Configuring Entra ID CA Policies for Authentication Flows

Field	Details
Document Type	Configuring Entra ID CA Policies for Authentication Flows
Applies To	Microsoft Entra ID, Conditional Access policy
Audience	2nd Line / Entra ID Admins / IT Engineer
Author	AK. Udofeh
Last Updated	May 2026

Overview

This guide outlines how to configure Conditional Access policies in Microsoft Entra ID to control:

* Device Code Flow

* Authentication Transfer

These authentication methods can introduce elevated phishing and unmanaged device risks if not explicitly governed.

Device Code Flow

Device Code Flow is similar to signing in to Netflix or Xbox on a Smart TV, where the TV displays a code and instructs the user to complete sign-in on another device such as a phone or laptop. Once authentication is completed, the Smart TV is automatically signed in.

Example:

Example: Go to https://microsoft.com/devicelogin or https://www.netflix.com/tv2 and enter this code.

Authentication Transfer

Authentication Transfer is similar to being signed in on Device A and then scanning a QR code using Device B, allowing the authenticated session or trust to be transferred so that Device B becomes signed in without performing a full standalone authentication process again.

This guide demonstrates how to govern these flows using Conditional Access policies to reduce exposure to indirect authentication attacks.

Prerequisites

* Microsoft Entra ID P1 or higher

* Conditional Access Administrator role

* Emergency / break-glass accounts identified

* Access to Microsoft Entra admin center

Step 1: Create New Conditional Access Policy

1. Sign in to the Microsoft Entra admin center

2. Navigate to: **Entra ID > Protection > Conditional Access > Policies**

3. Select **+ New policy**

4. Enter a policy name:

    * Example: CA - Block Authentication Flows

Step 2: Configure User Scope

Under **Assignments → Users**:

* Include:

All users (recommended)

* Exclude:

* Emergency access accounts

* Break-glass administrator accounts

> Avoid applying policies to all accounts without exclusions.

Step 3: Configure Target Resources

Under **Assignments → Target resources**:

* Select:

*. **All cloud apps**

This ensures consistent enforcement across Microsoft 365 resources.

Step 4: Configure Authentication Flows

1. Navigate to:
Conditions > Authentication flows

2. Set:

* **Configure = Yes**

1. Select required flows:

* Device Code Flow

* Authentication Transfer

2. Click **Done**

Step 5: Configure Access Control

Under **Access controls → Grant**:

* Select:

* Block access

* Click **Select**

This blocks authentication attempts using the selected flows.

Step 6: Enable Report-Only Mode

Before enforcement:

* Set policy state to:

* **Report-only**

* Click **Create**

This allows impact analysis without disrupting users.

Validation

Review:

* **Entra ID > Monitoring > Sign-in logs**

Validate:

* Impacted users

◦ Authentication flow usage

* Conditional Access evaluation results

Monitor for:

* Developer tooling dependencies

* Shared device authentication

* QR-based onboarding scenarios

Enforcement

Once validated:

1. Edit the Conditional Access policy

2. Change:

◦ **Report-only > On**

3. Continue monitoring sign-in activity and failures post-deployment.

? Flow Overview

User Authentication Attempt
* Authentication Flow Detection
* Conditional Access Evaluation
* Block / Allow Decision
* Resource Access Outcome

Security Control Points:

· Device Code Flow restriction

· Authentication Transfer restriction

· Sign-in logging and monitoring

Summary

This configuration strengthens Microsoft Entra ID security posture by restricting high-risk authentication flows commonly associated with phishing and indirect access scenarios.

Revision #1
Created 2026-05-13 14:10:30 UTC by AK. Udofeh
Updated 2026-05-13 14:32:20 UTC by AK. Udofeh