Configuring Phishing?Resistant MFA (PR?MFA) in Entra ID Conditional Access

Field	Details
Document Type	How-To Guide - Configure Phishing-Resistant MFA (PR-MFA)
Applies To	Microsoft Entra ID, Conditional Access policy
Audience	2nd Line / Entra ID Admins / IT Engineer
Author	AK. Udofeh
Last Updated	March 2026

Overview

Phishing-Resistant MFA (PR-MFA) is the strongest authentication assurance level available in Microsoft Entra ID. It requires cryptographically bound authentication methods such as **FIDO2 security keys, device-bound passkeys, or Windows Hello for Business**.

Microsoft formally introduced **Phishing-resistant MFA Authentication Strength** as part of Conditional Access by 2025. This prevents attackers from bypassing MFA via techniques like real-time phishing proxies, MFA fatigue, push spam, or OTP interception.

Use Cases

Use PR-MFA for:

- **Administrators and privileged roles** (Global Admin, Security Admin, Conditional Access Admin)
- **Users accessing high-value or regulated workloads**
- **Teams handling sensitive data**: finance, HR, legal
- **Zero-Trust access strategies requiring high authentication assurance**

Prerequisites
Licensing

- Microsoft Entra ID P1/P2 (Authentication Strengths supported).

Technical Requirements

- Supported phishing-resistant methods enabled (FIDO2, Windows Hello, Passkeys).
- Users must have registered a phishing-resistant method before enforcement to avoid lockouts

Supported Authenticators

- FIDO2 security keys (hardware)
- Windows Hello for Business
- Device-bound passkeys (Windows/macOS/iOS/Android, depending on platform)

> **Do not enforce PR-MFA without ensuring users have registered the required method.** Risk of tenant lockout. Break-glass (emergency access) accounts **must be excluded**. Legacy apps that do not support modern authentication may require exceptions or re-architecture.

Step?by?Step Configuration

Step 1: Enable Phishing-Resistant Authentication Methods

- Go to Entra Admin Center > Identity > Protection > Authentication Methods.
- Enable: Passkeys (FIDO2) and Windows Hello for Business

Step 2: Create a Security Group for Pilot Users

- Create a group like PR-MFA-Pilot.
- Add admin users or a testing cohort.

Step 3: Configure Authentication Strength

- Go to Identity > Protection > Conditional Access > Authentication Strengths.
- Select Phishing-resistant MFA strength.

This explicitly enforces device-bound cryptographic methods.

Step 4: Create the PR-MFA Conditional Access Policy

- Go to Conditional Access > Policies > + New Policy.
- Name: Require Phishing-Resistant MFA
- Assignments:
  - Users: select PR-MFA-Pilot group
  - Cloud apps: All cloud apps (recommended for admins)
- Access Controls > Grant > Require Authentication Strength
- Select Phishing-resistant MFA
- Enable policy = Report-only (first phase).
- After validation, switch to ON.

Validation Steps

- Validate sign-in logs to confirm Phishing-Resistant MFA was the effective control.
  Entra Admin Center > Monitoring & Logs > Sign-in logs.
- Test phishing-resistant methods:
  - FIDO2 key
  - Windows Hello
  - Device-bound passkey

These should satisfy the authentication requirement if configured correctly.

========== Troubleshooting ==========

Issue	Resolution
Users locked out	Confirm registration at https://aka.ms/mysecurityinfo and exclude user temporarily
FIDO2 key not accepted	Ensure attestation not restricted & key model supported
Windows Hello not offered	Check if device is Entra-joined/registered
App can't satisfy PR-MFA	App may be legacy / does not support modern auth

---

Revision #3
Created 2026-03-19 11:08:02 UTC by AK. Udofeh
Updated 2026-03-19 11:27:06 UTC by AK. Udofeh