GUIDE ON PASSKEY (FIDO2) VS PASSWORDLESS FOR WINDOWS VS MOBILE DEVICES
PREPARED BY ESWAR KONETI (@ESKONR) V1.0 / 1-JUL-2025

Here's a breakdown of how **Passkeys (FIDO2) vs. Passwordless (Authenticator Push)** work on **Windows devices** for **browser/app logins**:

1. Using Passkeys (FIDO2) on Windows

Scenario	**Requires Windows Hello?**	**Works with Hardware Token (YubiKey)?**
Browser/App Login	✅ **Yes** (if using software passkey in Authenticator)	✅ **No** (if using YubiKey instead)
Local Windows Login	✅ **Yes** (must set up Hello PIN/biometrics)	✅ **No** (YubiKey replaces Hello)

Key Points:

- **If using Microsoft Authenticator as a passkey (FIDO2):**
  - Requires **Windows Hello** (biometrics/PIN) to unlock the passkey.
  - ❌ **Fails if Windows Hello isn't set up.**
- **If using a hardware token (YubiKey):**
  - ✅ **No Windows Hello needed** (the YubiKey itself acts as the authenticator).
  - User just **inserts/taps the YubiKey** when logging into browsers/apps.

2. Using Passwordless (Authenticator Push)

Scenario	**Requires Windows Hello?**	**Works with Hardware Token?**
Browser/App Login	❌ **No** (just phone approval)	❌ **No** (uses phone, not hardware key)

Scenario	**Requires Windows Hello?**	**Works with Hardware Token?**
Local Windows Login	❌ **No** (unless policy enforces it)	❌ **No**

Key Points:

- **Authenticator Push (Passwordless):**
  - Works **without Windows Hello** or YubiKey.
  - User gets a **notification on their phone** to approve login.
  - Best for users **without biometric devices** or hardware keys.

Summary of Your Understanding

✅ **Correct:**

- **Passkey (Authenticator FIDO2) on Windows requires Windows Hello** for browser/app logins.
- **Hardware token (YubiKey) bypasses Windows Hello**—just plug/tap the key.
- **Passwordless (Authenticator Push) works independently** of both.

✅ **Best Practice:**

- **For users without Windows Hello:** Use **YubiKey (FIDO2)** or **Authenticator Push**.
- **For users with Windows Hello:** Let them use **Authenticator Passkey (FIDO2)** + Hello.

How to Configure for Each Scenario

1. Users with YubiKey (No Windows Hello Needed)

1. **Admin:** Enable **FIDO2 Security Keys** in **Entra ID → Authentication Methods**.
2. **User:** Register YubiKey at https://aka.ms/mysecurityinfo.
3. **Login:** At teams.microsoft.com, select **"Sign in with a security key"** → Tap YubiKey.

2. Users with Authenticator Push (No Windows Hello Needed)

1. **Admin:** Enable **Passwordless Phone Sign-In** (Authenticator) in Entra ID.
2. **User:** Register Authenticator at https://aka.ms/mysecurityinfo.
3. **Login:** At teams.microsoft.com, select **"Approve a request on my Authenticator app"**.

3. Users with Windows Hello + Authenticator Passkey

1. **Admin:** Enable **FIDO2** and **Windows Hello for Business**.
2. **User:** Set up Windows Hello (PIN/biometrics) + register Authenticator as passkey.
3. **Login:** At teams.microsoft.com, select **"Use Windows Hello or security key"**.

Final Answer

- ✅ **If users have YubiKey:** No Windows Hello needed—just the key.
- ❌ **If users rely on Authenticator Passkey (FIDO2):** Windows Hello is required.
- ✅ **If users use Authenticator Push (Passwordless):** No Hello or hardware needed.

Passkey vs. Passwordless (Authenticator) on Mobile Devices

Here's how **Passkeys (FIDO2)** and **Passwordless (Authenticator Push)** work on **iOS and Android**, compared to Windows:

📱 Mobile Device Compatibility Chart

Scenario	Passkey (FIDO2)	Passwordless (Authenticator Push)
Supported on Mobile?	✅ **Yes** (iOS 16+/Android 9+)	✅ **Yes** (All devices with Authenticator app)
How It Works	Uses **device-stored FIDO2 keys** (biometric-locked).	Uses **push notifications + number matching**.
Login Experience	Select **"Passkey"** → Authenticate with FaceID/fingerprint.	Enter email → **Approve notification** in Authenticator app.

Scenario	Passkey (FIDO2)	Passwordless (Authenticator Push)
Works in Browsers?	✅ **Yes** (Chrome, Edge, Safari with limitations).	✅ **Yes** (All major browsers).
Works in Native Apps?	✅ **Yes** (Teams, Outlook, etc. if app supports FIDO2).	✅ **Yes** (All Entra ID-integrated apps).
Phishing Resistance	✅ **Strong (FIDO2 standard)**.	✅ **Good (but less secure than FIDO2)**.
Requires Biometrics?	✅ **Yes** (FaceID, fingerprint, or PIN).	❌ **No** (just phone approval).
Offline Login?	✅ **Yes** (key is stored locally).	❌ **No** (needs internet for push).
Best For	High-security users (admins, finance).	General workforce (simpler, no hardware needed).

🔹 Key Differences on Mobile

1. Passkey (FIDO2) on Mobile

- **How it works:**
  - User selects **"Sign in with a passkey"** → Authenticates via **FaceID/fingerprint**.
  - The passkey is **stored in the device's secure enclave** (like Apple Keychain/Google Password Manager/MS Authenticator).
- **Limitations:**
  - ❌ **Safari (iOS) doesn't fully support FIDO2 yet** (works best in Chrome/Edge).
  - ❌ **Shared devices?** Passkeys are tied to the user's biometrics.

2. Passwordless (Authenticator Push) on Mobile

- **How it works:**
  - User enters email → **Gets a push notification** → Approves with number matching.
- **Advantages:**
  - ✅ **Works everywhere** (even on older devices).
  - ✅ **No biometrics required** (just phone unlock).

📌 Summary: What Should You Use?

User Case	Recommended Method
iPhone/Android users	✅ **Passkey (FIDO2)** for security, **Passwordless Push** for simplicity.
Shared tablets/kiosks	❌ Avoid passkeys (biometric-locked). Use **Passwordless Push** or **YubiKey**.
Admins/high-security	✅ **Passkey (FIDO2) + YubiKey** (best phishing protection).
General workforce	✅ **Passwordless Push** (easiest for most users).

🛠️ How to Configure in Entra ID

1. **For Passkeys (FIDO2):**
   - Enable **FIDO2 Security Keys** in **Authentication Methods**.
   - Users register at aka.ms/mysecurityinfo.
2. **For Passwordless Push:**

  - Enable **Microsoft Authenticator → Passwordless Phone Sign-In**.
  - Users add Authenticator in **My Security Info**.

🚀 Final Answer

- **Passkeys (FIDO2) on mobile:** Best for **personal devices with biometrics** (FaceID/fingerprint).
- **Passwordless Push:** Best for **shared devices or users without biometrics**.
- **YubiKey (FIDO2):** Works on mobile **via NFC/USB** (no biometrics needed).

Step-by-Step Guide: Enabling Passkeys & Passwordless (Authenticator) on Mobile in Entra ID

This guide covers **two methods** for mobile users:

1. **Passkey (FIDO2)** – Uses device biometrics (FaceID/fingerprint).
2. **Passwordless (Authenticator Push)** – Uses phone notifications.

🔹 Prerequisites

- **Microsoft Entra ID P1/P2 license** (required for passwordless).
- **Microsoft Authenticator app** installed on user phones.
- **Admin access** to Entra ID (Azure AD).

📱 Method 1: Enable Passkey (FIDO2) for Mobile

(Best for personal iPhones/Android with biometrics.)

Step 1: Admin – Enable FIDO2 in Entra ID

1. Go to **Microsoft Entra Admin Center**.
2. Navigate to:
   Protection → Authentication Methods → Policies → FIDO2 Security Key.
3. **Configure:**
   - **Enable:** Yes

   - **Target:** All users (or a specific group).
   - **Enforcement:** Allow FIDO2 security keys (for mobile passkeys).

4. Click **Save**.

Step 2: User – Register Passkey on Mobile

1. User opens [My Security Info](#).
2. Clicks **+ Add method** → **FIDO2 Security Key**.
3. Follows prompts:
   - **On iPhone:** Uses FaceID/TouchID to create passkey.
   - **On Android:** Uses fingerprint/PIN.
4. **Success!** Passkey is stored in device's secure enclave.

Step 3: User Logs In with Passkey

1. Visits teams.microsoft.com (or any M365 app).
2. Selects **"Sign in with a passkey"**.
3. Authenticates with **FaceID/fingerprint**.
4. Logged in! ✅

📲 Method 2: Enable Passwordless (Authenticator Push)

(Works on any phone, no biometrics required.)

Step 1: Admin – Enable Passwordless Push

1. Go to [Microsoft Entra Admin Center](#).
2. Navigate to:
   Protection → **Authentication Methods** → **Policies** → **Microsoft Authenticator**.
3. **Configure:**
   - **Enable:** Yes
   - **Authentication mode:** Passwordless phone sign-in

- **Target:** All users (or a group).

4. Click **Save**.

Step 2: User – Register Authenticator

1. User installs **Microsoft Authenticator** (if not already).
2. Signs in to [My Security Info]().
3. Clicks **+ Add method** → **Microsoft Authenticator**.
4. Follows prompts to **scan QR code** and link account.

Step 3: User Logs In with Passwordless Push

1. Visits outlook.office.com (or any M365 app).
2. Enters email → Clicks **Next**.
3. Selects **"Approve a request on my Authenticator app"**.
4. **Approves notification** (with number matching).
5. Logged in! ✅

🛡️ Conditional Access (Optional, for Security)

To enforce **Passkeys or Passwordless** for specific apps:

1. Go to **Entra ID** → **Security** → **Conditional Access**.
2. Create a new policy:
    - **Users:** Select a group.
    - **Apps:** Select (e.g., Microsoft Teams, Outlook).
    - **Grant:** Require authentication strength → Choose **"Phishing-resistant MFA"** (for FIDO2) or **"Passwordless MFA"** (for Authenticator).

📌 Key Notes

Scenario	Use Passkey (FIDO2)	Use Passwordless Push
Personal iPhone/Android	✅ Best (secure)	✅ Works
Shared/Kiosk Devices	❌ No (biometric lock)	✅ Best
No Biometrics	❌ Fails	✅ Best
Highest Security	✅ Yes (FIDO2)	❌ Less secure

🚀 Final Steps

1. **Admins:** Enable **FIDO2 and/or Authenticator Passwordless** in Entra ID.
2. **Users:** Register at **aka.ms/mysecurityinfo**.
3. **Test:** Try logging into portal.office.com with both methods.