Blocking Authentication Transfer in Microsoft Entra ID

Field	Details
Document Type	Blocking Authentication Transfer in Microsoft Entra ID
Applies To	Microsoft Entra ID, Conditional Access policy
Audience	2nd Line / Entra ID Admins / IT Engineer
Author	AK. Udofeh
Last Updated	April 2026

Overview

Authentication Transfer allows a user to authenticate on one device and transfer that session to another (e.g. scanning a QR code to sign into a mobile app).

While convenient, it introduces risks where authentication can be extended to unmanaged or untrusted devices.

This guide shows how to restrict or block this behaviour using Conditional Access.

Prerequisites

- Microsoft Entra ID P1 (or higher)
- Conditional Access Administrator role
- Identified exclusion accounts (break-glass)

Step 1: Access Conditional Access Policies

1. Sign in to the Microsoft Entra admin center
2. Navigate to:
   Entra ID > Conditional Access > Policies
3. Select **+ New policy**

Step 2: Define Policy Scope

Users

- Include:
  - All users OR specific groups
- Exclude:
  - Emergency / break-glass accounts

> Exclusions should be tightly controlled and reviewed regularly

Step 3: Target Resources

- Select:
  Target resources (Cloud apps)
- Include:
  - **All resources** or specific applications

Step 4: Configure Authentication Flow Condition

1. Navigate to:
   Conditions > Authentication Flows
2. Set **Configure = Yes**
3. Select:
   - **Authentication Transfer**
4. Click **Done**

Step 5: Block Access

1. Go to:
   Access Controls > Grant
2. Select:
   - **Block access**
3. Click **Select**

Step 6: Enable Policy

- Set policy state to: **On**
- Click **Create**

Step 7: Validate Behaviour

- Test scenarios:
  - QR-based login
  - Cross-device sign-in flows
- Review:
  - Sign-in logs
  - Conditional Access results

Important Considerations

Blocking Authentication Transfer may impact:

- Mobile app onboarding flows
- QR code-based sign-ins
- Cross-device authentication experiences

> This feature is enabled by default and must be explicitly controlled via policy

Best Practices

- Apply to high-risk user groups first
- Consider restricting instead of fully blocking where needed
- Combine with:
  - Device compliance policies
  - MFA enforcement

Summary

Blocking Authentication Transfer prevents authentication from being silently extended across devices, reducing the risk of unauthorized access from unmanaged endpoints.

This ensures authentication remains tied to trusted and controlled environments.

Revision #1
Created 2026-04-22 14:56:31 UTC by AK. Udofeh
Updated 2026-04-22 15:09:25 UTC by AK. Udofeh