Passwordless MFA Method Registration in Entra ID

Field	Details
Document Type	How-To Guide / Runbook
Applies To	Microsoft Entra ID, Microsoft 365, Windows 10/11, Web sign-ins
Audience	Entra ID / Microsoft 365 Administrators (2nd Line / Systems Admin)
Author	AK. Udofeh
Last Updated	March 2026

Overview

This document explains how to enable and configure passwordless authentication methods (Microsoft Authenticator phone sign-in, FIDO2 / Passkey security keys, and Windows Hello for Business) in Microsoft Entra ID, and how admins should guide users to register them. It is intended for Entra ID administrators responsible for identity security, MFA, and Conditional Access in Microsoft 365 environments.

Background

- Users currently authenticate primarily with passwords and traditional MFA (SMS/voice/OTP), which are weak against phishing, replay, and credential stuffing attacks.
- Standard self-service MFA registration does not guarantee that users will enrol in passwordless methods unless those methods are explicitly enabled and promoted by administrators.
- Regulatory or internal security policies may require stronger, phishing-resistant or passwordless authentication for privileged roles, high-value apps, or all users over time.

Basic steps that do not resolve the issue on their own:

- Enabling MFA “per user” without configuring modern authentication methods policy.
- Relying on SMS / voice codes alone, which remain phishable and weaker than passwordless methods.
- Asking users to “use the Authenticator app” without enabling phone sign-in or FIDO2 / Passkey in the Authentication methods policy.

Other affected services/systems:

- Microsoft 365 workloads (Exchange Online, SharePoint Online, Teams, Entra admin center, Azure portal, etc.) rely on Entra ID sign-in and benefit directly from passwordless configuration.

Current setup

- By default, Entra ID tenants may only have legacy MFA methods widely used (phone call, SMS, app OTP) and password-based sign-in, while modern passwordless options are disabled or scoped to no users.
- This leaves accounts exposed to phishing and password-based attacks and prevents admins from enforcing phishing-resistant authentication strengths in Conditional Access.

Desired End state

1. Admin enables passwordless authentication methods in Entra admin center > Protection > Authentication methods and targets appropriate groups.
2. Users register Microsoft Authenticator phone sign-in, FIDO2 / Passkey security keys, or Windows Hello for Business via My Sign-ins or Windows enrolment flows.
3. Conditional Access and authentication strengths can then require passwordless / phishing-resistant MFA for specific users and apps.

What currently missing:

- Passwordless methods are not enabled or targeted correctly, so users cannot register them, Conditional Access cannot require them reliably, and the organisation remains password-dependent.

Known triggers:

- New tenant where no Authentication methods policy is configured.
- Tenants migrated from legacy per-user MFA, where admins never moved to a unified authentication methods policy.
- Hybrid or legacy Windows devices are not meeting Windows Hello for Business prerequisites.

?Before You Start

Use this checklist before enabling passwordless methods.

Check	Where
Confirm you have at least Authentication Administrator / Authentication Policy Administrator role	Entra admin centre > Roles and administrators
Ensure modern MFA is already in use (at least for admins)	Entra admin centre > Protection > MFA or Conditional Access
Identify break-glass / emergency access accounts and exclude them from strong requirements initially	Entra admin centre > Users > Filter for emergency accounts

Check	Where
Verify users have compatible devices (iOS/Android for Authenticator, Windows 10/11 for Hello, supported FIDO2 keys)	Hardware/software inventory, Intune, or asset list
Communicate upcoming changes and registration steps to end users	Internal IT communications plan

Implementation Steps

1. Enable Microsoft Authenticator Passwordless Sign-in

1. Sign in to https://entra.microsoft.com with an account that has Authentication Policy Administrator or Global Administrator role.
2. Go to Entra ID > Authentication methods > Policies.
3. Select Microsoft Authenticator from the list of built-in methods.
4. Set Enable to On.
5. Under Target, select All users or a dedicated pilot group (recommended initially).

> Be sure that at least two admins are in the pilot group.

6. Confirm Authentication mode includes Passwordless sign-in (phone sign-in) as allowed.

7 Click Save.

2. Enable FIDO2 / Passkey Security Keys

1. In Authentication methods > Policies, select Passkey (FIDO2) (may appear as FIDO2 security key in some portals).
2. Set Enable to On.
3. Under Target, select a pilot group or All users depending on readiness.

> Start with a small group if you have never deployed keys before.

4. Open the Configure tab and ensure Allow self-service setup is enabled so users can register keys at

https://mysignins.microsoft.com/security-info

5. (Optional but recommended) In the same Configure tab:

   - Enable Enforce attestation in production so only trusted hardware keys from approved manufacturers can be registered.
   - Configure Key restriction policy with allowed AAGUIDs if you want to restrict to specific key models.

6. Click Save.

3. Configure Windows Hello for Business (if required)

1. Confirm devices run Windows 10 version 1809+ or Windows 11 and are Entra-joined or hybrid-joined as per your design.
2. Configure Windows Hello for Business via Intune device configuration or Group Policy according to Microsoft guidance (PIN and biometrics on devices with TPM).
3. Ensure Windows Hello for Business is enabled as an authentication method in Authentication methods > Policies and targeted to groups/devices that meet prerequisites.
4. For hybrid environments requiring on-prem sign-in with FIDO2, ensure you also follow passwordless security key sign-in to on-premises resources guidance.

4. Instruct Users to Register Passwordless Methods

1. Ask users in the pilot group to sign in to https://mysignins.microsoft.com/security-info
2. For Microsoft Authenticator phone sign-in:
   1. Install the Microsoft Authenticator app on iOS/Android.
   2. Add the work/school account and enable phone sign-in when prompted in the app.
3. For FIDO2 / Passkey security keys:
   1. Users open Security info > Add sign-in method.
   2. Choose Security key and follow browser prompts to register the FIDO2 key (USB/NFC/Bluetooth).
4. For Windows Hello for Business:
   1. During Windows out-of-box experience or after sign-in, users will be prompted or can go to Settings > Accounts > Sign-in options to configure PIN and biometric sign-in.
5. Confirm that at least two passwordless-capable methods are configured for each admin account where possible.

5. Validate Sign-in Behaviour

1. In a test browser, go to https://portal.office.com or https://portal.azure.com and initiate sign-in as a pilot user.
2. Verify that passwordless options (Authenticator notification number match, security key, or Windows Hello) are available and functioning.
3. Check Entra admin centre > Protection > Authentication methods > Activity or sign-in logs to confirm passwordless usage.

Automated / Script Option (PowerShell for Policy Creation – Example for FIDO2)

> This is an example script using Microsoft Graph PowerShell to enable FIDO2 (Passkey) for all users; adjust scoping for production.

```
# Connect to Microsoft Graph with appropriate scopesConnect-MgGraph -Scopes "Policy.Read.All","Policy.ReadWrite.AuthenticationMethod"# Get existing FIDO2 authentication method policy$fidoPolicy = Get-MgPolicyAuthenticationMethodPolicyAuthenticationMethodConfiguration `  -Filter "id eq 'Fido2'"# If the policy does not exist, throw an errorif (-not $fidoPolicy) {    throw "FIDO2 authentication method policy not found."}# Enable the FIDO2 policy and target all users$updateBody = @{    state  = "enabled"                        # Turn the method on    includeTargets = @(        @{            id   = "all_users"              # Target all users (adjust for groups if needed)            targetType = "group"            # TargetType can be group or user            isRegistrationRequired = $true  # Require registration        }    )}# Update the FIDO2 policyUpdate-MgPolicyAuthenticationMethodPolicyAuthenticationMethodConfiguration `  -AuthenticationMethodConfigurationId $fidoPolicy.Id `  -BodyParameter $updateBody# Output the updated policy to confirm changesGet-MgPolicyAuthenticationMethodPolicyAuthenticationMethodConfiguration `  -AuthenticationMethodConfigurationId $fidoPolicy.Id
```

Deployment notes:

- Run from an admin workstation or Cloud Shell as a **Global Administrator / Authentication Policy Administrator**.
- Requires Microsoft Graph PowerShell SDK and appropriate API permissions (delegated or app).

Expected output / success indicators:

- Final `Get-MgPolicyAuthenticationMethodPolicyAuthenticationMethodConfiguration` output shows `state` as `enabled` and `includeTargets` scoped as configured.

Script Breakdown

- `Connect-MgGraph -Scopes ...` connects to Microsoft Graph with permissions to read and update authentication method policies.
- `Get-MgPolicyAuthenticationMethodPolicyAuthenticationMethodConfiguration` retrieves the current FIDO2 authentication method configuration by ID (`Fido2`).
- The `if (-not $fidoPolicy)` block ensures the script fails fast if the FIDO2 configuration is not present.
- `$updateBody` defines the new policy state and targeting, setting the method to **enabled** and targeting `all_users` (which you may replace with a specific group object ID).
- `Update-MgPolicyAuthenticationMethodPolicyAuthenticationMethodConfiguration` applies the update to the existing FIDO2 policy.
- The final `Get-...` call outputs the updated policy so you can verify the changes.

Troubleshooting

Users do not see passwordless options at sign-in

- Confirm the relevant method (Authenticator, FIDO2, Windows Hello) is **enabled** and targeted to the user in **Authentication methods > Policies**.
- Verify the user has successfully registered the method at **https://mysignins.microsoft.com/security-info** and that the device/app is healthy.

FIDO2 key registration fails in the browser

- Ensure the browser and OS support WebAuthn/FIDO2 (modern versions of Edge, Chrome, etc.).
- Check if **Enforce attestation** or key restriction policies are blocking the model; test with a known-good, supported key.

Windows Hello for Business not offered

- Confirm device meets OS and TPM requirements and is Entra-joined or hybrid-joined.
- Verify Windows Hello policies are enabled via Intune or Group Policy and that no conflicting policies disable it.

Graph script fails with permission/403 errors

- Ensure the signed-in admin has the required Graph permissions and has granted consent where needed.
- Confirm the Microsoft Graph PowerShell module is up to date.

Expected Outcome

Item	Detail
Resolution time	30–90 minutes for tenant policy configuration, plus phased user enrolment over days/weeks
User impact	Users see new sign-in experiences (Authenticator notification, FIDO2 key prompts, Windows Hello) and fewer password prompts
Recurrence risk	Low once configured; periodic review needed for new apps, roles, and user groups

---

Revision #2
Created 2026-03-27 11:45:26 UTC by AK. Udofeh
Updated 2026-03-27 12:45:43 UTC by AK. Udofeh