

Change username

Description

Connect to Azure Active Directory in Powershell	Connect-MsolService <Provider credentials of admin account when prompted>
Change Username	Set-MsolUserPrincipalName -UserPrincipalName "<Old Username>" -NewUserPrincipalName "<New Username>"

Enable Modern Authentication

Description

Connect to Exchange Online in Powershell	Connect-ExchangeOnline <Provider credentials of admin account when prompted>
Check status of Modern Authentication	get-OrganizationConfig FT name, oAuth*
Enable Modern Authentication	Set-OrganizationConfig - OAuth2ClientProfileEnabled:\$True

Enable Audit Log Search

May require specific O365 role

Connect to Exchange Online in Powershell	Connect-ExchangeOnline <Provider credentials of admin account when prompted>
Check status of Audit Log Ingestion	Get-AdminAuditLogConfig FL UnifiedAuditLogIngestionEnabled
Enable Audit Log Ingestion	Set-AdminAuditLogConfig -UnifiedAuditLogIngestionEnabled \$true

Azure AD Connect - Hard/Soft Match Duplicate accounts

<https://dirteam.com/sander/2020/03/27/explained-user-hard-matching-and-soft-matching-in-azure-ad-connect/>

Create "Duplicates" OU	Open Active Directory and create an child OU under the OU where user accounts are stored.	
------------------------	---	--

Move Duplicates	Move any duplicate accounts to the new "Duplicates" OU	
Ensure that Azure AD Connect is configured to not sync accounts located in the "Duplicates" OU	<ul style="list-style-type: none"> • Run Azure AD Connect and run through configuration wizard • When prompted, choose Customize Synchronization Options • Continue to run through the wizard • At the Domain/OU and filtering stage, choose Sync selected domains and OUs • Uncheck the "Duplicates" OU • Finish the wizard, this should kick off another sync process. 	
Sync changes to Microsoft 365	On Domain Controller running Azure AD Sync, run: <code>Start-ADSyncSyncCycle -PolicyType Delta</code>	
Ensure that the MSOnline module is installed	Install-Module MSOnline	Only required one time per machine. The Connect-MSOLService command will fail otherwise
Connect to the Microsoft Online Service	<code>Connect-MSOLService</code>	A connection to this service is required to run *-MSOL* commands.
Delete the duplicate account	<code>Remove-MSOLUser -UserPrincipalName <ADDomainUPN></code> <code>Remove-MSOLUser -UserPrincipalName <ADDomainUPN> -RemoveFromRecycleBin</code>	WARNING: DO NOT delete the Cloud Only account. This step may be skipped if the account was never synced.
Ensure that the AD Domain UPN and the Cloud User UPN match	On the Domain controller run: <code>Get-Aduser <username> fl UserPrincipalName</code> and match this with the username of the target Office 365 user account	If these do not match, you may need to change this using the dropdown on the account tab in ADUC. If the correct UPN suffix is not available, you can add an alternate UPN suffix in Active Directory Domains and Trusts.
Identify the AD user's Immutable ID	On Domain controller, run: <code>\$guid = (Get-Aduser <username>).ObjectGUID</code> <code>\$immutableID = [System.Convert]::ToBase64String(\$guid.tobytearray())</code>	
Set ImmutableID on cloud account	<code>Set-MSOLUser -UserPrincipalName <clouduserUPN> -ImmutableID \$immutableID</code>	

Move target User accounts back to the original OU		Remember: Accounts in the Duplicates OU are configured to not sync with Office 365. This allows them to be synced again
Sync changes to Microsoft 365	On Domain Controller running Azure AD Sync, run: <code>Start-ADSyncSyncCycle -PolicyType Delta</code>	