

MFA Token Leakage – Forensics Case Report

Test: Entra ID MFA Token Behavior

We initiated an MFA token leakage test using a newly activated Microsoft Entra ID tenant.

Environment Setup

- Activated a new Entra ID tenant using Hotmail account
- Created test accounts within the tenant
- Attempted to enforce MFA via Conditional Access Policies (CA)
- Noted that security defaults were already disabled

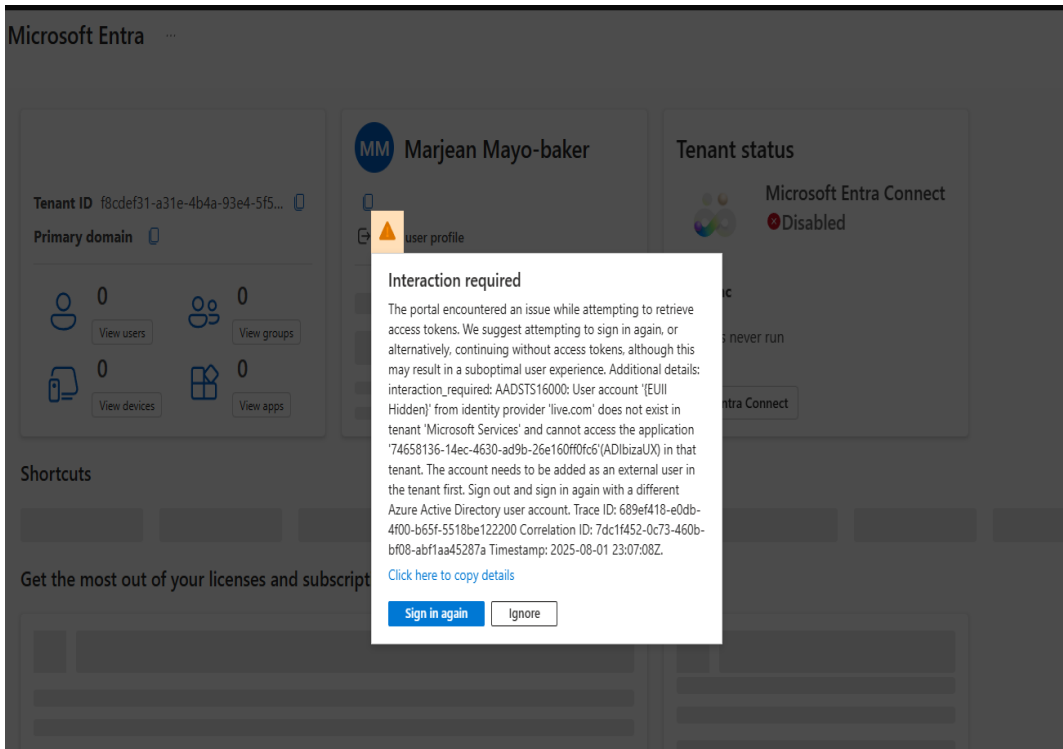
Initial Observations

- While re-registering MFA for a user, an old token persisted in the Microsoft Authenticator app.
- This ghost token prevented the new registration from functioning correctly.
- Attempts to remove the old token from UI or Authenticator did not always clear the stale entry.

Testing Steps Conducted

1. Uninstalled and reinstalled the Authenticator app.
2. Switched between devices (tablet and phone).
3. Attempted re-registration through the Security Info portal.
4. Confirmed that cloud backup status influenced persistence.
5. Verified that deleted tokens did not always replicate on fresh install.
6. Identified ghost devices through Security Info panel.

Screenshots (Reference Placeholders)



Something went wrong

Please try again later.

0x80190001

[Send feedback](#)

26F028E9-290A-46DF-B6B3-B6AEAAAD3676

Fri, 01 Aug 2025 21:44:54 GMT

Interaction required



The portal encountered an issue while attempting to retrieve access tokens. We suggest attempting to sign in again, or alternatively, continuing without access tokens, although this may result in a suboptimal user experience. Additional details: interaction_required: AADSTS16000: User account '{EUII Hidden}' from identity provider 'live.com' does not exist in tenant 'Microsoft Services' and cannot access the application '74658136-14ec-4630-ad9b-26e160ff0fc6'(ADlbizaUX) in that tenant. The account needs to be added as an external user in the tenant first. Sign out and sign in again with a different Azure Active Directory user account. Trace ID: ee426618-b431-453e-bd65-12d928efb300 Correlation ID: 502739c3-ea64-482f-b069-3495d8cc6cf4 Timestamp: 2025-08-01 20:24:11Z.

[Click here to copy details](#)

Sign in again

Ignore

+ Add sign-in method

<div><div>...</div><div>Password</div></div>	<div>Last updated: an hour ago</div>	<div>Change</div>
<div><div>...</div><div>App password</div></div>	<div>thepasswordname</div>	<div>Delete</div>
<div><div></div><div>Microsoft Authenticator Push multi-factor authentication (MFA)</div></div>	<div>SM-S926U</div>	<div>Delete</div>
<div><div></div><div>Microsoft Authenticator Push multi-factor authentication (MFA)</div></div>		<div>Delete</div>

Lost device? [Sign out everywhere](#)

Root Cause Hypothesis

Old tokens remain cached or synced due to:

- Cloud backup re-syncing entries across installs
- Manual MFA additions in Security Info causing duplicates
- Failure to fully purge device data from Azure/Entra backend

Remediation Strategy

- Disable cloud backup before deleting Authenticator tokens
- Use Security Info to remove all old tokens
- Reinstall app after a clean wipe
- Re-register MFA from secure browser (incognito suggested)

Lessons Learned

1. Stale MFA tokens are hard to detect without proper audit logs.
2. Authenticator app behavior can cause shadow entries.
3. Admins must document MFA re-registration SOPs clearly.
4. Need for Conditional Access Policy to restrict per-device registration and enforce fresh token lifecycle.

Follow-Up Actions

- Write a Standard Operating Procedure (SOP) for MFA token removal
- Submit documentation and findings to security leadership
- Propose a script or governance control for stale token cleanup