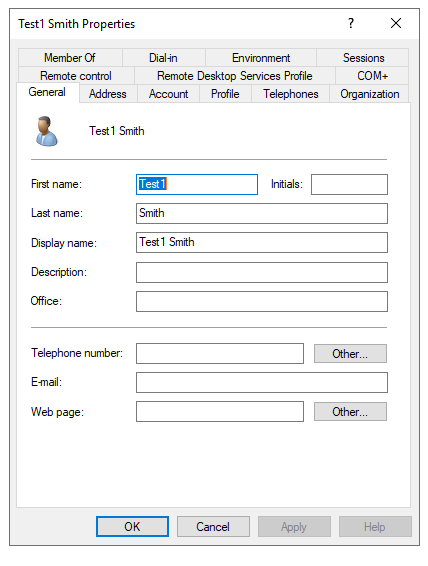
# AD Sync Configuration on Test AD

AD Connect Tool has been installed on ad.logiway.eu Domain Controller (dc01logiwayeu.westeurope.cloudapp.azure.com virtual machine)

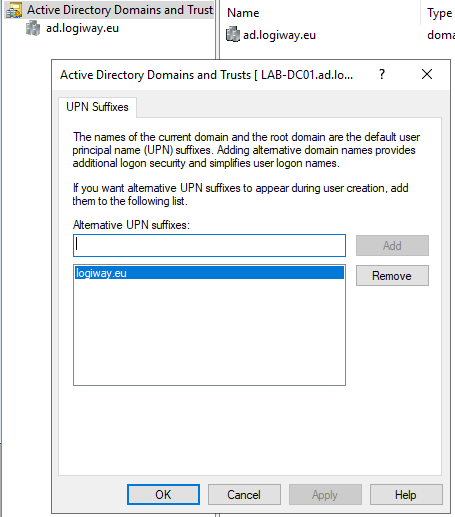
Test users have been created in on-premise AD:

​​​​​​​​​​​

Passwords are: Passw0rd!

Add alternate UPN suffixes to the forest:

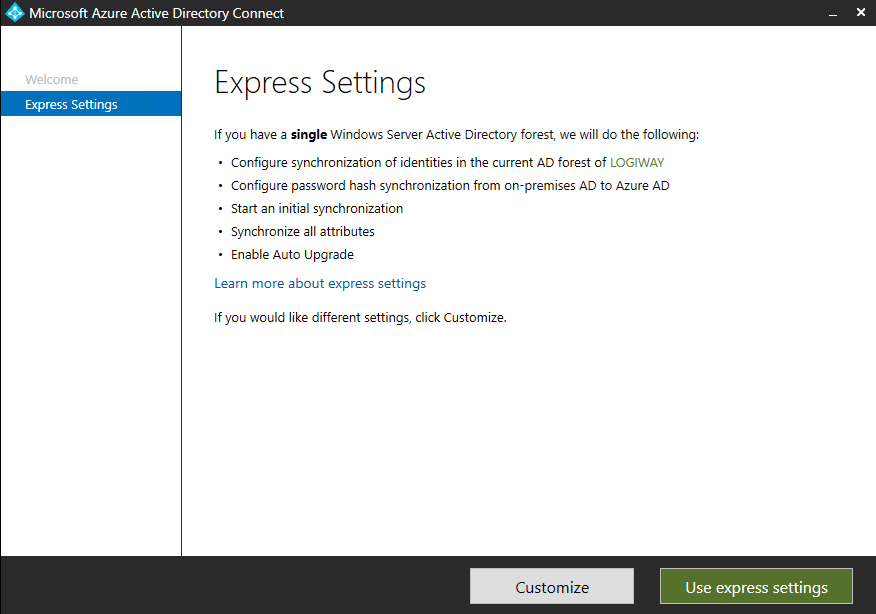
<https://docs.microsoft.com/en-us/office365/enterprise/prepare-a-non-routable-domain-for-directory-synchronization?redirectSourcePath=%252fen-us%252farticle%252fhow-to-prepare-a-non-routable-domain-such-as-local-domain-for-directory-synchronization-e7968303-c234-46c4-b8b0-b5c93c6d57a7>



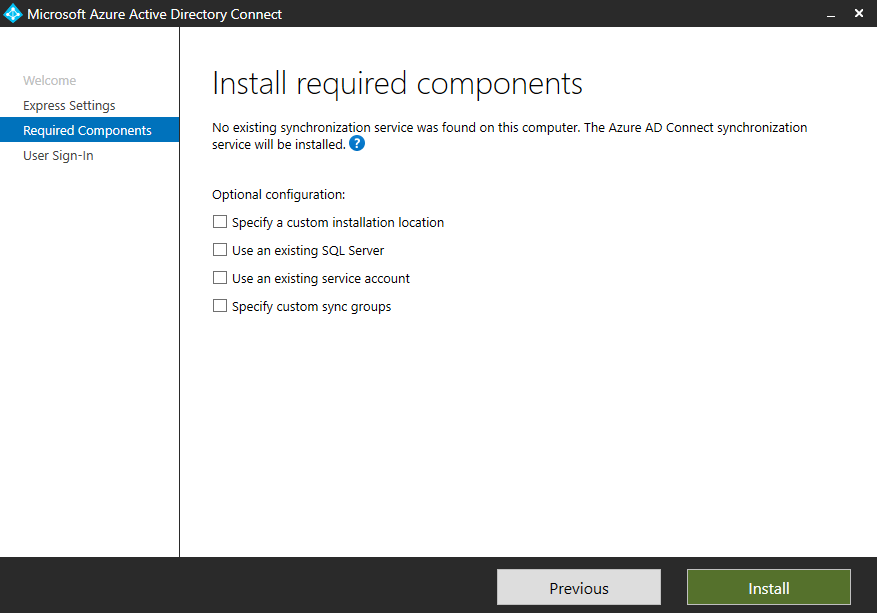
# AD Connect

Run AzureADConnect.msi

Click “Customize” (not “Use express settings”)

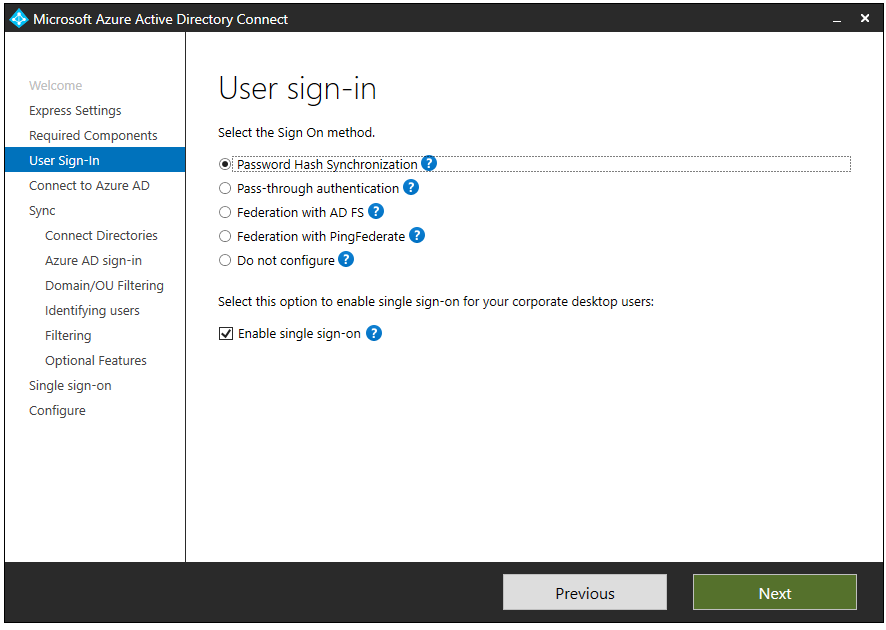


Unless required, don’t check any checkboxes on the next page:

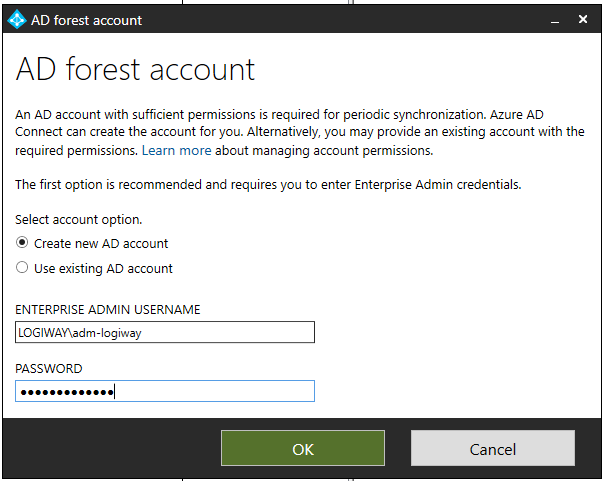


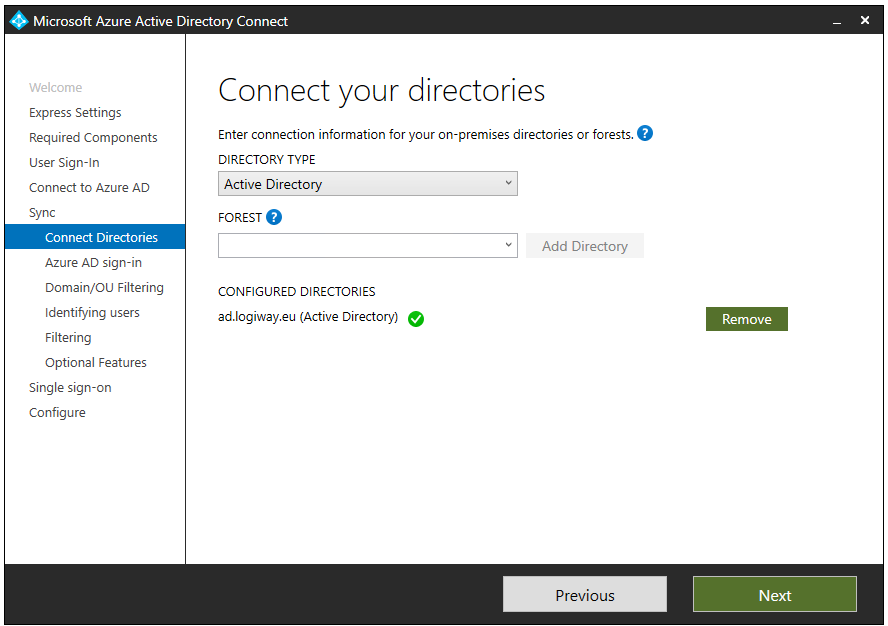
## Password Hash Synchronization

Select “Password Hash Synchronization” option together with “Single Sign-on”



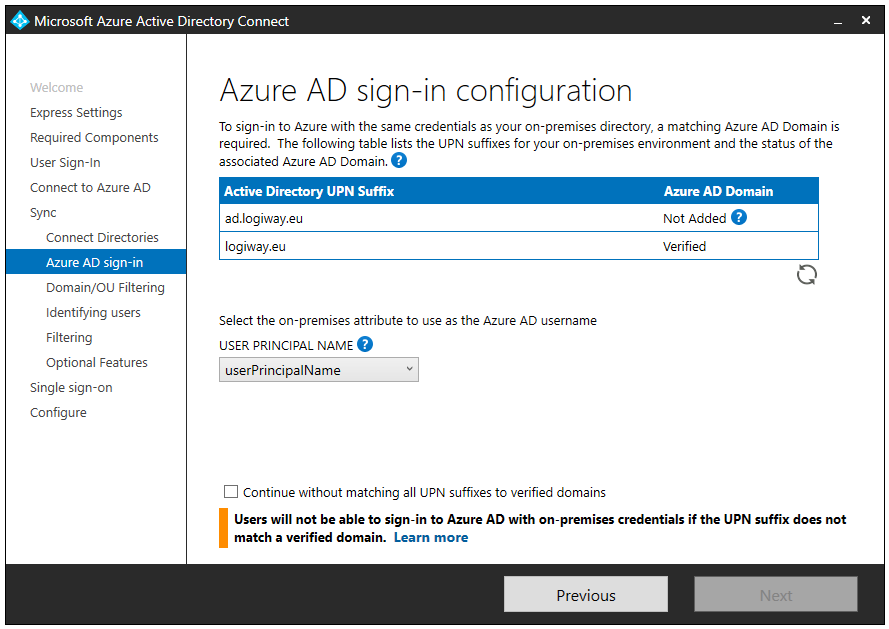
Add ad.logiway.eu AD Tree to configured directories



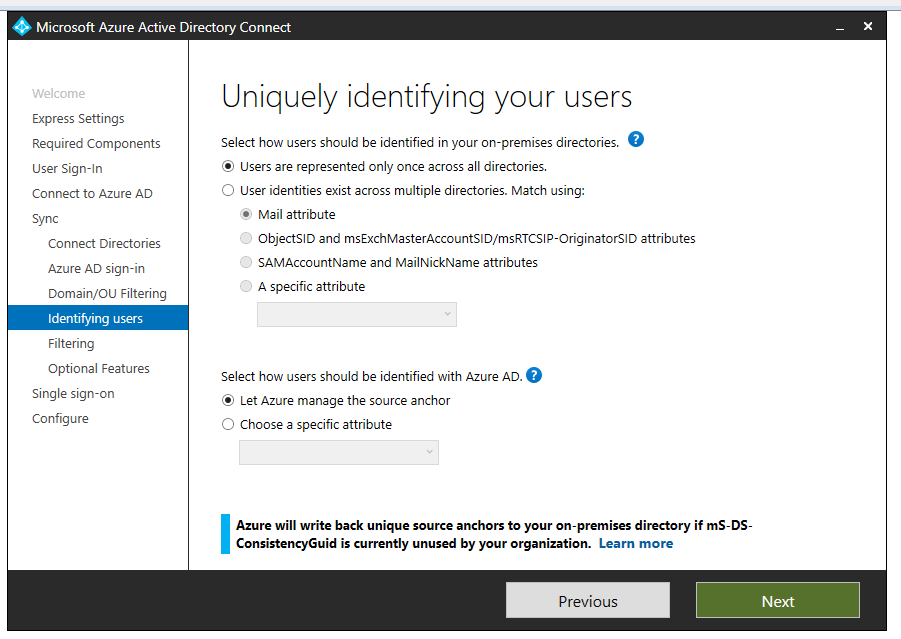


​UPN is selected as "primary key" for synchronization.

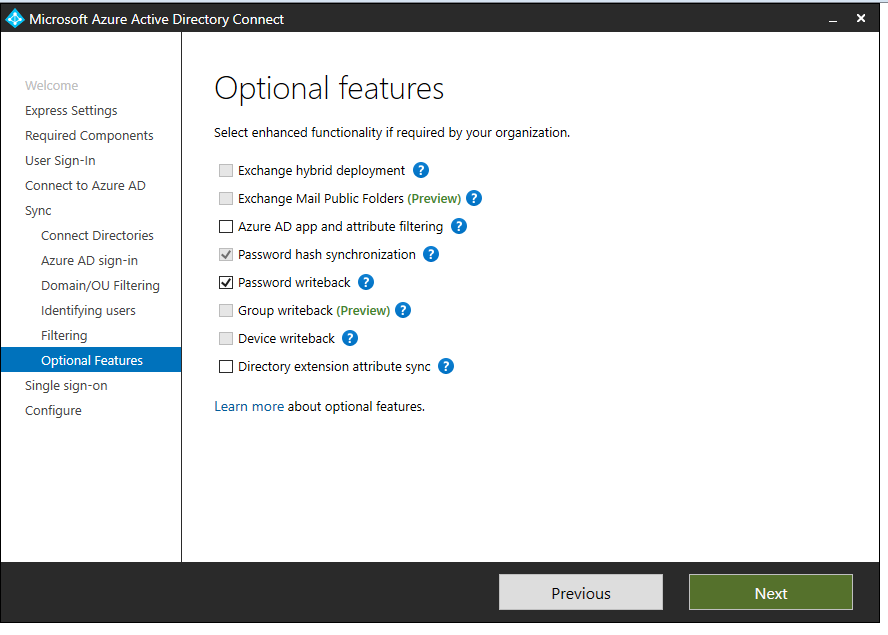
Note that only @logiway.eu users will be synchronized

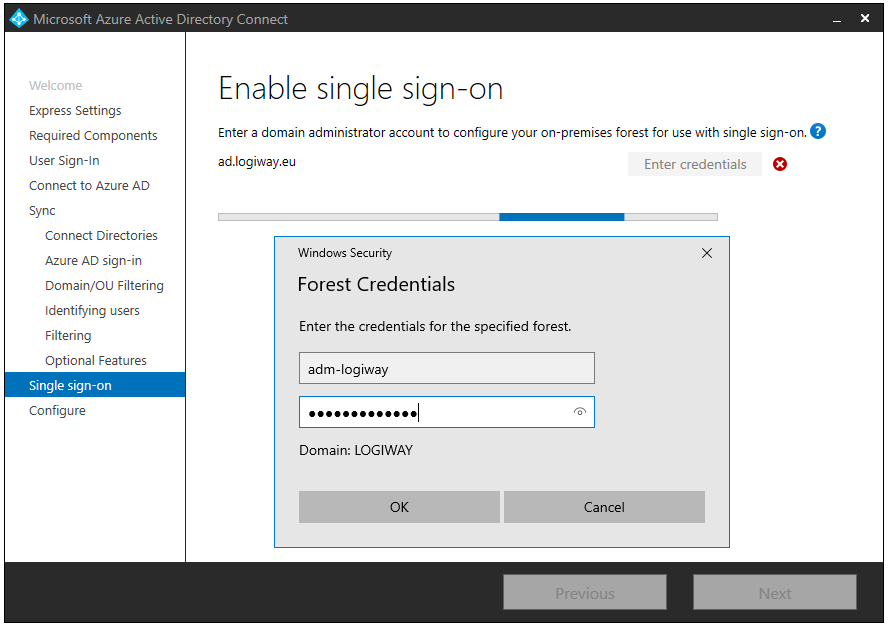


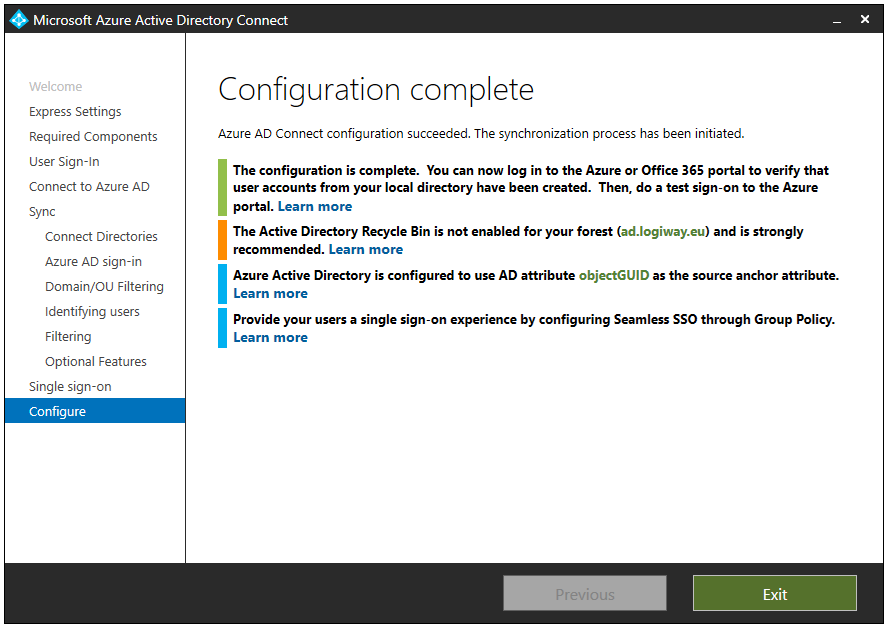
​Users are unique.

Password writeback is enabled.

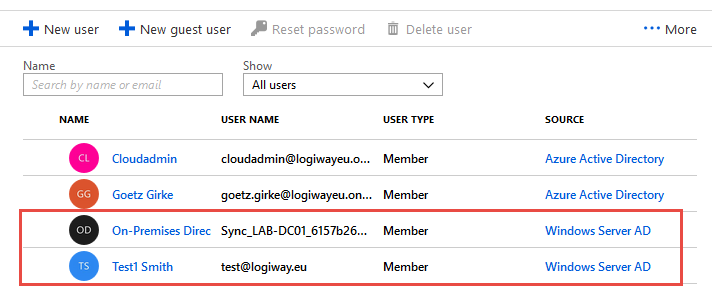
<https://docs.microsoft.com/en-us/azure/active-directory/authentication/quickstart-sspr#enable-users-to-reset-or-change-their-ad-passwords>

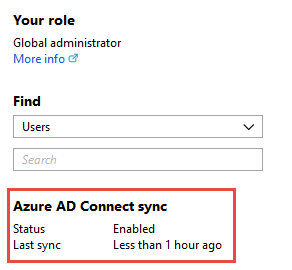
[https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment#)

Single Sign-on requires admin account

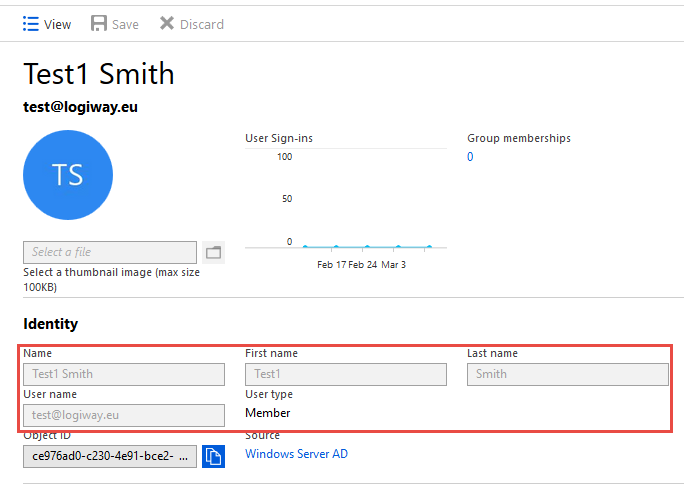
​

After some minutes, Users from On-Prem AD are imported in Azure AD:

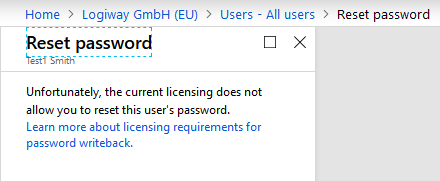




Editing of those users' settings is disabled:

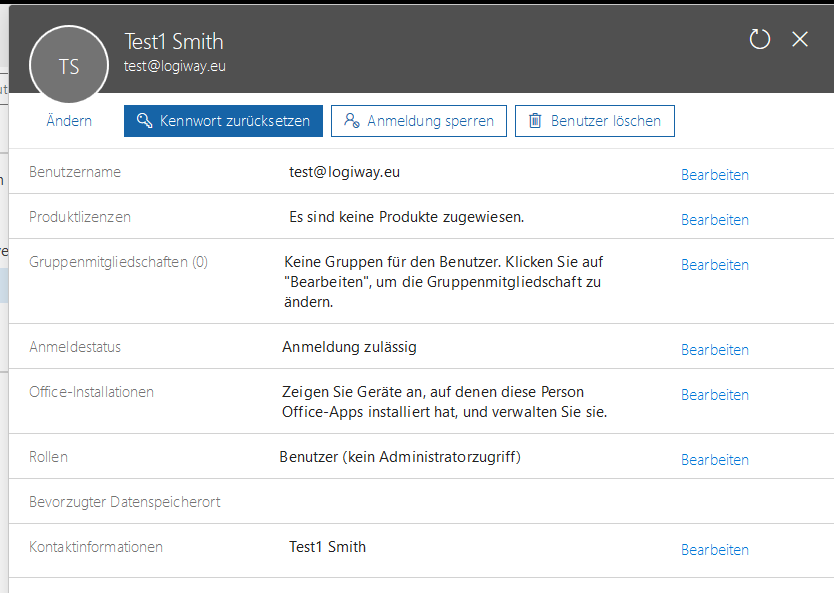


Password reset was disabled due to licensing level, currently there’s Premium subscription assigned to the tenant:

​

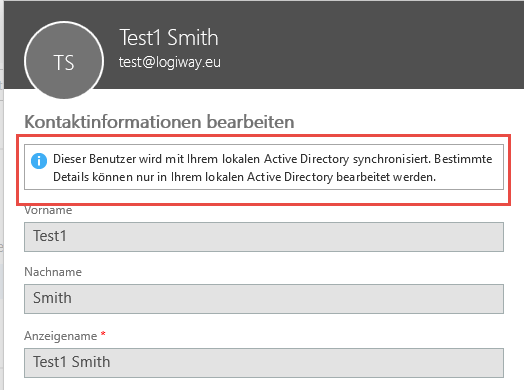
<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-writeback#licensing-requirements-for-password-writeback>

It is possible although to change the password in O365 Portal



When password is updated on DC01, it is then synchronized to Azure AD (tested with Test1).

User information is either not editable in O365 Portal



References:

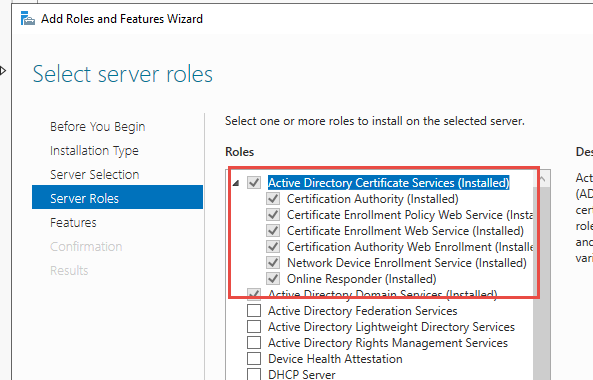
<https://azure.microsoft.com/en-us/resources/videos/configuring-ad-fs-for-user-sign-in-with-azure-ad-connect/>

<https://medium.com/in-the-weeds/create-a-test-active-directory-federation-services-3-0-instance-on-an-azure-virtual-machine-9071d978e8ed>

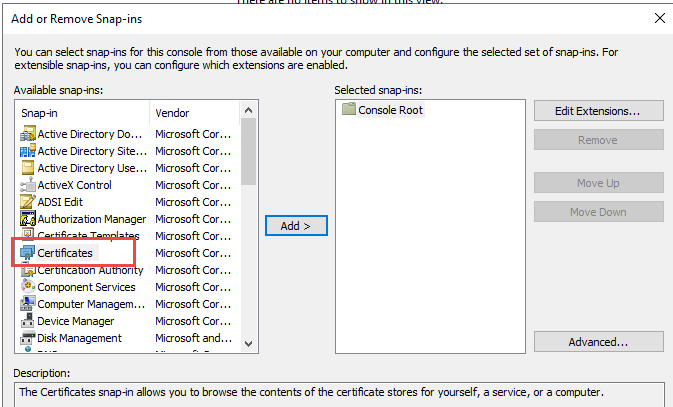
## Federation with ADFS

ADFS Configuration re quires valid certificate to enable trust relations between parts.

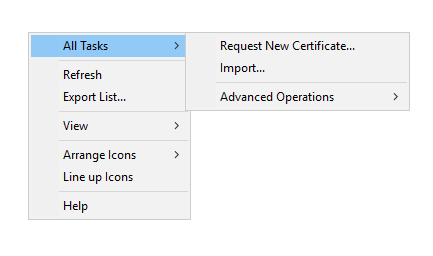
Thus “Certificate Authority” Role must be installed on Windows Server, it is not enough to have



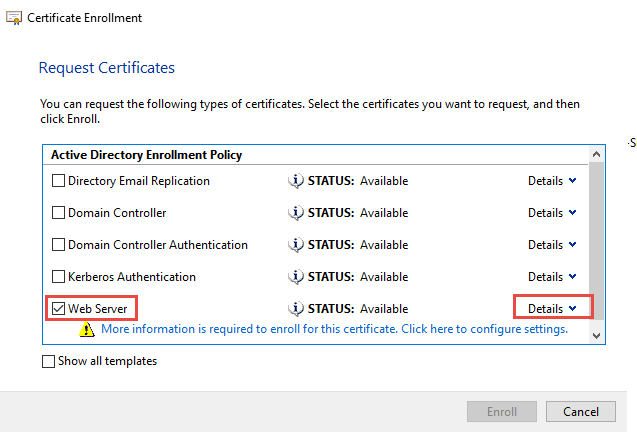
Start mmc.exe, add “Certificates” snap-in for local computer account.



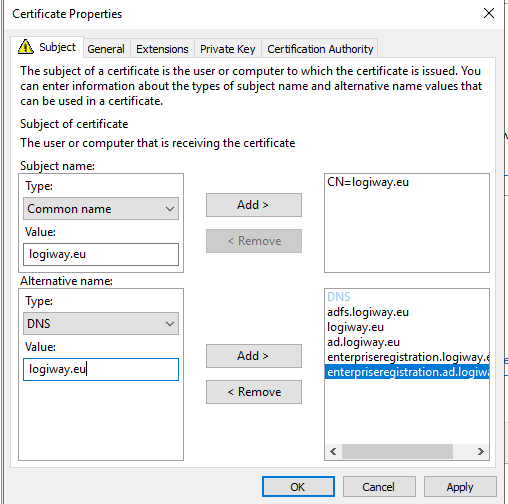
Then request new certificate



Click Next and then select “Web Server” Template (if template is missing, add “Certificate Templates” snap-in to mmc and ensure that current user has enroll permissions).



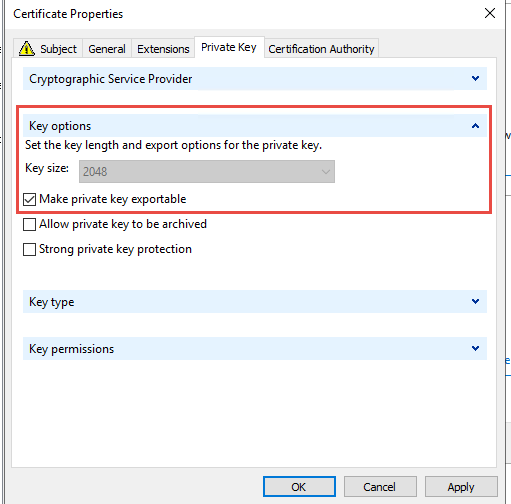
Configure “Common name” and “Alternative name”



CN = logiway.eu

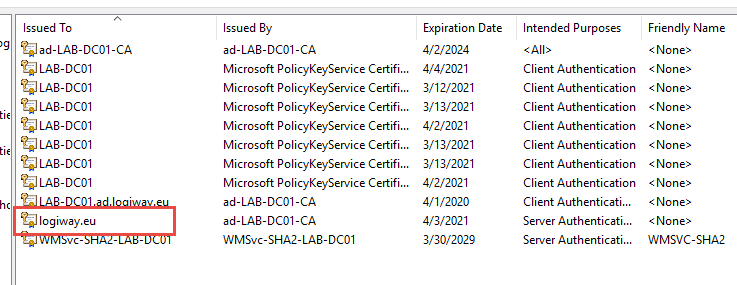
Alternative = adfs.logiway.eu, logiway.eu, ad.logiway.eu, enterpriseregistration.logiway.eu, enterpriseregistration.ad.logiway.eu, dc01logiwayeu.westeurope.cloudapp.azure.com (add each value separately)

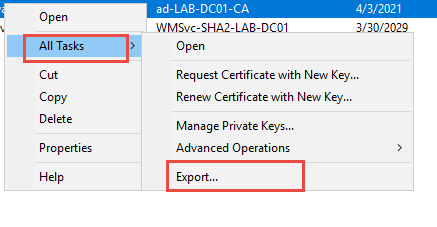
Enable Private key



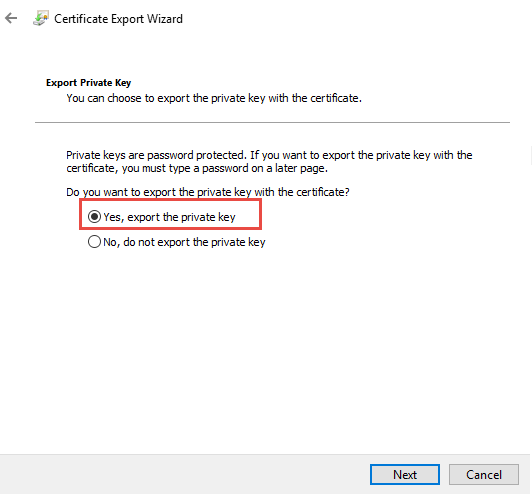
Click “OK” and then “Enroll”.

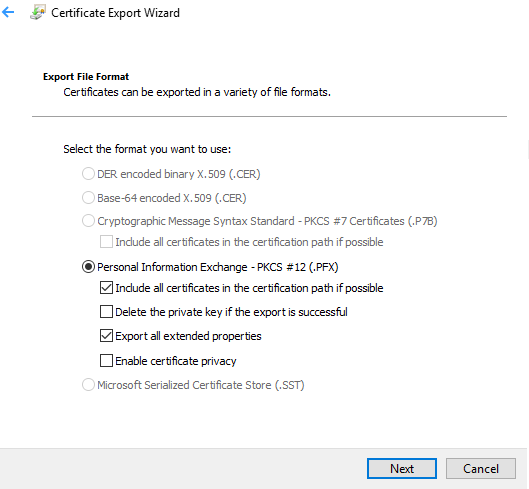
Certificate appears in the list. Not export it to a file:



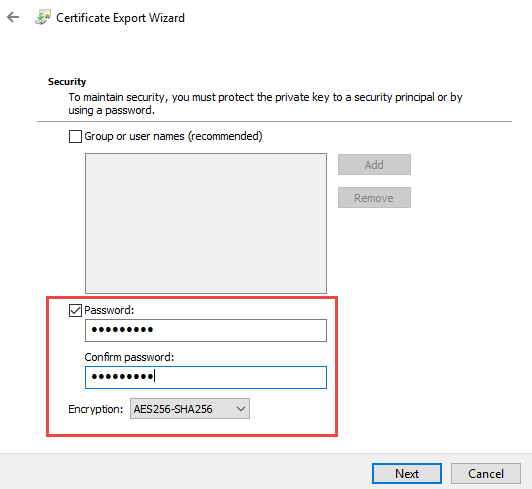


Select “Export the private key”

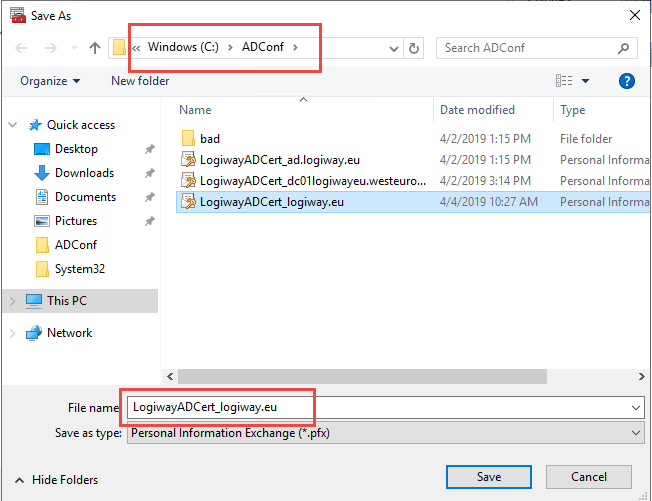




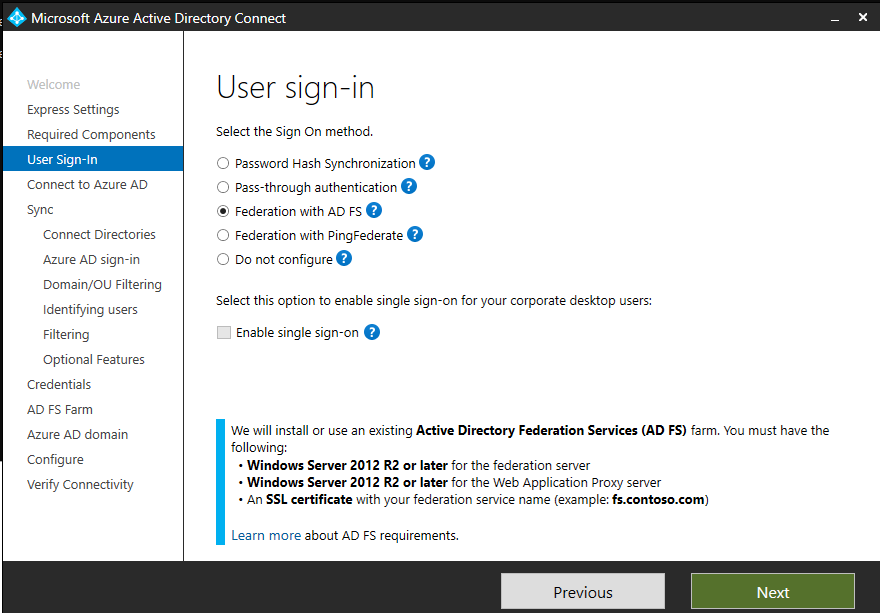
Enter password for the certificate (“Passw0rd!”):

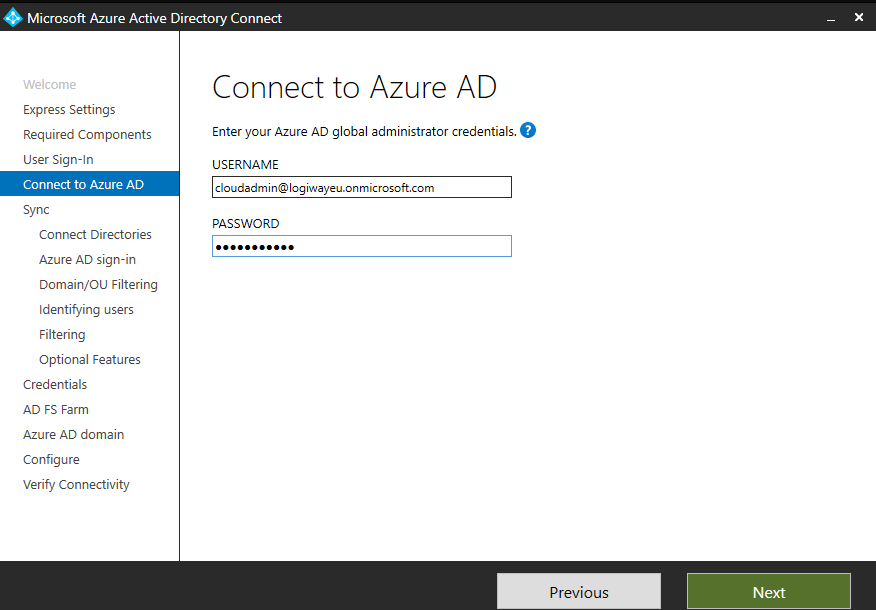


And store the certificate in safe place (under C:\ADConf).



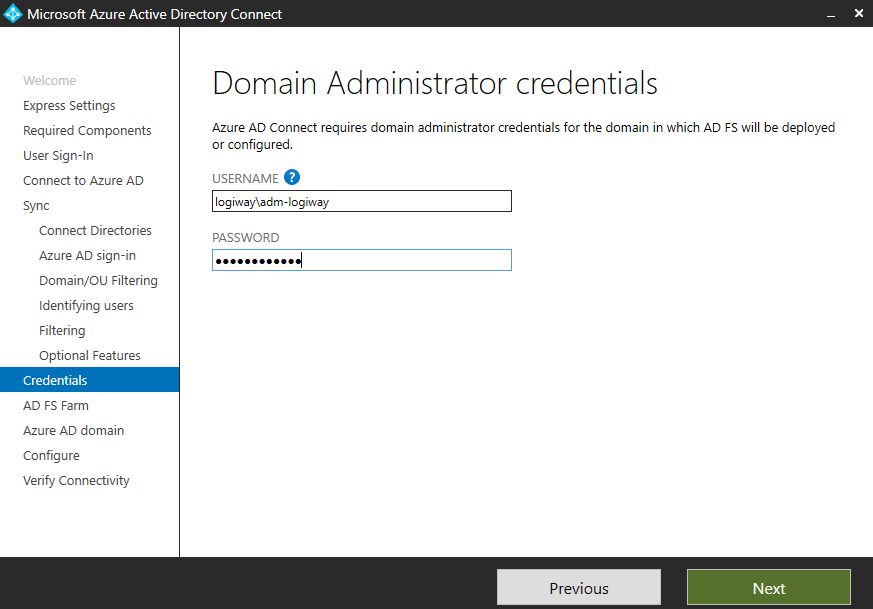
Now run AD Connect wizard, nut on “User sign-in” page select “Federation with ADFS”



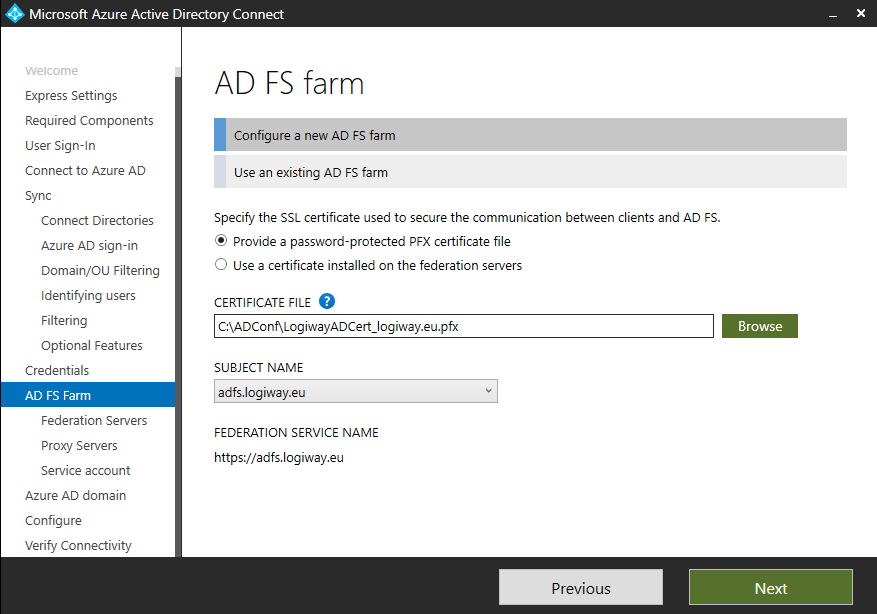


Then as for password hash synchronization, select directories, configure filtering if needed, select password hash synchronization on “Optional features” page.

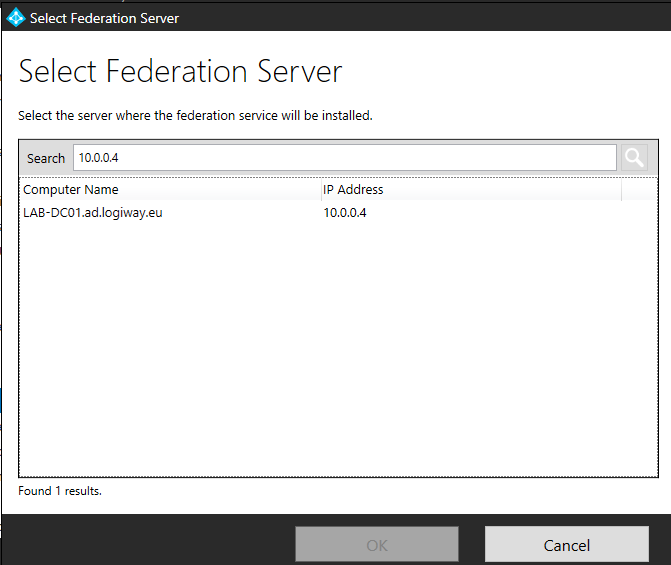
Enter domain administrator credentials



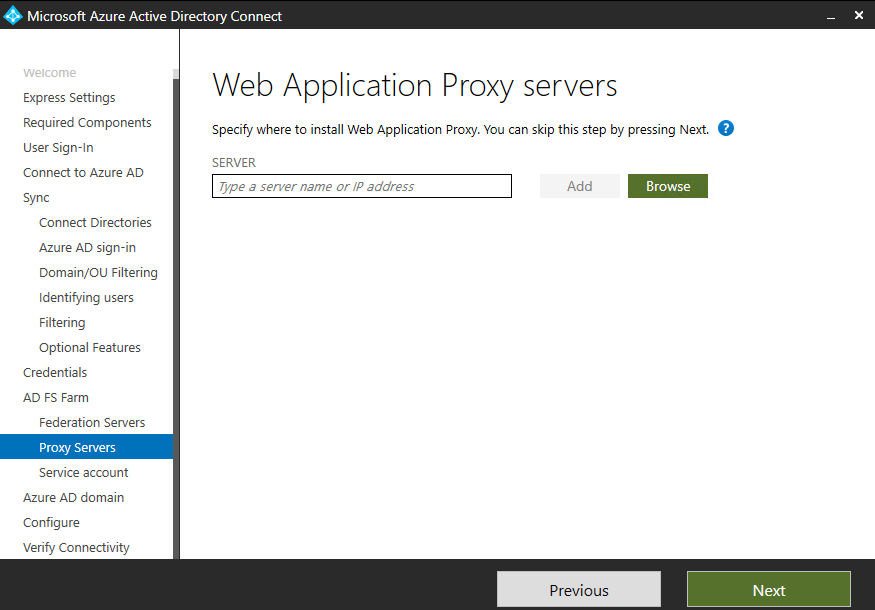
Enter path to certificate file, answer to the prompt on password (“Passw0rd!”), select subject name for ADFS (adfs.logiway.eu):

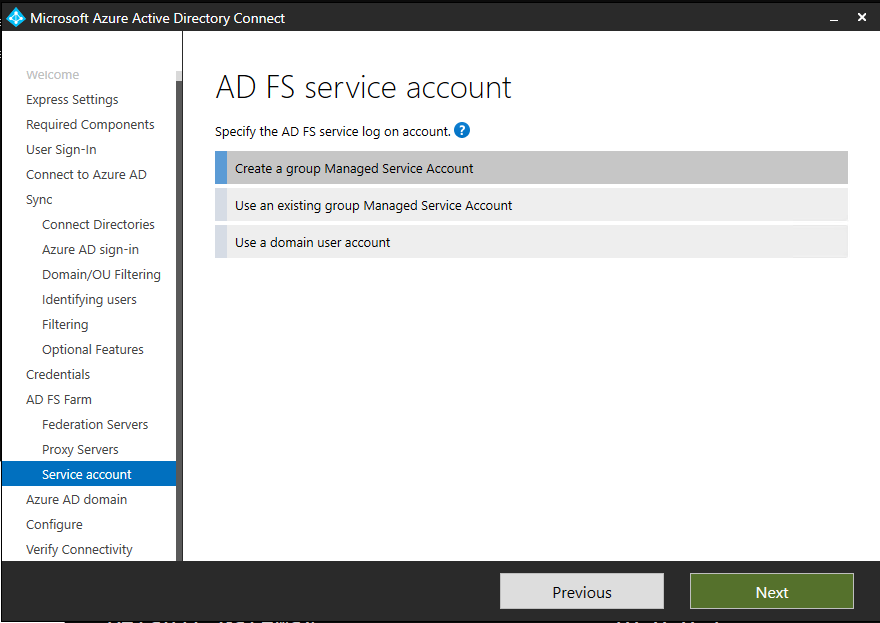


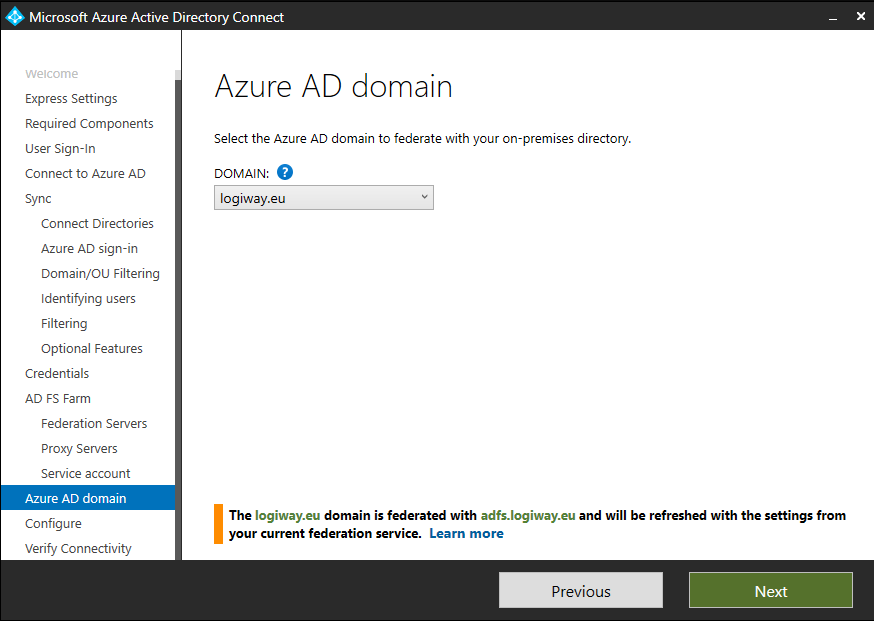
Select server on which to install Federation Server:

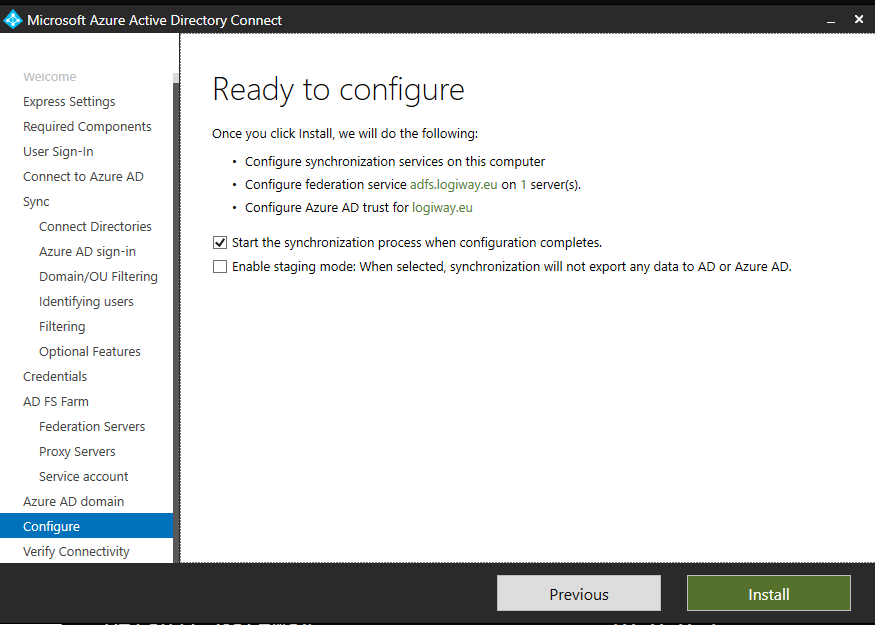


Proxy servers must be installed on another machines, so leave this page empty.









After installation, Azure AD and local domain will be federated, users will be synchronized and SSO is enabled.

But: User properties are still not editable in Azure AD Portal.