Azure Active Directory Federated Services

Wednesday, January 20, 2021 4:15 PM

The example below demonstrates how to create, configure and validate Azure Active Directory Federation Service. It creates a fictional Azure Active Directory, Toaster inc., a Custom domain, toaster.tk, and a Global Azure Active Directory admin, toaster@toasterc.onmicrosoft.com.

Even though it is recommended to secure a computer with Hyper-V installed. It is suggested to do this on either a Windows 10 or a Windows Server 2016 computer. But, since this PoC was done in the Azure lab environment, a VM was created with at least 8 GB of memory and Microsoft Windows Server 2016-Datacenter.

It creates a Windows Server, dc1-vm1 and a Windows Server AD user, Allie McCray. It registers the domain (toaster.tk) with Freenom.com. It adds both TXT and A records with the registrar. It uses myapps.microsoft.com to validate that the federated trust works.

This PoC is based on Tutorial: Federate a single AD forest environment to Azure | Microsoft Docs.

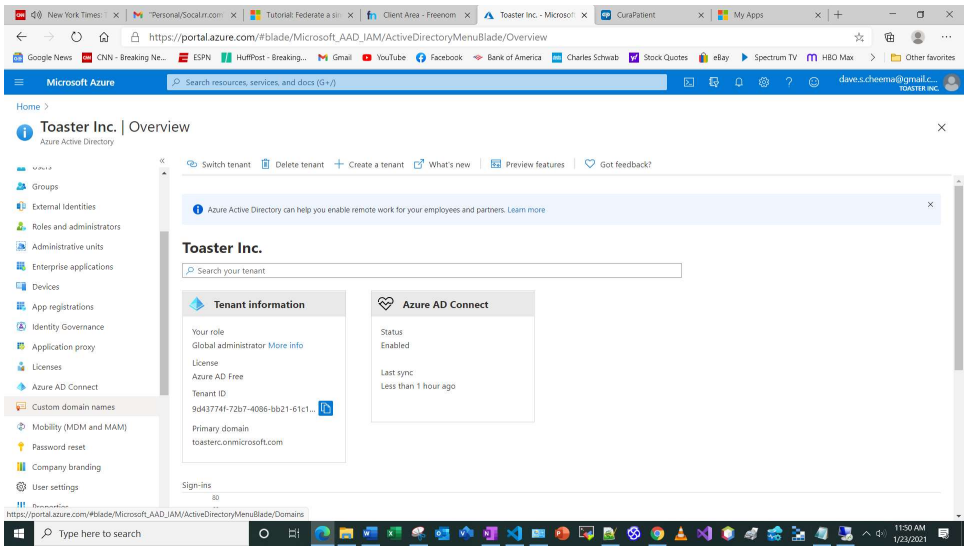
Overview:

- Create an Azure Active Directory instance
- Create a custom domain name, register it with the Registrar and ensure that the domain name is verified
- Create a Windows server VM on which the federation and synch services will run
- RDP into the windows server VM instance
- Install pre-requisites tools
- Create a Windows server AD environment
- Install AD DS, DNS and GPMC (Policy Management Console)
- Generate/import a security certificate for the AD FS
- Create an Azure AD tenant by installing Azure AD Connect
- Ensure Customize option is selected for the AAD Connect during installation
- Ensure that Federation with AD FS is selected
- Connect to your directory(s)
- Be sure to select Password hash synchronization option
- Install configurations
- Very that the connectivity work.
- Validate that the Windows Server AD user can login to your Azure Active Directory account

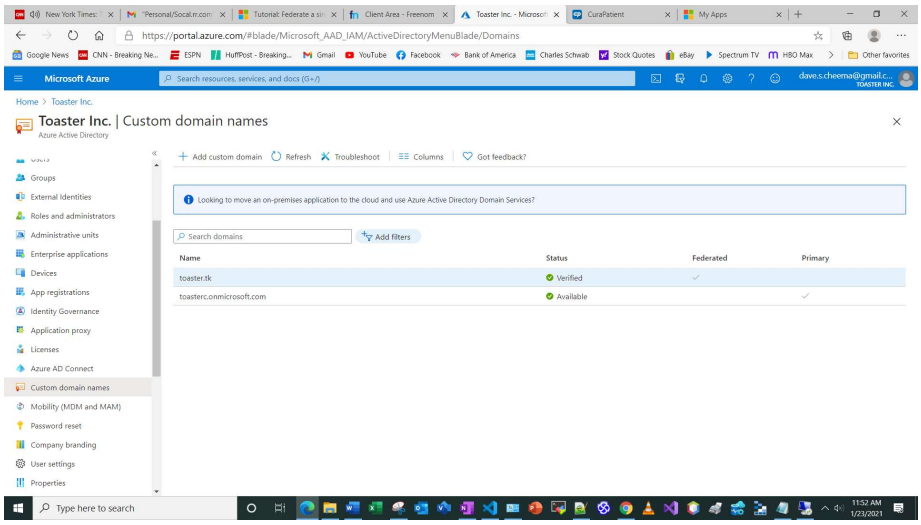
Detailed:

- Create a VM, dc1-vm1, with minimum 8 GB memory. Create a static IP address, e.g., 104.42.51.190

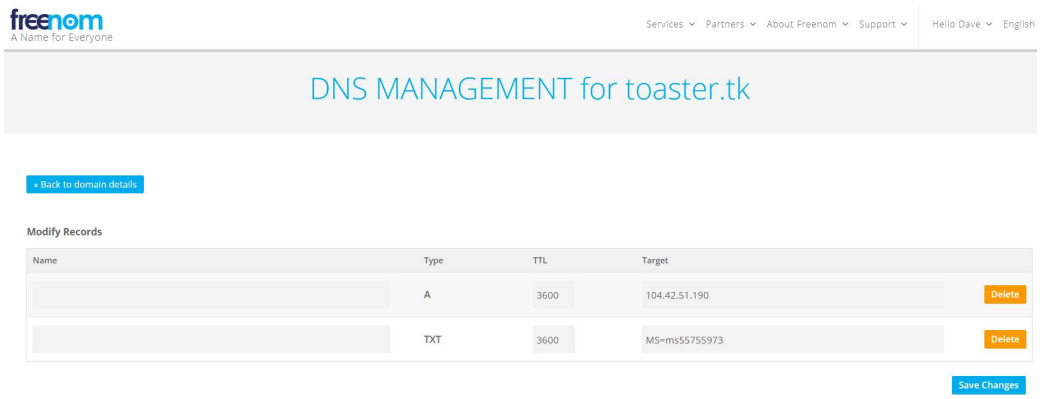
- Create an Azure Active Directory tenant, Toaster Inc.



- Click on Custom names.



- Create a custom domain, e.g., toaster.tk. Primary domain is toasterc.onmicrosoft.com
- Register the custom domain name with a registrar, e.g., Freenom.com



- Register TXT and A records with the registrar
- After a while (30 minutes), verify your custom domain
- Ensure that your custom domain, e.g., toaster.tk is verified. If not verified, click on it and click Verify button at the bottom of custom domain detail screen. If still does not verify, ensure that you have properly registered you domain settings and keep trying
- Create a Global Administrator user: toaster, toaster@toasterc.onmicrosoft.com
- RDP into the VM, e.g., dc1-vm1, using admin credentials you entered during the VM creation
- Open Powershell ISE session in the VM, dc1-vm1
- Install required features

  Run the following set of command

```
$featureLogPath = "c:\poshlog\featurelog.txt"
$addsTools = "RSAT-AD-Tools"

#Install features
New-Item $featureLogPath -ItemType file -Force
Add-WindowsFeature $addsTools
Get-WindowsFeature | Where installed >>$featureLogPath

#Restart the computer
Restart-Computer
```

Create a Windows Server AD environment

Run the following code to setup tools:

```
#Declare variables
$DatabasePath = "c:\windows\NTDS"
$DomainMode = "WinThreshold"
$DomainName = "toaster.tk"
$DomainNetBIOSName = "TOASTER"
$ForestMode = "WinThreshold"
$LogPath = "c:\windows\NTDS"
$SysVolPath = "c:\windows\SYSVOL"
$featureLogPath = "c:\poshlog\featurelog.txt"
```

```
$Password = ConvertTo-SecureString "Dave123#" -AsPlainText -Force

#Install AD DS, DNS and GPMC
start-job -Name addFeature -ScriptBlock {
Add-WindowsFeature -Name "ad-domain-services" -IncludeAllSubFeature -IncludeManagementTools
Add-WindowsFeature -Name "dns" -IncludeAllSubFeature -IncludeManagementTools
Add-WindowsFeature -Name "gpmc" -IncludeAllSubFeature -IncludeManagementTools }
Wait-Job -Name addFeature
Get-WindowsFeature | Where installed >>$featureLogPath

#Create New AD Forest
Install-ADDSForest -CreateDnsDelegation:$false -DatabasePath $DatabasePath -DomainMode $DomainMode -DomainName $DomainName -SafeModeAdministratorPassword $Password -
DomainNetbiosName $DomainNetBIOSName -ForestMode $ForestMode -InstallDns:$true -LogPath $LogPath -NoRebootOnCompletion:$false -SysvolPath $SysVolPath -Force:$true
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

Create a Windows Server AD user

To add a Windows Server AD user, execute the following code:

```
#Declare variables
$Givenname = "Allie"
$Surname = "McCray"
$Displayname = "Allie McCray"
$Name = "amccray"
$Password = "Toaster2010!"
$Identity = "CN=ammccray,CN=Users,DC=toaster,DC=tk"
$SecureString = ConvertTo-SecureString $Password -AsPlainText -Force

#Create the user
New-ADUser -Name $Name -GivenName $Givenname -Surname $Surname -DisplayName $Displayname -AccountPassword $SecureString

#Set the password to never expire
Set-ADUser -Identity $Identity -PasswordNeverExpires $true -ChangePasswordAtLogon $false -Enabled $true
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

Create a certificate for AD FS

Execute the following code:

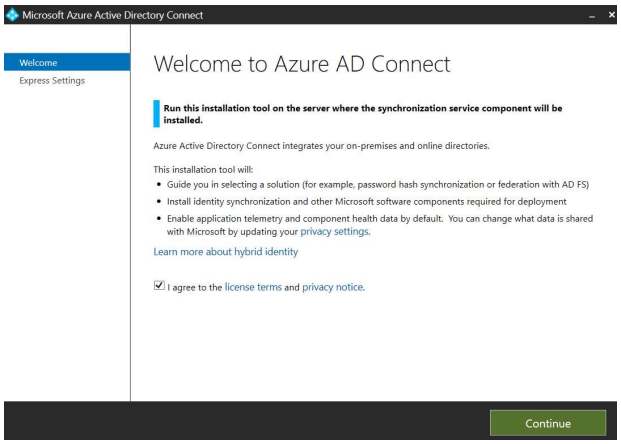
```
# Define your own DNS name used by your managed domain
$dnsName="toaster.tk"

# Get the current date to set a one-year expiration
$lifetime=Get-Date

# Create a self-signed certificate for use with Azure AD DS
New-SelfSignedCertificate -Subject *.$dnsName `
  -NotAfter $lifetime.AddDays(365) -KeyUsage DigitalSignature, KeyEncipherment `
  -Type SSLServerAuthentication -DnsName *.$dnsName, $dnsName
```

Export the security certificate in .PFX format and save it to a known location

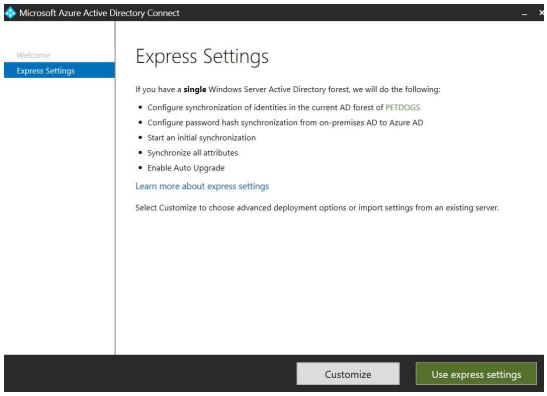
```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

Create an Azure AD tenant

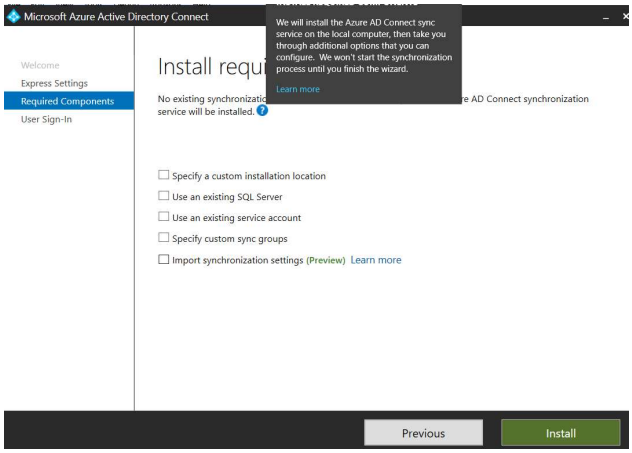
- Download Azure Active Directory Connect from [Download Microsoft Azure Active Directory Connect from Official Microsoft Download Center]
- Install Azure Active Directory Connect in the VM server, e.g., dc1-vm1, you created earlier



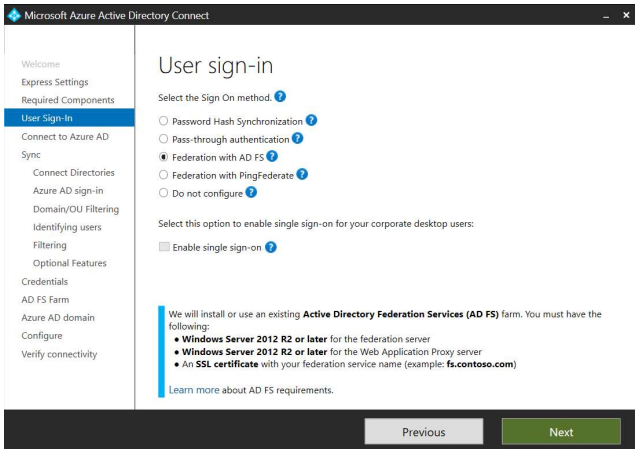
- Check I agree to the license terms and privacy notice and click on Continue



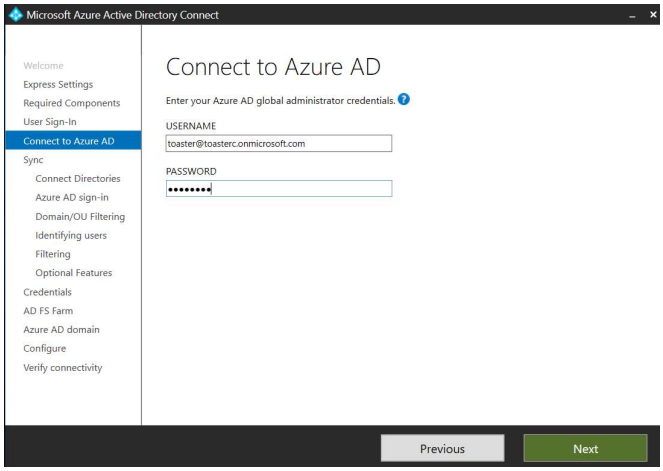
- Click on Customize button



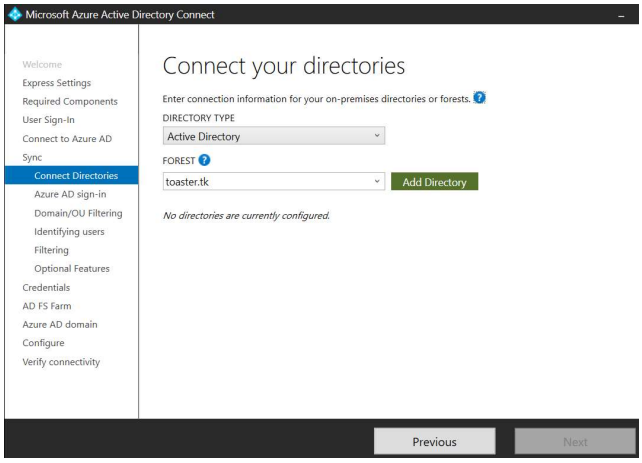
- Click on Install



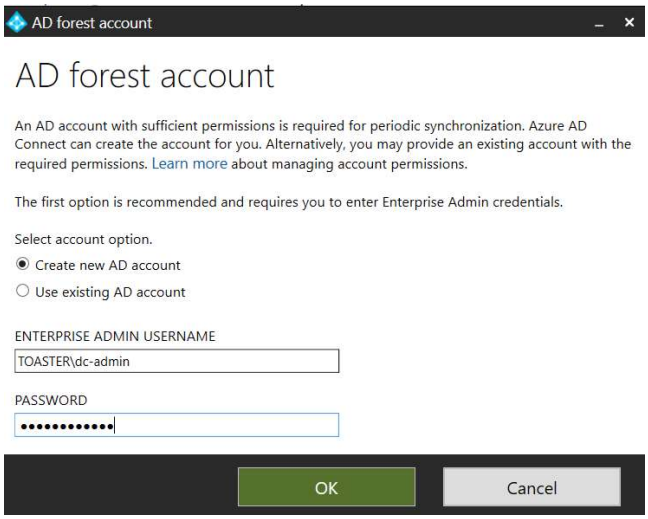
- Select Federation with ADFS and click Next



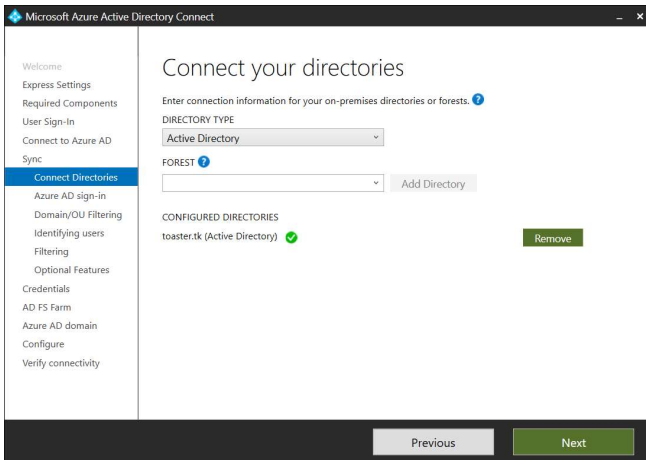
- Enter the Global administrator's credentials, the ones you had created in the Toaster Inc. Azure Active Directory, e.g., toaster@toasterc.onmicrosoft.com
- Click on Next button



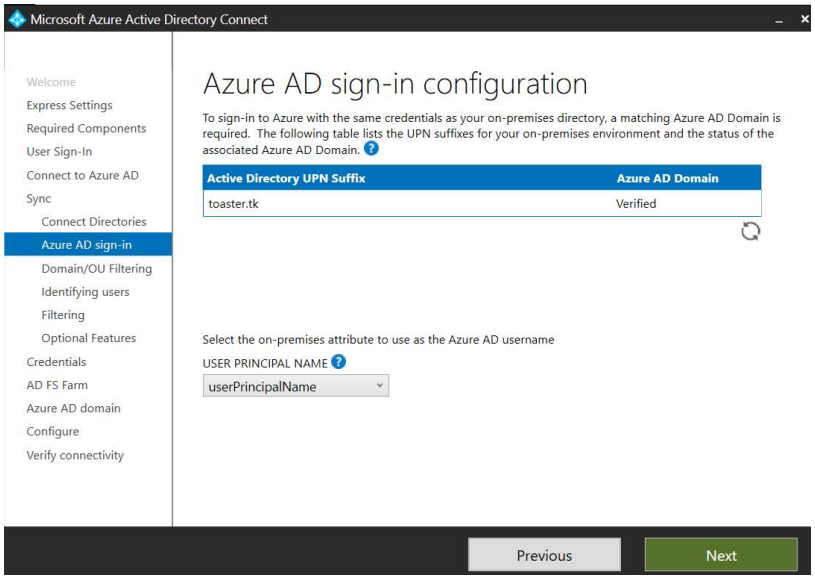
- Click on Add Directory



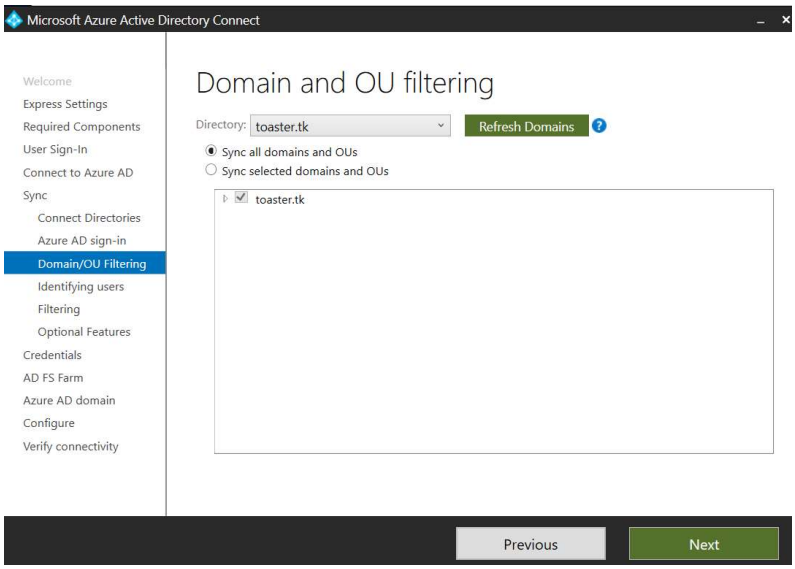
- Enter the Enterprise Admin Username, e.g., TOASTER\dc-admin (it is the same id that you entered when you created the server VM, e.g., dc1-vm1
- Click on OK



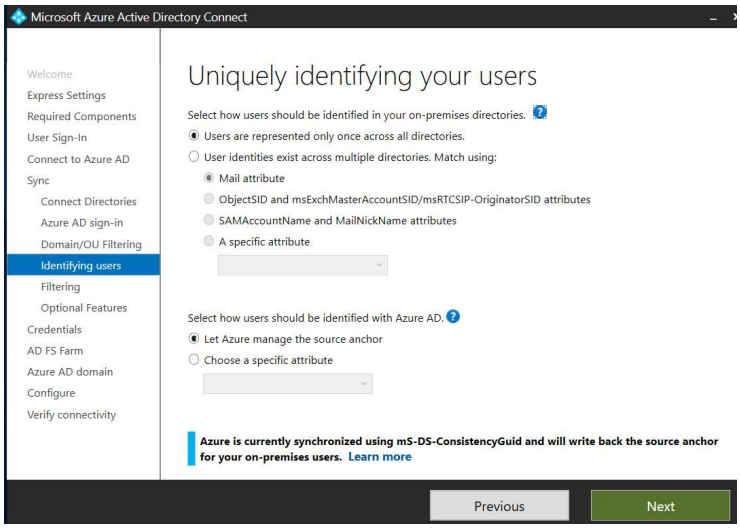
- If everything works, you will see a Green checkmark next to toaster.tk (Active Directory).
- Click Next



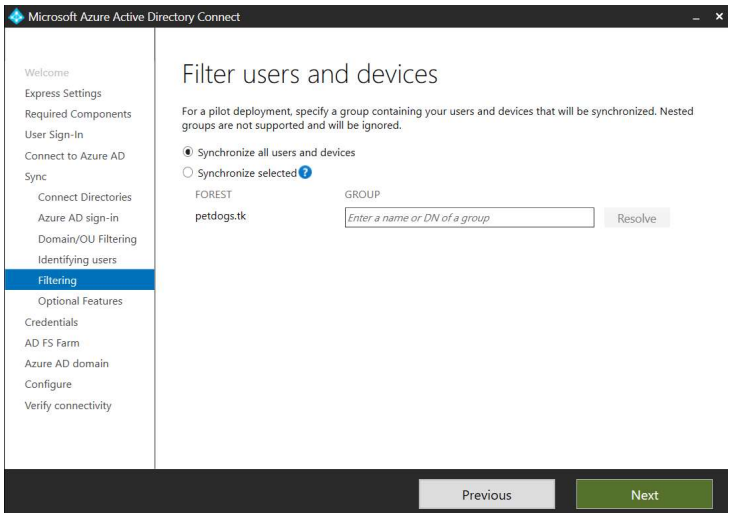
- Check Continue without matching all UPN suffixes to verified domains and click on Next



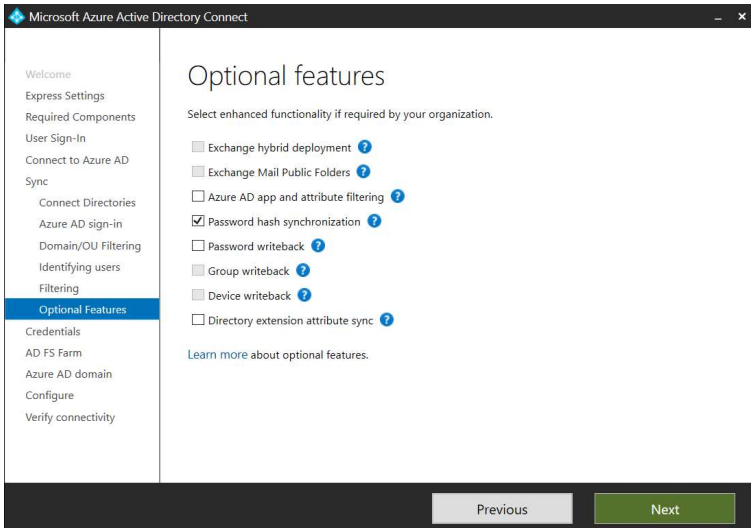
- Click on Next



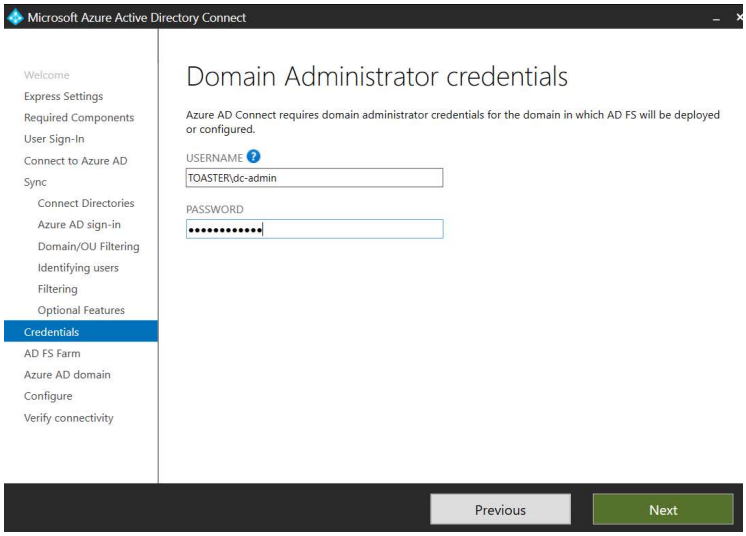
- Don't change anything, just click on Next



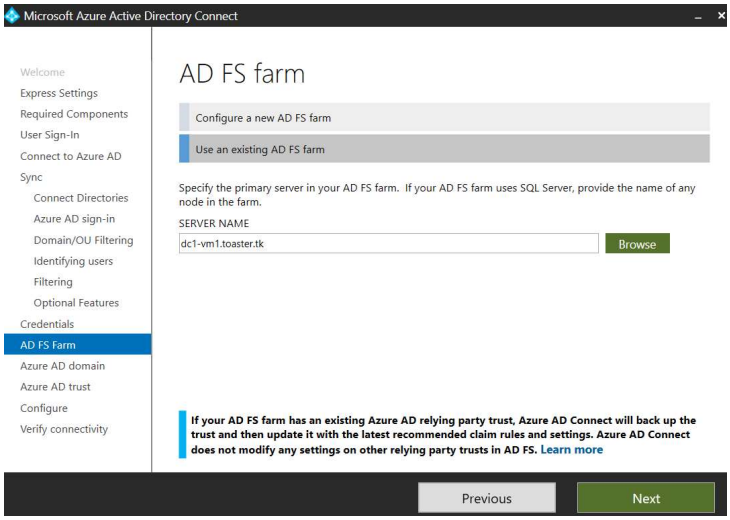
- Again, click on Next



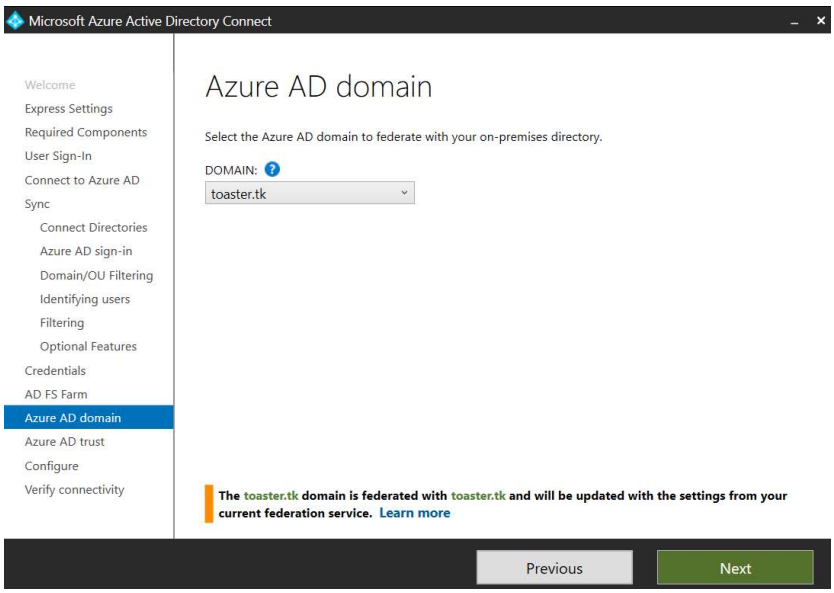
- Check Password hash synchronization and click on Next



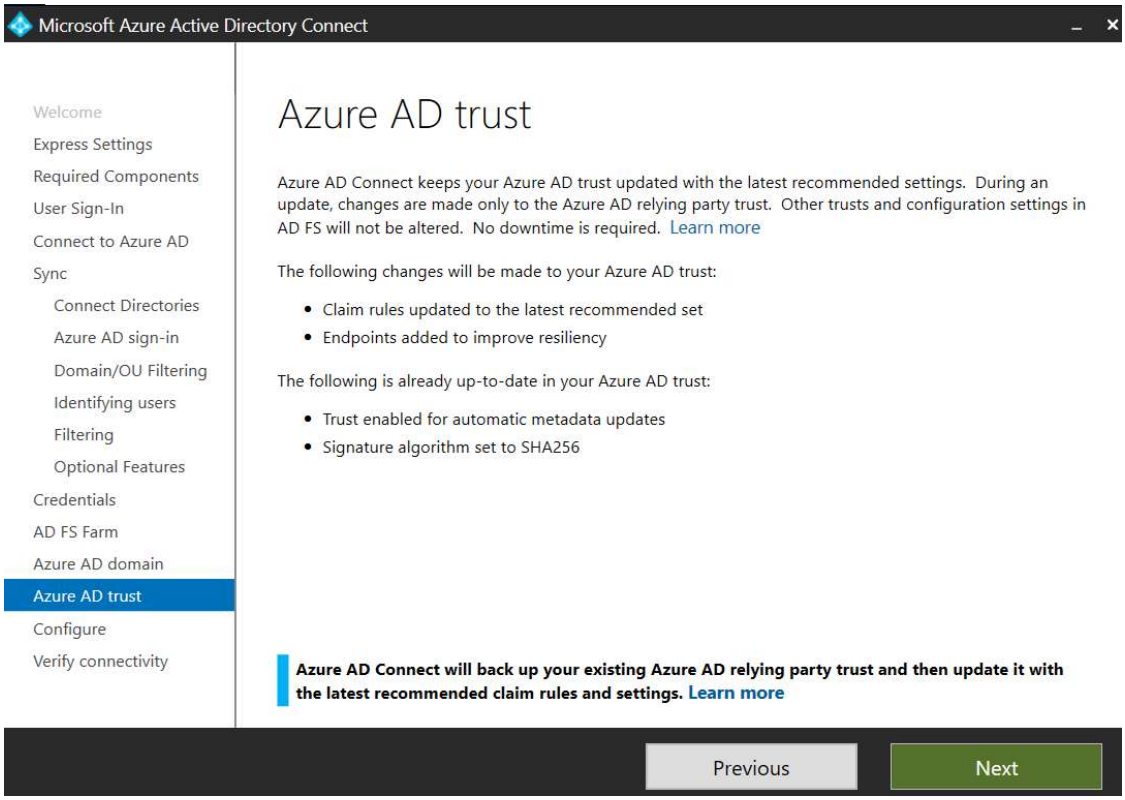
- Enter domain admin id, TOASTER\dc-admin and password and click on Next



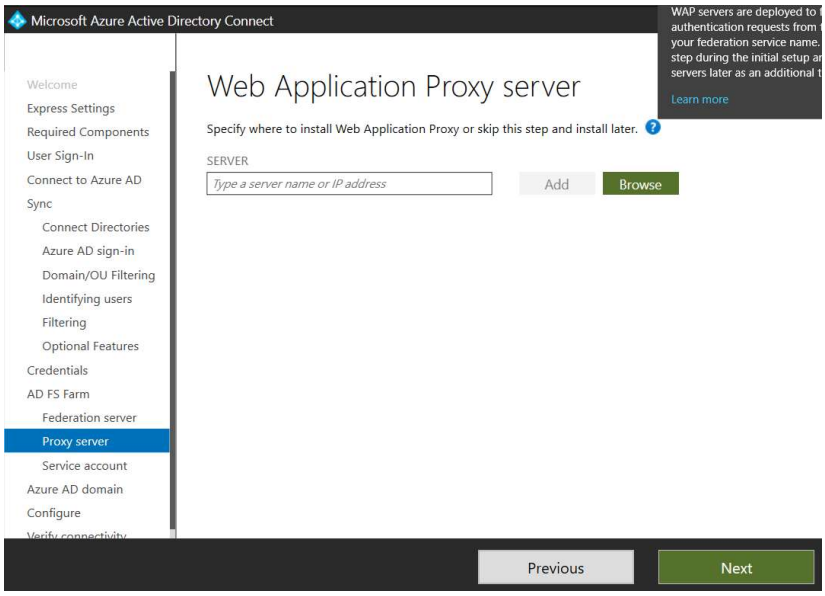
- Upload the self-signed (in production you may have a commercial certificate) .PFX certificate
- Select the SERVER NAME and click on Next



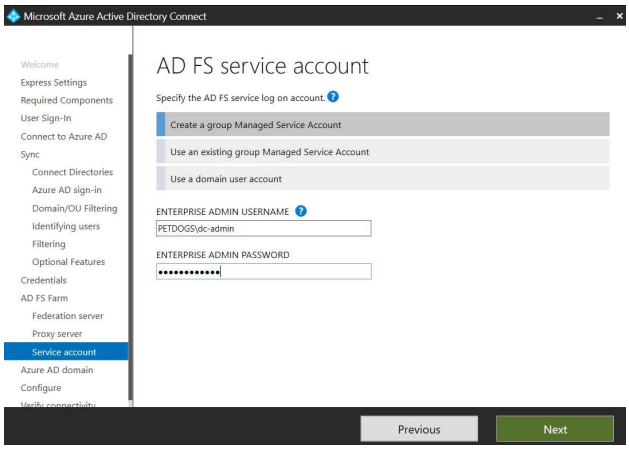
- Click Next



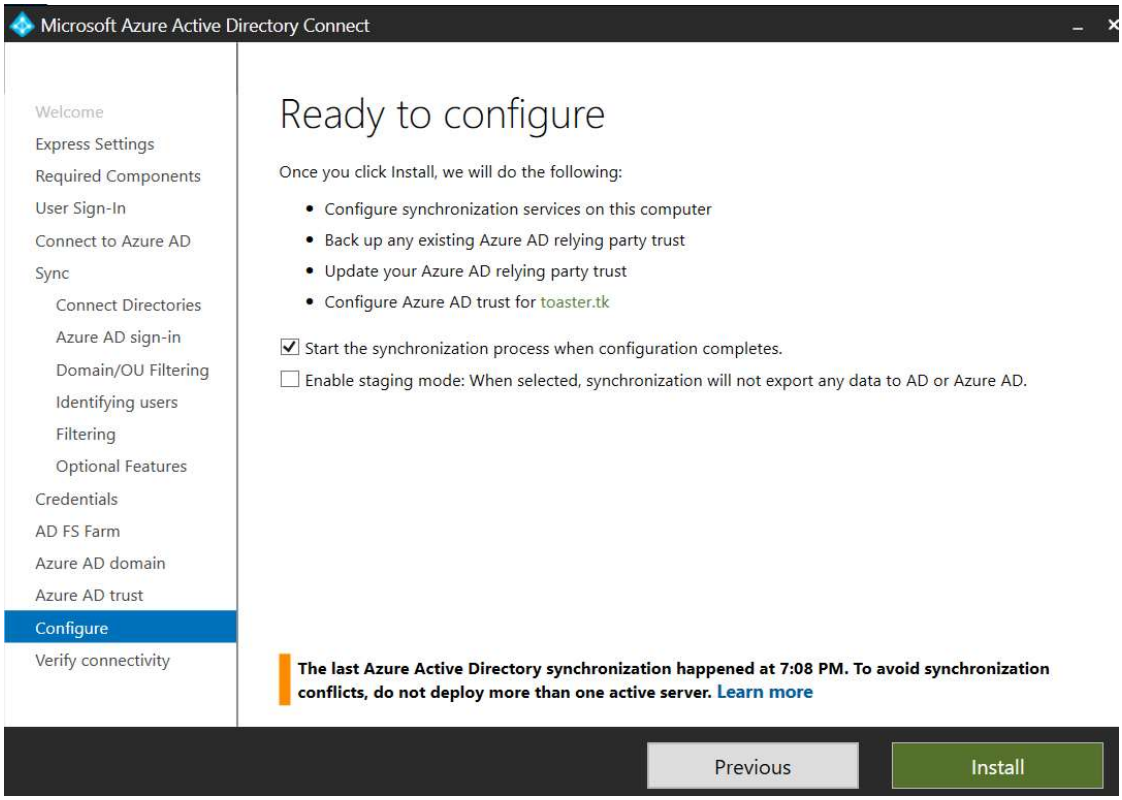
- Click on Next



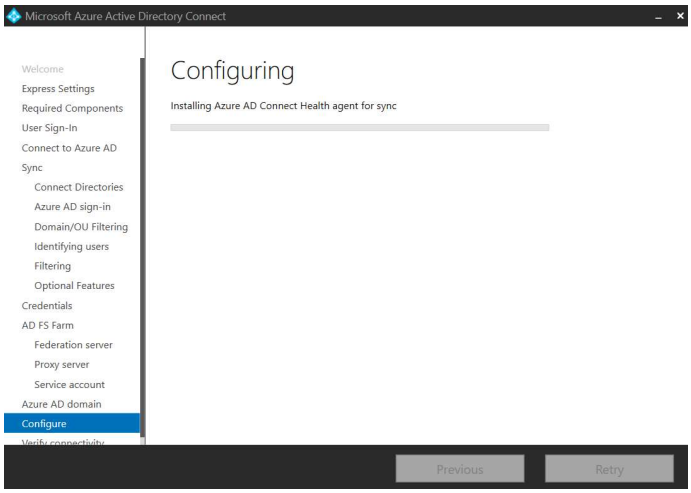
- If you have proxy server, enter it here, otherwise, just click on Next



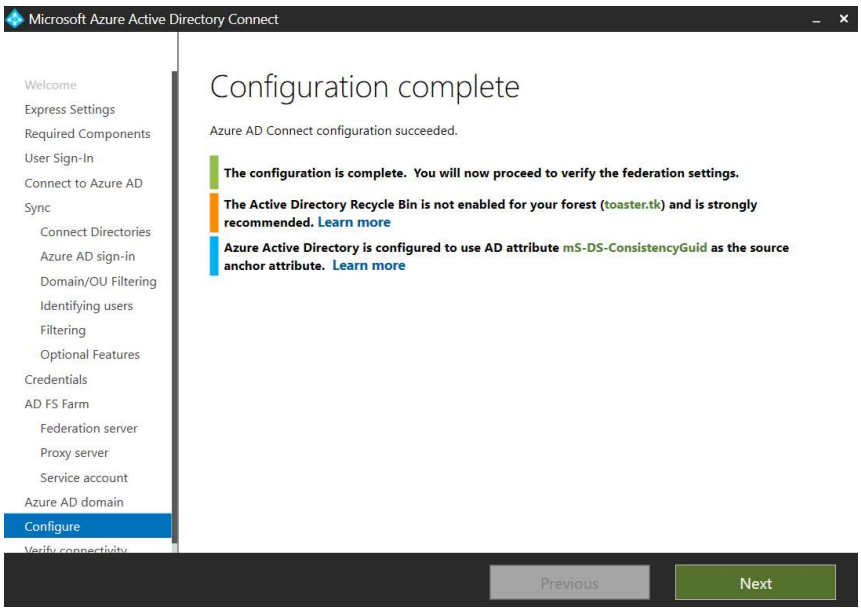
- Enter Enterprise Admin's login credentials and click Next



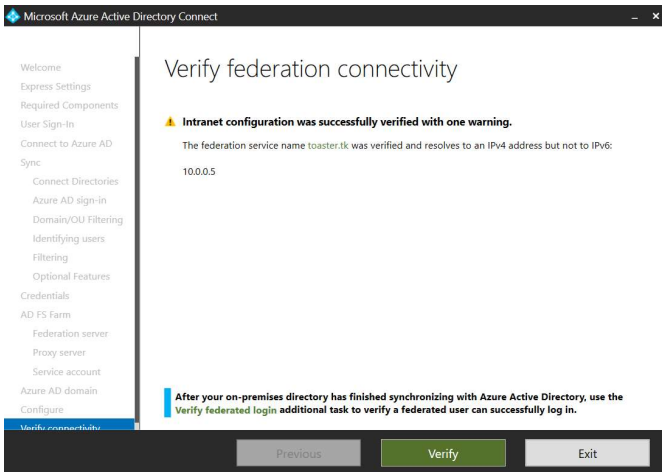
- Click on Install



- At completion, you will be notified that the configuration is complete



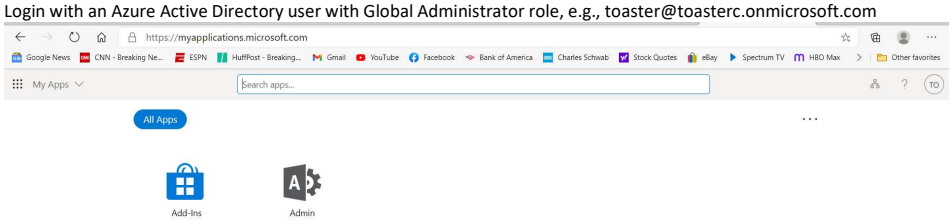
- Verify federation connectivity



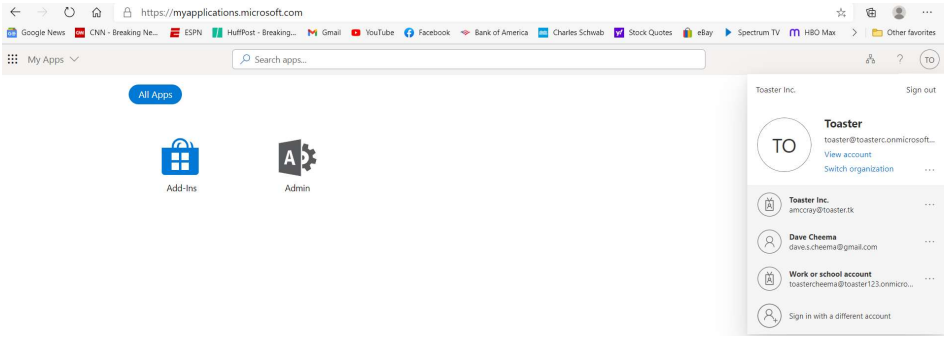
- At successful completion, you will get a message - Intranet configuration was successfully verified

Test Azure Active Directory Federated Service

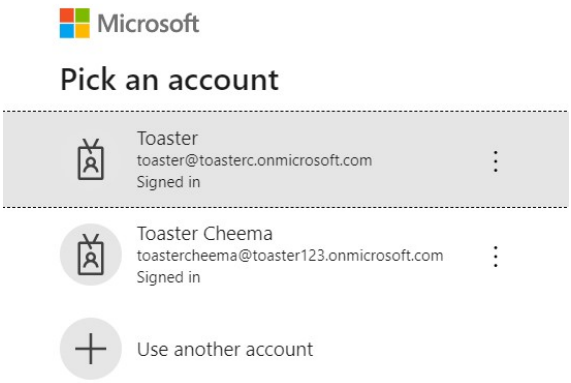
Go myapps.microsoft.com
Login with an Azure Active Directory user with Global Administrator role, e.g., toaster@toasterc.onmicrosoft.com



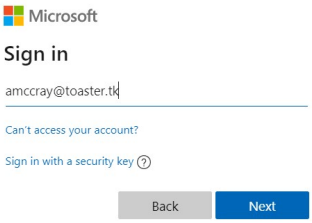
Click on TO (in circle, at top right corner)



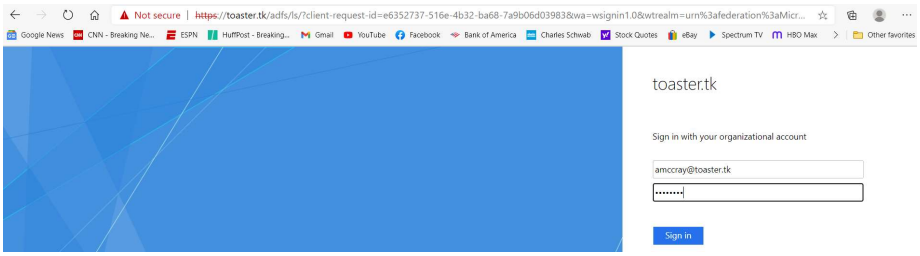
Click on Sign in with a different account



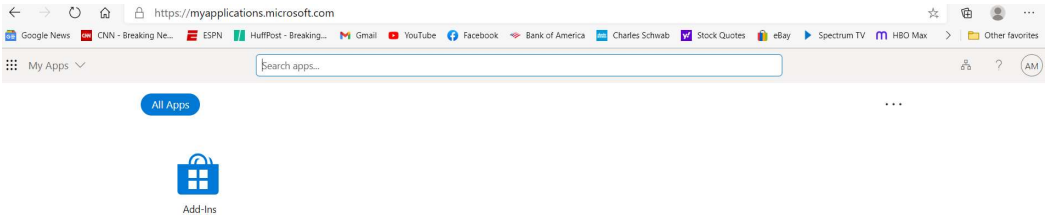
Click on Use another account



Enter a Windows Server AD user credentials, e.g., amccray@toaster.tk and click on Next



Enter Allie McCray's password and click on Sign in



Look in the top right corner and you see AM in circle.
Click on it and you'll see her identification.
IMPORTANT: The key to remember is that Allie McCray is not an Azure Active Directory user. Instead, she a Windows Server AD user, who has been federated with an AAD (toaster.tk).