

Linking Multiple On-Prem AD Users to Azure AD via Immutable IDs

Manually fixing ImmutableIDs one user at a time can get old fast. If you've got a whole OU of users to sync up, it's much easier to handle them in bulk.

This PowerShell script does exactly that. You pick an OU, it grabs all the enabled AD users inside, checks for matching Azure AD accounts, and then sets the correct ImmutableID. To make it quicker, it even caches all Azure AD users into memory so lookups are fast.

Here's the full script:

```
# Requires: ActiveDirectory module and AzureAD module
# Connect to Azure AD
Connect-AzureAD

# Prompt to select an OU
$OUs = Get-ADOrganizationalUnit -Filter * | Select-Object -Property Name, DistinguishedName
$OUSelection = $OUs | Out-GridView -Title "Select an OU to process" -PassThru

if (-not $OUSelection) {
    Write-Host "No OU selected, exiting."
    exit
}

# Cache all Azure AD users once into a hashtable for O(1) lookups
Write-Host "Fetching all Azure AD users..."
$AllAzureUsers = Get-AzureADUser -All $true | Select-Object ObjectId, UserPrincipalName
$AzureUserLookup = @{}
foreach ($user in $AllAzureUsers) {
    $AzureUserLookup[$user.UserPrincipalName.ToLower()] = $user
}
Write-Host "Cached $($AllAzureUsers.Count) Azure AD users."

# Get all enabled AD users in the selected OU
Write-Host "Fetching AD users from OU: $($OUSelection.Name)"
```

```
Get-ADUser -SearchBase $OUSelection.DistinguishedName -Filter * -Properties ObjectGUID,
UserPrincipalName, Enabled |
    Where-Object { $_.Enabled -eq $true } |
    ForEach-Object {
        $UPN = $_.UserPrincipalName
        Write-Host "Processing AD user: $UPN"

        # Lookup in hashtable
        $AzureUser = $AzureUserLookup[$UPN.ToLower()]

        if (-not $AzureUser) {
            Write-Warning "No matching 365 user found for $UPN"
            return
        }

        # Convert ObjectGUID to Base64 for ImmutableID
        $ImmutableID = [System.Convert]::ToBase64String($_.ObjectGUID.ToByteArray())

        # Set ImmutableID in Azure AD
        try {
            Set-AzureADUser -ObjectId $AzureUser.ObjectId -ImmutableId $ImmutableID
            Write-Host "Linked AD user $UPN to 365 user $($AzureUser.UserPrincipalName)"
        }
        catch {
            Write-Warning ("Failed to set ImmutableID for {0}: {1}" -f $UPN,
$_ .Exception.Message)
        }
    }

Write-Host "Done processing OU: $($OUSelection.Name)"
```

Revision #1

Created 18 September 2025 15:33:44 by Luke Carter

Updated 18 September 2025 15:34:49 by Luke Carter