**Export Email Alias to CSV From AD**

**##Exports raw data, needs refining###**

Get-ADUser -Filter \* -Properties proxyaddresses | Select-Object Name, @{L = "ProxyAddresses"; E = { $\_.ProxyAddresses -join ";"}} | Export-Csv -Path c:\Users\jshepherd\Desktop\proxyaddresses.csv -NoTypeInformation

**AD/O365 Delta Sync**

**##Syncs AD with O365##**

Start-ADSyncSyncCycle -PolicyType Delta

**Fill Out Address Tab Fields**

**##Filter by office location##**

Get-ADUser -Filter “Office -eq ‘New York’”

**##Filter by OU##**

Get-ADUser -SearchBase "OU=Branch Users,dc=yourdomain,dc=com" -Filter \*

$users = **##Paste filter here##**

foreach ($user in $users)

{

Set-ADUser $user.samaccountname -city "new city" -country "new country" -POBox "New PObox" -Postalcode "new postal code" -State "new state" -streetaddress "new street address"

}

**Set Manager Field For AD User**

Set-ADUser ##ADuser## -manager ##ADuser##

**How to Enable and Disable MFA using Windows Powershell.**

Pre-Requisites:

Authentication Administrators AD Role

Windows Powershell - Run As Admin

Powershell MSOnline Module

Connect to JJINS Azure AD

Install MSOnline Module

Open Powershell:

Copy and Paste-> Install-Module MSOnline

Type "A"

Connect:

Copy and Paste-> Connect-MsolService

You will recieve our organizations prompts. Perform. This confirms you have connected to our Azure domain safely.

ENABLE MFA FOR SPECIFIC USER: Replace "INPUT USER JJ EMAIL HERE" Remove the parenthesese. Then, COPY PASTE ENTIRE SCRIPT.

Import-Module MSOnline

$st = New-Object -TypeName Microsoft.Online.Administration.StrongAuthenticationRequirement

$st.RelyingParty = "\*"

$st.State = "Enabled"

$sta = @($st)

Set-MsolUser -UserPrincipalName (INPUT USER JJ EMAIL HERE) -StrongAuthenticationRequirements $sta

DISABLE MFA FOR SPECIFIC USER:

Set-MsolUser -UserPrincipalName (INPUT USER JJ EMAIL HERE) -StrongAuthenticationRequirements @()