Standard Operating Procedure (SOP): Ghost Microsoft Authenticator MFA Entry Removal

This SOP outlines the process to fully remove ghost or duplicate Microsoft Authenticator MFA entries that persist due to cloud backup restores or UI sync issues in Microsoft Entra ID (Azure AD). These steps apply when users report ghosted entries or push notifications being routed to unintended devices.

Step 1: List MFA Methods with Graph API

Use the Microsoft Graph API to enumerate all authentication methods for the target user. Endpoint: GET https://graph.microsoft.com/beta/users/{userId}/authentication/methods Look for multiple entries of type: microsoftAuthenticatorAuthenticationMethod

Step 2: Delete Each Method by ID

Use the DELETE method on each MFA method ID found in Step 1. Endpoint: DELETE https://graph.microsoft.com/beta/users/{userId}/authentication/methods/{methodId} This ensures stale tokens are fully removed from the backend, not just the UI.

Step 3: Clean Up from UI

Have the user visit https://mysignins.microsoft.com/security-info. Manually delete any remaining entries. Then click 'Sign out everywhere' and disable Authenticator cloud backup if enabled.

Step 4: Re-enroll MFA Once

Add Microsoft Authenticator again using the official 'Add sign-in method' on https://mysignins.microsoft.com — NOT during sign-in prompts. Use only one device during this registration to avoid reghosting.

Root Cause Summary

Cause	Behavior
Authenticator Cloud Backup	Restores old tokens and re-registers as ghost entries.
Manual re-add + restore	Duplicates method entries in backend.
UI vs Backend Desync	Entries removed in UI may still exist in Graph.
Old tokens not deleted	Remain linked unless Graph or PowerShell is used.

For org-wide cleanup, this process can be automated via Microsoft Graph and monitored using sign-in logs for MFA registration anomalies.

Prepared by: Marjean Mayo-Baker | NullCypher SIM