HARD MATCH AN AZURE AD ACCOUNT

Prepared by: Elie Karkafy

HOW TO HARD MATCH AN AZURE AD ACCOUNT TO A LOCAL ACTIVE DIRECTORY ACCOUNT

The following tutorial will detail the procedure of performing a Hard-Match between an on- premises Active User and an Azure AD (Office365) user using the immutable ID of the local AD User.

Before we proceed, understand how accounts are created in office 365.

- Azure AD to Office 365 to Exchange Online and other services
- Exchange Online to Azure AD (Ex. Shared Mailboxes)
- On-premises Local AD to Azure AD through a Dir Sync Agent like Azure AD connect Also bear in mind that there is Soft-Matching also known as SMTP match and Hard Matching.

In SMTP Soft-Matching, the Azure AD account, is already going to have a primary SMTP address that you probably don't want to change.

To successfully link the cloud account to an on-prem account you just need to stamp the

same primary SMTP to the on-prem account and run a directory sync.

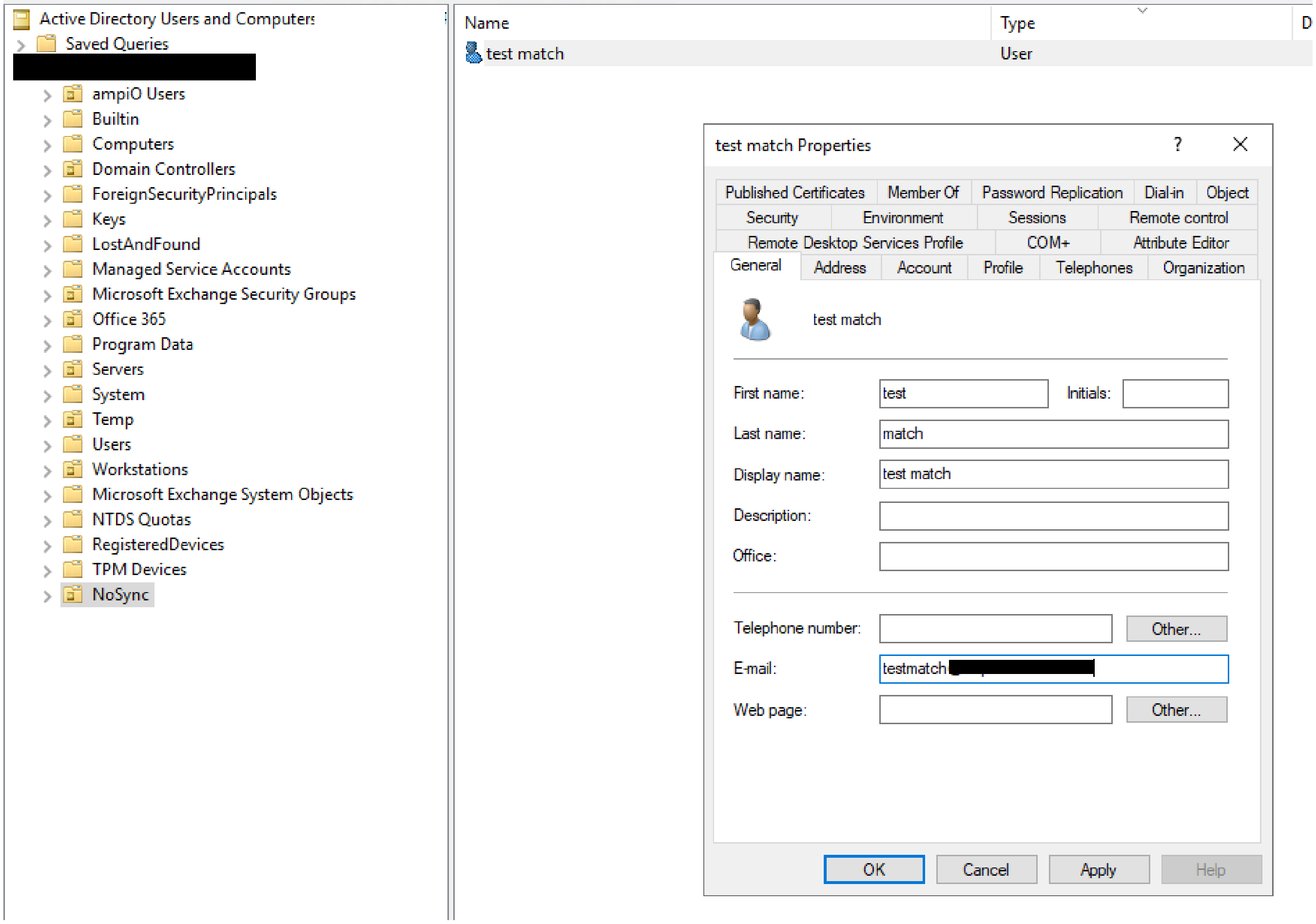
But we are more concerned with Hard-Matching.

Hard Matching may be required where a synced account fails to sync from the local AD which causes the account to enter and a soft-deleted state and then disconnects from the AD account.

Secondly, we may need to convert a cloud only account into a Synced account.

We can follow the steps below on the domain controller.

- We are going to recreate the user on the Local AD and then export the ObjectGUID that will be used to match the cloud account.
- Recreate the User on the Local AD inside a Non-Syncing OU to avoid creating a duplicate copy in Azure AD because we are not stopping the sync service.
- Ensure that the local AD, under 'General tab' the email address tab of the user should have the same UPN as is on cloud.



Name	Type
test match	User

test match

First name: test

Initials:

Last name: match

Display name: test match

Description:

Office:

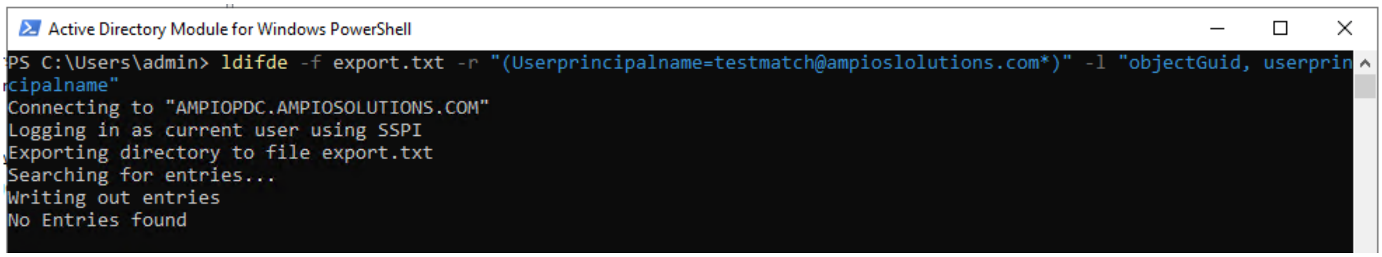
Telephone number:

E-mail: testmatch[redacted]

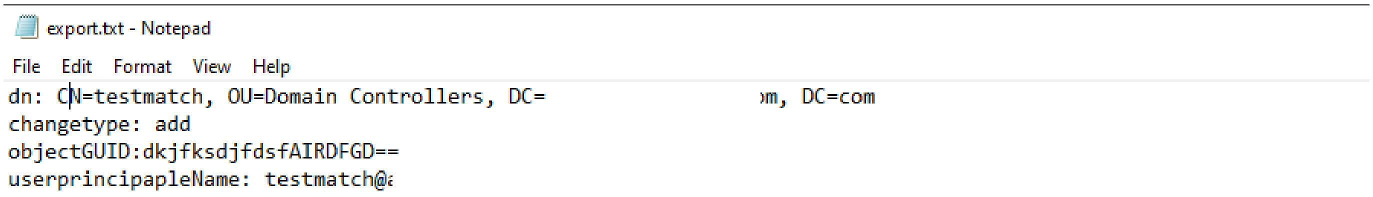
Web page:

Get the ObjectGUID of the local AD.

- Launch PowerShell on your local AD server,
- Run the following commands.
  ldifde -f export.txt -r "(Userprincipalname=user@domain.com)" -l "objectGuid, userprincipalname"*
  (Make sure to replace the user@domain.com with the local AD UPN of the user)
- Open the exported data using Notepad and copy the value of the ObjectGUID. (This will be stored in current working directory on PowerShell)
  (Looks something like this: 1wfM9xV8fUSHbcAbDlqeOA==)

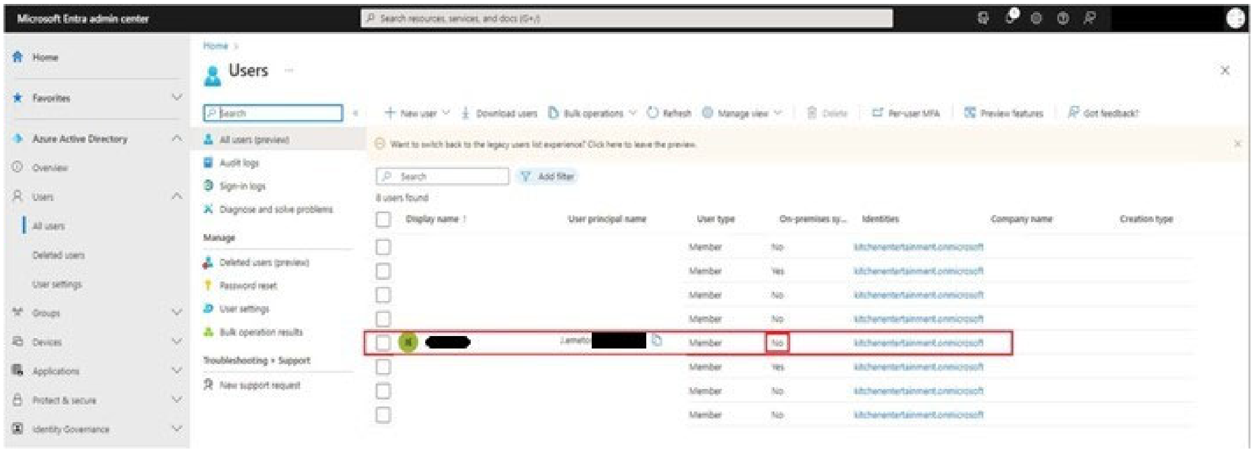


```
PS C:\Users\admin> ldifde -f export.txt -r "(Userprincipalname=testmatch@ampioslolutions.com*)" -l "objectGuid, userprin
cipalname"
Connecting to "AMPIOPDC.AMPIOSOLUTIONS.COM"
Logging in as current user using SSPI
Exporting directory to file export.txt
Searching for entries...
Writing out entries
No Entries found
```



```
dn: CN=testmatch, OU=Domain Controllers, DC=                  om, DC=com
changetype: add
objectGUID:dkjfksdjfdsfAIRDFGD==
userprincipapleName: testmatch@a
```

Restore the User from deleted users on Azure AD if the user is still in the deleted folder (this converts the account to a cloud only account).



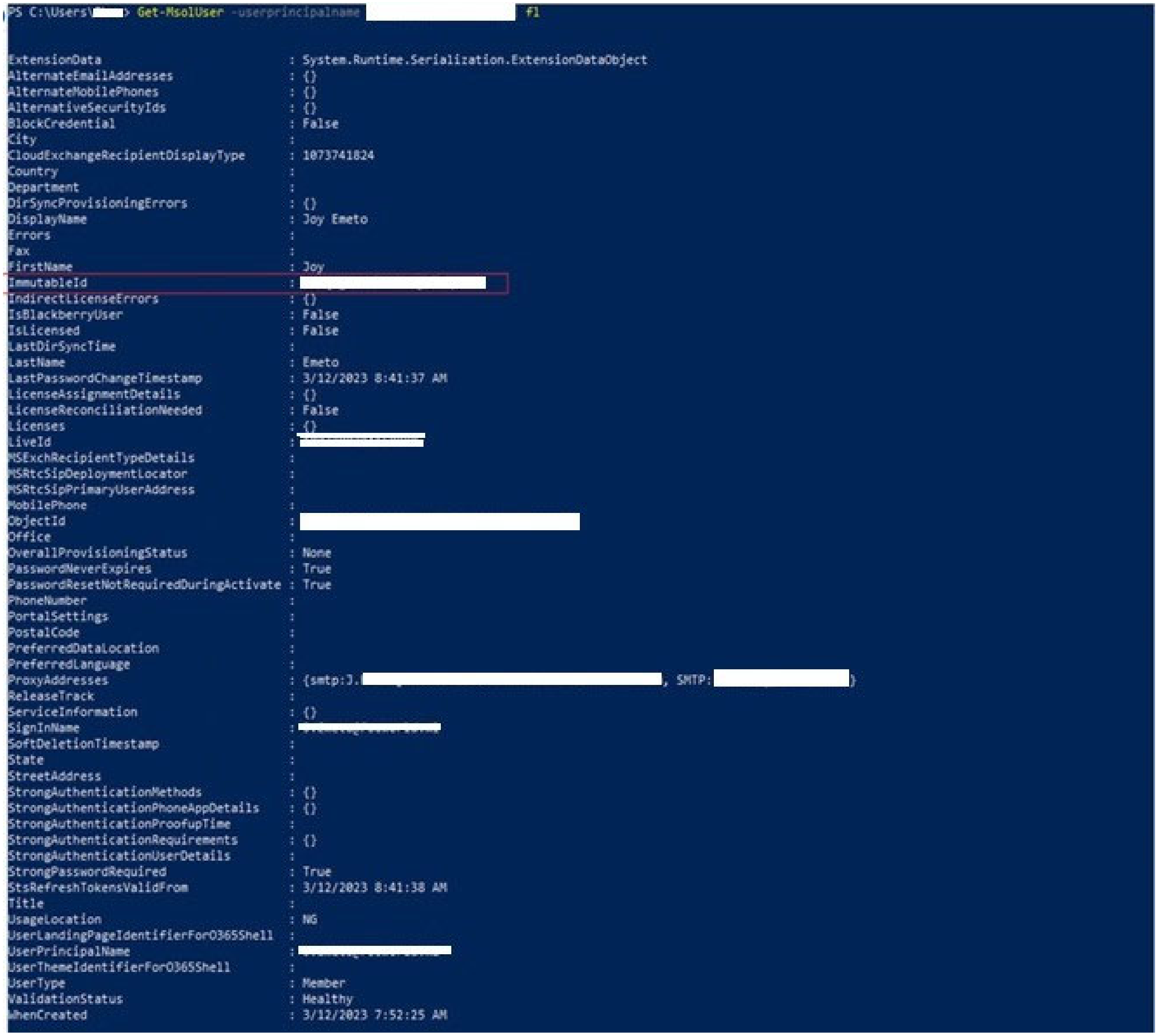
8 users found

Display name ↑	User principal name	User type	On-premises sy...	Identities	Company name	Creation type
		Member	No	kitchenentertainment.onmicrosoft		
		Member	Yes	kitchenentertainment.onmicrosoft		
		Member	No	kitchenentertainment.onmicrosoft		
		Member	No	kitchenentertainment.onmicrosoft		
[redacted]	[redacted]	Member	No	kitchenentertainment.onmicrosoft		
		Member	Yes	kitchenentertainment.onmicrosoft		
		Member	No	kitchenentertainment.onmicrosoft		
		Member	No	kitchenentertainment.onmicrosoft		

Run this command on the Msonline PowerShell module.

- Connect to MSOnline by running this PowerShell command; *Connect- MsolService*
- If you do not have the MSOnline PowerShell module installed, run *Install- Module -Name MSOnline* to install.
- *Get-MsolUser -userprincipalname User@domain| fl*

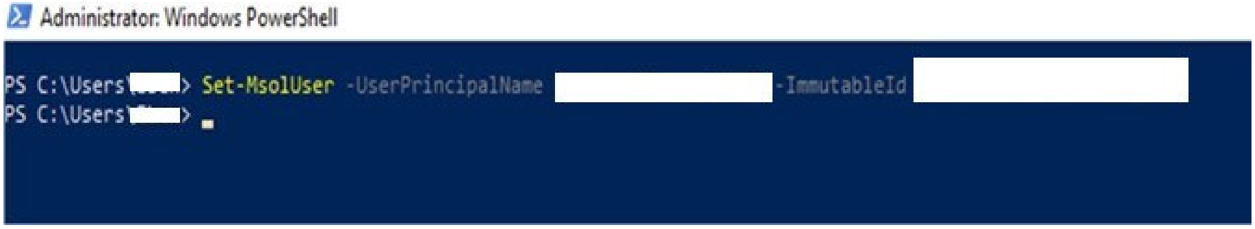
This will get the cloud user details user details and display. Take note of the current Immutable ID on the cloud account like we have in the image below.



```
PS C:\Users\[redacted]> Get-MsolUser -userprincipalname [redacted] fl


ExtensionData                          : System.Runtime.Serialization.ExtensionDataObject
AlternateEmailAddresses                : {}
AlternateMobilePhones                  : {}
AlternativeSecurityIds                 : {}
BlockCredential                        : False
City                                   :
CloudExchangeRecipientDisplayType      : 1073741824
Country                                :
Department                             :
DirSyncProvisioningErrors              : {}
DisplayName                            : Joy Emeto
Errors                                 :
Fax                                    :
FirstName                              : Joy
ImmutableId                            : [redacted]
IndirectLicenseErrors                  : {}
IsBlackberryUser                       : False
IsLicensed                             : False
LastDirSyncTime                        :
LastName                               : Emeto
LastPasswordChangeTimestamp            : 3/12/2023 8:41:37 AM
LicenseAssignmentDetails               : {}
LicenseReconciliationNeeded            : False
Licenses                               : {}
LiveId                                 : [redacted]
MSExchRecipientTypeDetails             :
MSRtcSipDeploymentLocator              :
MSRtcSipPrimaryUserAddress             :
MobilePhone                            :
ObjectId                               : [redacted]
Office                                 :
OverallProvisioningStatus              : None
PasswordNeverExpires                   : True
PasswordResetNotRequiredDuringActivate : True
PhoneNumber                            :
PortalSettings                         :
PostalCode                             :
PreferredDataLocation                  :
PreferredLanguage                      :
ProxyAddresses                         : {smtp:J.[redacted], SMTP:[redacted]}
ReleaseTrack                           :
ServiceInformation                     : {}
SignInName                             : [redacted]
SoftDeletionTimestamp                  :
State                                  :
StreetAddress                          :
StrongAuthenticationMethods            : {}
StrongAuthenticationPhoneAppDetails    : {}
StrongAuthenticationProofupTime        :
StrongAuthenticationRequirements       : {}
StrongAuthenticationUserDetails        :
StrongPasswordRequired                 : True
StsRefreshTokensValidFrom              : 3/12/2023 8:41:38 AM
Title                                  :
UsageLocation                          : NG
UserLandingPageIdentifierForO365Shell  :
UserPrincipalName                      : [redacted]
UserThemeIdentifierForO365Shell        :
UserType                               : Member
ValidationStatus                       : Healthy
WhenCreated                            : 3/12/2023 7:52:25 AM
```

Then we proceed to set the immutable ID of the cloud account to match that of the Local AD account using the Object GUID we exported earlier.

- Run this command *Set-MsolUser -UserPrincipalName User@domain- ImmutableId ObjectGUID* from Export (Make sure to replace the user@domain.com with the UPN of the cloud user)

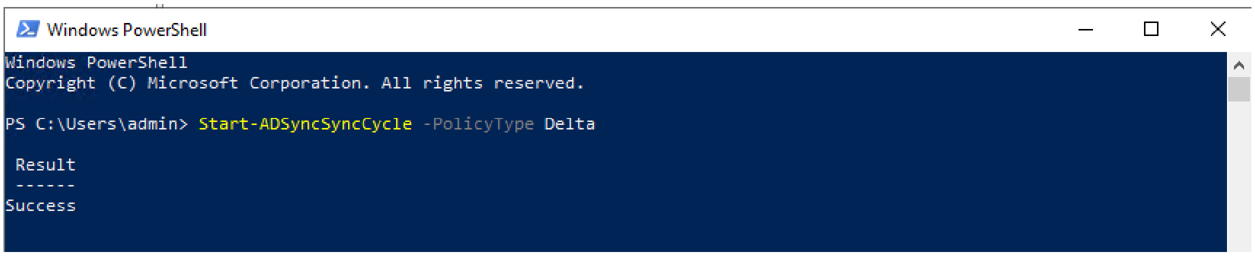


```
PS C:\Users\[redacted]> Set-MsolUser -UserPrincipalName [redacted] -ImmutableId [redacted]
PS C:\Users\[redacted]> _
```

- Move the Cloud account into deleted users again.
- Move the AD account back to a syncing OU.

Run a delta sync *Start-ADSyncSyncCycle -PolicyType Delta* on the local AD powershell

Allow a sync for about 10 mins.

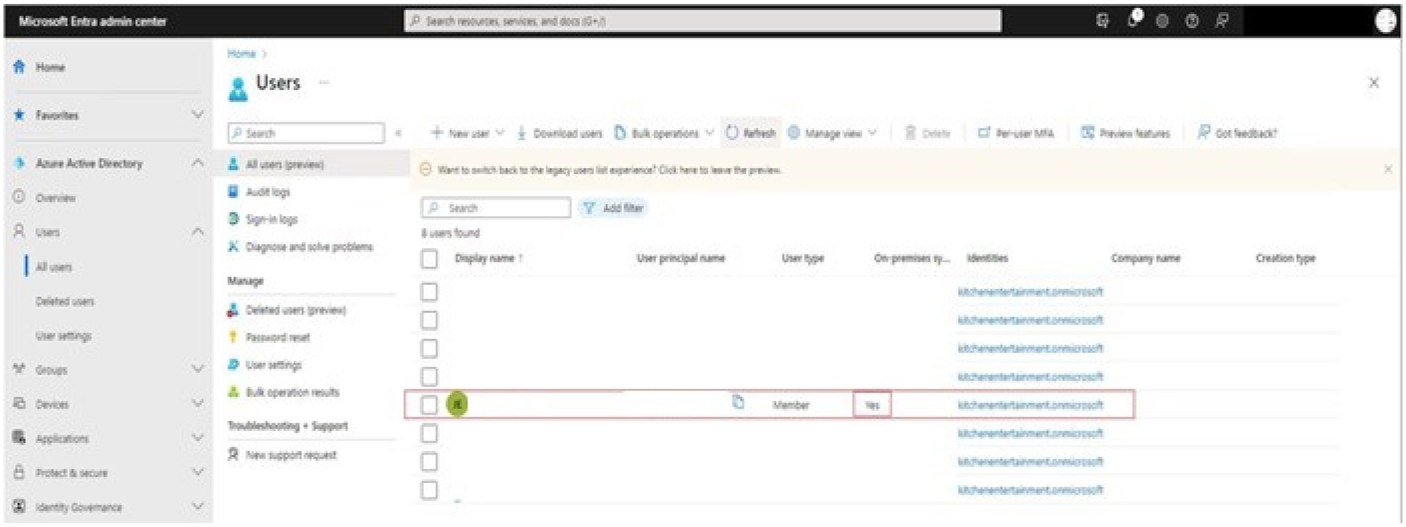


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\admin> Start-ADSyncSyncCycle -PolicyType Delta

 Result
 ------
Success
```

If the account doesn't restore automatically, you can go the deleted user's folder on Azure AD and restore the account.

This is what you should have after the sync completes successfully. The user with a YES under the on-premises sync column.

Also take note of the of the new immutable ID of the cloud account matching that of the Local AD account.



Want to switch back to the legacy users list experience? Click here to leave the preview.

8 users found

Display name ↑	User principal name	User type	On-premises sy...	Identities	Company name	Creation type
				kitchenentertainment.onmicrosoft		
				kitchenentertainment.onmicrosoft		
				kitchenentertainment.onmicrosoft		
				kitchenentertainment.onmicrosoft		
		Member	Yes	kitchenentertainment.onmicrosoft		
				kitchenentertainment.onmicrosoft		
				kitchenentertainment.onmicrosoft		
				kitchenentertainment.onmicrosoft		