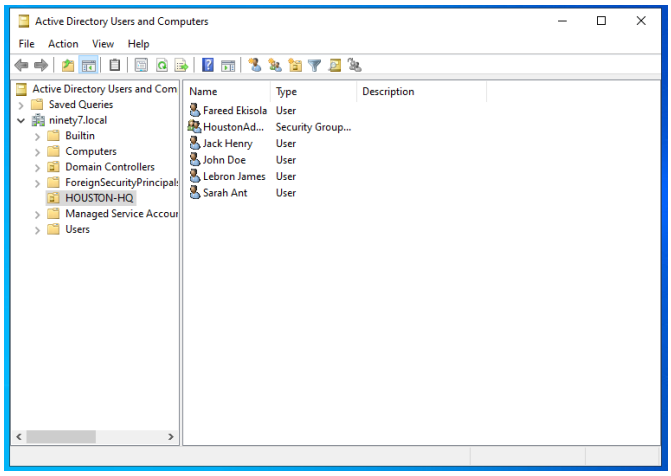
In this documentation, I migrated a company from on-prem AD to Cloud (Hybrid Setup) using modern tools like Entra ID Connect Sync, Microsoft Server.

This is a hybrid setup which means users can still be managed on-prem and in Entra ID.

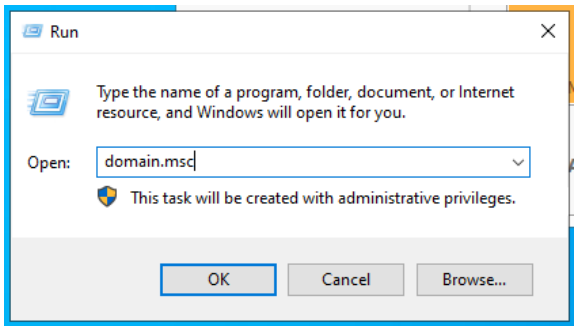
You need to set up an Azure or Entra ID account and tenant and have at least a Microsoft Free Subscription for this.

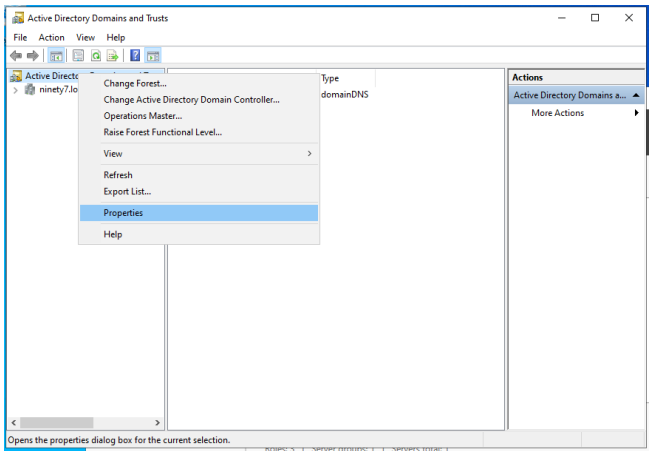
For me I used my existing Azure account for this.

As you can see, I added some more users to my on-prem AD (view NINETY7-DC1 documentation to see how to add users in DC)

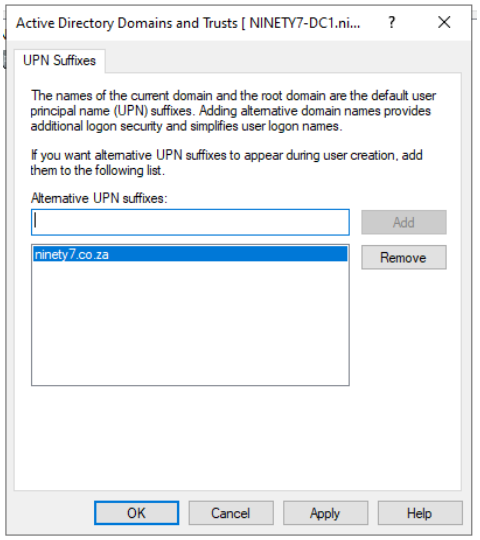


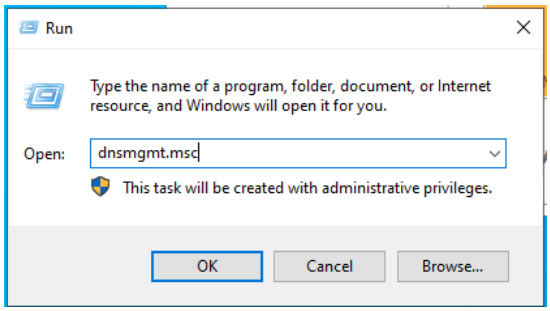
Microsoft Entra ID relies on publicly resolvable domains to ensure proper identity federation, authentication, and access management. So first step is to add my registered public domain name to my AD environment.



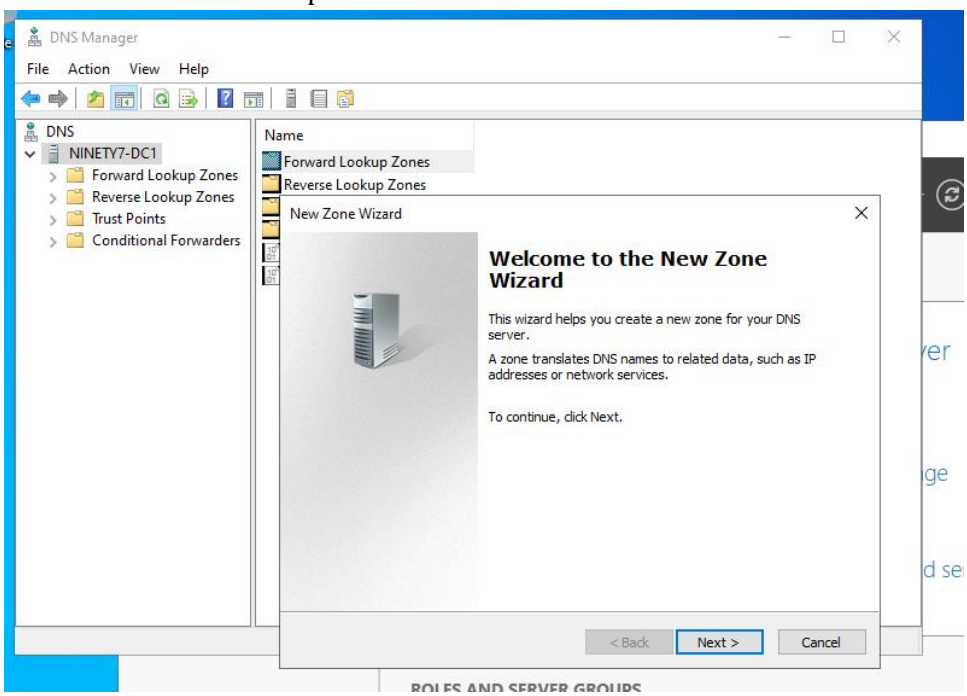


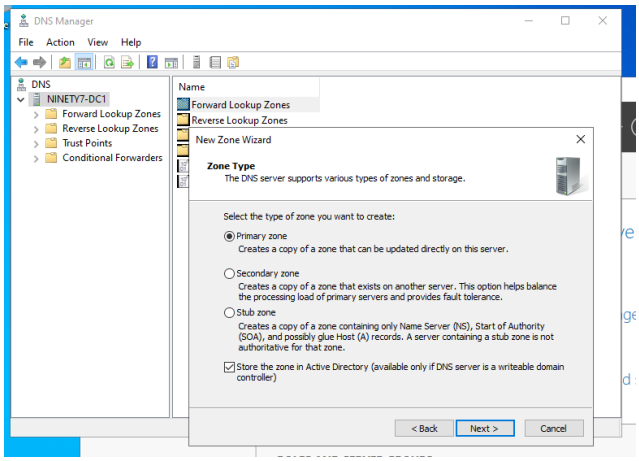
Added my public registered domain (ninety7.co.za)

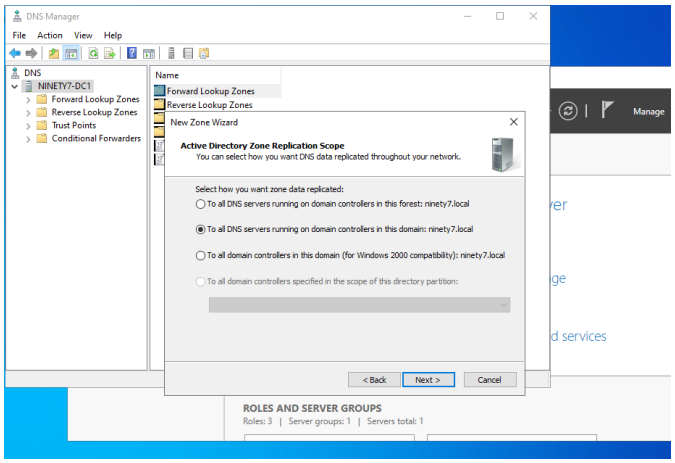




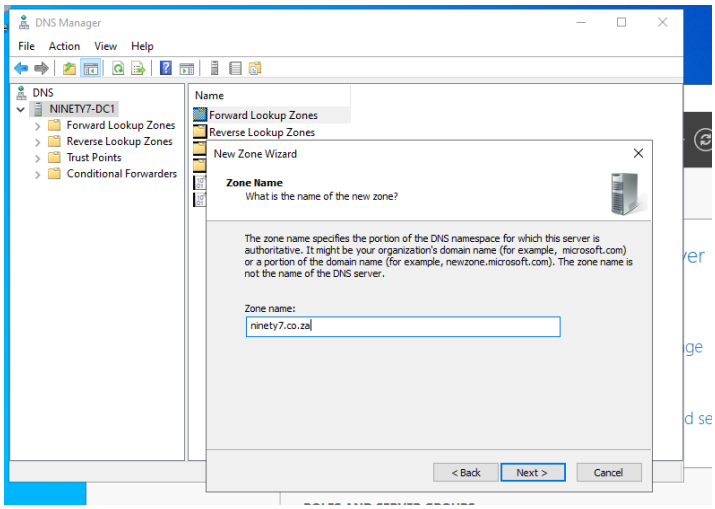
Create a Forward Lookup Zone in Windows Server DNS

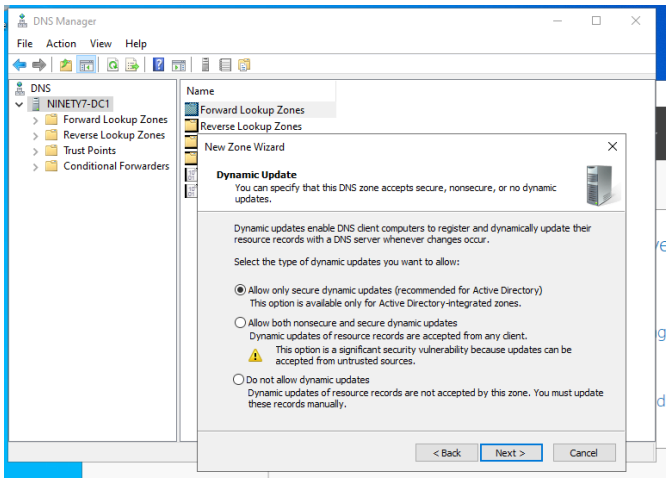


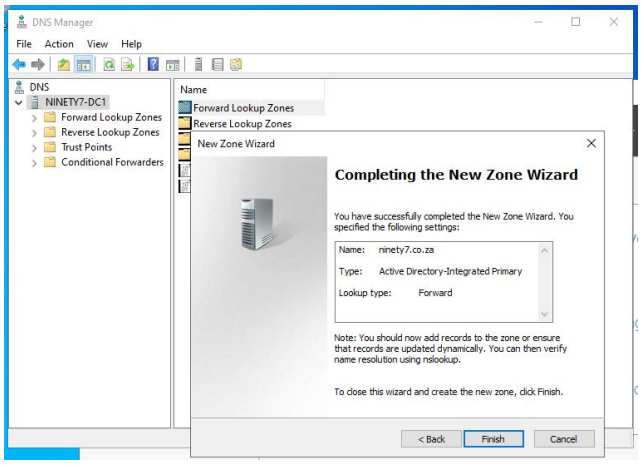




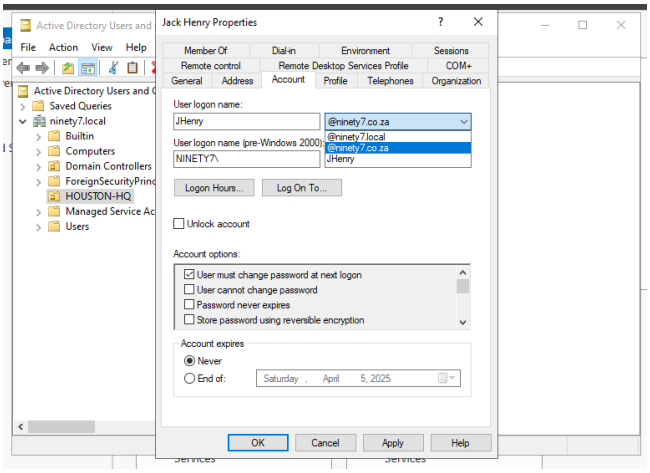
Specify zone name (my registered domain name)



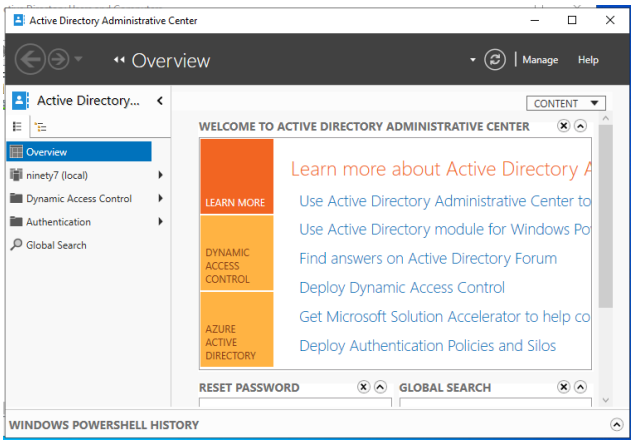


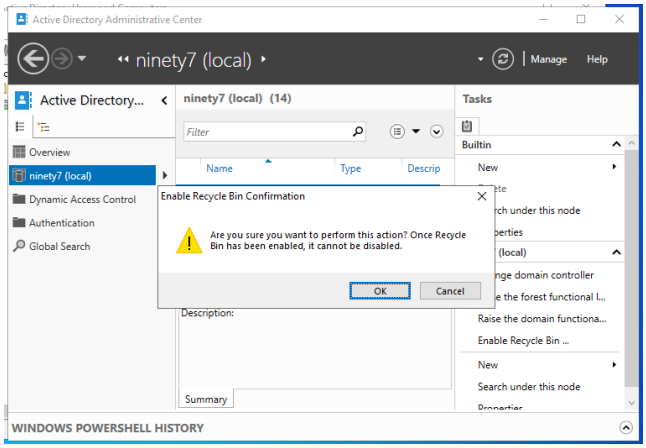


Update all users (users you plan to sync) UPN to use public domain (Updating UPNs before migrating to Microsoft Entra ID ensures: Successful sync with Microsoft Entra Connect, Seamless user authentication & SSO, Elimination of login conflicts & errors)

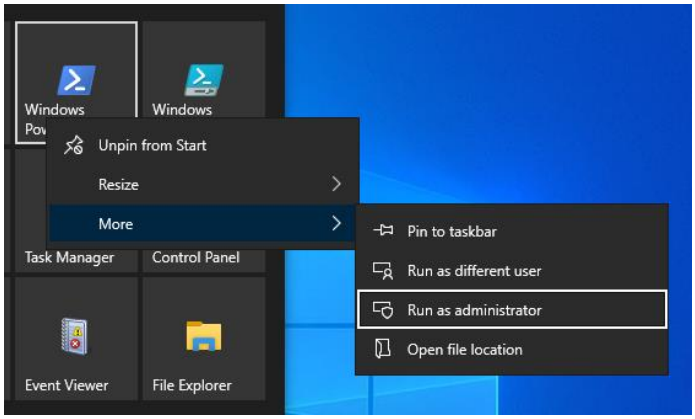


Enable Recycle Bin in your AD DS domain.

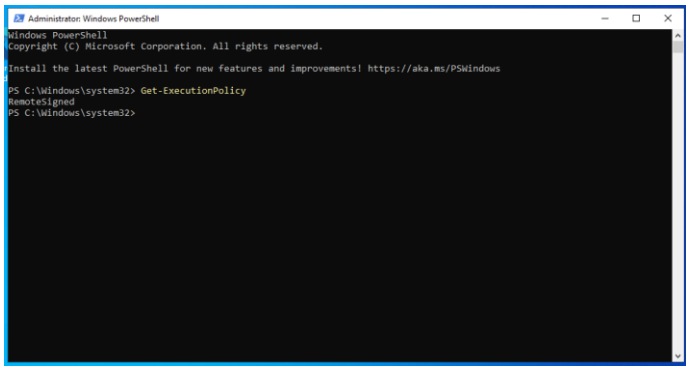




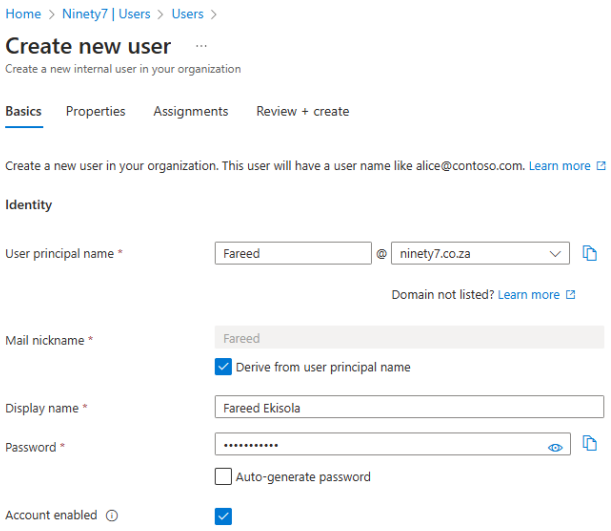
Ensure PowerShell execution policy is set to Remote Signed. (Scripts an more info on my GitHub)

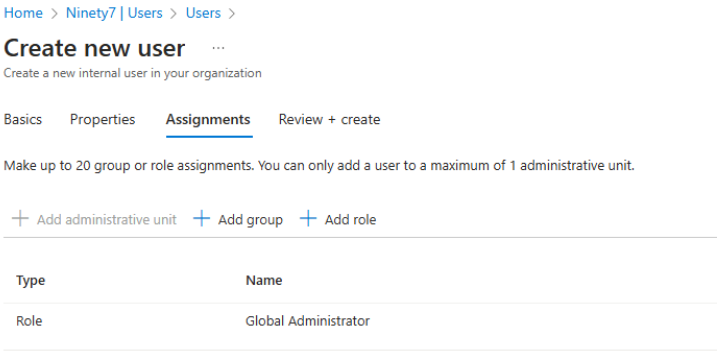


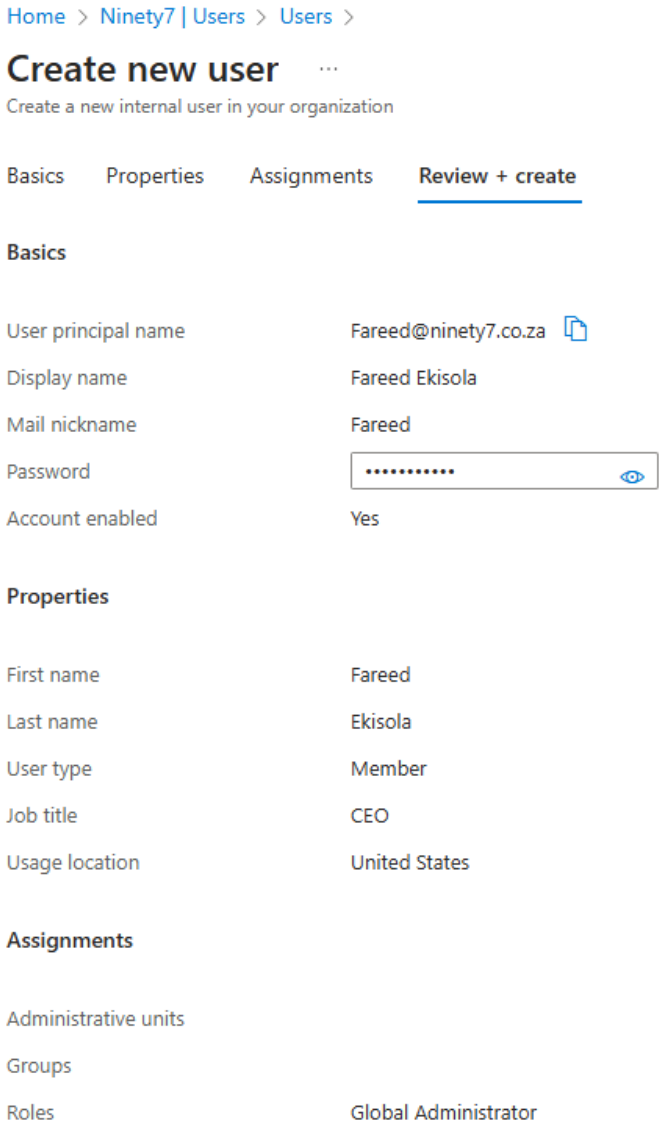
Run Get – ExecutionPolicy to check.



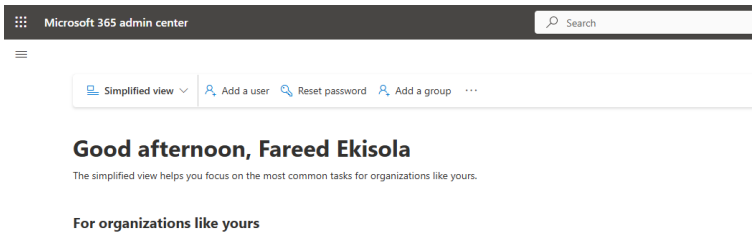
It is good practice to have more than one Global Admins, so I made another account in my Entra ID and assigned the Global Admin role.




Home > Ninety7 | Users > Users >
Create new user
Create a new internal user in your organization
Basics
Properties
Assignments
Review + create
Make up to 20 group or role assignments. You can only add a user to a maximum of 1 administrative unit.
Add administrative unit
Add group
Add role
Type
Name
Role
Global Administrator


Home > Ninety7 | Users > Users >
Create new user
Create a new internal user in your organization
Basics
Properties
Assignments
Review + create
Basics
User principal name
Fareed@ninety7.co.za
Display name
Fareed Ekisola
Mail nickname
Fareed
Password
Account enabled
Yes
Properties
First name
Fareed
Last name
Ekisola
User type
Member
Job title
CEO
Usage location
United States
Assignments
Administrative units
Groups
Roles
Global Administrator

Login to your tenants 365 Admin Center to test new user role and permission.

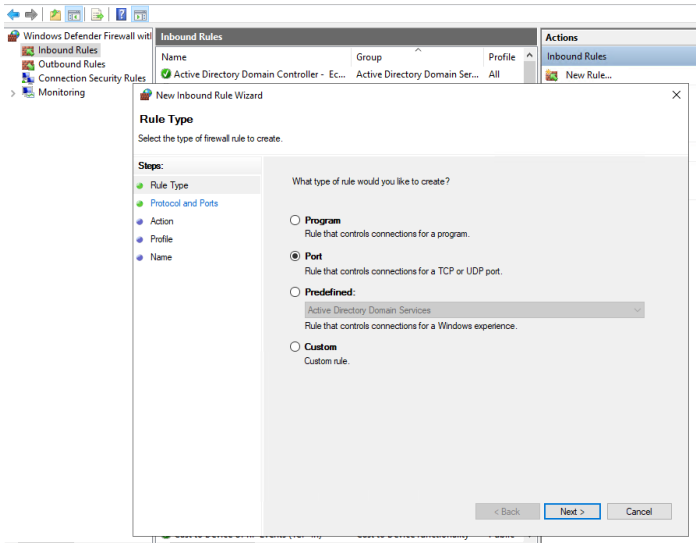


Open required ports for Entra Connect Sync setup.

DNS 53 (TCP/UDP), Kerberos 88 (TCP/UDP), MS-RPC 135 (TCP), LDAP 389 (TCP/UDP), SMB 445 (TCP), LDAP/SSL 636 (TCP/UDP), RPC 49152- 65535 (Random high RPC Port) (TCP), WinRM 5985 (TCP), AD DS Web Services 9389 (TCP), Global Catalog 3268 (TCP)

HTTP 80 (TCP), HTTPS 443 (TCP)

You can use Windows Defender Firewall to perform this task. But I will use PowerShell since it can perform bulk operations, hence faster.



Run PowerShell scripts, I have added the PowerShell scripts in my GitHub for your convenience.

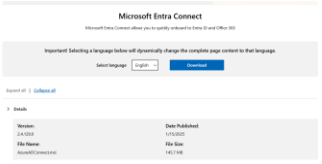
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator.NINETY7> New-NetFirewallRule -DisplayName "Allow DNS Port 53" -Protocol TCP -LocalPort 53 -Action Allow


Name                          : {2228697f-df90-493b-9ab5-9e32ef9d9061}
DisplayName                   : Allow DNS Port 53
Description                   :
DisplayGroup                  :
Group                         :
Enabled                       : True
Profile                       : Any
Platform                      : {}
Direction                     : Inbound
Action                        : Allow
EdgeTraversalPolicy           : Block
LooseSourceMapping            : False
LocalOnlyMapping              : False
Owner                         :
PrimaryStatus                 : OK
Status                        : The rule was parsed successfully from the store. (65536)
EnforcementStatus             : NotApplicable
PolicyStoreSource             : PersistentStore
PolicyStoreSourceType         : Local
RemoteDynamicKeywordAddresses : {}


PS C:\Users\Administrator.NINETY7> New-NetFirewallRule -DisplayName "Allow DNS Port 53 UDP" -Protocol UDP -LocalPort 53 -Action Allow


Name                          : {95d3f5a4-da2c-4c6d-bc65-b21f3c24b5e7}
DisplayName                   : Allow DNS Port 53 UDP
Description                   :
DisplayGroup                  :
Group                         :
Enabled                       : True
Profile                       : Any
Platform                      : {}
Direction                     : Inbound
Action                        : Allow
```

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator.NINETY7> New-NetFirewallRule -DisplayName "Allow HTTP Port 80" -Protocol TCP -LocalPort 80 -Ac
tion Allow


Name                          : {fcf142a2-9924-4aa1-b33d-0058aadbd3c7}
DisplayName                   : Allow HTTP Port 80
Description                   :
DisplayGroup                  :
Group                         :
Enabled                       : True
Profile                       : Any
Platform                      : {}
Direction                     : Inbound
Action                        : Allow
EdgeTraversalPolicy           : Block
LooseSourceMapping            : False
LocalOnlyMapping              : False
Owner                         :
PrimaryStatus                 : OK
Status                        : The rule was parsed successfully from the store. (65536)
EnforcementStatus             : NotApplicable
PolicyStoreSource             : PersistentStore
PolicyStoreSourceType         : Local
RemoteDynamicKeywordAddresses : {}
```

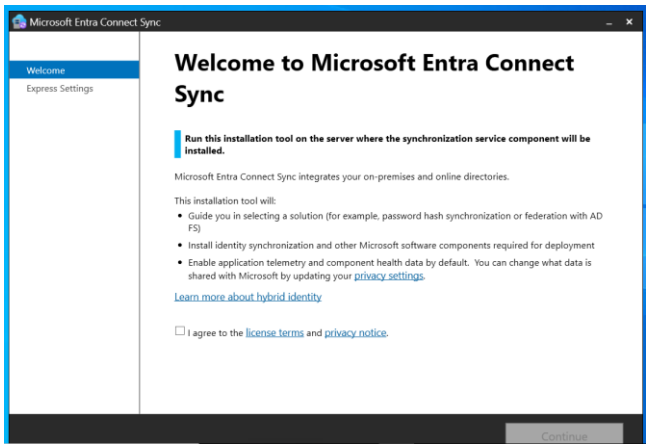
```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator.NINETY7> [Net.ServicePointManager]::SecurityProtocol
SystemDefault
PS C:\Users\Administrator.NINETY7> Invoke-WebRequest -Uri https://google.com
>> [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12


StatusCode        : 200
StatusDescription : OK
Content           : <!doctype html><html itemscope="" itemtype="http://schema.org/WebPage" lang="en"><head><meta
                    content="Search the world's information, including webpages, images, videos and more. Google has
                    many speci...
RawContent        : HTTP/1.1 200 OK
                    Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-src
                    'nonce-7Oak2DObKpgBAPOIeUDxpA' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline'
                    https: ...
Forms             : {f}
Headers           : {[Content-Security-Policy-Report-Only, object-src 'none';base-uri 'self';script-src
                    'nonce-7Oak2DObKpgBAPOIeUDxpA' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline'
                    https: http:;report-uri https://csp.withgoogle.com/csp/gws/other-hp], [Accept-CH,
                    Sec-CH-Prefers-Color-Scheme], [X-XSS-Protection, 0], [X-Frame-Options, SAMEORIGIN]...}
Images            : {@{innerHTML=; innerText=; outerHTML=<IMG id=hplogo style="PADDING-BOTTOM: 14px; PADDING-TOP:
                    28px; PADDING-LEFT: 0px; PADDING-RIGHT: 0px" alt=Google
                    src="/images/branding/googlelogo/1x/googlelogo_white_background_color_272x92dp.png" width=272
                    height=92>; outerText=; tagName=IMG; id=hplogo; style=PADDING-BOTTOM: 14px; PADDING-TOP: 28px;
                    PADDING-LEFT: 0px; PADDING-RIGHT: 0px; alt=Google;
```

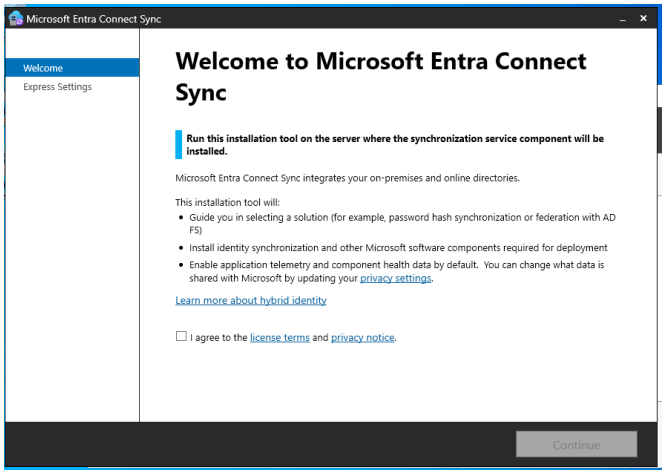
Download Microsoft Entra Connect Setup from Microsoft Official website.

Make sure you download from the official Microsoft Website and you are getting the latest version.

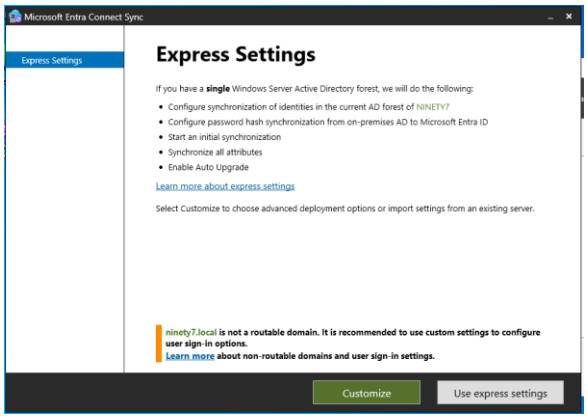


Run program.

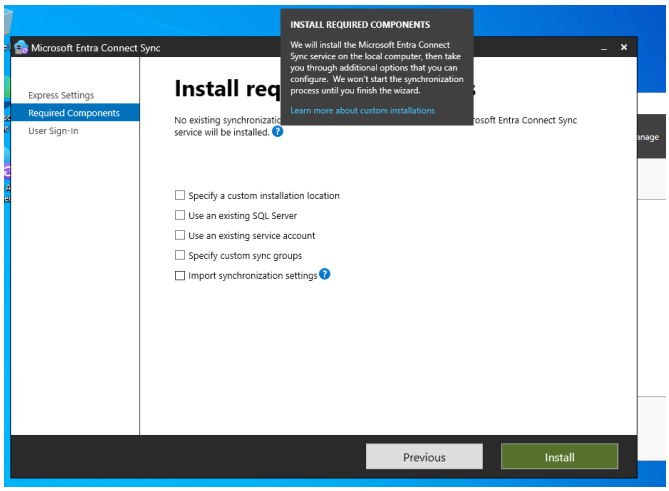




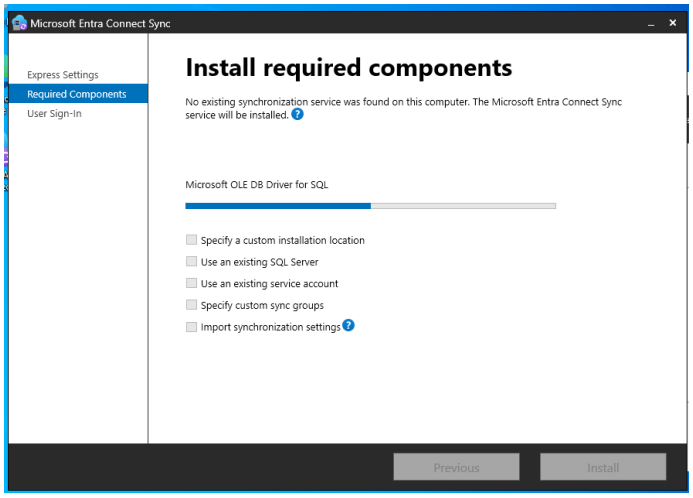
The warning in the screenshot indicates I have to manually configure my domain settings in the Microsoft Entra Connect Setup.



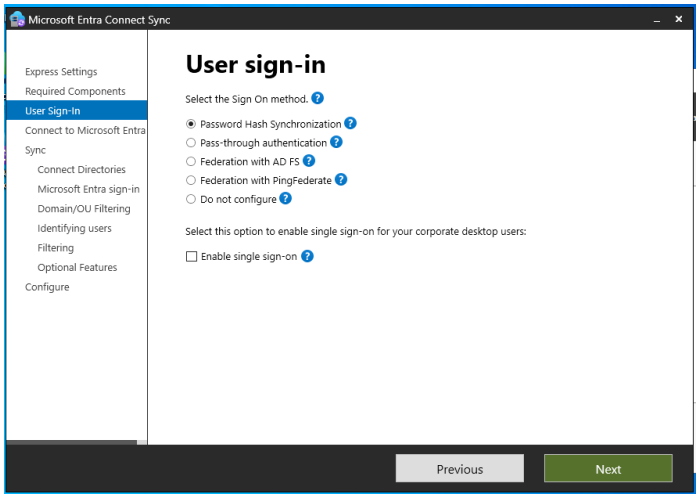
So I will proceed with custom settings.

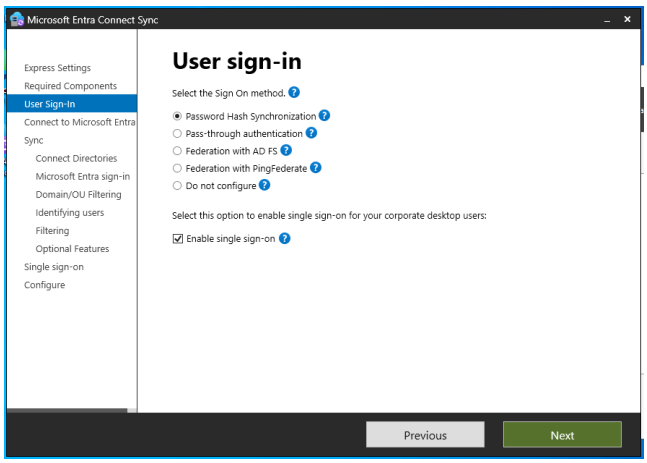


No required components needed so I will leave this page as default.



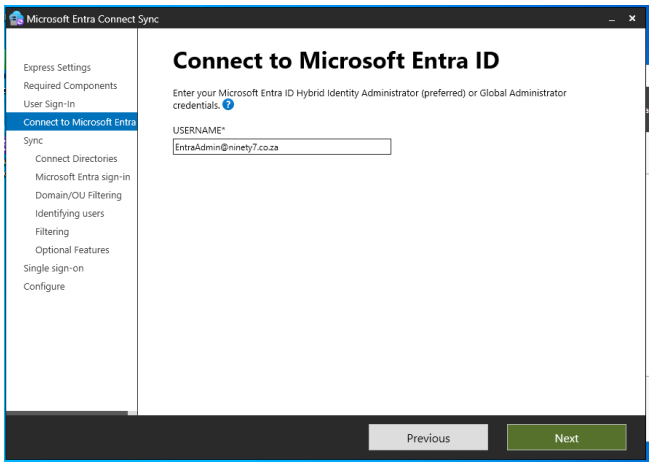
Enable PHS & SSO



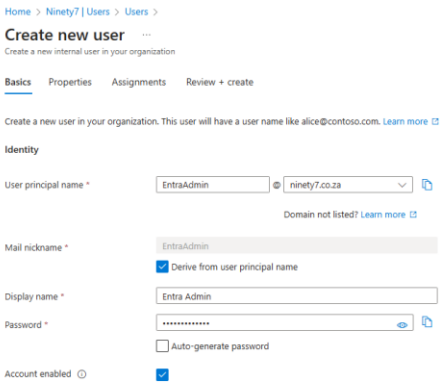


Enter credentials for a user with Hybrid Identity or Global Admin permissions.

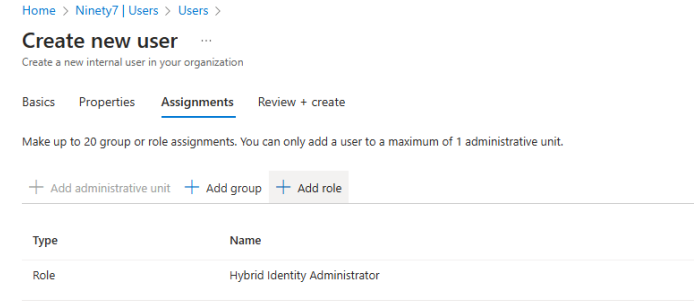
It is good practice to create a dedicated account for this. This account should not be used for anything else. So I created EntraAdmin.



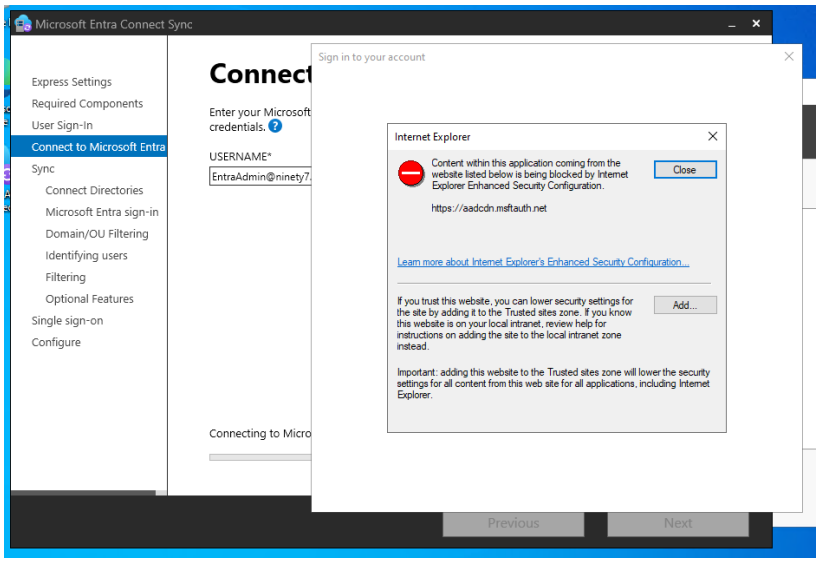
Steps I took in creating EntraAdmin user in my Entra ID tenant.



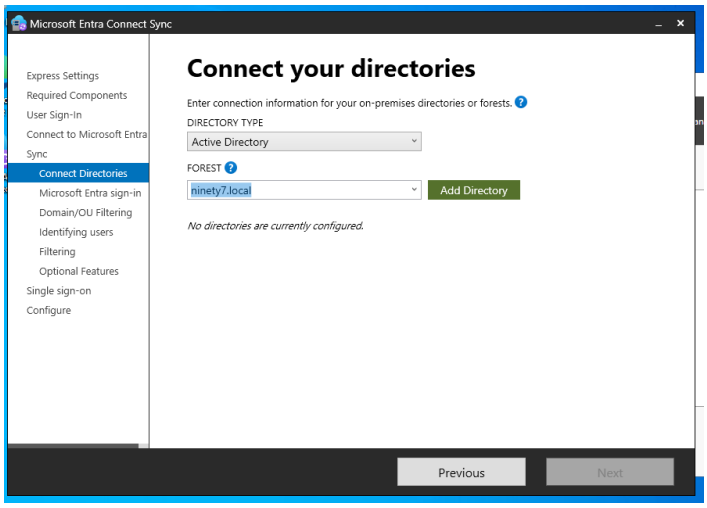
Assigned EntraAdmin the Hybrid Identity Administrator role.



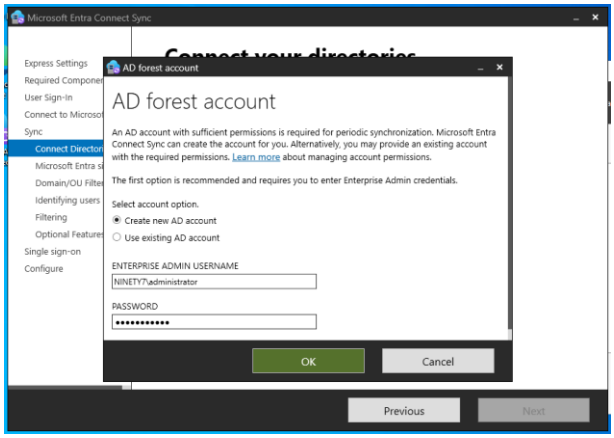
Add required websites to trusted websites in Internet Explorer



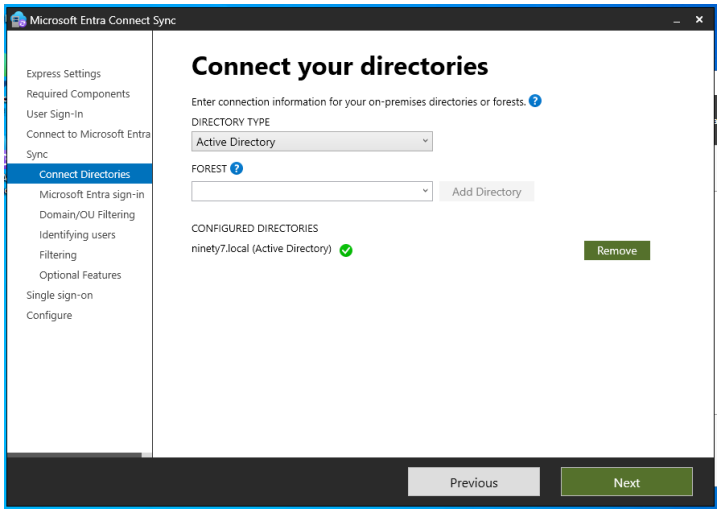
Enter your directory information.



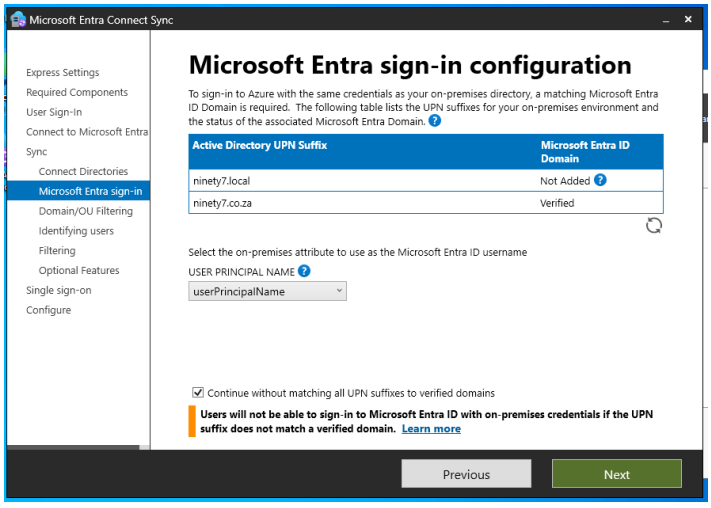
Input credentials for an Enterprise Admin credentials on your server. It is recommended to use a dedicated AD enterprise admin account for this.



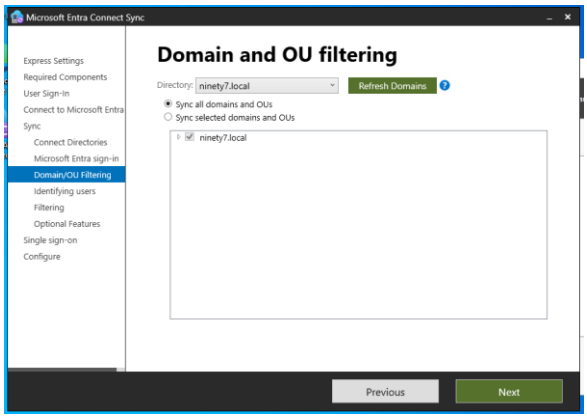
Specify directory.



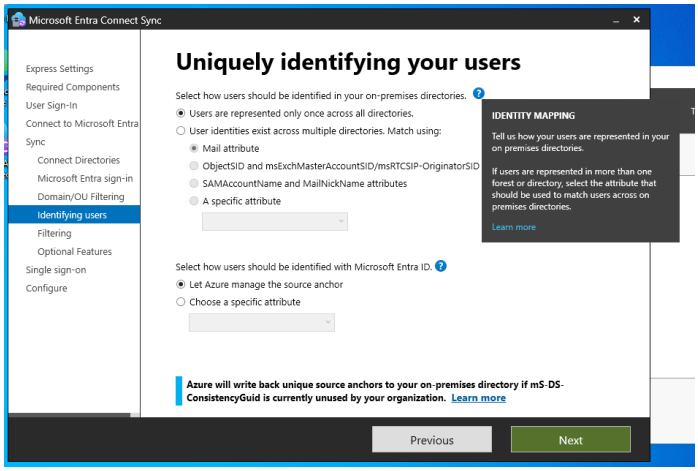
Confirm.



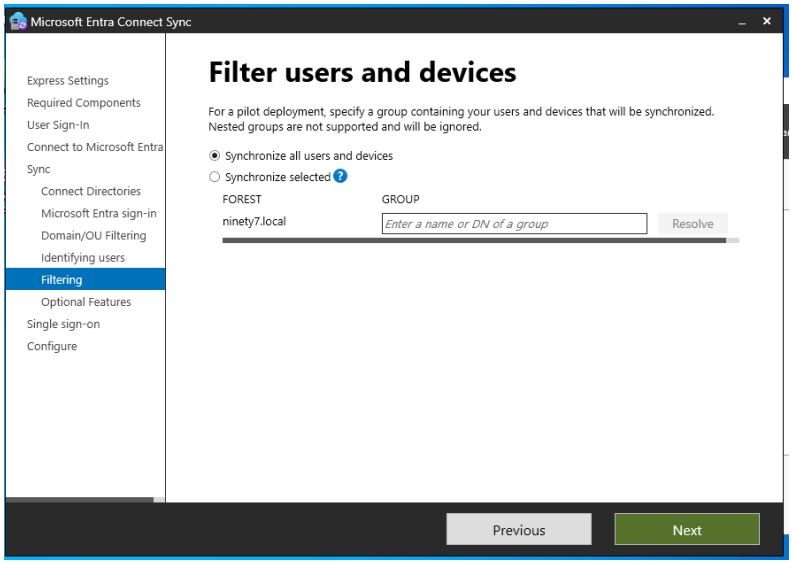
Leave default selections



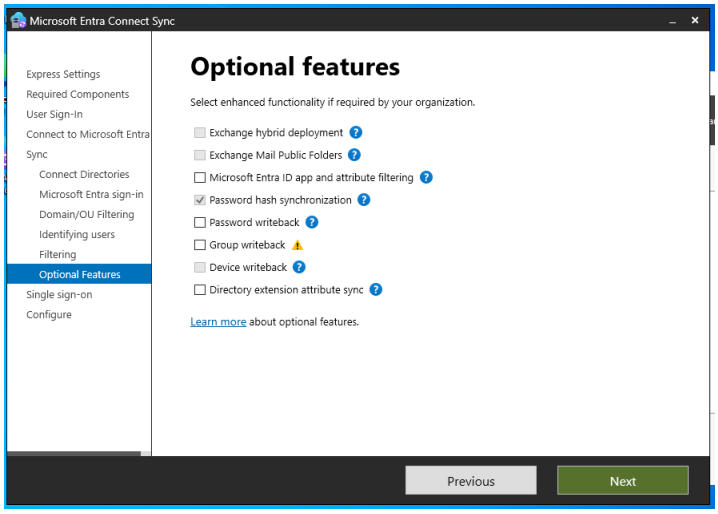
I used default selections.



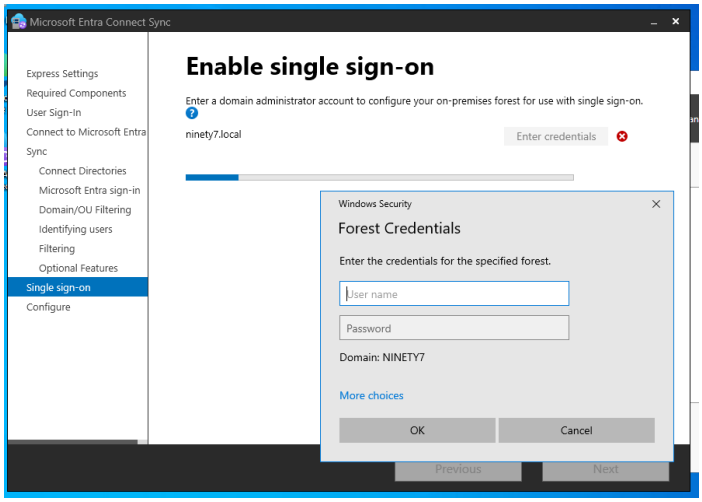
I will be syncing all users and devices so I left as default.



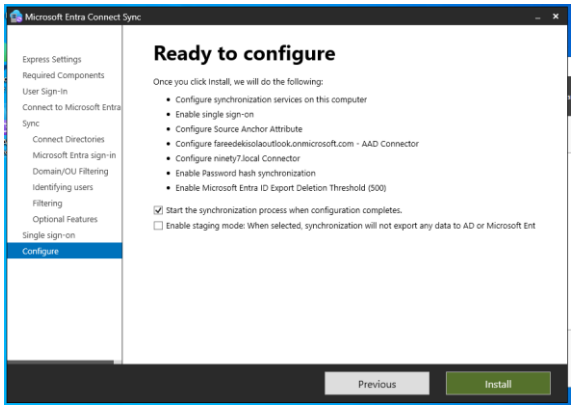
No need for extra features. Cannot use them for this project anyways since most of them require a paid subscription.

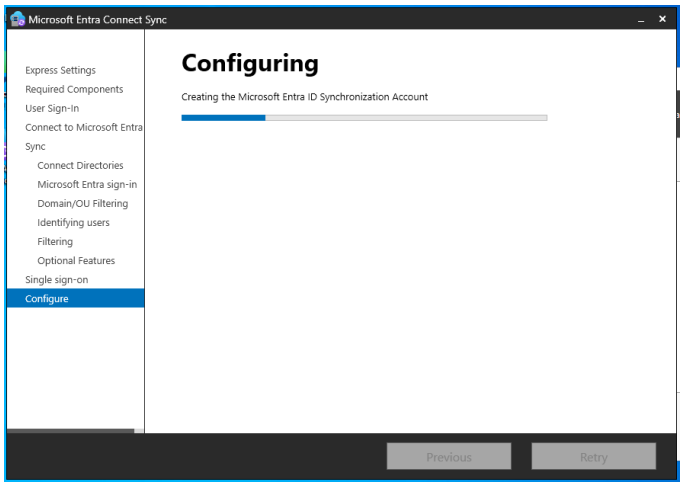


Enable SSO, enter a domain admin credentials.

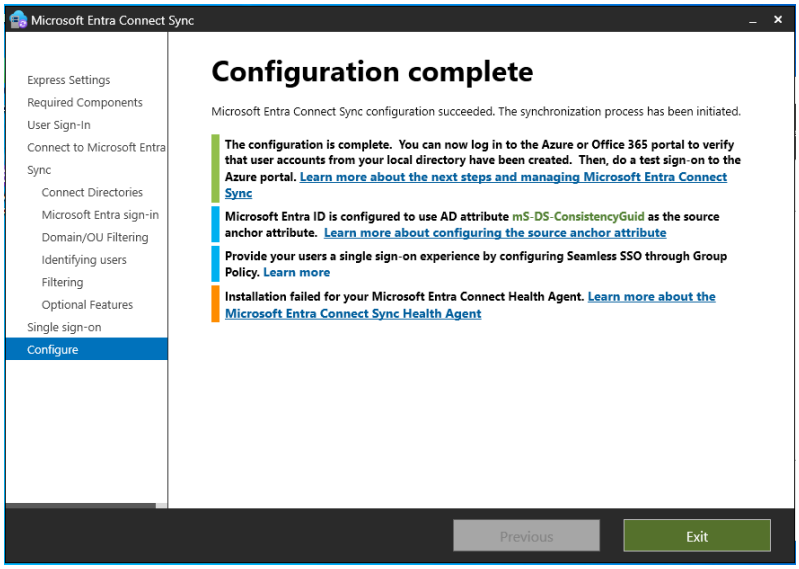


Confirm all selections.





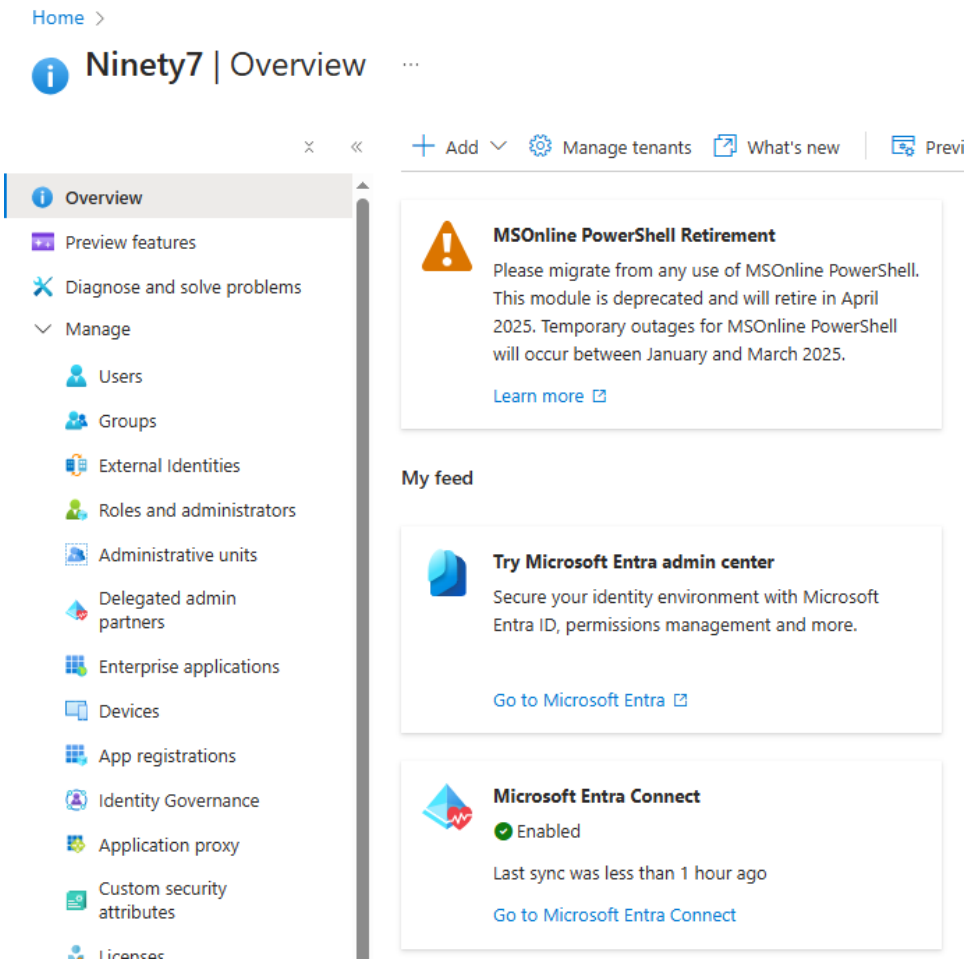
Configuration complete. Successful. Notice the error message; that is because Microsoft Entra Connect Health requires Entra P1/P2 but I am using Entra Free subscription.



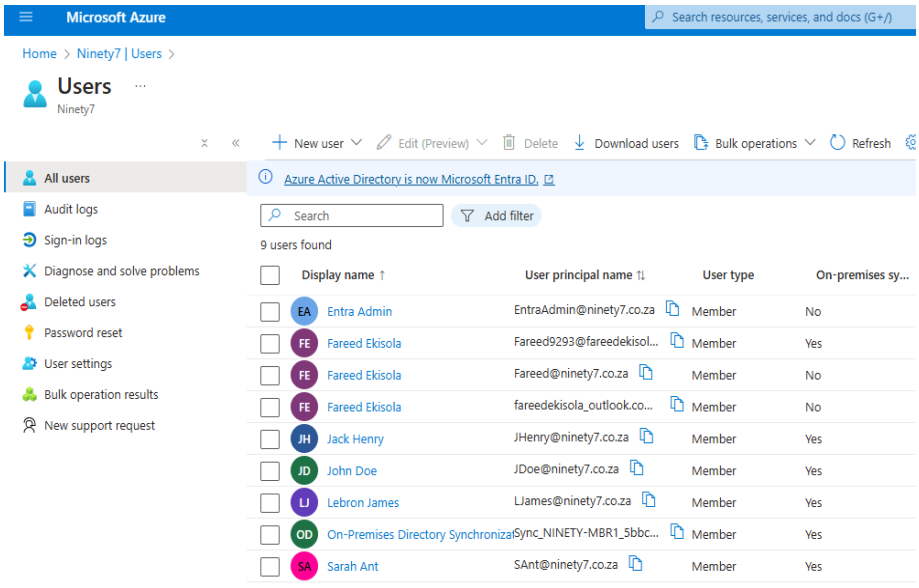
Log in to your Entra ID tenant/ Admin center.

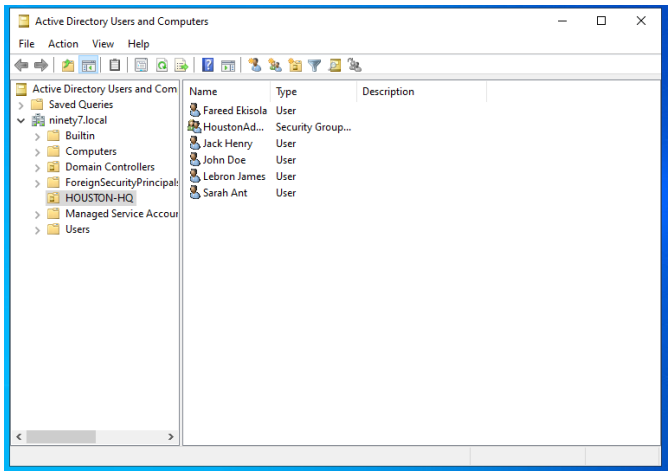
Ensure Entra Connect is enabled.

Ensure Synchronization is in place ad working properly.

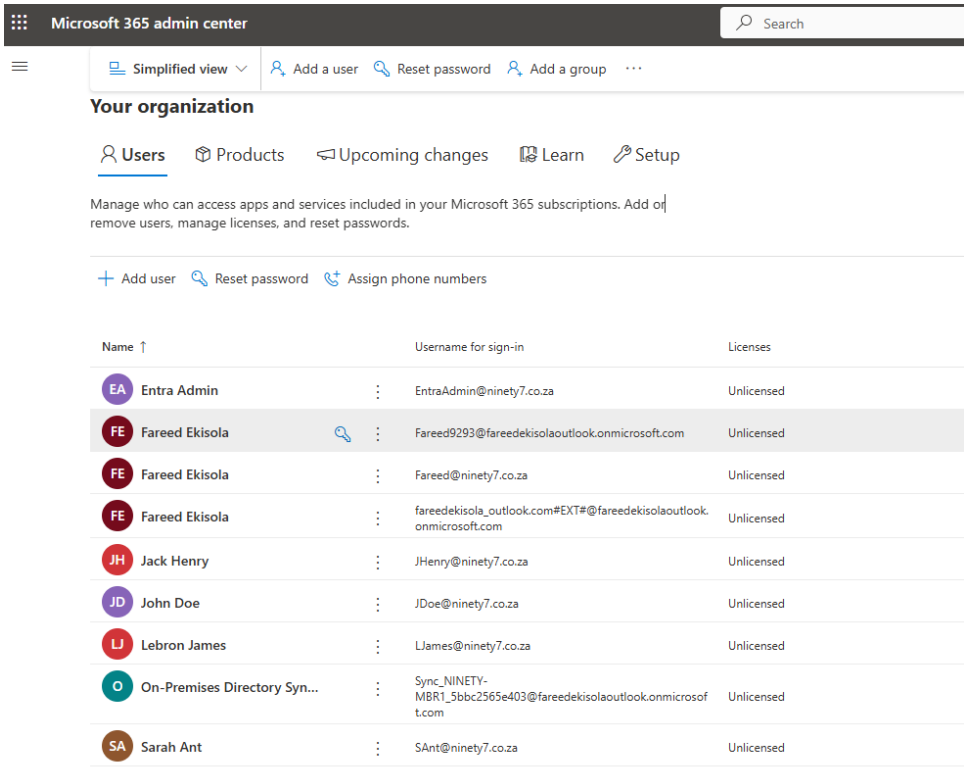


Ensure your On-Prem users have successfully synced to your Entra Tenant





Ensure users are also showing up in 365 Admin Center.



Test other Microsoft Entra Connect sync capabilities.

And that's it I successfully migrated an on-prem directory to Entra ID.