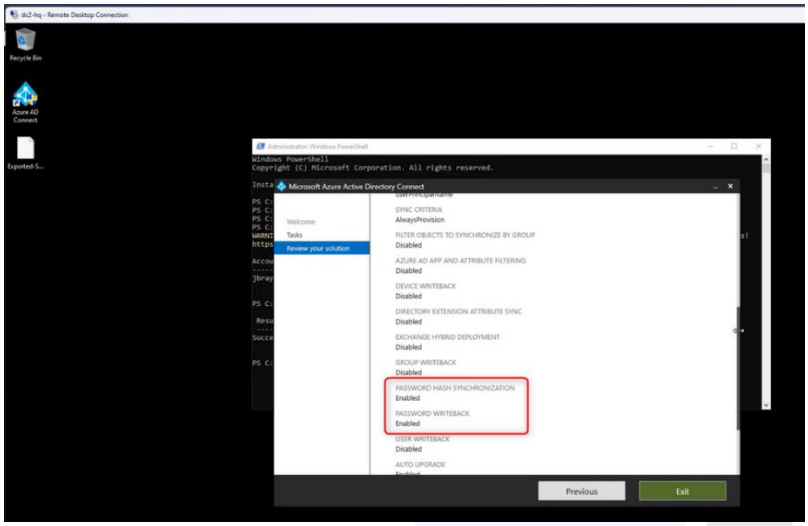
# Password Expiration policy Sync (On-Premises and Azure)

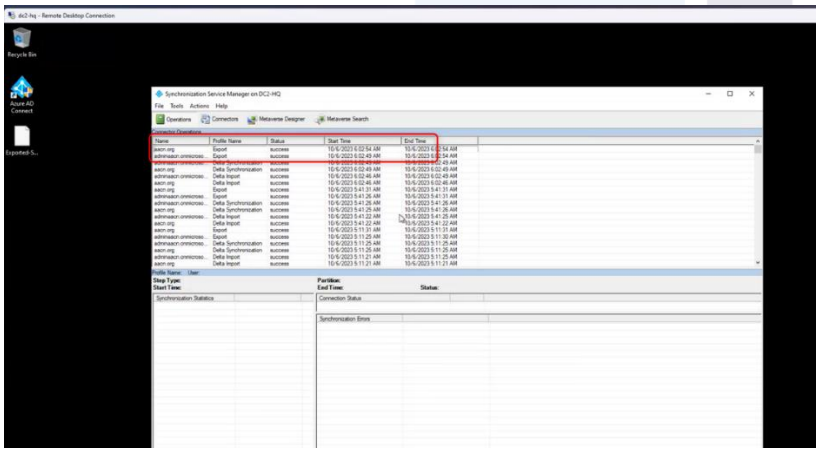
## *Environment – AACN*

*Prepared By:*
*--Shivam Shah*
*--Vatsal Patel*

**Pre-requisites:**

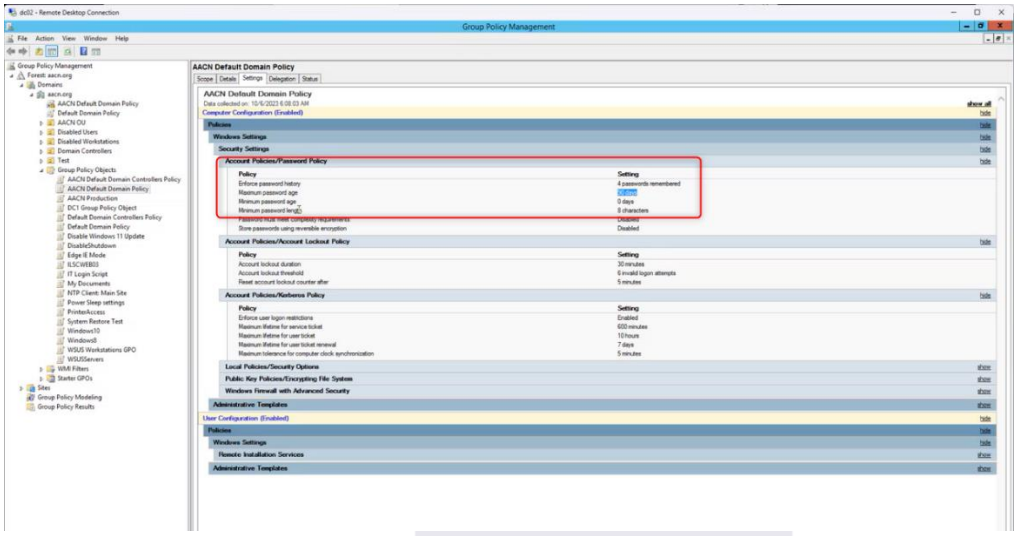
- AD sync tool should be enabled and working
- Password hash sync and password write back should be enabled.
- In on-premises AD, password never expire should be disabled.
- In on-premises AD, user cannot reset the password should be disabled.



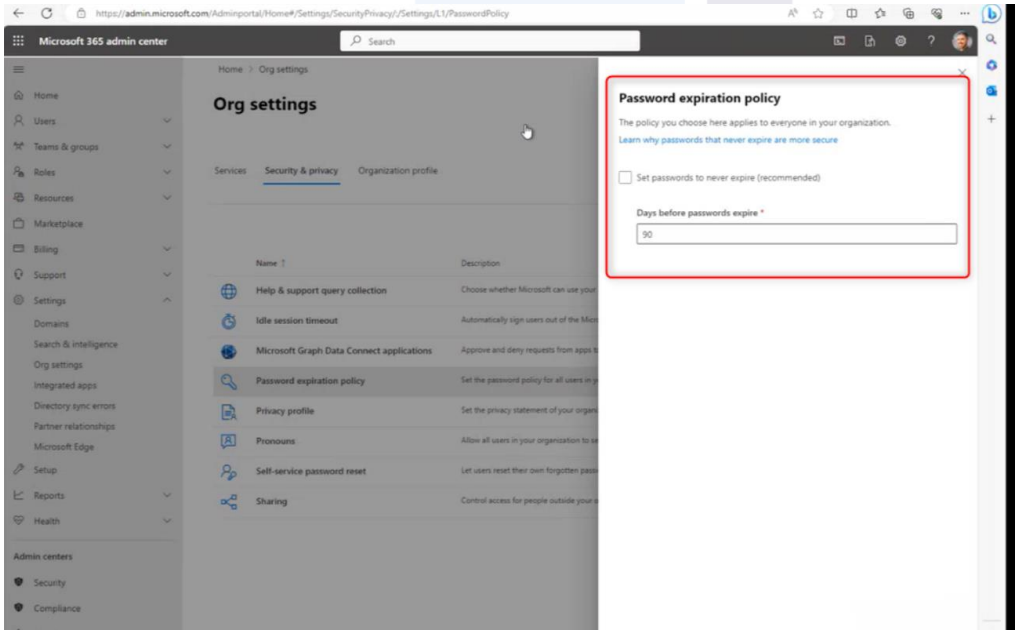



**Steps:**

**1.** Set password expiration policy **on -premises AD** (x days (90 days))




**2.** Set same expiration days in **office 365** for 90 days:



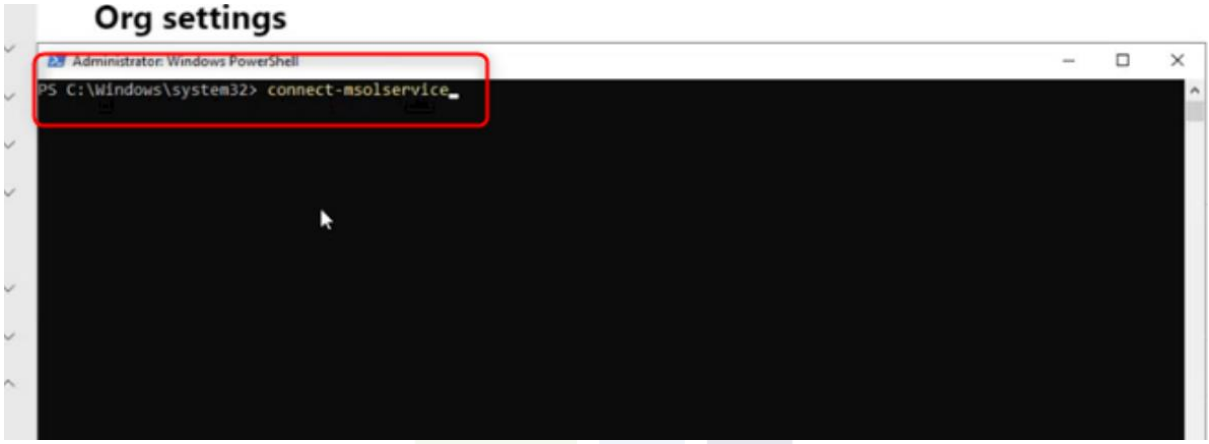
**3. EnforceCloudPasswordPolicyForPasswordSyncedUsers feature:**

Enabling this feature will sync password policy. By default, the password policy on cloud(azure) for synced users is set to **disablepasswordexpiration**. Enabling this will change the password policy for cloud synced users to set it to 90 days once the password is reset from AD or by from azure.

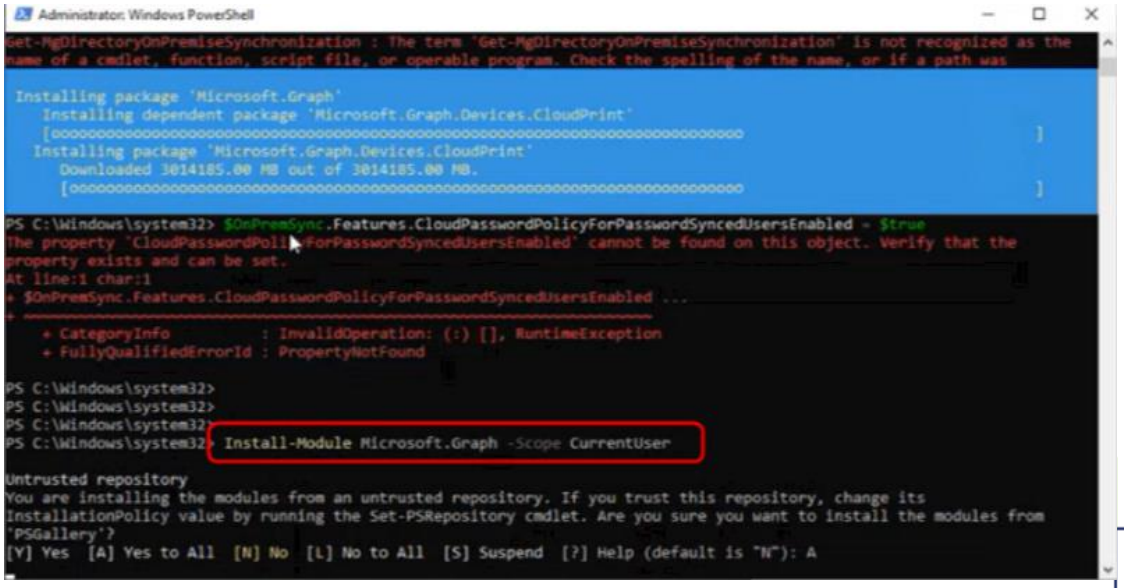
To enable this we would be required to install, Microsoft.Graph module and give permission to the user(global admin):

**3.1** Login to msol.service from PowerShell:

command : *connect-msolservice*, login with global admin credentials.




**3.2** Install *microsoft.graph* module:



--Verify it using get command :

```
Administrator: Windows PowerShell
ption
    + FullyQualifiedErrorId : CommandNotFoundException

PS C:\Windows\system32> $OnPremSync.Features.CloudPasswordPolicyForPasswordSyncedUsersEnabled = $true
The property 'CloudPasswordPolicyForPasswordSyncedUsersEnabled' cannot be found on this object. Verify that the
property exists and can be set.
At line:1 char:1
+ $OnPremSync.Features.CloudPasswordPolicyForPasswordSyncedUsersEnabled ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (:) [], RuntimeException
    + FullyQualifiedErrorId : PropertyNotFound

PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32> Install-Module Microsoft.Graph -Scope CurrentUser

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): A
PS C:\Windows\system32> Get-InstalledModule Microsoft.Graph

Version    Name                                Repository           Description
-------    ----                                ----------           -----------
2.7.0      Microsoft.Graph                     PSGallery            Microsoft Graph PowerShell module


PS C:\Windows\system32>
```

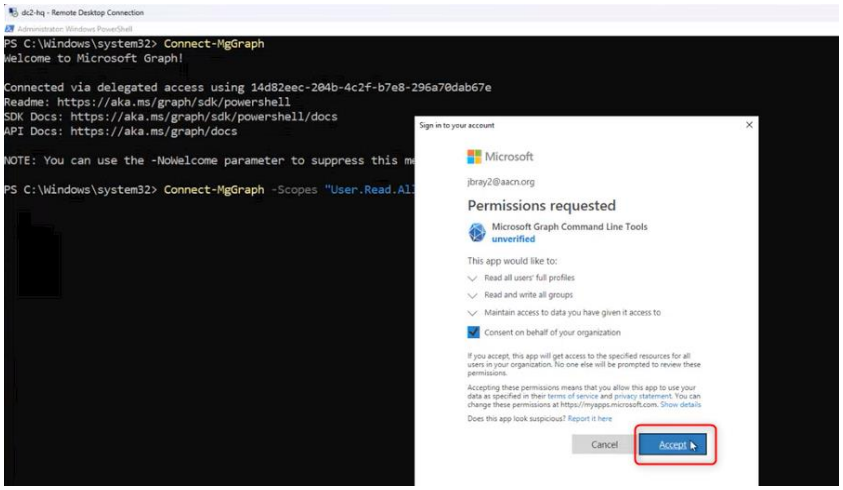
**3.3** connect mg-graph

```
dc2-hq - Remote Desktop Connection
Administrator: Windows PowerShell
PS C:\Windows\system32> Connect-MgGraph
Welcome to Microsoft Graph!

Connected via delegated access using 14d82eec-204b-4c2f-b7e8-296a70dab67e
Readme: https://aka.ms/graph/sdk/powershell
SDK Docs: https://aka.ms/graph/sdk/powershell/docs
API Docs: https://aka.ms/graph/docs

NOTE: You can use the -NoWelcome parameter to suppress this message.

PS C:\Windows\system32>
```

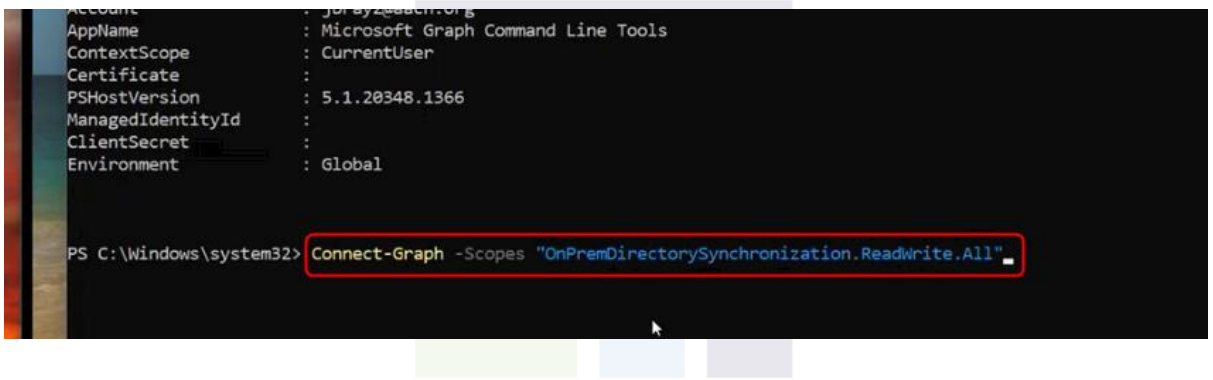
-- command: *Connect-MgGraph -Scopes "User.Read.All", "Group.ReadWrite.All"*

```
dc2-hq - Remote Desktop Connection
Administrator: Windows PowerShell
PS C:\Windows\system32> Connect-MgGraph
Welcome to Microsoft Graph!

Connected via delegated access using 14d82eec-204b-4c2f-b7e8-296a70dab67e
Readme: https://aka.ms/graph/sdk/powershell
SDK Docs: https://aka.ms/graph/sdk/powershell/docs
API Docs: https://aka.ms/graph/docs

NOTE: You can use the -NoWelcome parameter to suppress this message.

PS C:\Windows\system32> Connect-MgGraph -Scopes "User.Read.All", "Group.ReadWrite.All"
Welcome to Microsoft Graph!

Connected via delegated access using 14d82eec-204b-4c2f-b7e8-296a70dab67e
Readme: https://aka.ms/graph/sdk/powershell
SDK Docs: https://aka.ms/graph/sdk/powershell/docs
API Docs: https://aka.ms/graph/docs

NOTE: You can use the -NoWelcome parameter to suppress this message.

PS C:\Windows\system32>
```

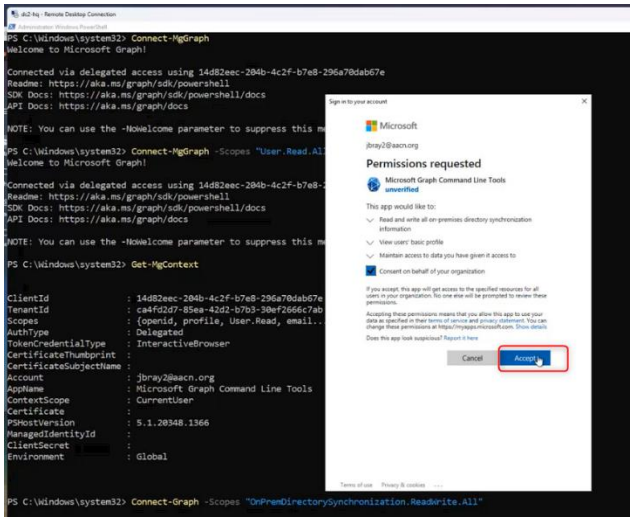
Approve the connection:




-- command: *Connect-Graph -Scopes "OnPremDirectorySynchronization.ReadWrite.All"*




Approve the connection:



-- command: *Get-MgContext command to verify the delegation:*

```
API Docs: https://aka.ms/graph/docs

NOTE: You can use the -NoWelcome parameter to suppress this message.

PS C:\Windows\system32> Get-MgContext


ClientId              : 14d82eec-204b-4c2f-b7e8-296a70dab67e
TenantId              : ca4fd2d7-85ea-42d2-b7b3-30ef2666c7ab
Scopes                : {Group.ReadWrite.All, openid, profile, User.Read...}
AuthType              : Delegated
TokenCredentialType   : InteractiveBrowser
CertificateThumbprint :
CertificateSubjectName :
Account               : jbray2@aacn.org
AppName               : Microsoft Graph Command Line Tools
ContextScope          : CurrentUser
Certificate           :
PSHostVersion         : 5.1.20348.1366
ManagedIdentityId     :
ClientSecret          :
Environment           : Global
```

Now, Microsoft.Graph module is installed with delegate permissions provided to user (global admin) performing this activity. Next, we will enable **CloudPasswordPolicyForPasswordSyncedUsers** using below command: (this will sync the password related attributes)

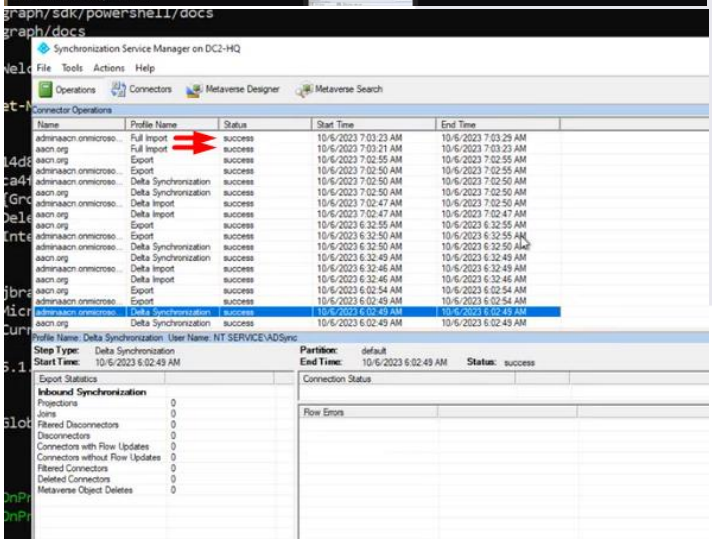
*$OnPremSync = Get-MgDirectoryOnPremiseSynchronization*
*$OnPremSync.Features.CloudPasswordPolicyForPasswordSyncedUsersEnabled = $true*

*Update-MgDirectoryOnPremiseSynchronization*
*-OnPremisesDirectorySynchronizationId $OnPremSync.Id*
*-Features $OnPremSync.Features*

```
dc2-hq - Remote Desktop Connection
Administrator: Windows PowerShell
Readme: https://aka.ms/graph/sdk/powershell
SDK Docs: https://aka.ms/graph/sdk/powershell/docs
API Docs: https://aka.ms/graph/docs

NOTE: You can use the -NoWelcome parameter to suppress this message.

PS C:\Windows\system32> Get-MgContext


ClientId              : 14d82eec-204b-4c2f-b7e8-296a70dab67e
TenantId              : ca4fd2d7-85ea-42d2-b7b3-30ef2666c7ab
Scopes                : {Group.ReadWrite.All, openid, profile, User.Read...}
AuthType              : Delegated
TokenCredentialType   : InteractiveBrowser
CertificateThumbprint :
CertificateSubjectName :
Account               : jbray2@aacn.org
AppName               : Microsoft Graph Command Line Tools
ContextScope          : CurrentUser
Certificate           :
PSHostVersion         : 5.1.20348.1366
ManagedIdentityId     :
ClientSecret          :
Environment           : Global


PS C:\Windows\system32> $OnPremSync = Get-MgDirectoryOnPremiseSynchronization
PS C:\Windows\system32> $OnPremSync.Features.CloudPasswordPolicyForPasswordSyncedUsersEnabled = $true
PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32> Update-MgDirectoryOnPremiseSynchronization `
>>   -OnPremisesDirectorySynchronizationId $OnPremSync.Id `
>>   -Features $OnPremSync.Features
PS C:\Windows\system32>
```

**4.** Enforce initial adsync from PowerShell:

```
Connected via delegated access using 14d82eec-204b-4c2f-b7e8-296a70dab67e
Readme: https://aka.ms/graph/sdk/powershell
SDK Docs: https://aka.ms/graph/sdk/powershell/docs
API Docs: https://aka.ms/graph/docs

NOTE: You can use the -NoWelcome parameter to suppress this message.

PS C:\Windows\system32> Get-MgContext


ClientId              : 14d82eec-204b-4c2f-b7e8-296a70dab67e
TenantId              : ca4fd2d7-85ea-42d2-b7b3-30ef2666c7ab
Scopes                : {Group.ReadWrite.All, openid, profile, User.Read...}
AuthType              : Delegated
TokenCredentialType   : InteractiveBrowser
CertificateThumbprint :
CertificateSubjectName :
Account               : jbray2@aacn.org
AppName               : Microsoft Graph Command Line Tools
ContextScope          : CurrentUser
Certificate           :
PSHostVersion         : 5.1.20348.1366
ManagedIdentityId     :
ClientSecret          :
Environment           : Global


PS C:\Windows\system32> $OnPremSync = Get-MgDirectoryOnPremiseSynchronization
PS C:\Windows\system32> $OnPremSync.Features.CloudPasswordPolicyForPasswordSyncedUsersEnabled = $true
PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32>
PS C:\Windows\system32> Update-MgDirectoryOnPremiseSynchronization `
>>   -OnPremisesDirectorySynchronizationId $OnPremSync.Id `
>>   -Features $OnPremSync.Features
PS C:\Windows\system32> Start-ADSyncSyncCycle -PolicyType Initial

 Result
 ------
Success


PS C:\Windows\system32>
```



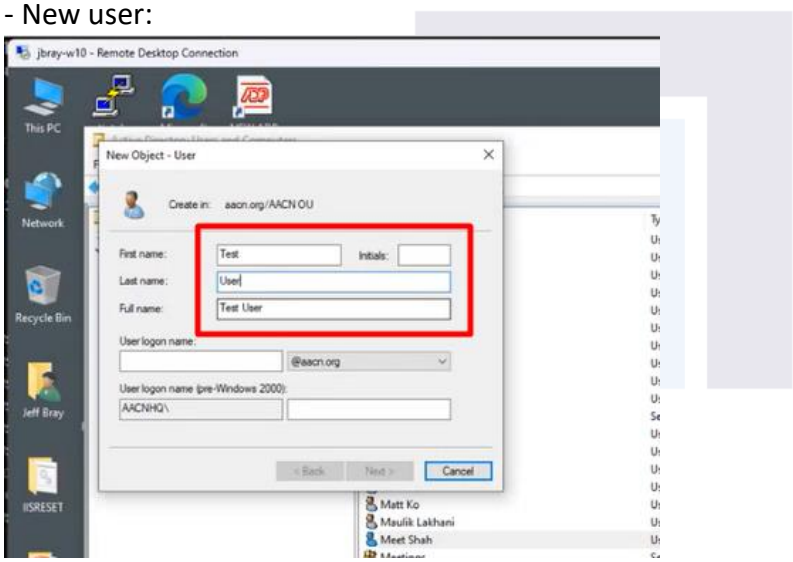
**5.** As the ADsync feature – password hash sync was already enabled; this policy will work for new synced users which are created after enabling **CloudPasswordPolicyForPasswordSyncedUsers**.

So, to apply the same policy for existing synced users, either password needs to be reset from on-premises AD and execute sync command or let user reset his/her password from cloud with change the password policies from DisablePasswordExpiration to None (90 days which we have applied from office 365).

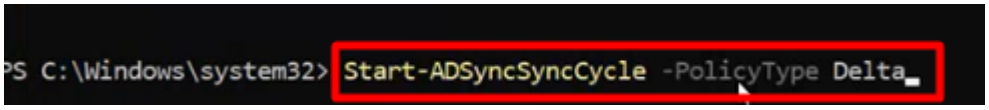
**5.1** Test case, for new user created on premise, the password policy would be set to none. (if this cloud password policy for password synced users would not be enabled it property value of password policies would be DisablePasswordExpiration):

-- Create a new user on on-premise and sync it on cloud and check the password policy property:

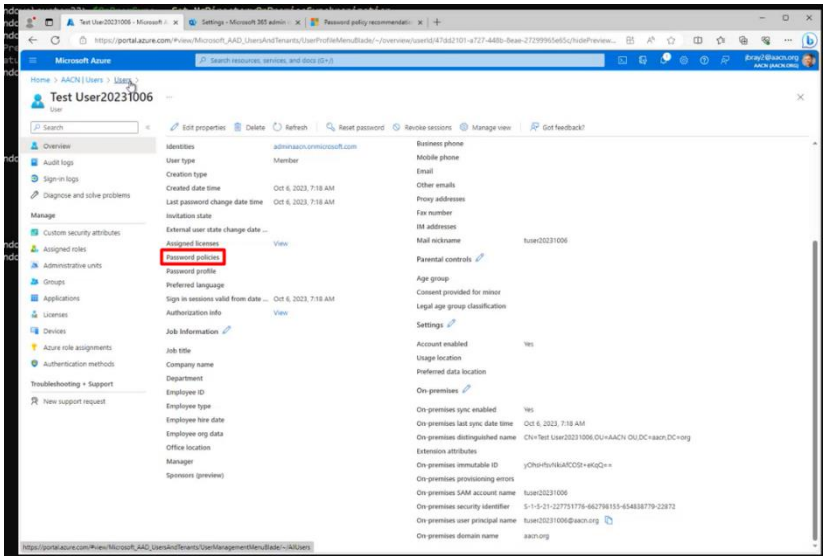
- New user:




- Delta Sync:

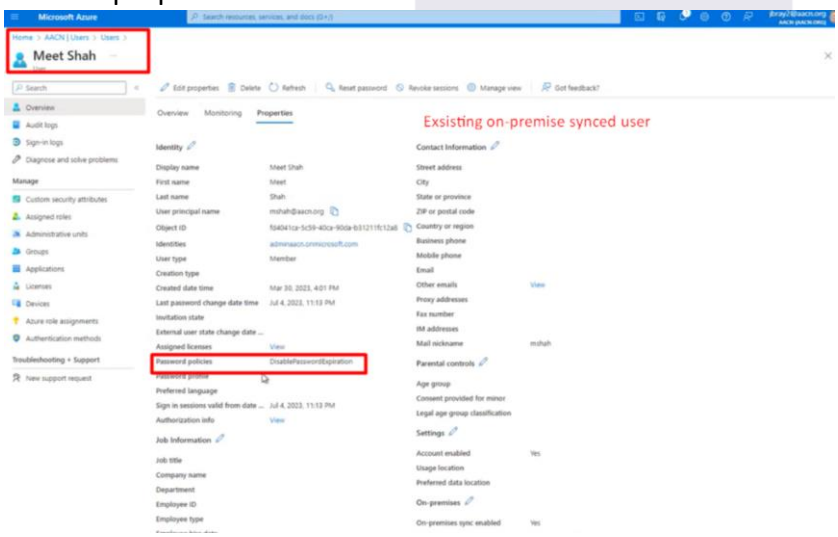


- Check in azure AD, users:

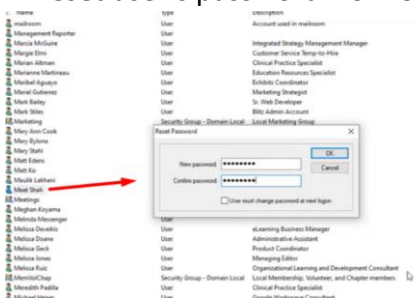



**5.2.1** Test case, for existing cloud synced user resetting password from on-premise AD:

-- check properties in Azure AD:



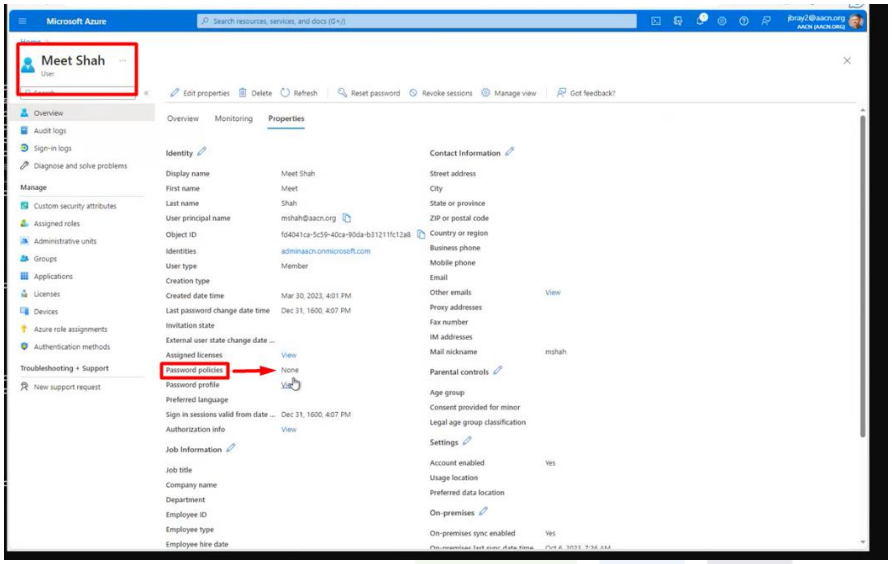

-- Reset user's password from on-premise AD:



-- Delta sync:

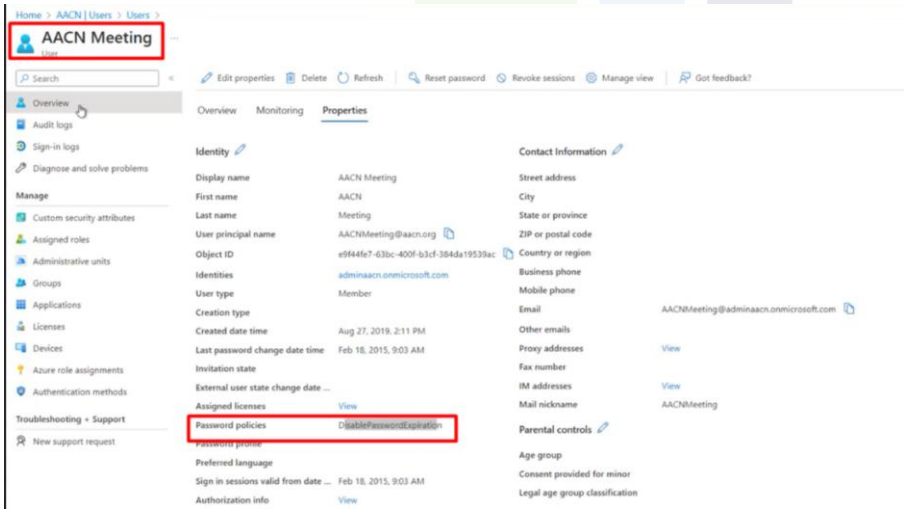
```
PS C:\Windows\system32> Start-ADSyncSyncCycle -PolicyType Delta

Result
------
Success

PS C:\Windows\system32>
```

-- Now, check the properties in AzureAD:

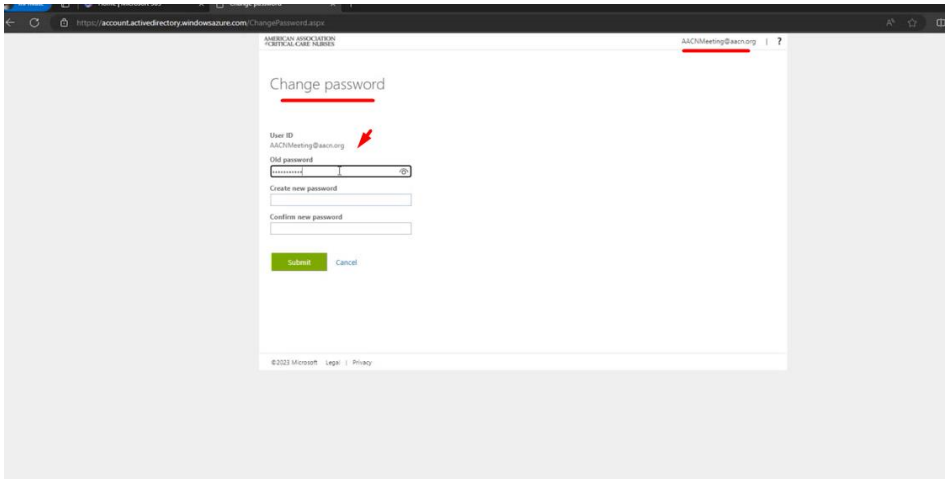



**5.2.2** Test case, resetting password by user from cloud for synced users:

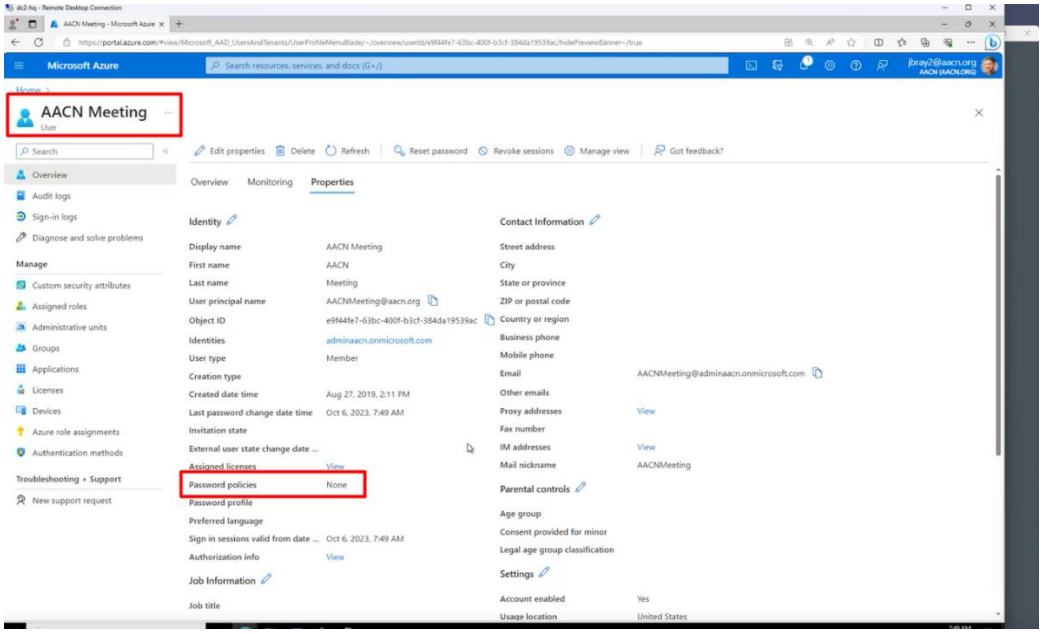
-- check the user properties in Azure AD:



-- Login with that user in office online and reset his/her password:




-- Check user properties from Azure AD:

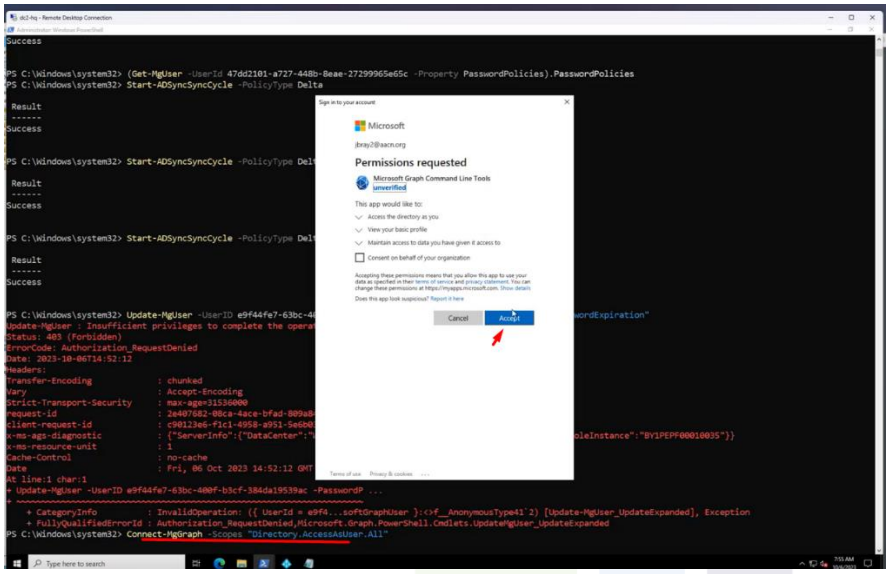


**6.** If you want to set any cloud synced user to “password never expire”:

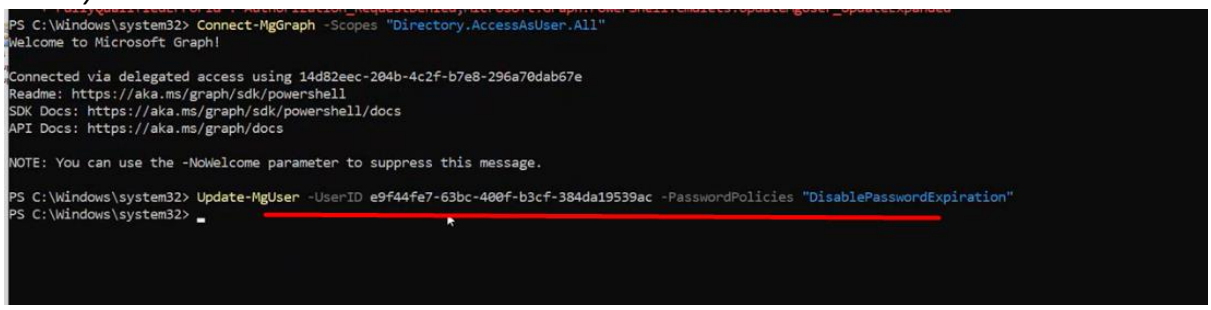
There are 2 options:

**Option1: using user id**:
-- Check mark password never expire for that particular user from on premise AD
-- Connect mgGraph service and use below command:

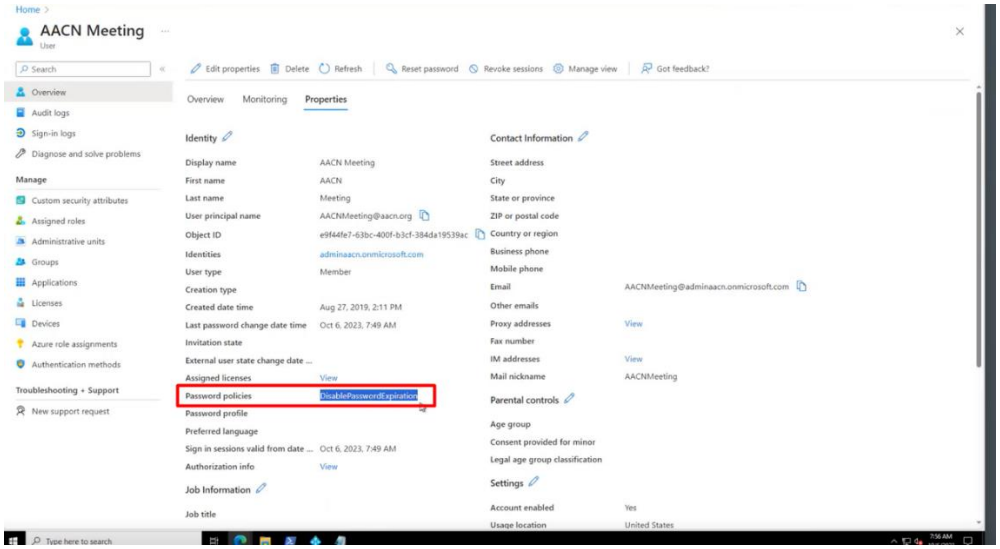
*Connect-Graph -Scopes "OnPremDirectorySynchronization.ReadWrite.All"*




Command:
*Update-MgUser -UserID <User Object ID> -PasswordPolicies "DisablePasswordExpiration", next do detla sync:*



-- check azure AD user properties, it would change to disable password expiration:




**Option2: using UPN (user principal name):**

-- Check mark password never expire for that user from on premise AD

--connect msol service and use below command:

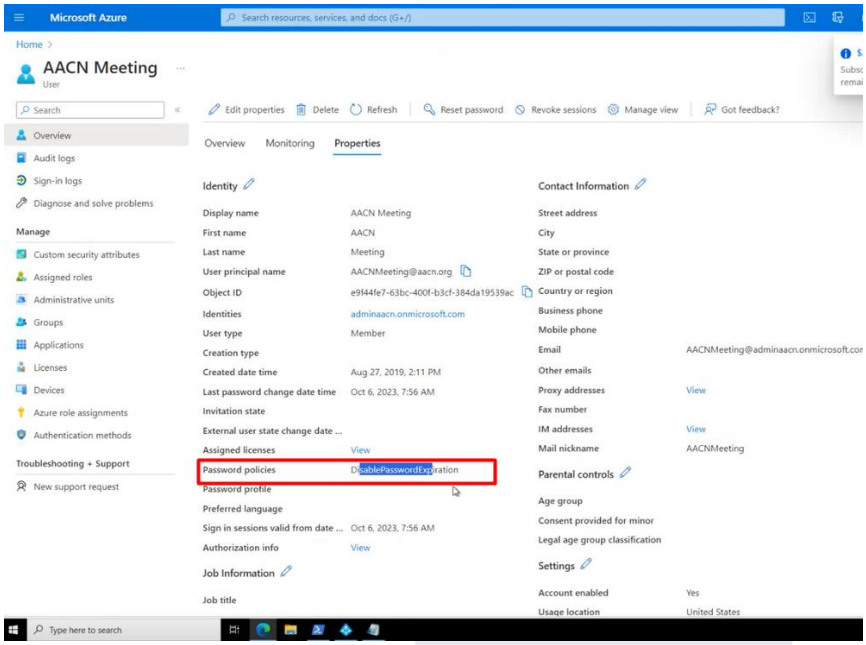
```
PS C:\Windows\system32> Start-ADSyncSyncCycle -PolicyType Delta

 Result
 ------
Success

PS C:\Windows\system32> connect-msolservice
```

command:

*Set-MsolUser -UserPrincipalName shivam.shah@dynatechconsultancy.com -PasswordNeverExpires $true*

```
PS C:\Windows\system32> connect-msolservice
PS C:\Windows\system32> Set-MsolUser -UserPrincipalName aacnmeeting@aacn.org -PasswordNeverExpires $true
PS C:\Windows\system32>
```

-- Execute detla sync and then check azure AD user properties:




***References:***

*https://learn.microsoft.com/en-us/microsoft-365/admin/manage/set-password-expiration-policy?view=o365-worldwide*

*https://learn.microsoft.com/en-us/answers/questions/721416/password-expiration-with-aad-connect-password-hash*

*https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-sspr-writeback*

*https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-password-hash-synchronization#enforcecloudpasswordpolicyforpasswordsyncedusers*