by Internet Explorer Enhanced Security Configuration.
Close
https://login.microsoftonline.com
Learn more about Internet Explorer's Enhanced Security Configuration...
If you trust this website, you can lower security settings for the site by adding it to the Trusted sites zone. If you know this website is on your local intranet, review help for instructions on adding the site to the local intranet zone instead.
Add...
Important: adding this website to the Trusted sites zone will lower the security settings for all content from this web site for all applications, including Internet Explorer.

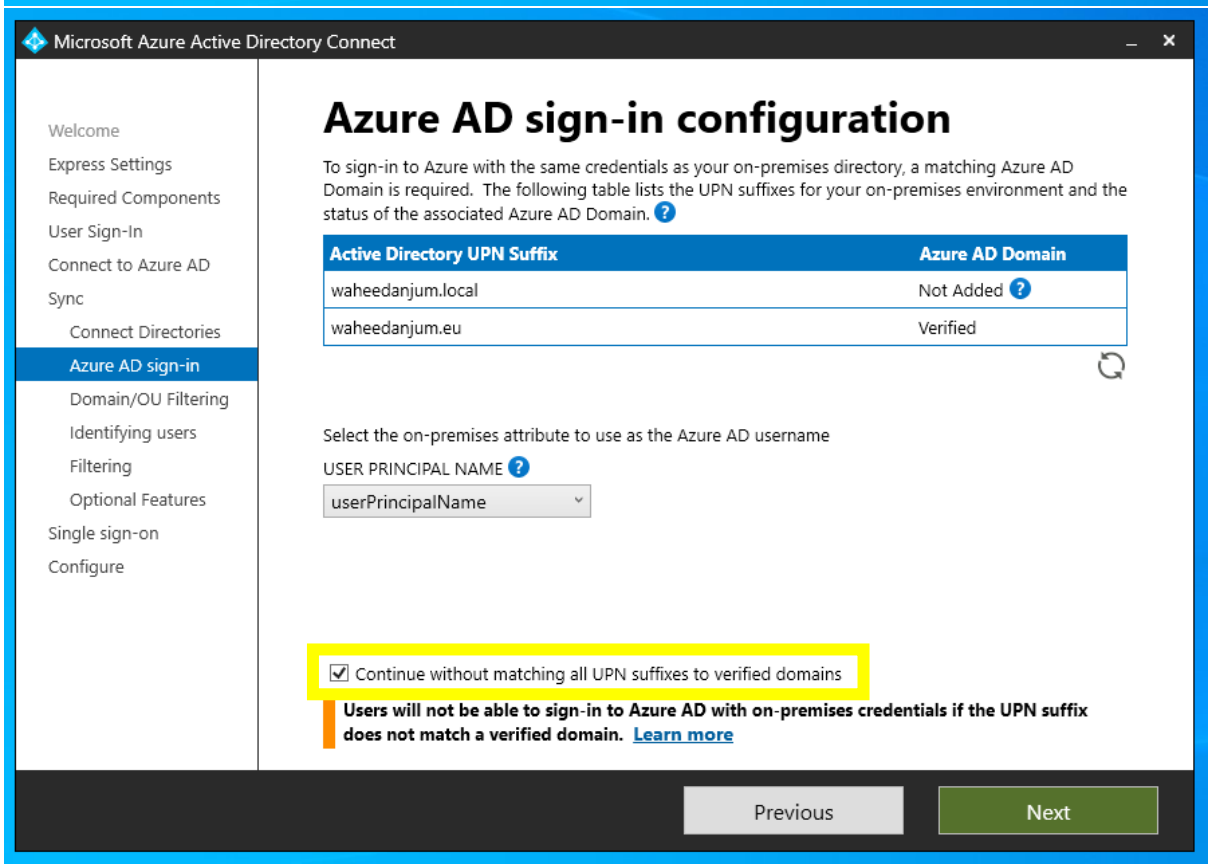

Microsoft Defender Antivirus
Real-Time Protection: On
Feedback & Diagnostics
Settings
IE Enhanced Security Configuration
On
Time zone
(UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
Product ID
00456-50300-64659-AA831 (activated)
Internet Explorer Enhanced Security Configuration
Internet Explorer Enhanced Security Configuration (IE ESC) reduces the exposure of your server to potential attacks from Web-based content.
Internet Explorer Enhanced Security Configuration is enabled by default for Administrators and Users groups.
Administrators:
On (Recommended)
Off
Users:
On (Recommended)
Off
More about Internet Explorer Enhanced Security Configuration
OK
Cancel
2.80GHz, 11th Gen Intel(R) C

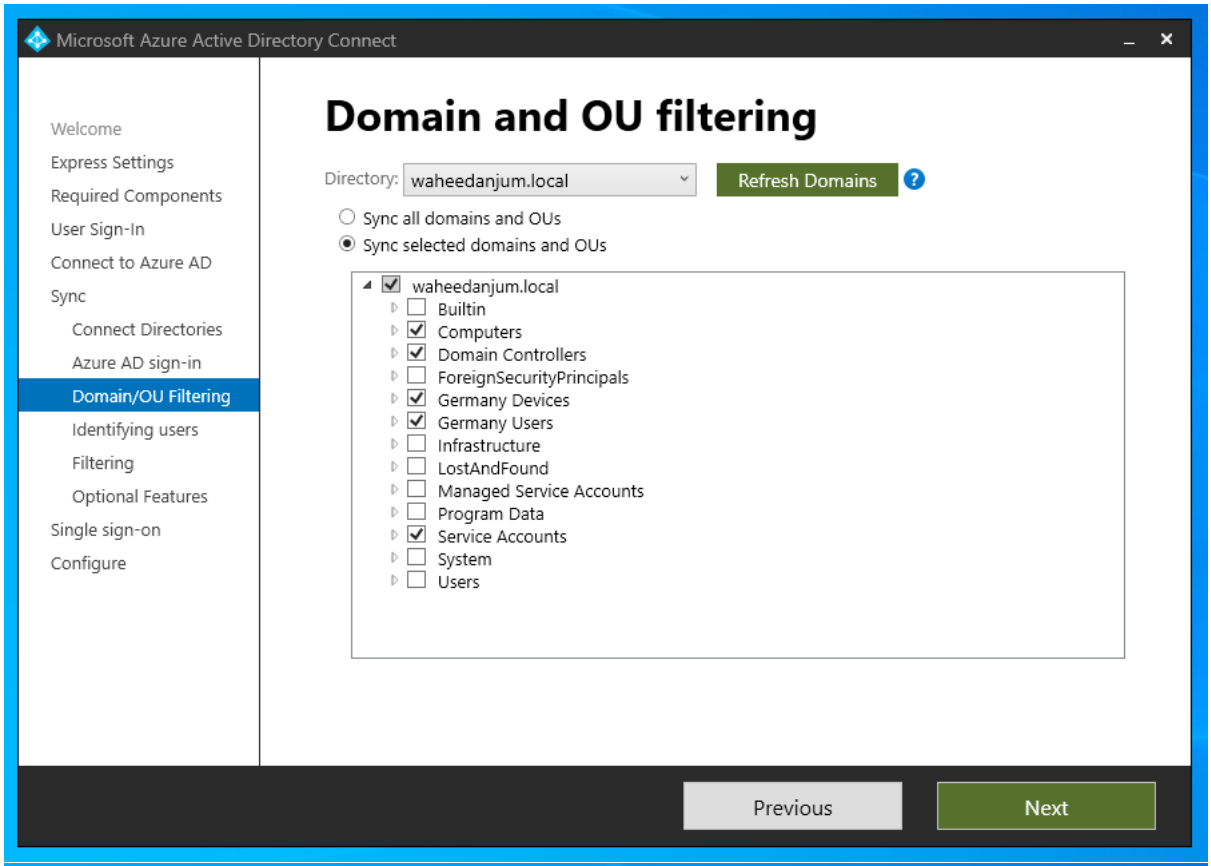

Microsoft Azure Act
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filterin
Identifying users
Filtering
Optional Features
Single sign-on
Configure
Next
Internet Explorer
Trusted sites
You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.
Add this website to the zone:
https://login.microsoftonline.com
Add
Websites:
Remove
Require server verification (https:) for all sites in this zone
Close

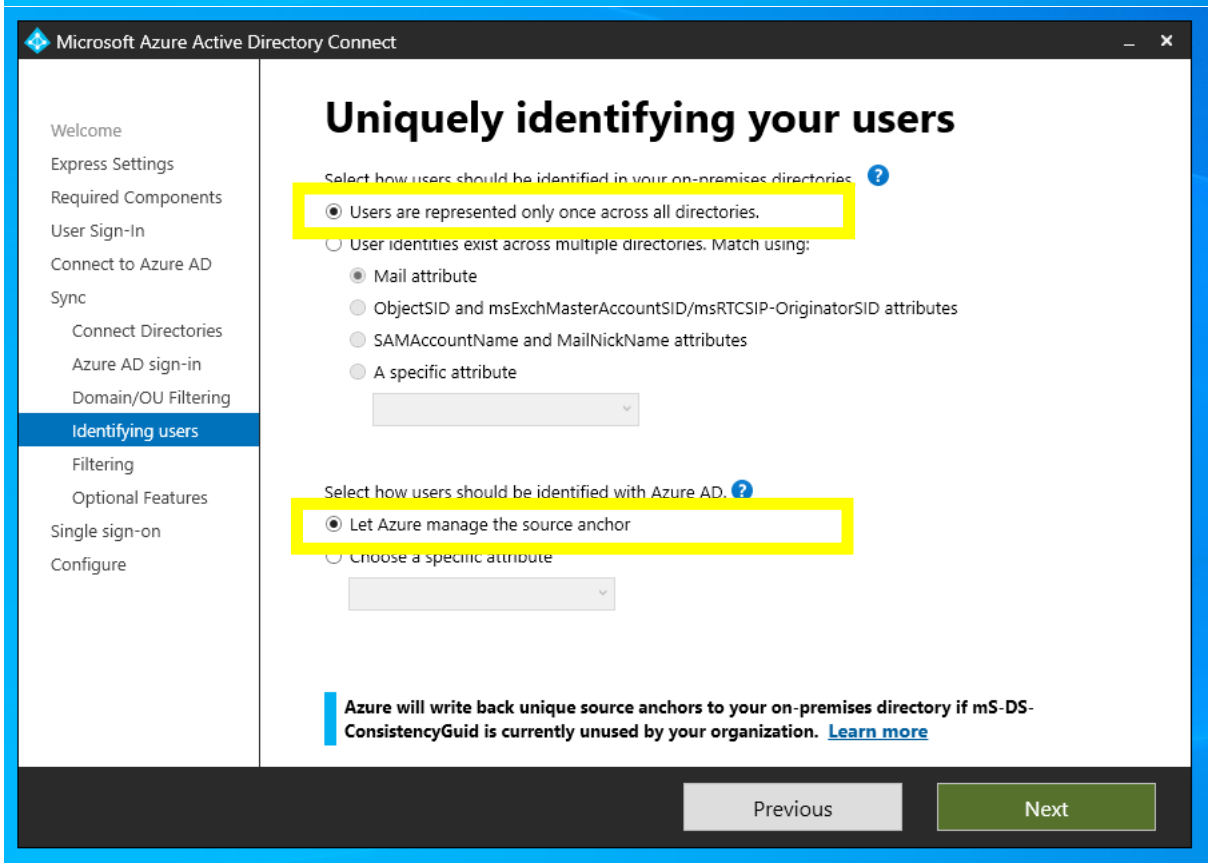

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Single sign-on
Configure
Connect your directories
Enter connection information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

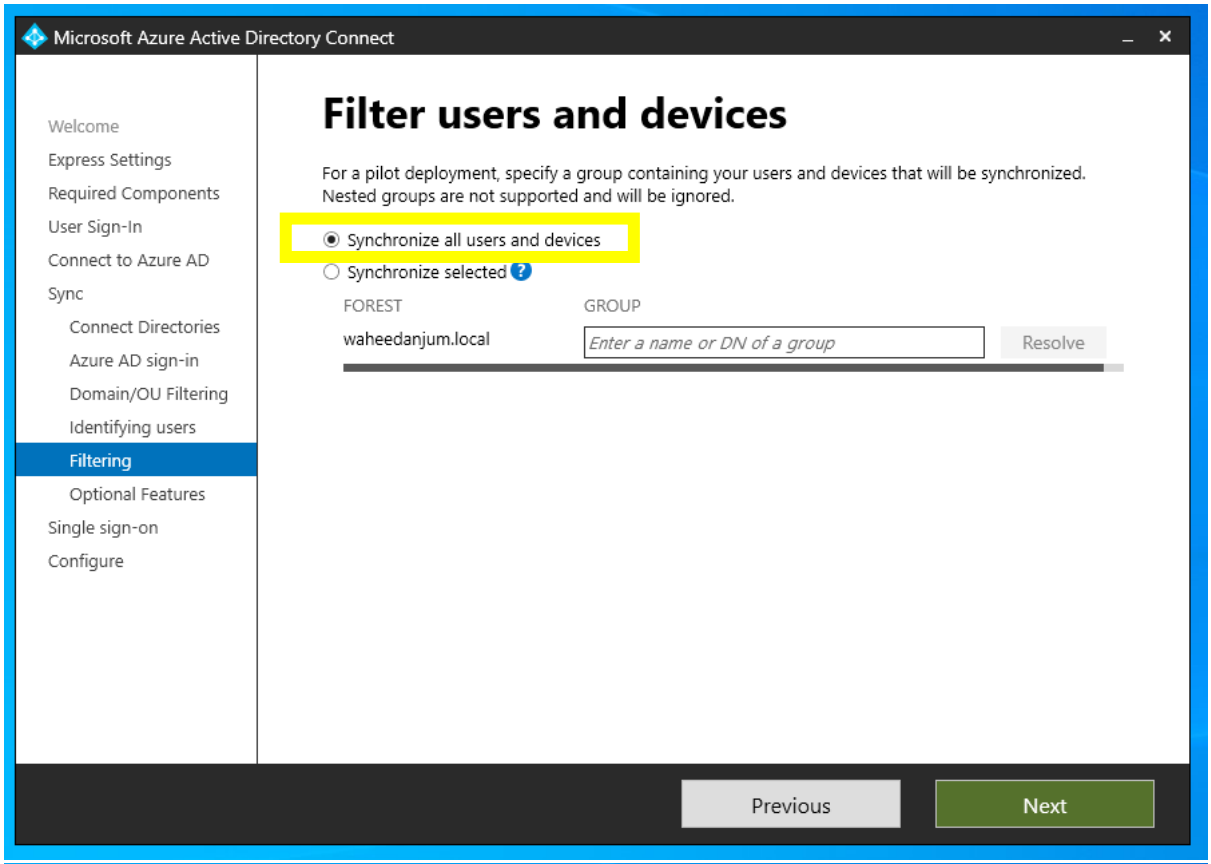

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Componer
User Sign-In
Connect to Azure AD
Sync
Connect Director
Azure AD sign-in
Domain/OU Filter
Identifying users
Filtering
Optional Features
Single sign-on
Configure
AD forest account
AD forest account
An AD account with sufficient 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
DOMAIN USERNAME
WAHEEDANJUM\aad.sync
PASSWORD
OK
Cancel
Previous
Next

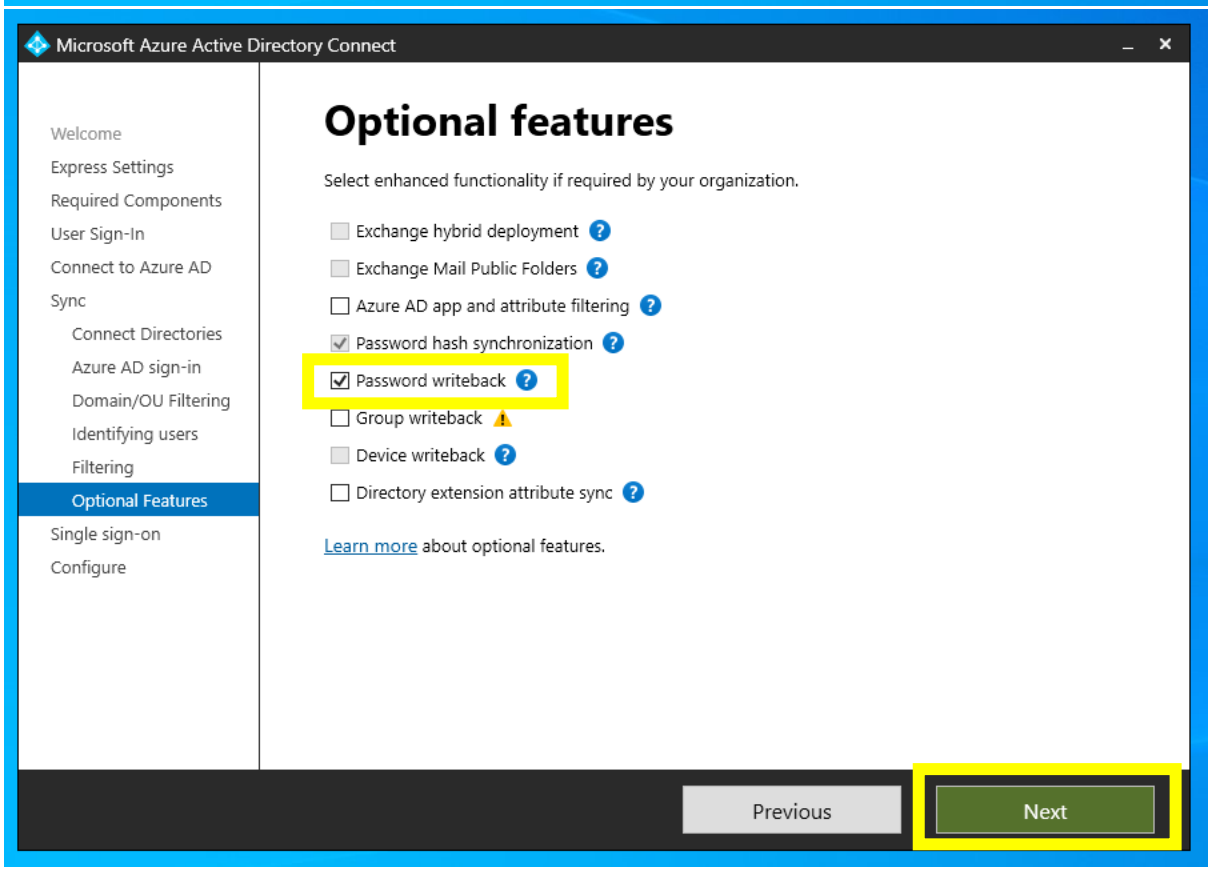

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Single sign-on
Configure
Connect your directories
Enter connection information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

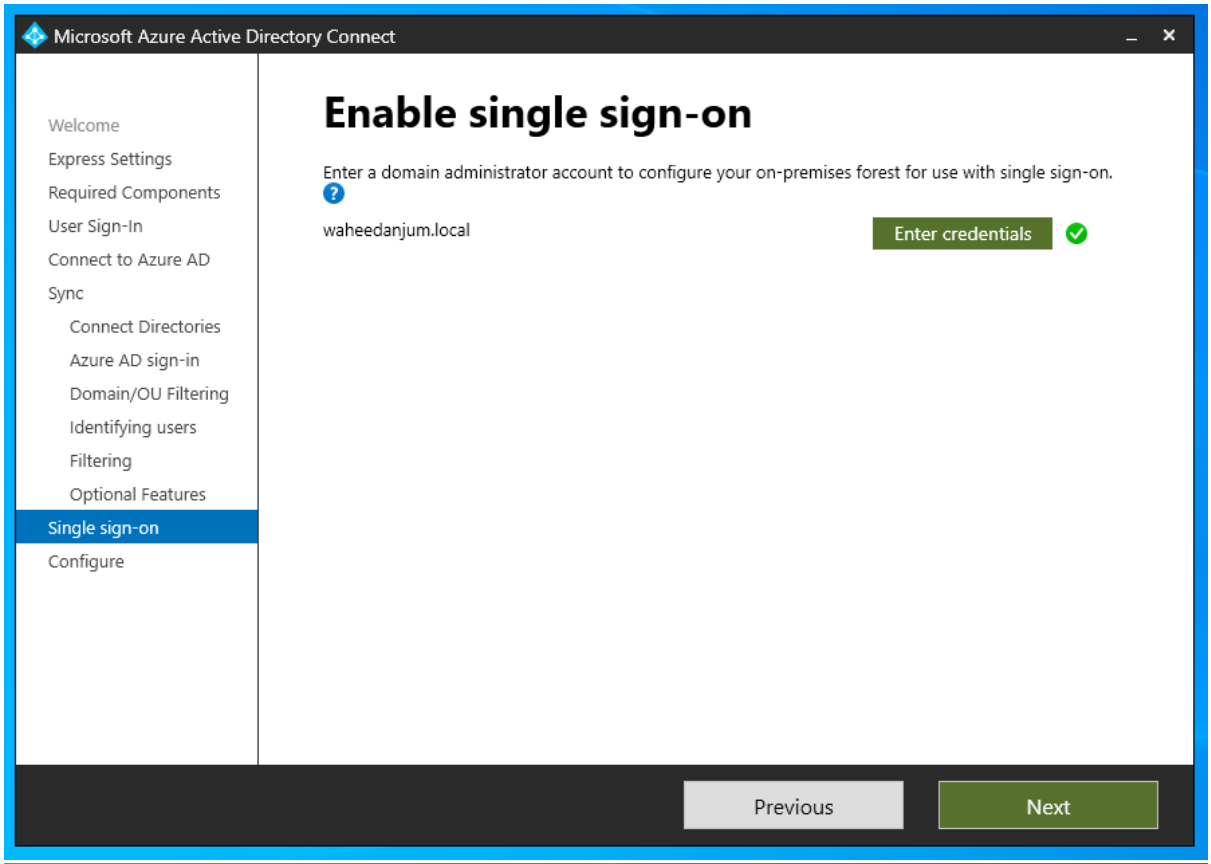

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Single sign-on
Configure
Azure AD sign-in configuration
To sign-in to Azure 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
waheedanjum.local
Not Added
waheedanjum.eu
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

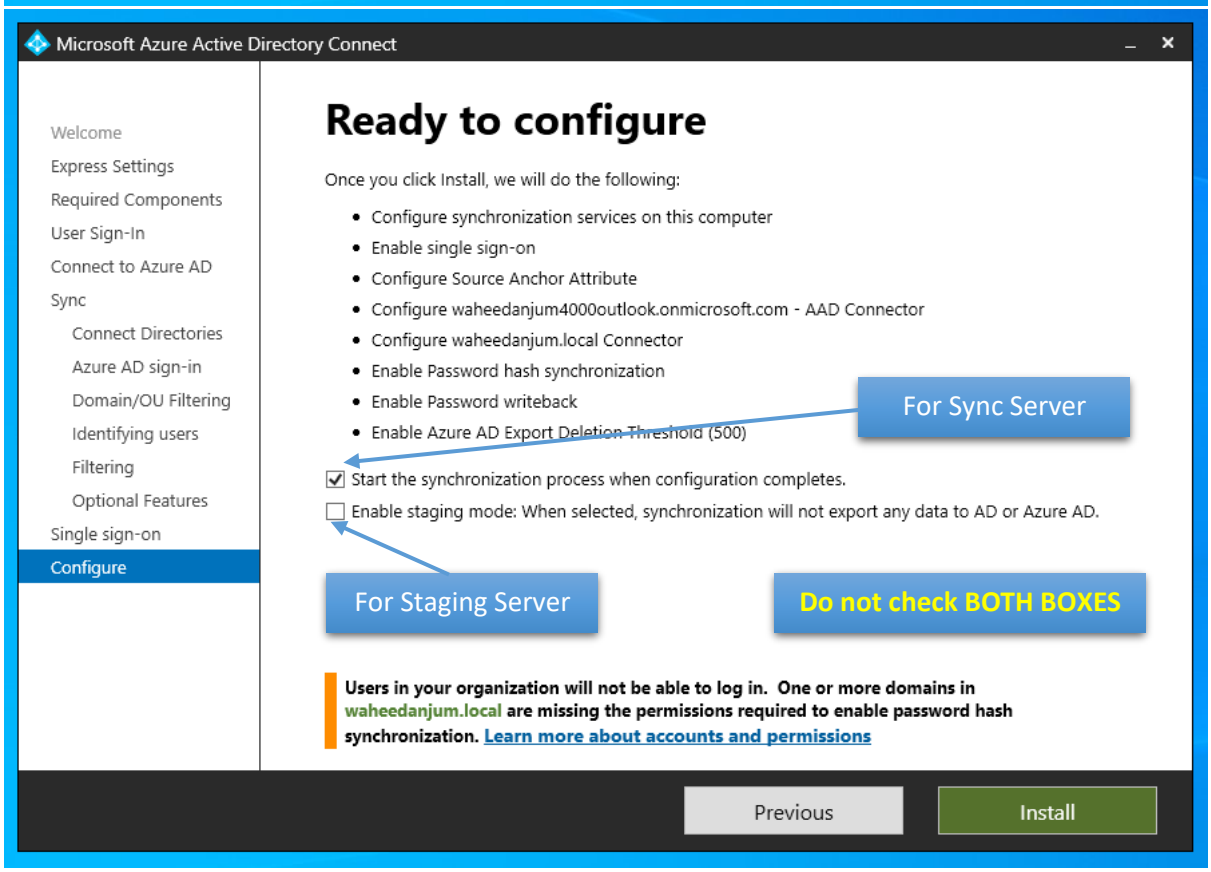

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Single sign-on
Configure
Domain and OU filtering
Directory: waheedanjum.local
Refresh Domains
Sync all domains and OUs
Sync selected domains and OUs
waheedanjum.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Germany Devices
Germany Users
Infrastructure
LostAndFound
Managed Service Accounts
Program Data
Service Accounts
System
Users
Previous
Next

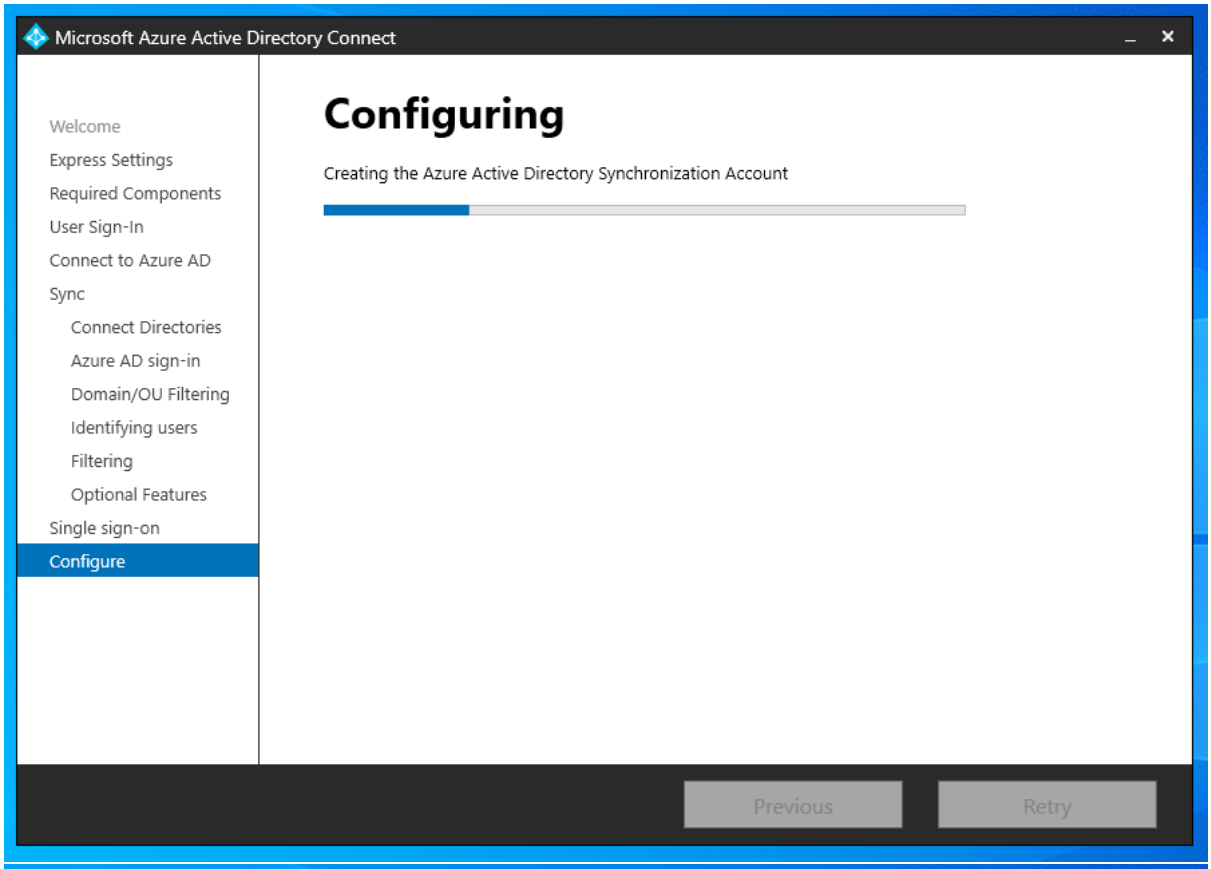

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Single sign-on
Configure
Uniquely identifying your users
Select how users 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

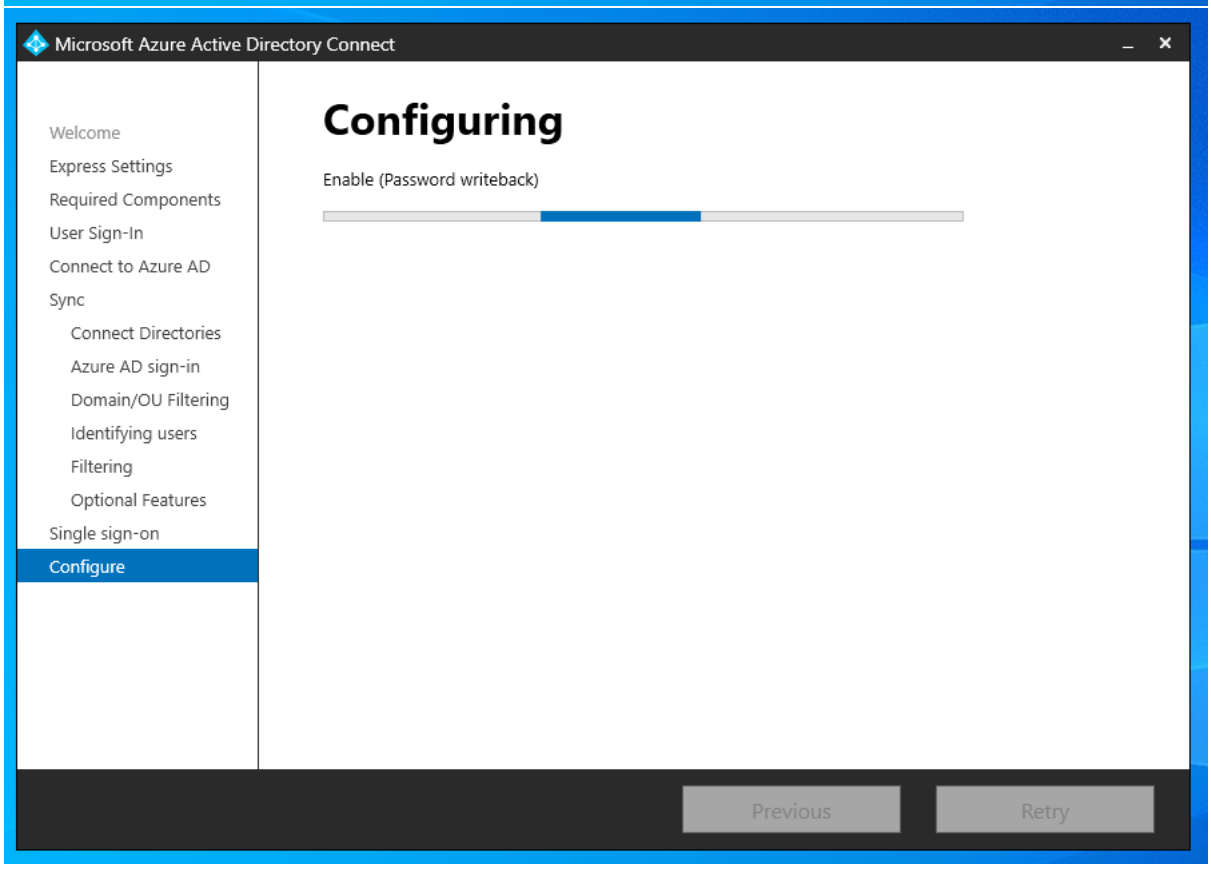

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Single sign-on
Configure
Filter users and devices
For a pilot deployment,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

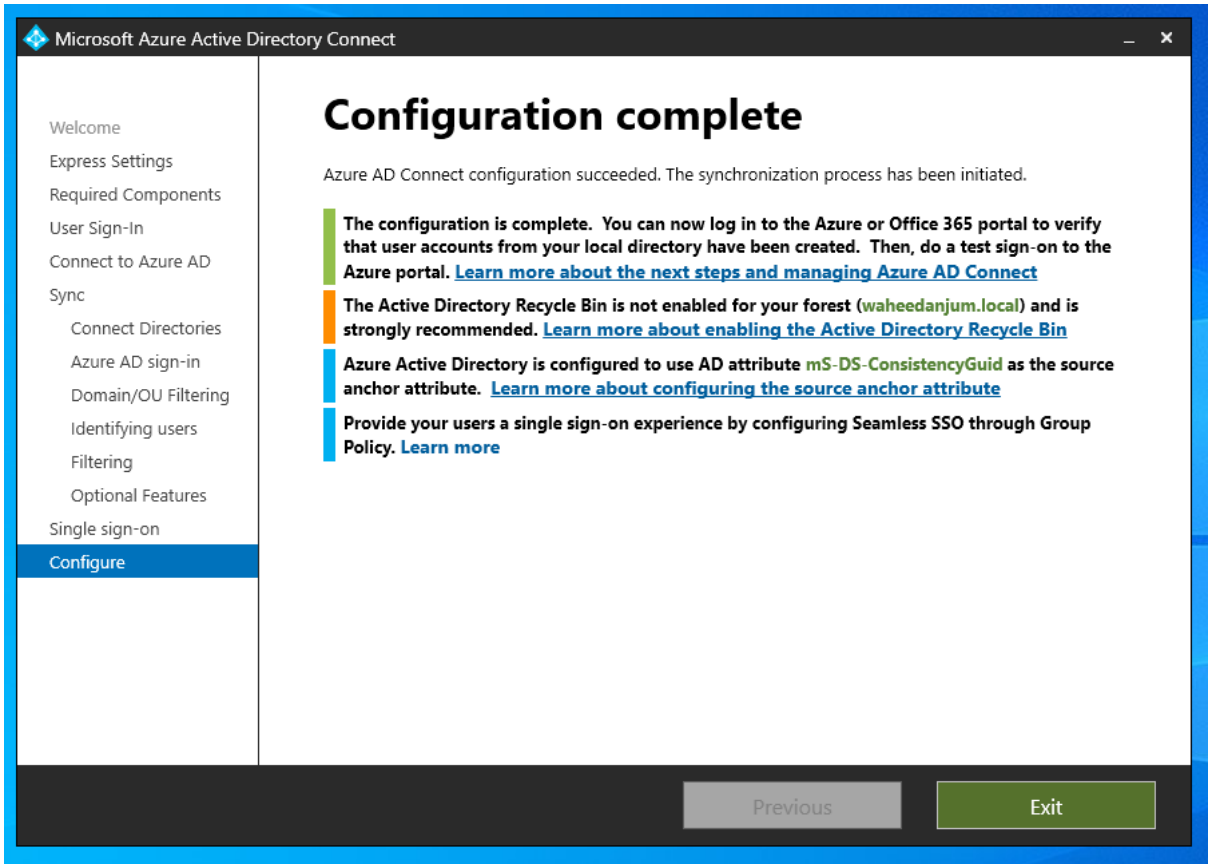

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Single sign-on
Configure
Optional features
Select enhanced functionality if required by your organization.
Exchange hybrid deployment
Exchange Mail Public Folders
Azure AD app and attribute filtering
Password hash synchronization
Password writeback
Group writeback
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
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.
waheedanjum.local
Enter credentials
Previous
Next

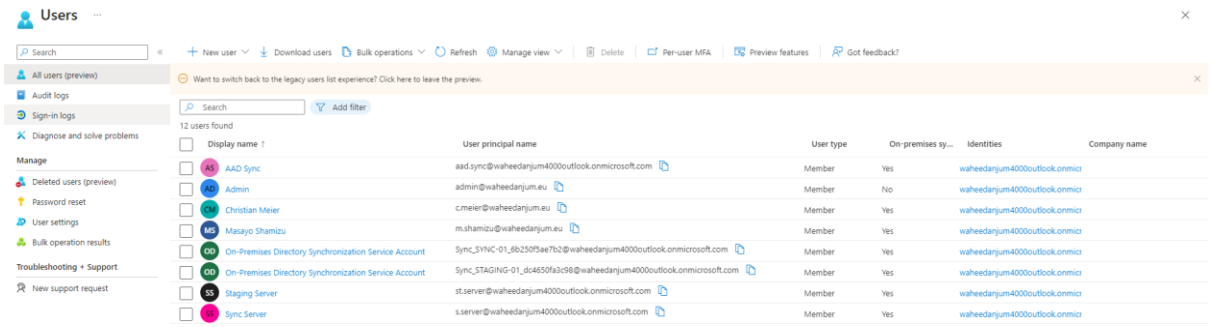

Microsoft Azure Active Directory Connect
Welcome
Express Settings
Required Components
User Sign-In
Connect to Azure AD
Sync
Connect Directories
Azure AD sign-in
Domain/OU Filtering
Identifying users
Filtering
Optional Features
Single sign-on
Configure
Ready to configure
Once you click Install, we will do the following:
Configure synchronization services on this computer
Enable single sign-on
Configure Source Anchor Attribute
Configure waheedanjum4000outlook.onmicrosoft.com - AAD Connector
Configure waheedanjum.local Connector
Enable Password hash synchronization
Enable Password writeback
Enable Azure AD Export Deletion Threshold (500)
For Sync Server
Start the synchronization process when configuration completes.
Enable staging mode: When selected, synchronization will not export any data to AD or Azure AD.
For Staging Server
Do not check BOTH BOXES
Users in your organization will not be able to log in. One or more domains in waheedanjum.local are missing the permissions required to enable password hash synchronization. Learn more about accounts and permissions
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
Single sign-on
Configure
Configuring
Creating the Azure Active Directory Synchronization Account
Previous
Retry


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
Configuring
Enable (Password writeback)
Previous
Retry



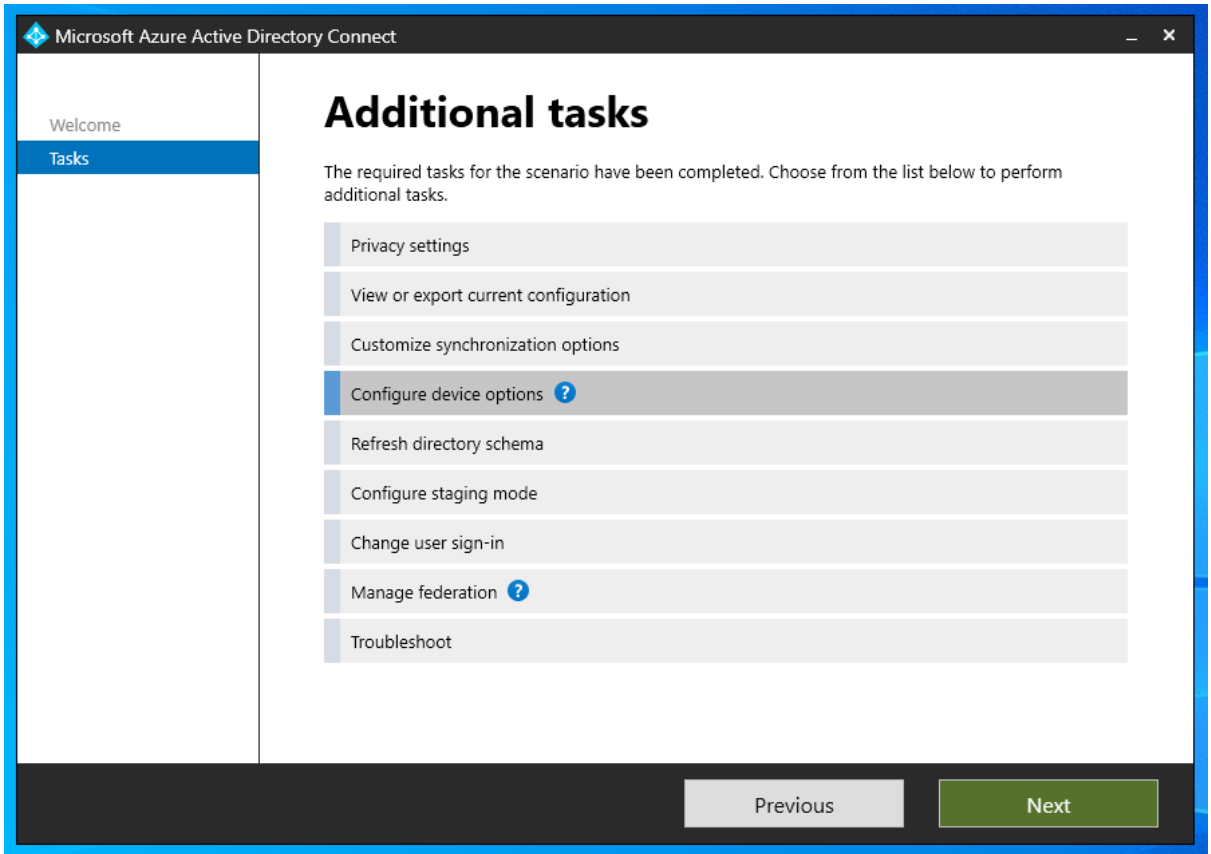
Go to Azure AD > Users > All the selected Local AD objects are synchronised**!**

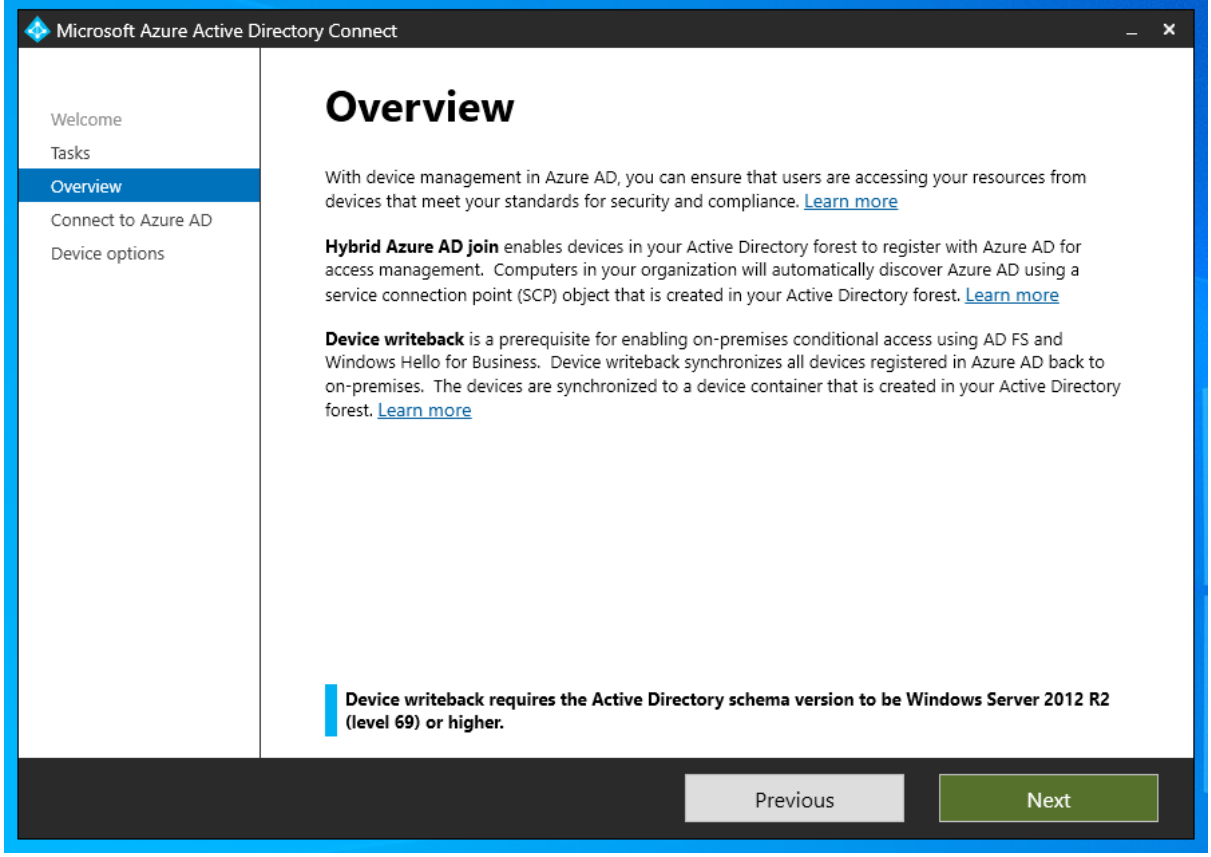


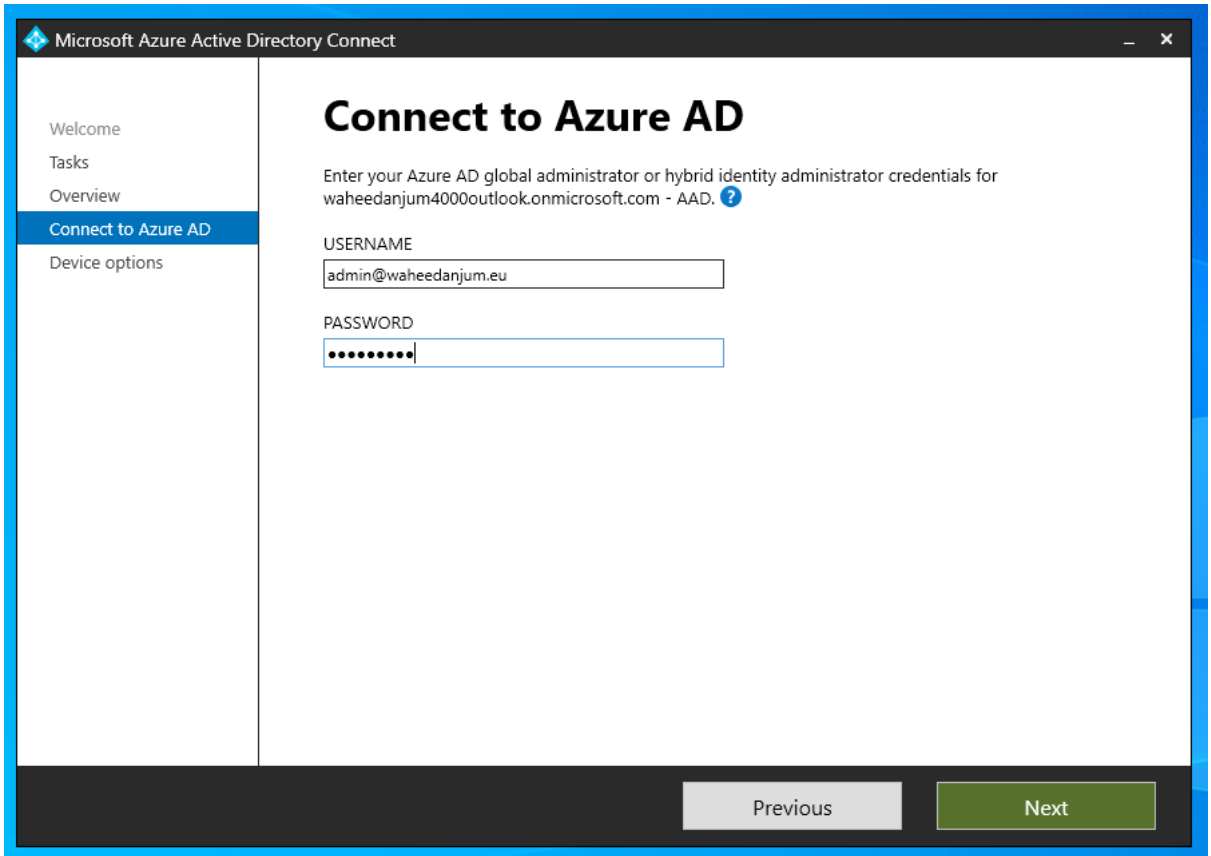
How to synchronize Local AD Devices to Azure Active Directory!

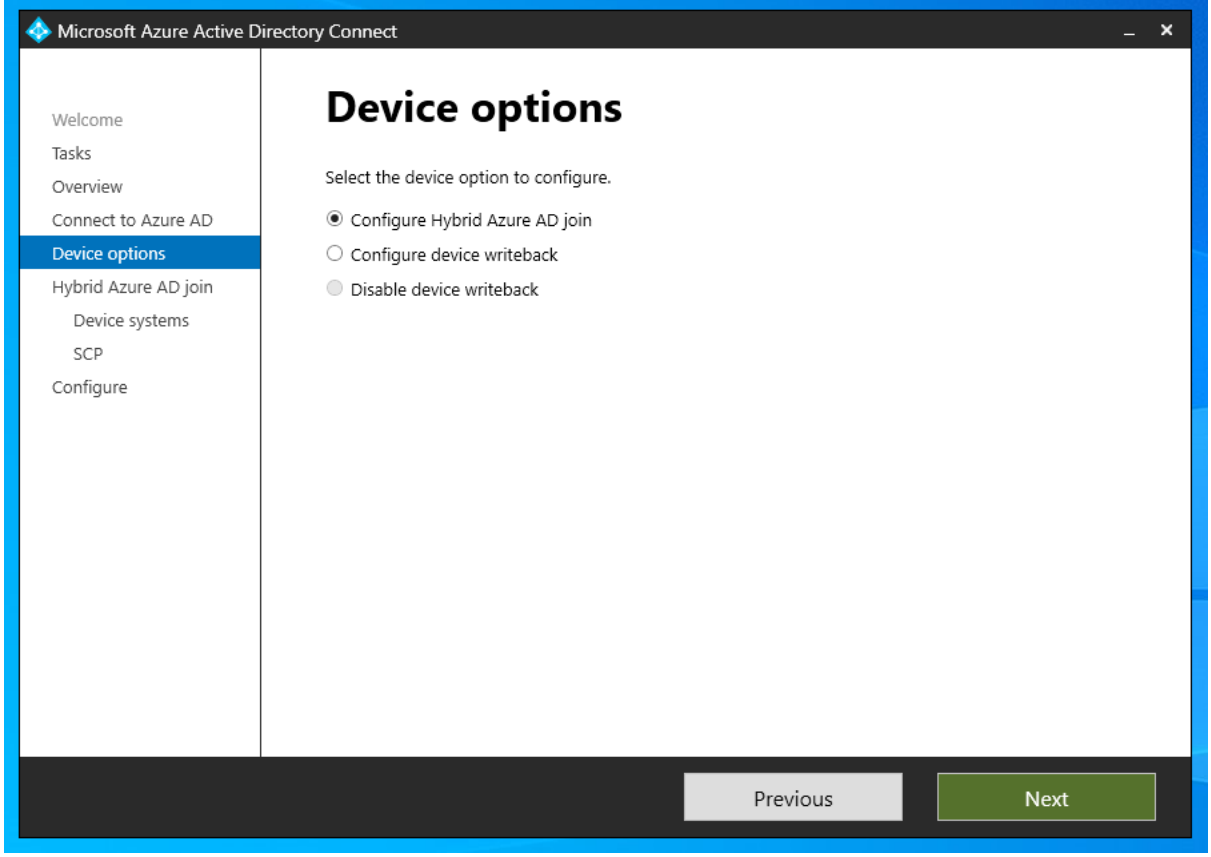
To synchronize local Active Directory (AD) devices to Azure AD, follow these steps:

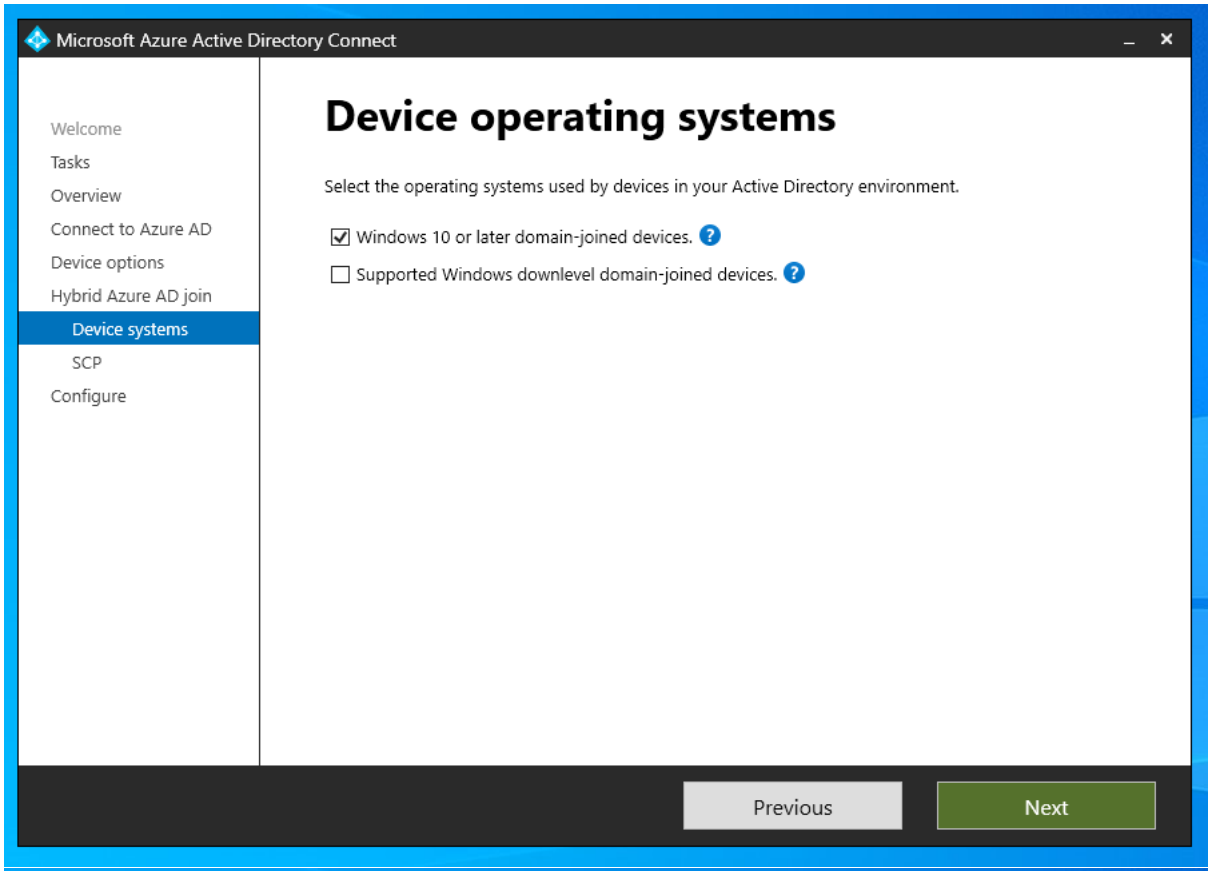
1. Log in to your Windows Server 2022 as an administrator.
2. Open Azure AD Connect Agent and follow the screenshots

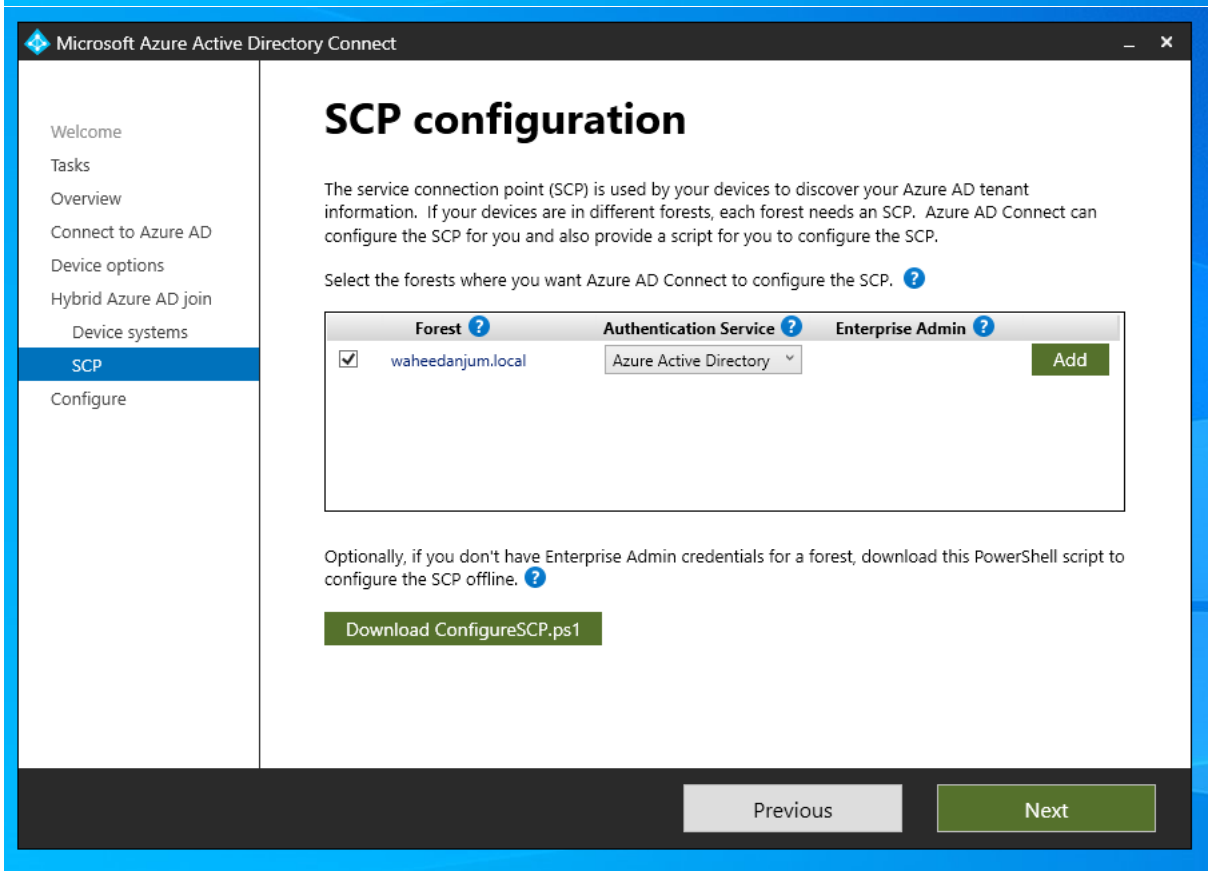

Microsoft Azure Active Directory Connect
Welcome
Tasks
Additional tasks
The required tasks for the scenario have been completed. Choose from the list below to perform additional tasks.
Privacy settings
View or export current configuration
Customize synchronization options
Configure device options
Refresh directory schema
Configure staging mode
Change user sign-in
Manage federation
Troubleshoot
Previous
Next

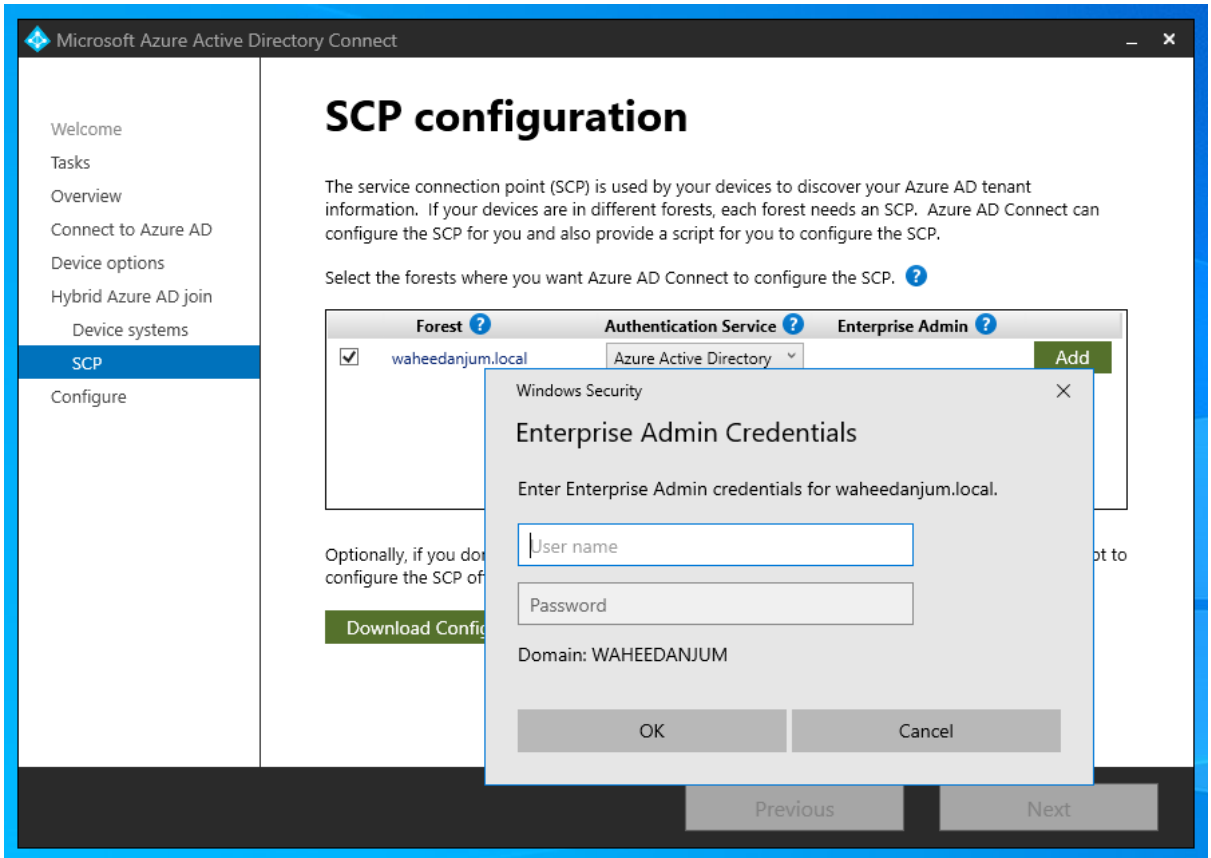

Microsoft Azure Active Directory Connect
Welcome
Tasks
Overview
Connect to Azure AD
Device options
Overview
With device management in Azure AD, you can ensure that users are accessing your resources from devices that meet your standards for security and compliance. Learn more
Hybrid Azure AD join enables devices in your Active Directory forest to register with Azure AD for access management. Computers in your organization will automatically discover Azure AD using a service connection point (SCP) object that is created in your Active Directory forest. Learn more
Device writeback is a prerequisite for enabling on-premises conditional access using AD FS and Windows Hello for Business. Device writeback synchronizes all devices registered in Azure AD back to on-premises. The devices are synchronized to a device container that is created in your Active Directory forest. Learn more
Device writeback requires the Active Directory schema version to be Windows Server 2012 R2 (level 69) or higher.
Previous
Next

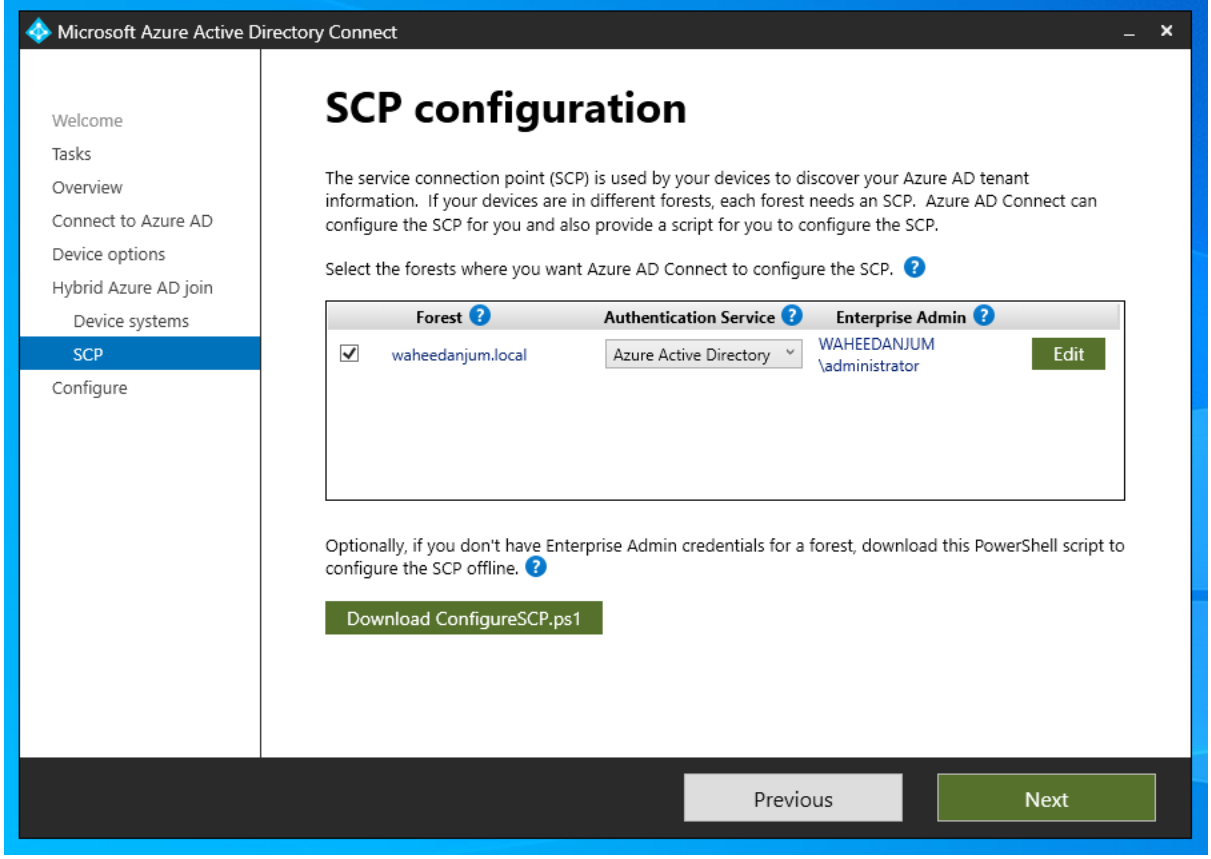

Microsoft Azure Active Directory Connect
Welcome
Tasks
Overview
Connect to Azure AD
Device options
Connect to Azure AD
Enter your Azure AD global administrator or hybrid identity administrator credentials for waheedanjum4000outlook.onmicrosoft.com - AAD.
USERNAME
admin@waheedanjum.eu
PASSWORD
Previous
Next

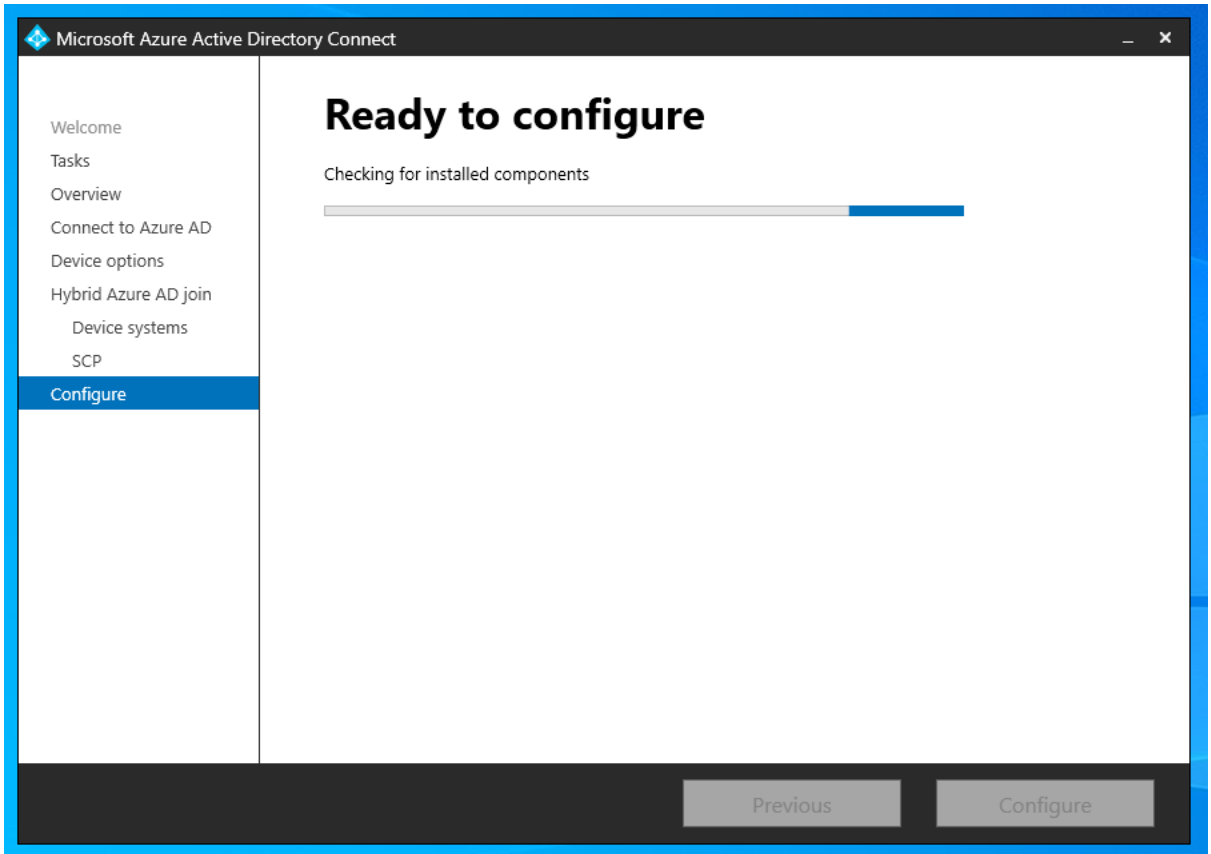

Microsoft Azure Active Directory Connect
Welcome
Tasks
Overview
Connect to Azure AD
Device options
Hybrid Azure AD join
Device systems
SCP
Configure
Device options
Select the device option to configure.
Configure Hybrid Azure AD join
Configure device writeback
Disable device writeback
Previous
Next

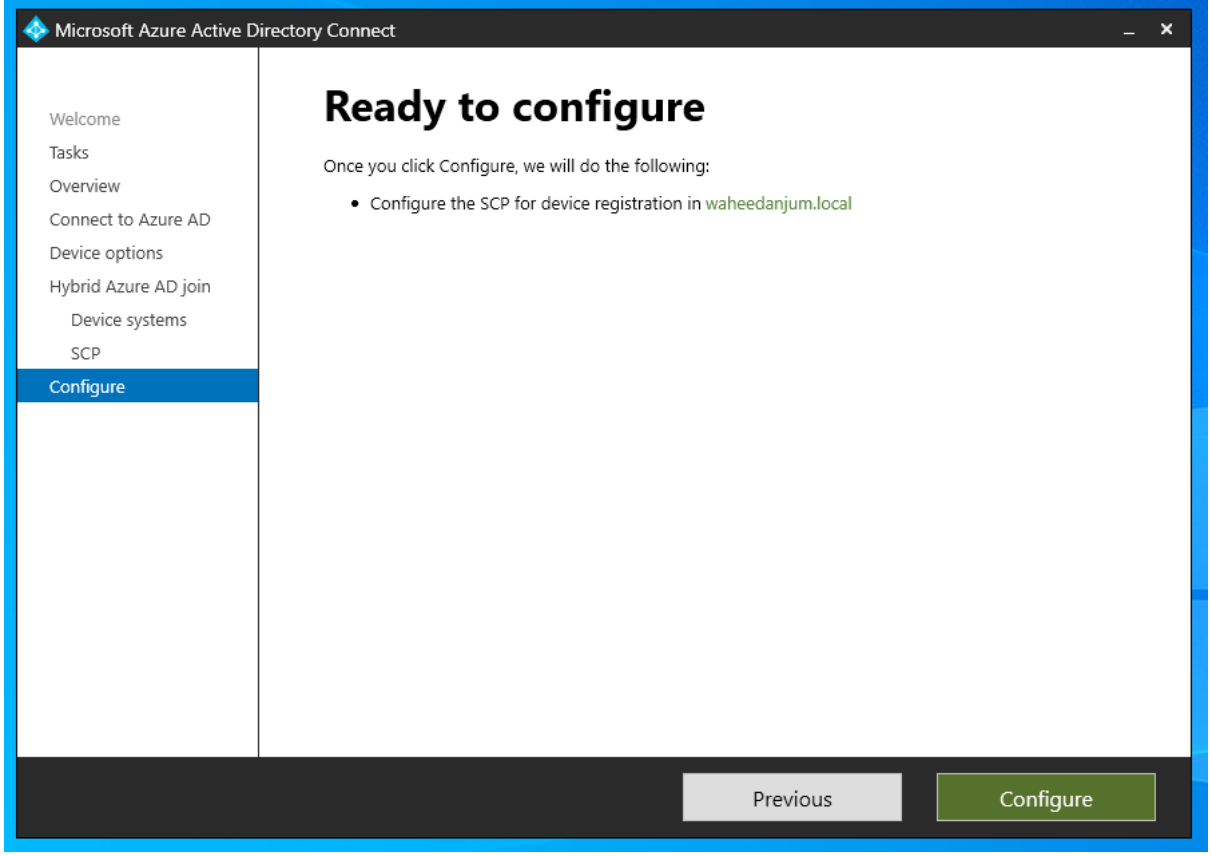

Microsoft Azure Active Directory Connect
Welcome
Tasks
Overview
Connect to Azure AD
Device options
Hybrid Azure AD join
Device systems
SCP
Configure
Device operating systems
Select the operating systems used by devices in your Active Directory environment.
Windows 10 or later domain-joined devices.
Supported Windows downlevel domain-joined devices.
Previous
Next

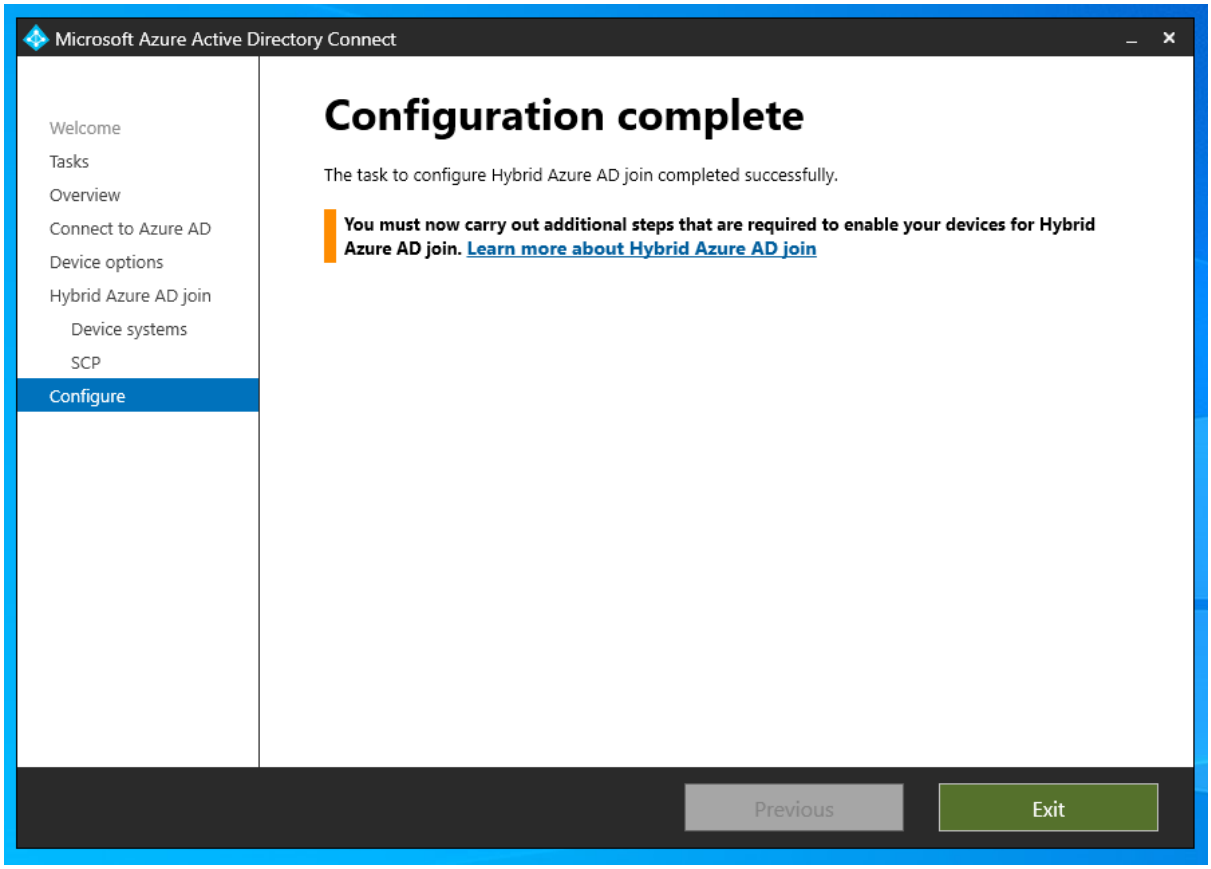

Microsoft Azure Active Directory Connect
Welcome
Tasks
Overview
Connect to Azure AD
Device options
Hybrid Azure AD join
Device systems
SCP
Configure
SCP configuration
The service connection point (SCP) is used by your devices to discover your Azure AD tenant information. If your devices are in different forests, each forest needs an SCP. Azure AD Connect can configure the SCP for you and also provide a script for you to configure the SCP.
Select the forests where you want Azure AD Connect to configure the SCP.
Forest
Authentication Service
Enterprise Admin
waheedanjum.local
Azure Active Directory
Add
Optionally, if you don't have Enterprise Admin credentials for a forest, download this PowerShell script to configure the SCP offline.
Download ConfigureSCP.ps1
Previous
Next


Microsoft Azure Active Directory Connect
Welcome
Tasks
Overview
Connect to Azure AD
Device options
Hybrid Azure AD join
Device systems
SCP
Configure
SCP configuration
The service connection point (SCP) is used by your devices to discover your Azure AD tenant information. If your devices are in different forests, each forest needs an SCP. Azure AD Connect can configure the SCP for you and also provide a script for you to configure the SCP.
Select the forests where you want Azure AD Connect to configure the SCP.
Forest
Authentication Service
Enterprise Admin
waheedanjum.local
Azure Active Directory
Add
Windows Security
Enterprise Admin Credentials
Enter Enterprise Admin credentials for waheedanjum.local.
User name
Password
Domain: WAHEEDANJUM
OK
Cancel
Optionally, if you do
configure the SCP of
ot to
Download Confi
Previous
Next

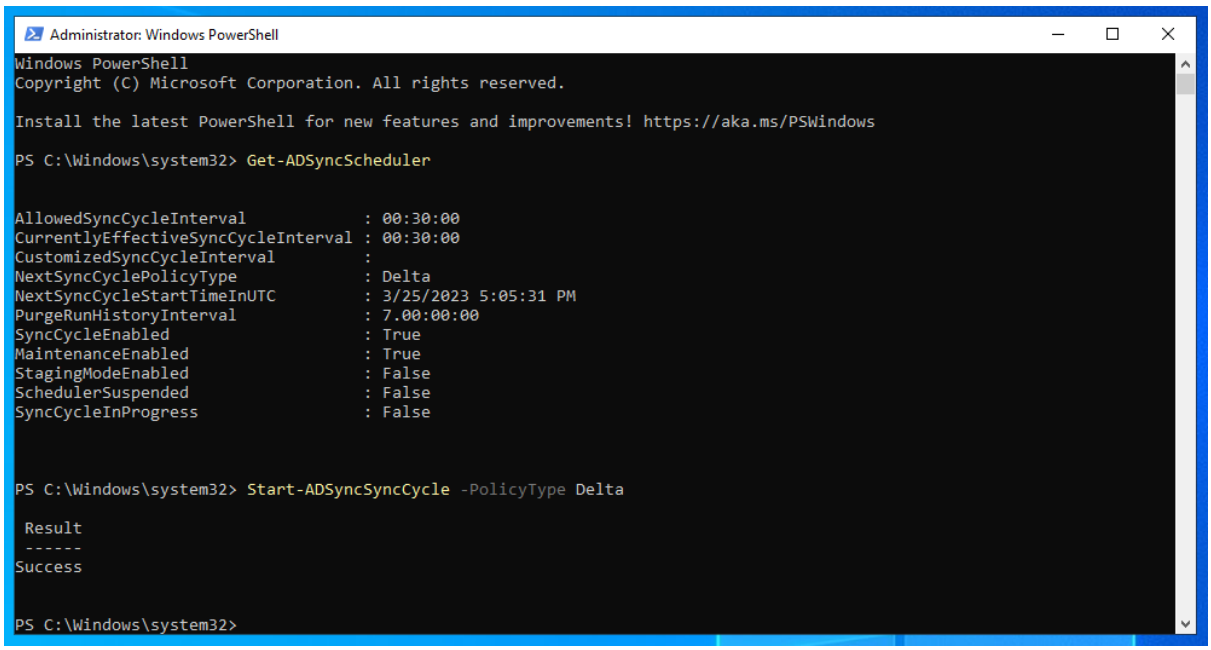

Microsoft Azure Active Directory Connect
Welcome
Tasks
Overview
Connect to Azure AD
Device options
Hybrid Azure AD join
Device systems
SCP
Configure
SCP configuration
The service connection point (SCP) is used by your devices to discover your Azure AD tenant information. If your devices are in different forests, each forest needs an SCP. Azure AD Connect can configure the SCP for you and also provide a script for you to configure the SCP.
Select the forests where you want Azure AD Connect to configure the SCP.
Forest
Authentication Service
Enterprise Admin
waheedanjum.local
Azure Active Directory
WAHEEDANJUM
\administrator
Edit
Optionally, if you don't have Enterprise Admin credentials for a forest, download this PowerShell script to configure the SCP offline.
Download ConfigureSCP.ps1
Previous
Next


Microsoft Azure Active Directory Connect
Welcome
Tasks
Overview
Connect to Azure AD
Device options
Hybrid Azure AD join
Device systems
SCP
Configure
Ready to configure
Checking for installed components
Previous
Configure


Microsoft Azure Active Directory Connect
Welcome
Tasks
Overview
Connect to Azure AD
Device options
Hybrid Azure AD join
Device systems
SCP
Configure
Ready to configure
Once you click Configure, we will do the following:
Configure the SCP for device registration in waheedanjum.local
Previous
Configure



Open PowerShell with Administrator rights and run the following command to make immediate sync with Azure AD.



Good Luck!