IT SUPPORT · IT-05

AD & Microsoft 365

Use this when: you unlock, reset, create or offboard users in Active Directory, Entra ID and Exchange Online.

BreakFixLearn

CompTIA A+ · MS-102 basics
Sheet v1.0 · Nov 2026

Scan to visit

Offboarding a leaver: do it in this order

Record each step in the ticket

1. **Disable** — AD account and Entra ID account
2. **Revoke sessions** — Kill refresh tokens in Entra ID
3. **Reset password** — Random value; twice if compromise is suspected
4. **Mailbox** — Convert to shared; give the manager access
5. **Licenses** — Remove them once the mailbox is shared
6. **Groups** — Remove; move to a Disabled OU
7. **Devices** — Retire or wipe; collect hardware
8. **Hand over** — Files, shared drives, MFA methods removed

Active Directory (on-prem)

RSAT ActiveDirectory module

`Get-ADUser jdoe -Properties LockedOut, PasswordLastSet, LastLogonDate`	Status at a glance
`Unlock-ADAccount -Identity jdoe`	Unlock
`Set-ADAccountPassword jdoe -Reset -NewPassword $pw`	Reset
`Disable-ADAccount -Identity jdoe`	Disable
`Get-ADPrincipalGroupMembership jdoe | Select-Object Name`	Groups the user is in
`Add-ADGroupMember SALES -Members jdoe`	Add to a group
`Search-ADAccount -AccountInactive -TimeSpan 90.00:00:00 -UsersOnly`	Unused 90 days

Set `$pw = Read-Host -AsSecureString` first so the password never appears on screen or in history.

Entra ID and Exchange Online

Microsoft Graph PowerShell · MSOnline and AzureAD modules are retired

`Connect-MgGraph -Scopes "User.ReadWrite.All"`	Sign in to Graph
`Update-MgUser -UserId $id -AccountEnabled:$false`	Block sign-in
`Revoke-MgUserSignInSession -UserId $id`	Revoke sessions
`Get-MgUserLicenseDetail -UserId $id`	Licenses
`Set-MgUserLicense -UserId $id -RemoveLicenses @($skuId) -AddLicenses @{}`	Remove a license
`Connect-ExchangeOnline` · `Set-Mailbox jdoe -Type Shared`	To shared mailbox
`Add-MailboxPermission jdoe -User manager -AccessRights FullAccess`	Manager access

A shared mailbox holds up to 50 GB with no license. Keep sign-in blocked on it.

Stay safe

DANGER Verify identity before any reset or unlock: call back on the number on file, not one in the ticket.

CAUTION After a revoke, apps may keep working until their access token expires (about 1 hour by default).

CAUTION Use Helpdesk or User Administrator roles, not Global Admin. Never put passwords in tickets.

REMEMBER

- Disable first, delete later
- Convert mailbox **before** removing the license
- Synced users: change them in on-prem AD

Sources: Microsoft Learn (revoke access, licenses, shared mailboxes) · Microsoft Entra blog

CC BY-NC 4.0 · IT-05 v1.0