Blocking Device Code Flow in Microsoft Entra ID

Field	Details
Document Type	Blocking Device Code Flow 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

Device Code Flow allows users to authenticate on one device by entering a code on another. While useful for devices with limited input, it introduces significant phishing risk and can enable access from unmanaged devices.

This guide walks through configuring a Conditional Access policy to block Device Code Flow.

Prerequisites

- Microsoft Entra ID P1 (or higher)
- Conditional Access Administrator (or equivalent role)
- Emergency / break-glass accounts identified

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 (recommended)**
- Exclude:

- Emergency access accounts
- Break-glass accounts

> Always maintain at least one account excluded to prevent lockout

Step 3: Target Resources

- Select **Target resources (Cloud apps)**
- Include: **All resources (recommended)**

Step 4: Configure Authentication Flow Condition

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

Step 5: Block Access

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

Step 6: Enable in Report-Only Mode (Recommended)

- Set policy state to: **Report-only**
- Click **Create**

> This allows you to assess impact before enforcing

Step 7: Validate Impact

- Navigate to:
  Monitoring > Sign-in logs
- Filter by:
  - Authentication Protocol = Device Code Flow

Identify:

- Users
- Applications
- Dependencies

Step 8: Enforce Policy

Once validated:

- Change policy state from **Report-only > On**
- Monitor for failures and adjust exclusions if required

Important Considerations

- Device Code Flow is often used by:
  - Azure CLI / PowerShell
  - Teams Rooms / shared devices
- Blocking may impact these scenarios

> Microsoft recommends blocking unless explicitly required

Best Practices

- Start in report-only mode
- Keep exclusions minimal and reviewed regularly
- Monitor sign-in logs continuously
- Prefer modern, secure authentication methods

Summary

Blocking Device Code Flow reduces exposure to phishing attacks that exploit cross-device authentication. This control strengthens identity security by eliminating a high-risk authentication path.

Revision #1
Created 2026-04-22 13:52:38 UTC by AK. Udofeh
Updated 2026-04-22 14:56:18 UTC by AK. Udofeh