Manually match On Premise AD-user to existing M365 user

For anyone running into this issue, I wrote a script to re-link users for an ou to Azure AD. In my case, I moved all users from the ou I wanted to re-sync to Temp, ran the script, moved users back to the desired ou and re-ran the sync.

```
Import-Module ActiveDirectory
$user = $null
$Path = “c:\temp\exporteduser.txt”

#Load all users in the specified OU.
$users = Get-ADUser -SearchBase “ou=Temp,dc=somedomain,dc=com” -Filter *

#Connect to Azure AD
Connect-MsolService

#Make sure Soft Match is enabled (It should be enabled by default after 2016).
Set-MsolDirSyncFeature -Feature EnableSoftMatchOnUpn -Enable $True

#Iterate through users and link their guid as Immutable ID in Azure.
ForEach($user in $users)
{
$distinguishedName = $user.distinguishedName

#Write the user data to a temp file with the guid in the correct format for AzureAD.
ldifde -d $distinguishedName -f $Path

#Find the objectGUID in the ouput file.
$guidLine = Select-String -Path $Path -Pattern ‘objectGUID’
$lineLenght = $guidLine.ToString().Length
$guidStart = $guidLine.ToString().IndexOf(“objectGUID:: “) + 13
$guid = $guidLine.ToString().Substring($guidStart, $lineLenght – $guidStart)
Write-Host “Setting Immutable ID: ” $guid ” for User: ” $user.UserPrincipalName

#Update the Immutable Id in Azure AD so the on premise user will match on sync.
```

```
set-msoluser -userprincipalname $user.userPrincipalName -ImmutableID $guid
}

#Force a resync with Azure AD.
Start-ADSyncSyncCycle -PolicyType Delta
Write-Host User re-link complete
```

Original Article

Revision #1
Created 2023-11-10 06:03:00 UTC by Ryan
Updated 2025-03-13 20:15:14 UTC by Ryan