Entra ID User Lifecycle Management

Handover Document

Azure Automation Runbooks for Managing Inactive Users in Microsoft Entra ID

LukeEvansTech
December 19, 2025

Contents

1 Overview

This solution provides Azure Automation runbooks that automate the lifecycle management of inactive user accounts in Microsoft Entra ID (Azure AD). The solution implements a two-stage approach for member users and a single-stage approach for guest users.

1.1 Azure Environment

Property	Value
Automation Account	`col-uks-mgmt-EntraID-aa`
Resource Group	`col-uks-rg-mgmt`
Location	UK South
Subscription	`col-sub-cop-management`
Subscription ID	`280f1edf-4eca-4558-bdaf-12db0a42dabc`

Table 1: Azure Automation Environment

1.2 Key Features

- **Two-Stage Member Lifecycle** – Member users are first disabled after 90 days of inactivity, then deleted after 180 days
- **Guest Cleanup** – Guest users are deleted after 90 days of inactivity to maintain a clean directory
- **Flexible Exclusions** – Exclude users by security group, domain, department, or license type
- **Safe by Default** – All runbooks default to WhatIf mode - preview changes before applying them
- **Soft Delete** – Deleted users are moved to the recycle bin and recoverable for 30 days
- **Managed Identity** – Uses Azure managed identity for secure, credential-free authentication

2 User Lifecycle Strategy

2.1 Member Users

The member user lifecycle follows a two-stage approach:

Stage	Days	Action
1	90	Disable account - User cannot sign in
2	180	Soft delete - User moved to deleted items
Auto	+30	Permanent deletion by Microsoft

Table 2: Member User Lifecycle Stages

Note: Users disabled at 90 days must remain disabled until they reach 180 days of inactivity to be processed by the deletion runbook.

2.2 Guest Users

Guest users follow a simplified single-stage lifecycle:

Stage	Days	Action
1	90	Soft delete - User moved to deleted items
Auto	+30	Permanent deletion by Microsoft

Table 3: Guest User Lifecycle Stages

3 Runbooks

3.1 Summary Table

Runbook	Target	Action	Days
Disable-Inactive-Member-Users-90-Days	Members	Disable	90
Delete-Inactive-Member-Users-180-Days	Members	Delete	180
Delete-Inactive-Guest-Users-90-Days	Guests	Delete	90
Get-Inactive-Users-With-Manager	Members	Report	30

Table 4: Runbook Overview

3.2 Disable Inactive Member Users (90 Days)

Purpose: Identifies and disables member users who have been inactive for 90+ days. This is the first stage of the member user lifecycle.

Target Users:
- User type: Member
- Account status: Enabled
- Excludes Cross-Tenant Sync users

Action: Sets `accountEnabled` to `false` for identified users.

3.3 Delete Inactive Member Users (180 Days)

Purpose: Identifies and soft deletes disabled member users who have been inactive for 180+ days. This is the second stage of the member user lifecycle.

Target Users:
- User type: Member
- Account status: Disabled
- Excludes Cross-Tenant Sync users

Action: Soft deletes identified users via `Remove-MgUser`. Users can be recovered for 30 days.

3.4 Delete Inactive Guest Users (90 Days)

Purpose: Identifies and soft deletes guest users who have been inactive for 90+ days.

Target Users:
- User type: Guest
- Any account status

Action: Soft deletes identified users via `Remove-MgUser`. Users can be recovered for 30 days.

3.5 Report Inactive Users with Manager

Purpose: Identifies licensed member users with managers who have been inactive for a specified period (default 30 days). Optionally adds users to a security group for line manager review.

Target Users:
- User type: Member

- Has a manager assigned
- Has specific licenses

Action: Reports inactive users and optionally adds them to a review group.

4 Default Exclusions

4.1 Member Runbooks

Member runbooks are pre-configured with these exclusions:

Type	Values
Domains	`cityoflondon.police.uk`, `freemens.org`
Departments	`Members`
Exclusion Group	`Line Manager - Inactive User Review - Exclusion`

Table 5: Member Runbook Exclusions

4.2 Guest Runbooks

Guest runbooks only filter by domain:

Type	Values
Domains	`cityoflondon.police.uk`, `freemens.org`

Table 6: Guest Runbook Exclusions

Note: Guest runbooks do not use group or department exclusions as these typically don't apply to guest accounts.

5 Setup & Configuration

5.1 Current Configuration

The Azure Automation environment is fully configured and operational:

- System-assigned managed identity enabled
- Microsoft Graph permissions granted
- PowerShell modules imported (Runtime 7.2)
- Runbooks imported and published
- Schedules configured

5.2 Required Modules

- `Microsoft.Graph.Authentication`
- `Microsoft.Graph.Users`
- `Microsoft.Graph.Groups`
- `Microsoft.Graph.Identity.DirectoryManagement`

5.3 Required Permissions

The managed identity requires these Microsoft Graph API permissions:

Permission	Purpose
`User.Read.All`	Read all user properties including sign-in activity
`User.ReadWrite.All`	Disable and delete users
`Group.Read.All`	Read exclusion group membership
`GroupMember.ReadWrite.All`	Add users to review groups (reporting runbook)
`AuditLog.Read.All`	Access sign-in activity data

Table 7: Required Microsoft Graph Permissions

6 Sign-In Activity Detection

All runbooks use Microsoft Graph's `signInActivity` property to determine the last sign-in date. The following properties are checked:

1. `LastSignInDateTime` – Interactive sign-ins
2. `LastNonInteractiveSignInDateTime` – Background/app sign-ins
3. `LastSuccessfulSignInDateTime` – Last successful authentication

The most recent date wins. If no sign-in activity is recorded, the user is considered inactive.

> **Important:** Users created within the grace period (90 or 180 days depending on the runbook) are automatically excluded, even if they have no sign-in activity recorded.

7 Safety Features

The runbooks include multiple safety mechanisms:

1. **WhatIf Mode** – All runbooks default to preview mode
2. **Exclusion Groups** – Skip users in specified security groups
3. **Domain Exclusions** – Skip users from specified domains
4. **Department Exclusions** – Skip users in specified departments
5. **License Filtering** – Only process users with specific licenses
6. **Creation Date Check** – Skip recently created accounts
7. **Soft Delete** – Deleted users recoverable for 30 days

Recommendation: Always run with `-WhatIf $true` first to review which users would be affected before executing with `-WhatIf $false`.

8 Scripts

8.1 Grant-ManagedIdentityPermissions.ps1

This script grants the required Microsoft Graph API permissions to the Azure Automation account's managed identity.

Usage:

```
./scripts/Grant-ManagedIdentityPermissions.ps1 -AutomationAccountName "col-uks-mgmt-EntraID-aa"
```

Requirements:

- PowerShell 7.x with Microsoft.Graph modules
- Global Admin or Privileged Role Administrator role

Permissions Granted:

Permission	Purpose
`User.Read.All`	Read user properties including sign-in activity
`User.ReadWrite.All`	Disable and delete user accounts
`Directory.Read.All`	Read directory data
`Group.Read.All`	Read exclusion group membership

Table 8: Permissions Granted by Script

Note: The script is idempotent - it can be run multiple times safely. Already-assigned permissions are skipped.

9 Repository Structure

```
col-entra-id/
├── runbooks/               # Azure Automation runbooks
│   ├── Entra-ID-Disable-Inactive-Member-Users-90-Days.ps1
│   ├── Entra-ID-Delete-Inactive-Member-Users-180-Days.ps1
│   ├── Entra-ID-Delete-Inactive-Guest-Users-90-Days.ps1
│   └── Entra-ID-Get-Inactive-Users-With-Manager-And-License.ps1
├── scripts/                # Supporting utility scripts
│   └── Grant-ManagedIdentityPermissions.ps1
├── docs/                   # Documentation (Zensical site)
└── typst/                  # Handover document generation
```

10 Contact & Support

For questions or issues with this solution:

- **Repository:** github.com/LukeEvansTech/col-entra-id
- **Documentation:** lukeevanstech.github.io/col-entra-id

Document generated on December 19, 2025