



# Passkeys in Microsoft 365

## The Good, the Bad and the Ugly

Jan Bakker

Oktober 2025





## Jan Bakker

Solution Architect Security & IAM



*Find my  
contact  
details here*

[aka.ms/janbakker](http://aka.ms/janbakker)



DUTCH MICROSOFT  
ENTRA COMMUNITY

JANBAKKER.TECH  
 sharing is caring

# Let's talk passkeys



Based on **FIDO** standards, passkeys are a **replacement** for **passwords** that provide **faster**, **easier**, and **more** secure sign-ins to websites and apps across a user's devices. Unlike passwords, passkeys are always strong and **phishing-resistant**.



Founded in 2013



# Joebie

# Kie



# yubico



# FIDO2 (security)keys

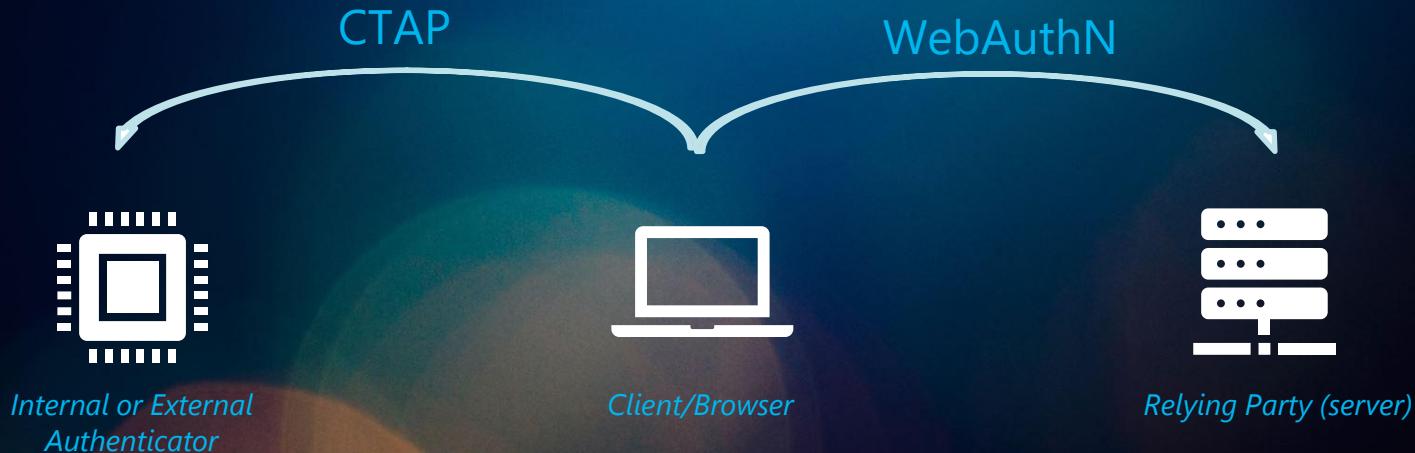
can store

# passkeys

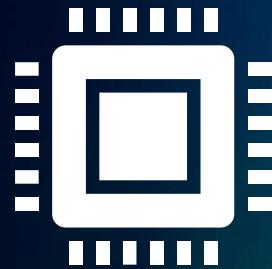


~~Passwords~~  
keys

# FIDO2 standard



# Authenticator types



*Platform Authenticator*

*Touch ID  
Face ID  
Windows Hello*



*Roaming Authenticator*

*Security keys  
(USB/NFC/BTE)*

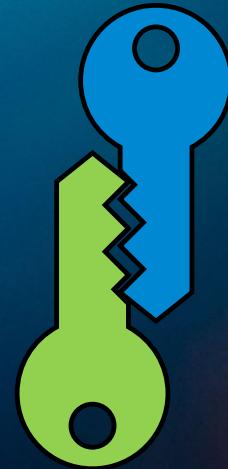
Most of your users already carry a platform authenticator in their pockets every day



Faster  
&  
Easier



# More Secure



Passkey are built on PKI

# Phishing Resistant



# How passkeys work (Registration)

## Authenticator



PIN or Biometrics

RP ID	Priv	Pub
Contoso.com		

## Client

I want to create a new passkey for **user A**

Sure, here's a challenge

Here's the public key and the origin challenge

I've linked the public key to **user A**. See you next time!

## Relying Party



User	Pub
User A	

No more **passwords**

No more **shared secrets**

No more **AiT M attacks**

Where do we  
store our passkeys?







# Device-bound passkeys

Bound to and used only on a single device

# Synced passkeys

Stored securely in a credential manager and accessed across devices

# Device-bound passkeys

Bound to a FIDO security key or platform and cannot be synced across devices.



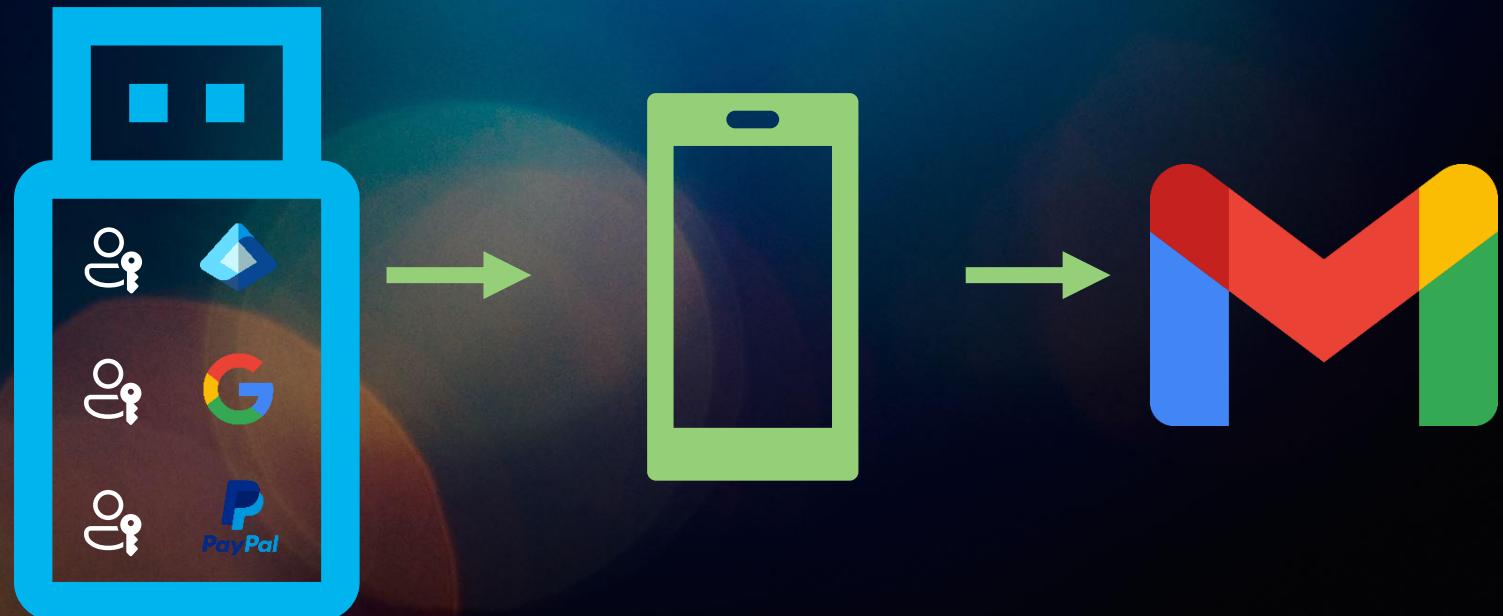
# Device-bound passkeys

Bound to a FIDO security key or platform and cannot be synced across devices.



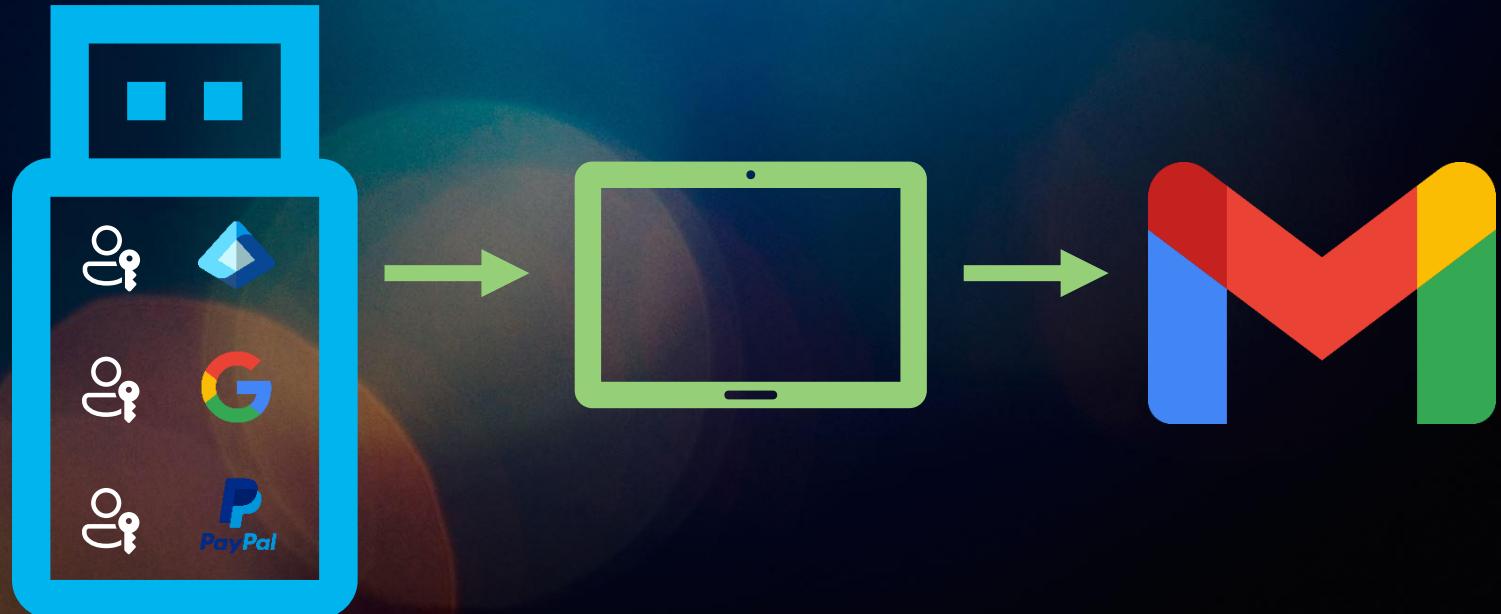
# Device-bound passkeys

Bound to a FIDO security key or platform and cannot be synced across devices.



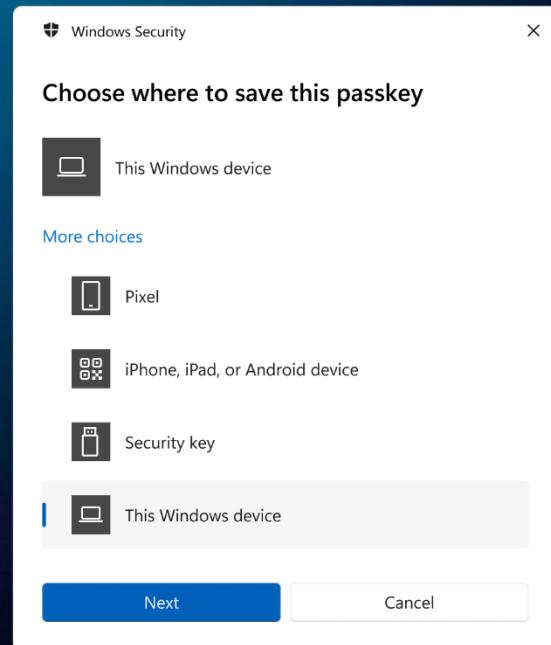
# Device-bound passkeys

Bound to a FIDO security key or platform and cannot be synced across devices.



# Support for passkeys in Windows

Linked device (**Android only**) →  
iPhone, iPad or Android device (**cross device via QR code**) →  
Security key (**USB or NFC**) →  
Local (**Windows Hello**) →



Passkeys for any  
supported services  
may already land on  
your **corporate**  
devices today.



← Settings



Jan Bakker

Find a setting  Q

- System
- Bluetooth & devices
- Network & internet
- Personalization
- Apps
- Accounts **(selected)**
- Time & language
- Gaming
- Accessibility
- Privacy & security
- Windows Update

## Accounts > Passkeys

Use the passkeys saved on this device to sign in to apps and websites without a password. Instead, your passkeys allow you to sign in using your face, fingerprint, or PIN through Windows Hello.

### Saved passkeys

Search passkeys  Q

9 apps and websites found

Sort by: Name (Z to A)

passkey.org Jan	...
login.microsoft.com	...
google.com	...

[Home](#)[Payment methods](#)[Passwords](#)[Personal info](#)[Order tracking](#)[Settings](#)

## Passwords

[+ Add](#)[Settings](#)[Passkeys](#)

...



### Add or import passwords to your Wallet

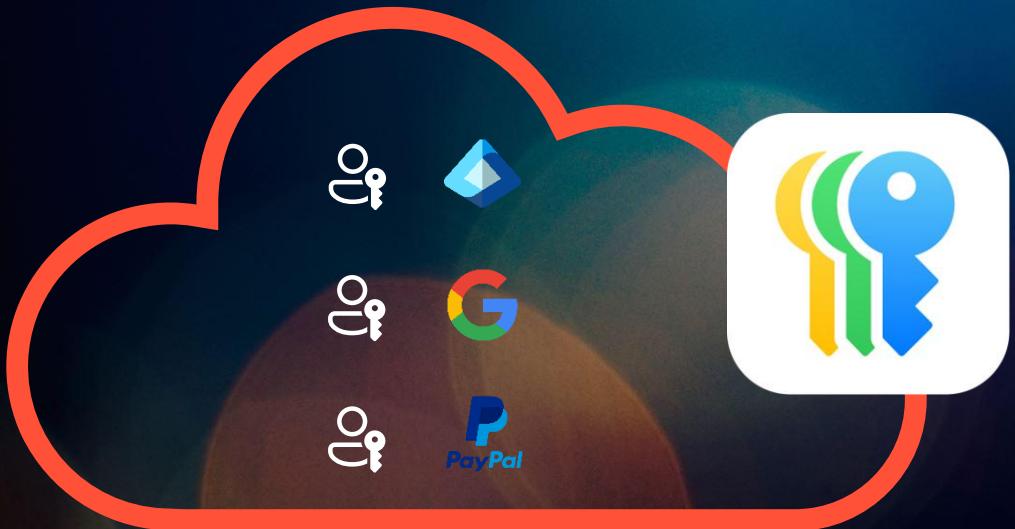
Improve your browsing and autofill experience when you add or import your passwords.

[Import passwords](#)



# Synced passkeys

Stored securely in a credential manager and accessed across devices.



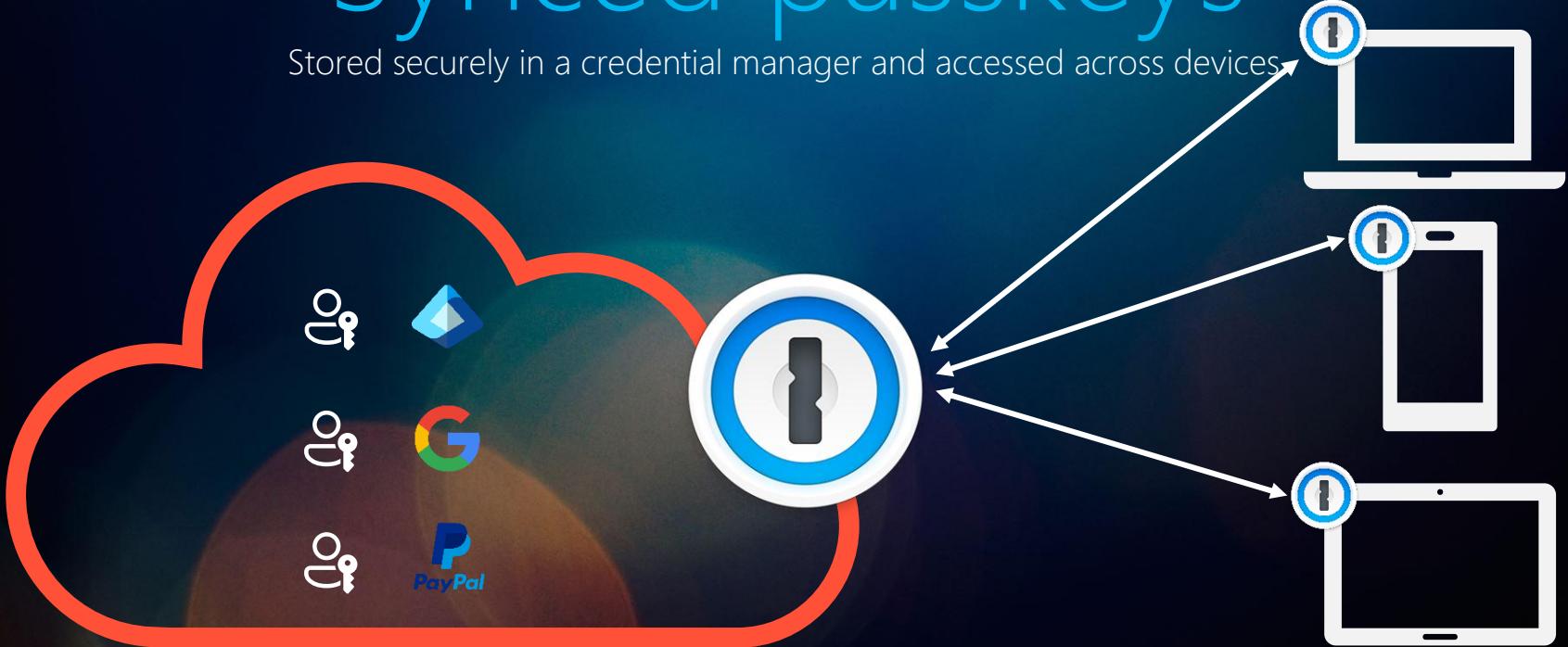
# Synced passkeys

Stored securely in a credential manager and accessed across devices.



# Synced passkeys

Stored securely in a credential manager and accessed across devices



# Passkey in Microsoft Authenticator App



- Lives in the Authenticator App
- Cannot leave the device
- Can be used cross-device
- Runs on iOS and Android



# How to enable passkeys in Entra ID?



# MC920300 - Microsoft Entra: Enablement of Passkeys in Authenticator for passkey (FIDO2) organizations with no key restrictions

Message ID	MC920300
Service	Microsoft Entra
Last Updated	Jan 24, 2025
Tag	Major change Updated message Admin impact
Act by	Mar 3, 2025

## Summary

Starting late January 2025, organizations with enabled passkey (FIDO2) policy and no key restrictions will have passkeys in the Microsoft Authenticator app. Users can add this via aka.ms/MySecurityInfo, and it's enforced by Conditional Access policy. Organizations preferring not to enable this can impose key restrictions.

## More information

Beginning late January 2025 (previously mid-January), after the General Availability of passkeys in the Microsoft Authenticator app, organizations with the passkey (FIDO2) authentication methods policy enabled with no key restrictions will be enabled for passkeys in the Microsoft Authenticator app in addition to FIDO2 security keys. This update aligns with the broader availability of passkeys in Entra ID, extending from device-bound passkeys on security keys to device-bound passkeys also on user devices. Users who navigate to aka.ms/MySecurityInfo will see "Passkey in Microsoft Authenticator" as an authentication method they can add. Additionally, when Conditional Access (CA) authentication strengths policy is used to enforce passkey authentication, users who don't yet have any passkey will be prompted inline to register passkeys in Authenticator to meet the CA requirements. If an organization prefers not to enable this change for their users, they can work around it by enabling key restrictions in the passkey (FIDO2) policy. This change will not impact organizations with existing key restrictions or organizations that have not enabled the passkey (FIDO2) policy.

### When this will happen:

General Availability (Worldwide, GCC, GCC High, DoD): Rollout will happen late January 2025 (previously mid-January).

### How this will affect your organization:

Home

What's new

Diagnose &amp; solve problems

Favorites

Identity

Overview

Users

Groups

Devices

Applications

Protection

Identity Governance

External Identities

Show more

Protection

Identity Protection

Conditional Access

Authentication methods

Password reset

Learn &amp; support

Home &gt;

## Authentication methods | Policies

Contoso - Microsoft Entra ID Security

Search

Add external method (Preview)

Refresh

Got feedback?

### Manage

Policies

Password protection

Registration campaign

Authentication strengths

Settings

### Monitoring

Activity

User registration details

Registration and reset events

Bulk operation results

Passkey (FIDO2)

Use authentication methods policies to configure the authentication methods your users may register and use. If a user is in scope for a method, they may use it to authenticate and for password reset (some methods aren't supported for some scenarios). [Learn more](#)

Method	Target	Enabled
All users	All users	Yes
SMS	All users	Yes
Temporary Access Pass	All users	Yes
Hardware OATH tokens (Preview)	All users	Yes
Third-party software OATH tokens		No
Voice call		No
Email OTP		No
Certificate-based authentication		No



Home

What's new

Diagnose &amp; solve problems

Favorites

Identity

Overview

Users

Groups

Devices

Applications

Protection

Identity Governance

External Identities

Show more

Protection

Identity Protection

Conditional Access

Authentication methods

Password reset

Learn &amp; support

Home &gt; Authentication methods | Policies &gt;

## Passkey (FIDO2) settings

...

Passkeys are a phishing-resistant, standards-based passwordless authentication method available from a variety of vendors. [Learn more](#). Passkeys are not usable in the Self-Service Password Reset flow.

[Enable and Target](#) [Configure](#)

### GENERAL

Allow self-service set up [Yes](#) [No](#)

Enforce attestation [Yes](#) [No](#)

### KEY RESTRICTION POLICY

Enforce key restrictions [Yes](#) [No](#)

Restrict specific keys [Allow](#) [Block](#)

Microsoft Authenticator ⓘ

[Add AAGUID](#)

No AAGuids have been added.

Home

What's new

Diagnose &amp; solve problems

Favorites

Identity

Overview

Users

Groups

Devices

Applications

Protection

Identity Governance

External Identities

... Show more

Protection

Identity Protection

Conditional Access

Authentication methods

Password reset

Learn &amp; support

Home &gt; Authentication methods | Policies &gt;

## Passkey (FIDO2) settings

...

Passkeys are a phishing-resistant, standards-based passwordless authentication method available from a variety of vendors. [Learn more](#). Passkeys are not usable in the Self-Service Password Reset flow.

Enable and Target [Configure](#)

### GENERAL

Allow self-service set up [Yes](#) [No](#)Enforce attestation [Yes](#) [No](#)

### KEY RESTRICTION POLICY

Enforce key restrictions [Yes](#) [No](#)Restrict specific keys [Allow](#) [Block](#) Microsoft Authenticator ⓘ[Add AAGUID](#)

90a3ccdf-635c-4729-a248-9b709135078f

...

de1e552d-db1d-4423-a619-566b625cdc84

...

# AAGUID





CHANGE RESPONSE

[Installing YubiKey Software on Linux](#)

[Getting Started on iOS](#)

[macOS Login Tool Configuration Guide](#)  
[Deprecated]

[YubiKey PIV Manager User's Guide](#)  
[deprecated]

[Using your YubiKey as a smart card in macOS](#)

[Can I duplicate a YubiKey?](#)

[Using a YubiKey with USB-C Adapters](#)

[Code Signing with the YubiKey on Windows](#)

[YubiCloud OTP Validation Service Guide](#)

[YubiKey for YubiCloud Configuration Guide](#)

[OATH-HOTP: Yubico Best Practices Guide](#)

[Achieving FedRamp Compliance with the YubiKey FIPS Series Devices](#)

[Using Your YubiKey with Keeper](#)

[Setting the NDEF Slot for NFC Usage](#)

[Windows Logon Tool & Configuration Guide \[Deprecated\]](#)

[Generating Base32 string examples](#)

YUBIKEY Security Key (Blue)

SN	MAC	
All	N/A	N/A
YubiKey 4 (Series)	4.4	N/A
<b>YubiKey 5 Series</b>		
YubiKey 5 (USB-A, No NFC)	5.1	cb69481e-8ff7-4039-93ec-0a2729a154a8
YubiKey 5 (USB-A, No NFC)	5.2, 5.4	ee882879-721c-4913-9775-3dfcce97072a
YubiKey 5 NFC	5.1	fa2b99dc-9e39-4257-8f92-a30d23c4118
YubiKey 5 NFC	5.2, 5.4	2fc0579f-8113-47ea-b116-bb5a8db9202a
YubiKey 5 NFC	5.7	a25342c0-3cdc-4414-8e46-f4807fca511c d7781e5d-e353-46aa-afe2-3ca49f13332a
YubiKey 5C NFC	5.2, 5.4	2fc0579f-8113-47ea-b116-bb5a8db9202a
YubiKey 5C NFC	5.7	a25342c0-3cdc-4414-8e46-f4807fca511c d7781e5d-e353-46aa-afe2-3ca49f13332a
YubiKey 5 Nano	5.1	cb69481e-8ff7-4039-93ec-0a2729a154a8
YubiKey 5 Nano	5.2, 5.4	ee882879-721c-4913-9775-3dfcce97072a
YubiKey 5 Nano	5.7	19083c3d-8383-4b18-bc03-8f1c9ab2fd1b ff4dac45-ede8-4ec2-aced-cf66103f4335
YubiKey 5C Nano	5.1	cb69481e-8ff7-4039-93ec-0a2729a154a8
YubiKey 5C Nano	5.2, 5.4	ee882879-721c-4913-9775-3dfcce97072a
YubiKey 5C Nano	5.7	19083c3d-8383-4b18-bc03-8f1c9ab2fd1b ff4dac45-ede8-4ec2-aced-cf66103f4335
YubiKey 5C	5.1	cb69481e-8ff7-4039-93ec-0a2729a154a8
YubiKey 5C	5.2, 5.4	ee882879-721c-4913-9775-3dfcce97072a
YubiKey 5C	5.7	19083c3d-8383-4b18-bc03-8f1c9ab2fd1b ff4dac45-ede8-4ec2-aced-cf66103f4335
YubiKey 5Ci	5.2, 5.4	c5ef55ff-ad9a-4b9f-b580-adebafe026d0
YubiKey 5Ci	5.7	a02167b9-ae71-4ac7-9a07-06432ebbf1c 24673149-6c86-4e27-98d9-433fb5b73296

# Security Advisory YSA-2024-03

## Security Advisory YSA-2024-03 Infineon ECDSA Private Key Recovery

Published Date: 2024-09-03

Tracking IDs: YSA-2024-03

CVE: In Process 

CVSS Severity: [4.9](#)

### Summary

A vulnerability was discovered in Infineon's cryptographic library, which is utilized in YubiKey 5 Series, and Security Key Series with firmware prior to 5.7.0 and YubiHSM 2 with firmware prior to 2.4.0. The severity of the issue in Yubico devices is moderate.

An attacker could exploit this issue as part of a sophisticated and targeted attack to recover affected private keys. The attacker would need physical possession of the YubiKey, Security Key, or YubiHSM, knowledge of the accounts they want to target, and specialized equipment to perform the

[Files](#)[main](#)[Go to file](#)[Entra](#)[Export-Fido2Info.ps1](#)[Scripts / Entra / Export-Fido2Info.ps1](#)

MichelvanVliet Update Export-Fido2Info.ps1

25d8d6c · 11 months ago

[History](#)[Code](#)[Blame](#)

130 lines (110 loc) · 4.72 KB

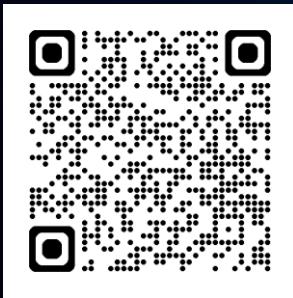
[Raw](#)

```
1  <#
2  .SYNOPSIS
3      Export all FIDO2 registration info for all users within an Entra OD tenant
4
5  .DESCRIPTION
6      PowerShell script to gather and export all FIDO2 registration information for all users to a .CSV file.
7
8  .NOTES
9      Requirements:
10     - Microsoft Graph PowerShell SDK (will be installed if not present)
11     - Graph permissions:
12         User.Read.All
13         UserAuthenticationMethod.Read.All
14         UserAuthMethod-Passkey.Read.All
15
16  .PARAMETER CsvFile
17      Specify the full output path and filename for the CSV report file.
18      If not specified, the script will produce a report in the current folder using the following file name: "Fido2Registration_Report.csv".
19
20  .PARAMETER Delimiter
21      Specify the delimiter character used for the CSV output file.
22      If not specified, ";" will be used as delimiter.
23
24  .EXAMPLE
25      PS> .\Export-Fido2Info.ps1 -CsvFile "C:\Temp\Fido2Registration_Report.csv" -Delimiter ";"
```

# Passkey enrollment



# Microsoft Entra end-user rollout templates and materials



**Microsoft** | Download Center Windows Office Web browsers Developer tools Xbox All Microsoft

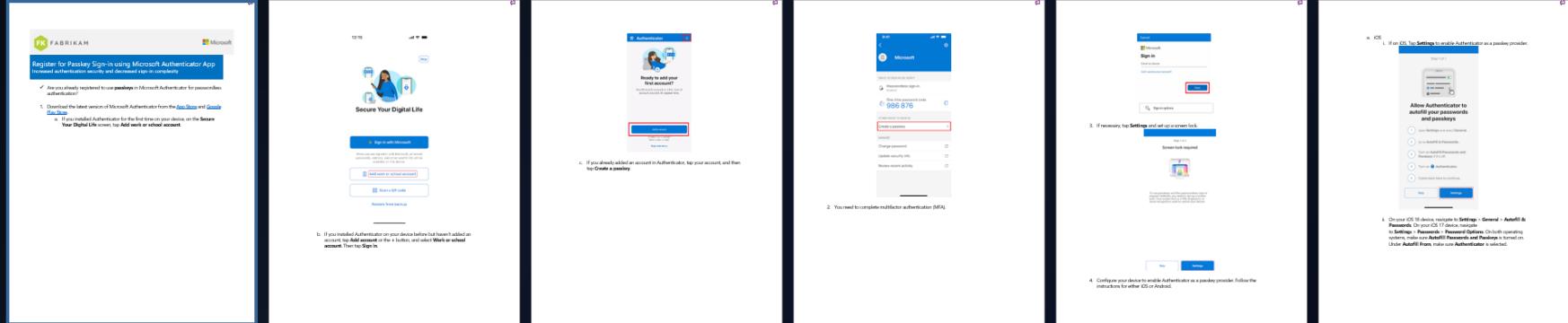
**Bring the world closer with Bing Wallpaper**  
Download the free app and enjoy breathtaking views with a new background each day.  
[Get Bing Wallpaper](#)



**Microsoft Entra end-user rollout templates and materials**  
Use these customizable posters, training, stickers, and email templates to roll out Azure Active Directory features in your organization

Important! Selecting a language below will dynamically change the complete page content to that language.

Select language  Download



1

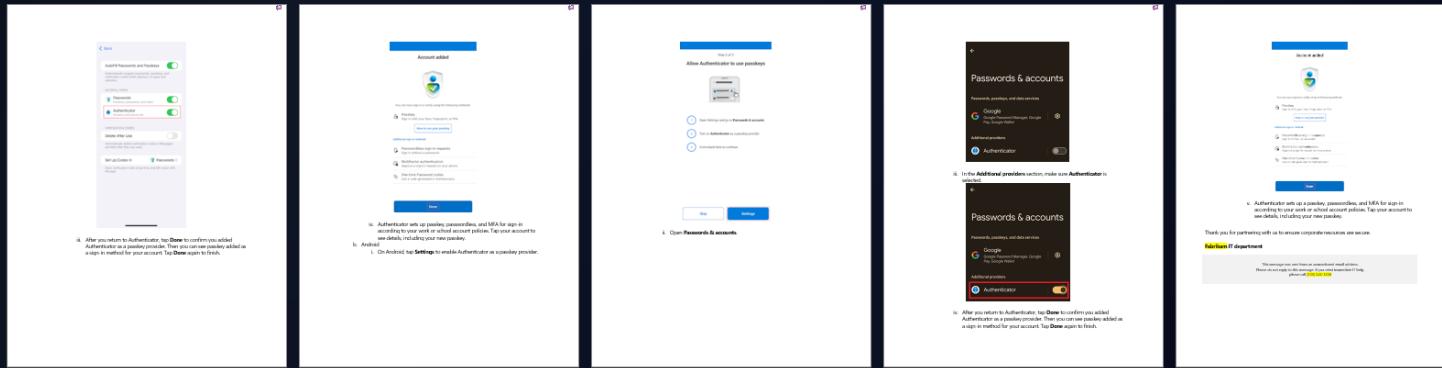
2

3

4

5

6



7

8

9

10

11

MFA is required for enrollment of strong auth methods

Security key

Windows Hello for Business

Passkey in Auth App

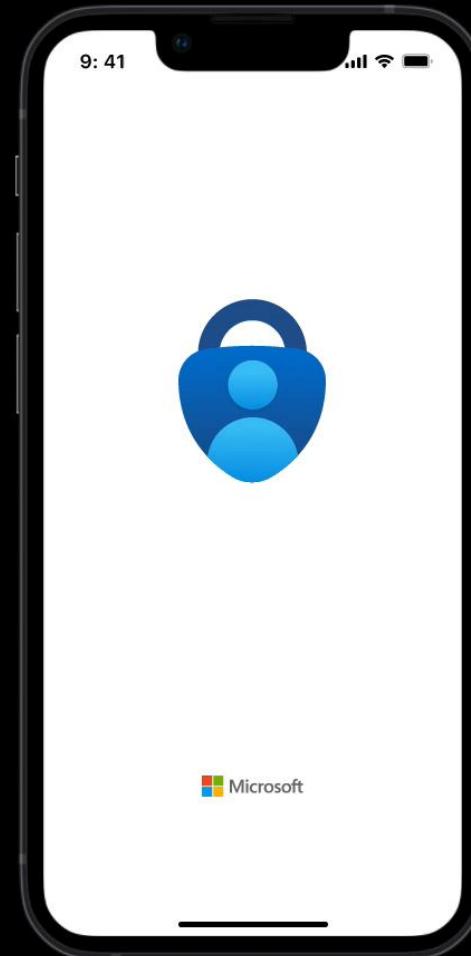


# Temporary Access Pass

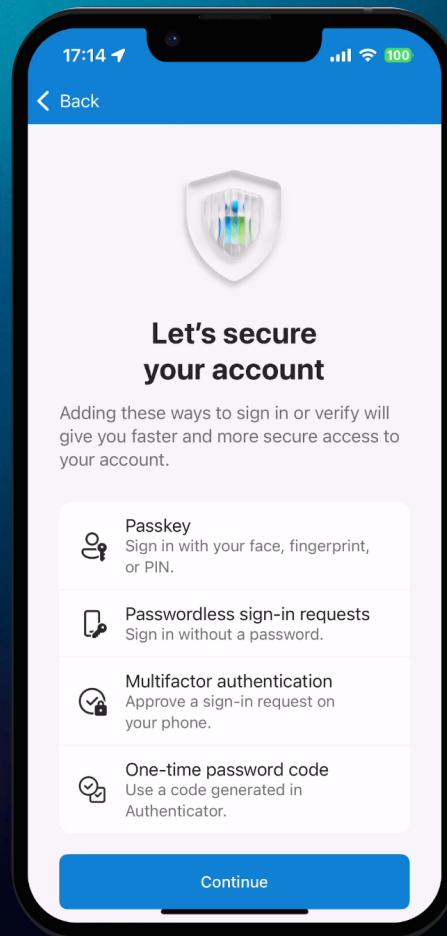


“The easiest and fastest way to add a passkey  
is to add it directly in the Authenticator app.”

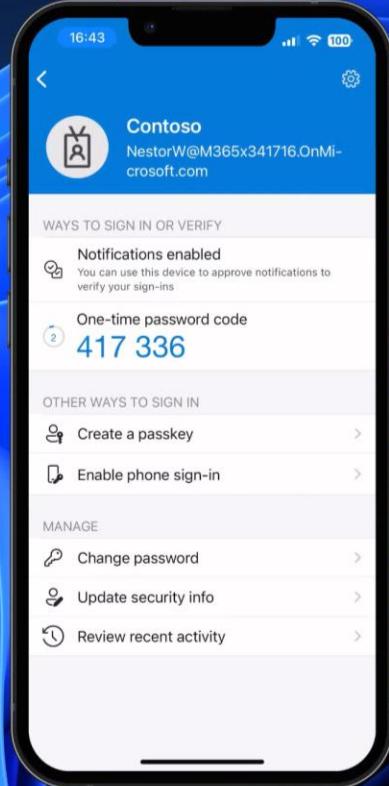
Register passkey in  
Authenticator App  
with Temporary  
Access Pass



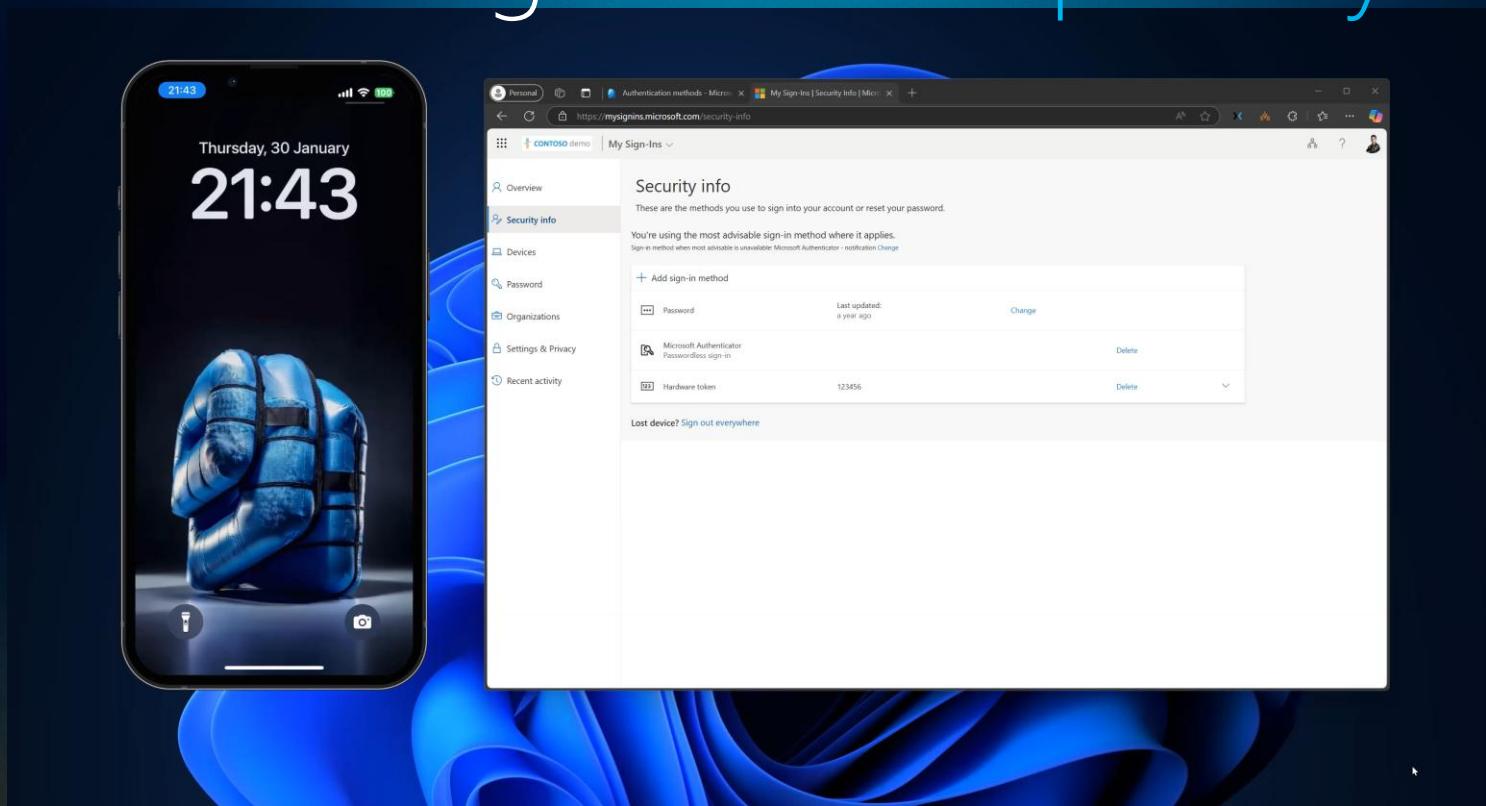
# All the methods!



# Register passkey for existing users with MFA



# Cross-device registration of passkeys



Overview

Security info

Devices

Password

Organizations

Settings & Privacy

Recent activity

## Security info

These are the methods you use to sign into your account or reset your password.

You're using the most advisable sign-in method where it applies.

Sign-in method when most advisable is unavailable: Microsoft Authenticator - notification [Change](#)

+ Add sign-in method

>Password

Last updated:  
a year ago

[Change](#)

Microsoft Authenticator  
Passwordless sign-in

**Passkey not accepted**

X



Delete this passkey in your Microsoft Authenticator app, then return here to create a new one. You'll need to sign in to Authenticator again with your admin@M365x341716.onmicrosoft.com account.

Lost device? [Sign out](#)

Having trouble?

OK

Attestation not supported  
using the WebAuthN flow

GET beta https://graph.microsoft.com/beta/users/90f43eac-70c3-4aa7-bcca-7ee3522b3845/authentication/fido2Methods

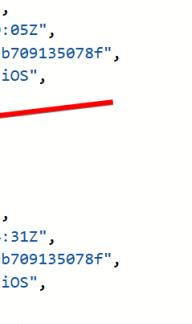
No resource was found matching this query

Request body Request headers Modify permissions Access token

OK - 200 - 470 ms

Response preview Response headers Code snippets Toolkit component Adaptive cards

```
{ "@odata.context": "https://graph.microsoft.com/beta/$metadata#users('90f43eac-70c3-4aa7-bcca-7ee3522b3845')/authentication/fido2Methods", "@microsoft.graph.tips": "Use $select to choose only the properties your app needs, as this can lead to performance improvements. For example: GET users('<guid>')/authentication/fido2Methods?$select=attestationCertificates", "value": [ { "id": "4IHwPDQyTk0C6t7DT9B7A2", "displayName": "Authenticator - iOS", "createdDateTime": "2025-01-30T21:00:05Z", "aaGuid": "90a3ccdf-635c-4729-a248-9b709135078f", "model": "Microsoft Authenticator - iOS", "attestationCertificates": [], "attestationLevel": "attested" }, { "id": "t3gCeWN4Q0mKuyB4miQkNg2", "displayName": "Authenticator - iOS", "createdDateTime": "2025-01-30T20:44:31Z", "aaGuid": "90a3ccdf-635c-4729-a248-9b709135078f", "model": "Microsoft Authenticator - iOS", "attestationCertificates": [], "attestationLevel": "notAttested" } ] }
```



Keep your account secure

## Microsoft Authenticator



Start by getting the app

On your phone, install the Microsoft Authenticator app. [Download now](#)

After you install the Microsoft Authenticator app on your device, choose "Next".

Next

Skip setup

# SelfServicePasswordReset

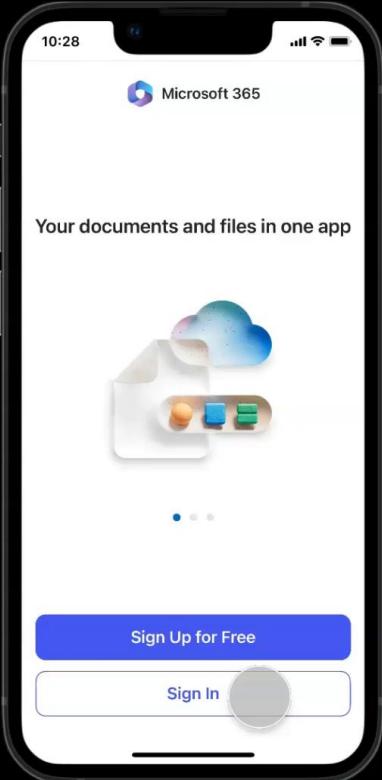
# Self Service Password Reset

Method	Primary authentication	Secondary authentication
Windows Hello for Business	Yes	MFA <sup>1</sup>
Microsoft Authenticator push	No	MFA and SSPR
Microsoft Authenticator passwordless	Yes	No <sup>2</sup>
Microsoft Authenticator passkey	Yes	MFA
Authenticator Lite	No	MFA
Passkey (FIDO2)	Yes	MFA
Certificate-based authentication (CBA)	Yes	MFA
Hardware OATH tokens (preview)	No	MFA and SSPR
Software OATH tokens	No	MFA and SSPR
External authentication methods (preview)	No	MFA
Temporary Access Pass (TAP)	Yes	MFA
Text	Yes	MFA and SSPR
Voice call	No	MFA and SSPR
QR code	Yes	No
Password	Yes	No

A photograph of a golf ball resting on a patch of green grass. In the background, a yellow flagstick stands upright in the ground. The scene is set outdoors on a golf course with trees visible in the distance.

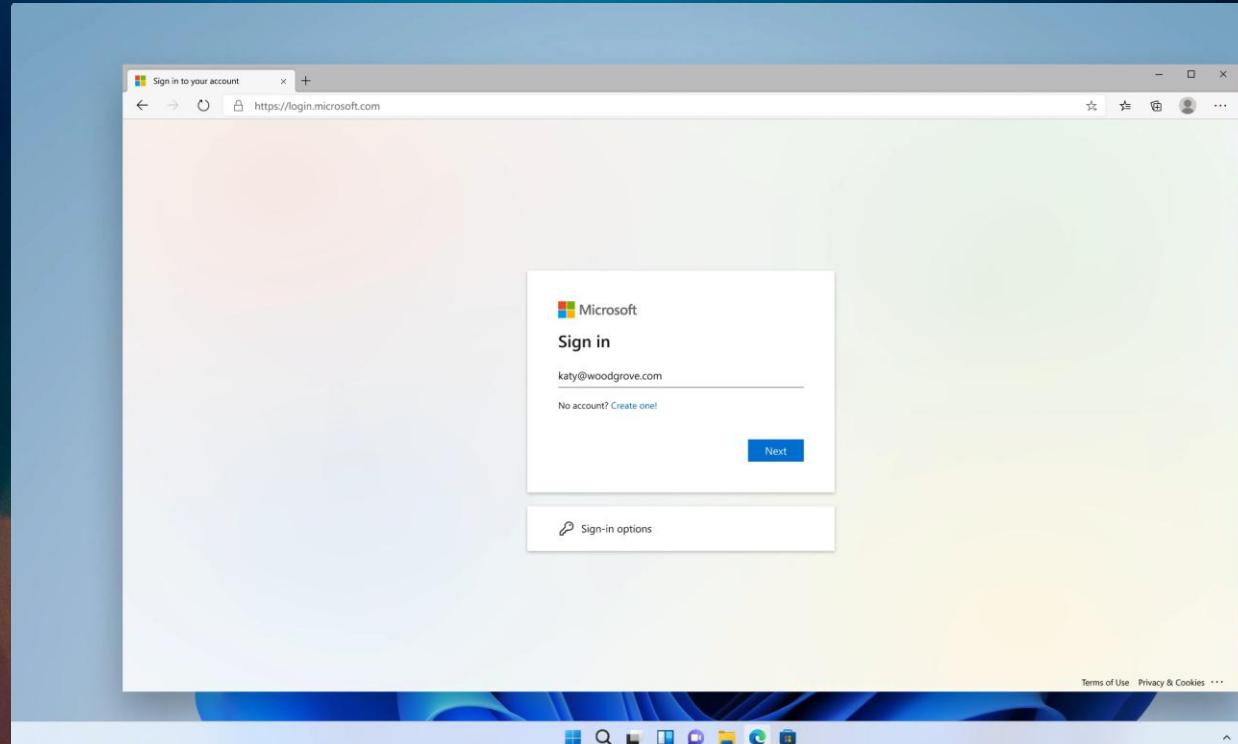
All set. Now let's **use** it!

# Same device sign-in



# Cross device sign-in

This sign-in option requires **Bluetooth** and an **internet connection** for both devices



# What does **not** work today?

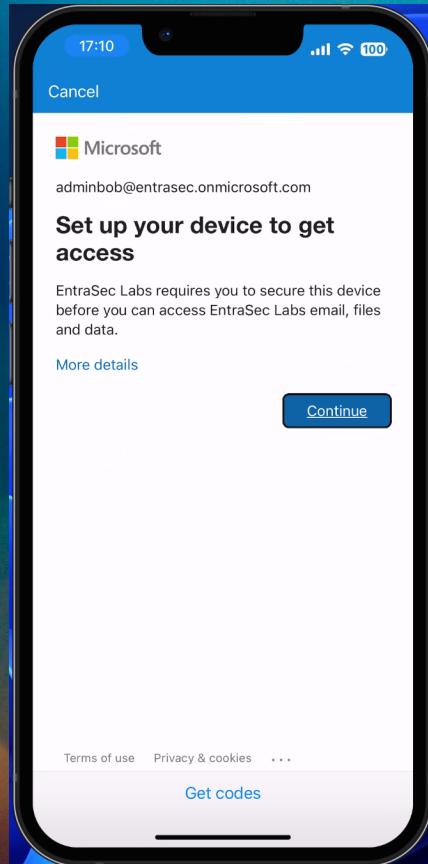
Store Entra ID passkeys in other credential providers like 1Passsword or Google Authenticator

Store 3<sup>rd</sup> party passkeys in Microsoft Authenticator

Sync passkeys from Entra ID to other devices

Conditional Access  
doing its job

All resources (formerly  
'All cloud apps')



Require multifactor authentication (i)

Require authentication strength (i)

**Require device to be marked as compliant** (i)

Require Microsoft Entra hybrid joined device (i)

Require approved client app (i)  
[See list of approved client apps](#)

**Require app protection policy** (i)  
[See list of policy protected client apps](#)

Require password change (i)

For multiple controls

**Require all the selected controls**

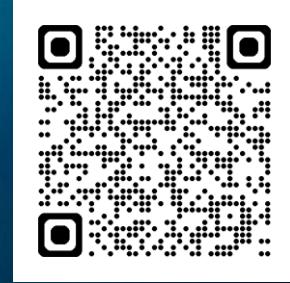
Require one of the selected controls

# Passkey provisioning

(only supported for hardware security keys)



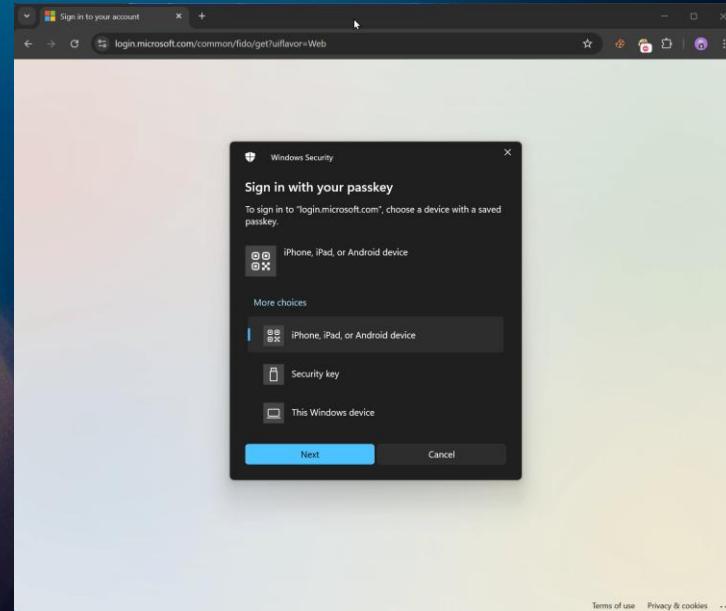
Learn how!



# Enforce PIN complexity and change on first use

```
PowerShell
Do you want to proceed with the above configuration? [y/N]: y
YubiKey will be factory reset. ANY EXISTING CREDENTIALS WILL BE LOST!
Remove the YubiKey from the USB port...
Re-insert the YubiKey...
Touch the YubiKey...
The YubiKey has been reset.
Creating credential on YubiKey...
Touch the YubiKey...
Credential created on YubiKey!
Registering credential with identity provider...
New credential registered!

YubiKey configuration summary:
Serial number: 33073988
Temporary PIN: 208624
NOTE: The PIN needs to be changed before it can be used!
PS C:\Program Files\Yubico\YubiEnroll> |
```



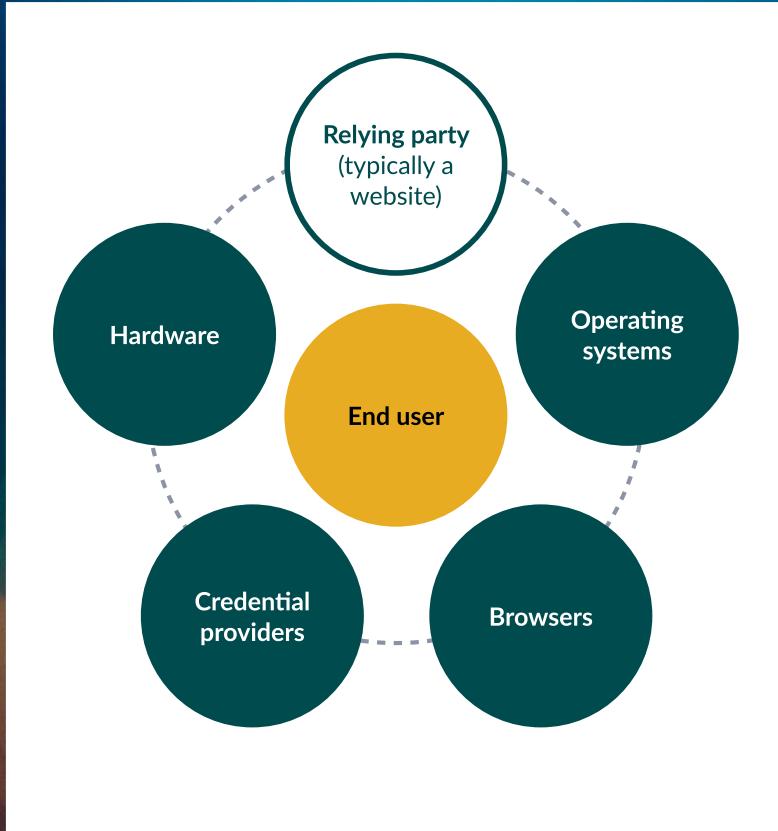
Are we there  
yet?





We are still in  
the early stage  
of passkeys

The API is  
there.....



# WWDC25

## Passkey improvements by Apple

Account creation API

**Keep passkeys up-to-date**

Automatic  
passkey upgrades

Passkey management  
endpoints

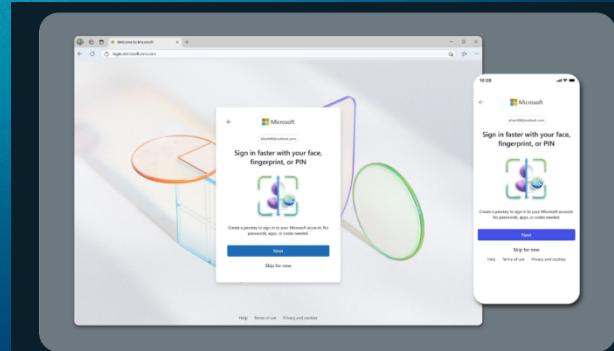
Importing and exporting  
passkeys



# Improvements by Microsoft

For now, only consumer accounts

<https://www.microsoft.com/en-us/security/blog/2025/05/01/pushing-passkeys-forward-microsofts-latest-updates-for-simpler-safer-sign-ins/>



We believe that great usability and great security go hand in hand, so as we continue our transition to a passwordless world, we're introducing some significant changes:

1. **New sign-in user experience (UX):** Earlier this year, we launched a new visual style that simplifies the sign-in and sign-up experience. The new design is modernized and streamlined and prioritizes passwordless methods for sign-in and sign-up.<sup>3</sup>
2. **New accounts are passwordless by default:** As part of this simplified UX, we're changing the default behavior for new accounts. Brand new Microsoft accounts will now be "passwordless by default." New users will have several passwordless options for signing into their account and they'll never need to enroll a password. Existing users can visit their account settings to delete their password.
3. **Passwordless-preferred sign-in:** We're also making it simpler to sign in with safer options. Instead of showing you all the possible ways for you to sign in, we automatically detect the best available method on your account and set that as the default. For example, if you have a password and "one time code" set up on your account, we'll prompt you to sign in with your one time code instead of your password. After you're signed in, you'll be prompted to enroll a passkey. Then the next time you sign in, you'll be prompted to sign in with your passkey. This simplified experience gets you signed in faster and in our experiments has reduced password use by over 20%. As more people enroll passkeys, the number of password authentications will continue to decline until we can eventually remove password support altogether.

# Android struggles

I'm on an Android 14 device, and I followed all the steps. Why can't I register passkeys in the Authenticator app?

The Authenticator app uses [Android APIs ↗](#) on Android 14 or higher to use passkeys. Manufacturers choose whether or not to implement these APIs for each device they make. If your device doesn't support these APIs, the Authenticator app might not work for your device on Android 14. For the best experience, we recommend that you upgrade to Android 15.



# Android struggles cont'd

## Store passkeys in Android profiles

Passkeys on Android are used only from the profile where they're stored. If a passkey is stored in an Android Work profile, it's used from that profile. If a passkey is stored in an Android Personal profile, it's used from that profile. To make sure that users can access and use the passkey they need, users with both an Android Personal profile and an Android Work profile should create their passkeys in Authenticator for each profile.



# Android struggles still cont.'s

## Why do I get prompted for PIN instead of biometric sign-in on my Android device?

If biometric sign-in fails on an Android device, the Authenticator app will prompt you to enter your PIN instead. The next time you sign in with the passkey, Authenticator continues to request the PIN rather than biometric sign-in. Authenticator periodically retries biometric sign-in. If biometric sign-in succeeds, it will be used for subsequent sign-ins.

## What happens to my passkey after I change my PIN or biometric sign-in on my Android device?

Your passkey is invalidated if you change your PIN, or if you change your biometric sign in from thumbprint to face, or vice-versa. If your passkey is invalidated, you need to sign-in by using a different method, and then create a new passkey.



# Does it work for External Guest Accounts?

Microsoft Entra admin center

Monitoring & health > Audit logs

Entra ID

- Overview
- Users
- Groups
- Devices
- Enterprise apps
- App registrations
- Roles & admins
- Delegated admin partners
- Domain services
- Conditional Access
- Multifactor authentication
- Identity Secure Score
- Authentication methods
- Password reset
- Custom security attributes
- Certificate authorities
- External Identities
- Cross-tenant synchronization
- Entra Connect

Search resources, services, and docs (G+)

Home > ExtraSec Labs > External Identities | Cross-tenant access settings > Inbound access settings - Contoso

B2B collaboration   B2B direct connect   **Trust settings**   Cross-tenant sync

Configure whether your Conditional Access policies will accept claims from other Microsoft Entra tenants when external users access your resources. The default settings apply to all external Microsoft Entra tenants except those with organization-specific settings.

You'll first need to configure Conditional Access for guest users on all cloud apps if you want to require multifactor authentication or require a device to be compliant or Microsoft Entra hybrid joined.

[Learn more](#)

Default settings

Customize settings

Trust multifactor authentication from Microsoft Entra tenants

Trust compliant devices

Trust Microsoft Entra hybrid joined devices

+ Enforce Conditional Access authentication strength

Automatic redemption

Check this setting if you want to automatically redeem invitations. If so, users from the specified tenant won't have to accept the consent prompt the first time they access this tenant using cross-tenant synchronization, B2B collaboration, or B2B direct connect. This setting will only suppress the consent prompt if the specified tenant checks this setting for outbound access as well.

[Learn more](#)

Automatically redeem invitations with the tenant Contoso.

Save   Discard

# Lack of scoping and profiles



Currently one policy to rule them all.....

# Passkey profiles soon in public preview!

Microsoft 365 Message Center Archive

Home Merill.Net Entra.News

[Share](#) [Edit](#) [Delete](#)

## MC1097225 - Microsoft Entra ID: Upcoming changes to support passkey profiles in the authentication methods policy (preview)

Message ID	MC1097225
Service	Microsoft Entra
Published	Jun 17, 2025
Tag	Major change Feature update User impact Admin impact Retirement

### Summary

In November 2025, Microsoft Entra ID will expand the passkey (FIDO2) authentication methods policy to support passkey profiles in public preview, allowing group-based control over configurations. The rollout will start mid-October 2025 and complete by mid-November 2025. No admin action is required before the rollout.

### More information

In November 2025, we will expand the passkey (FIDO2) authentication methods policy in Microsoft Entra ID to support passkey profiles in public preview. This update will enable granular, group-based control over passkey configurations and introduce new API schema changes.

**When this will happen:**

Public Preview (Worldwide, GCC, GCC High, DoD): We will begin rolling out mid-October 2025 and expect to complete by mid-November 2025.

We will update this message when the plan for General Availability is finalized.

**How this will affect your organization:**



**End-user  
confusion**

Overview

Security info

Devices

Password

Organizations

Settings &amp; Privacy

Recent activity

## Security info

These are the methods you use to sign into your account or reset your password.

You're using the most advisable sign-in method

Sign-in method when most advisable is unavailable: Microsoft Authenticator

Add sign-in method

Password

Microsoft Authenticator  
Passwordless sign-in

Hardware token

Passkey  
Microsoft Authenticator

Lost device? [Sign out everywhere](#)

### Add a sign-in method



#### Passkey in Microsoft Authenticator

Sign in with your face, fingerprint, PIN



#### Security key or passkey

Sign in with your face, fingerprint, PIN or security key



#### Security key

Sign in using a USB, Bluetooth, or NFC device



#### Microsoft Authenticator

Approve sign-in requests or use one-time codes



#### Hardware token

Sign in with a code from a hardware token



#### Phone

Get a call or text to sign in with a code



#### Email

Receive a code to reset your password



Windows Security



## Sign in with your passkey

To sign in to "login.microsoft.com", choose a device with a saved passkey.



iPhone, iPad, or Android device

More choices



iPhone, iPad, or Android device



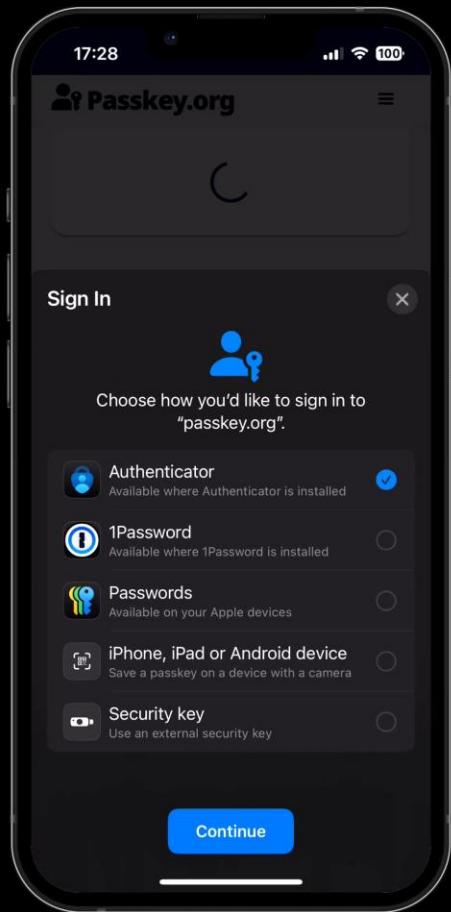
Security key

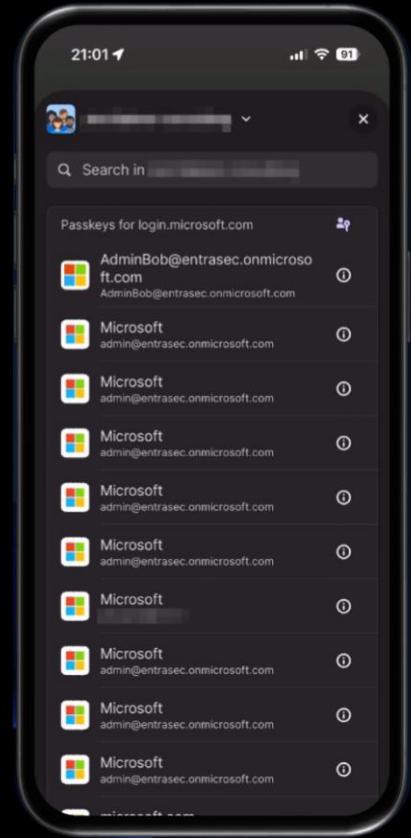


This Windows device

Next

Cancel





- Device-code phishing
- Malware
- Abuse onboard & recovery process



Hackers will go after tokens instead  
(post-auth attacks)

# Strengthen onboarding & recovery process



Trusted  
device



Trusted  
location



Temporary  
Access Pass

The screenshot shows the Microsoft My Access portal interface. At the top, there's a navigation bar with the 'CONTOSO demo' logo, 'My Access' dropdown, a search bar ('Search packages by name, description or resources'), and user profile icons.

The main area is titled 'Access packages' with the sub-instruction: 'Access groups and teams, SharePoint sites, applications, and more in a single package. Select from the following packages, or search to find what you're looking for.'

A sidebar on the left contains the following navigation items:

- Overview
- Access packages** (selected)
- Request history
- Approvals
- Access reviews

---

- My Account
- My Apps
- My Groups

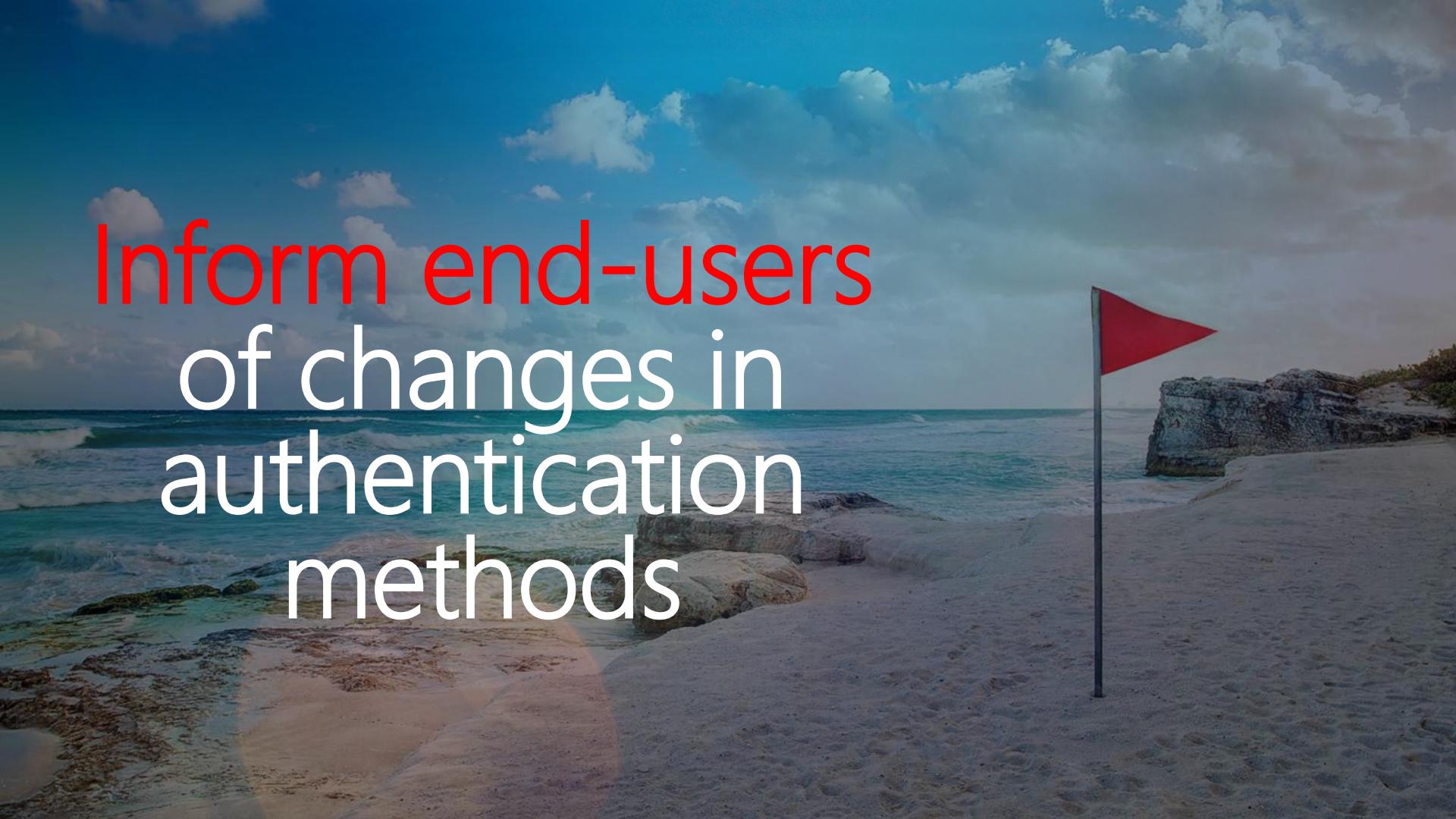
---

- Give feedback

The 'Access packages' section has tabs for 'Available (2)', 'Active (0)', and 'Expired (0)'. The 'Available' tab is selected, showing the following table:

Name ↑	Description	Resources	Actions
Exchange Admin Role	Request Exchange Admin Role	Exchange Administrator	Request
Temporary Access Pass	Temporary Access Pass		Request

# Request Temporary Access Pass on behalf of users

A photograph of a tropical beach at sunset. The sky is filled with large, white clouds against a blue and orange backdrop. In the foreground, there's a sandy beach with some rocks and low tide pools. On the right side, a red triangular flag stands in the sand. The ocean waves are visible in the background.

Inform end-users  
of changes in  
authentication  
methods



## New passkey added to your account



---

If you didn't add a passkey, someone might be using your account. Check and secure your account now.

[Check activity](#)

You can also see security activity at  
<https://myaccount.google.com/notifications>

You received this email to let you know about important changes to your Google Account and services.

© 2025 Google Ireland Ltd., Gordon House, Barrow Street, Dublin 4, Ireland



<https://janbakker.tech/microsoft-365-end-user-notifications-for-changes-in-authentication-methods/>

Contoso Electronics Outlook Search

Home View Help

New mail Delete Archive Report Sweep Move to Quick steps Read / Unread ...

Favorites

- Inbox 1
- Sent Items
- Drafts
- Add favorite

Inbox ★

Contoso | Alerts Security notification for Adele Vance 8:06 AM You recently changed your authentication methods

Contoso | Alerts To: Adele Vance Cc: Miriam Graham

Reply Reply all Forward Thu 2/22/2024 8:06 AM

You recently changed your authentication methods

We have been notified of the following action: Admin registered security info on 2/22/2024 7:01 AM.

If you initiated this, no action is required.

If this event does not look familiar, please report it now.

**Activity:** Admin registered security info  
**Details:** Admin registered temporary access pass method for user  
**Time:** 2/22/2024 7:01 AM  
**InitiatorUPN:** admin@M365x341716.onmicrosoft.com  
**IP-Address:** [REDACTED]

Instructions

- Review your account activity in [Microsoft Security Info](#).
- If you do not recognize this action, report it immediately and take action:
  - Inform your manager (reply in cc)
  - Delete any authentication method you don't know.

Information and Support

- Technical Assistance - Contact Helpdesk support services

Do NOT reply to this email. This is an unmonitored mailbox.  
For more help, contact [The A-Team](#)

Facilitated by

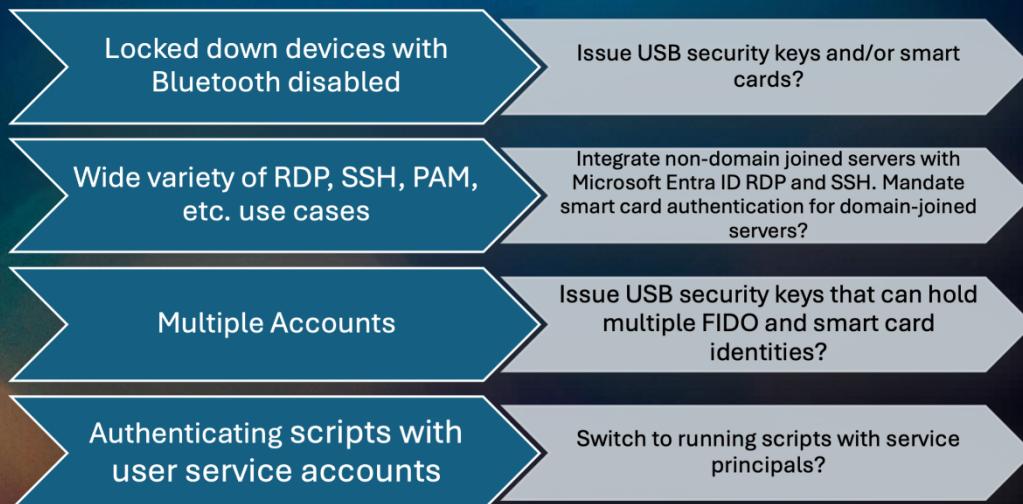
**JANBAKKER.TECH**  
sharing is caring

# Start today!



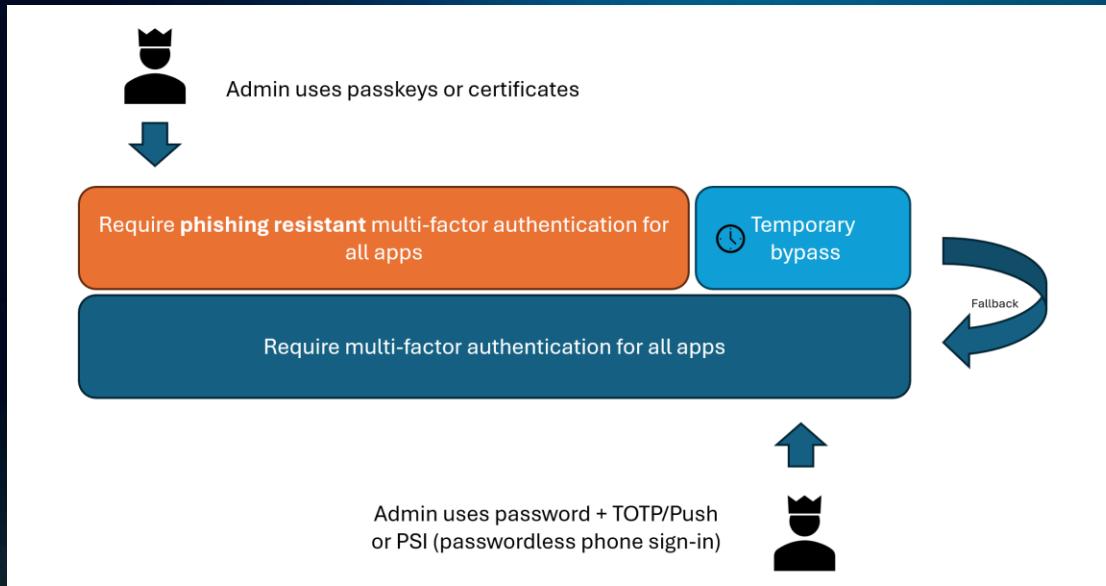
# IT pros/DevOps workers

Considerations for specific **personas** in a phishing-resistant passwordless authentication deployment in Microsoft Entra ID



<https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-plan-persona-phishing-resistant-passwordless-authentication#frontline-workers>

# Entra/Azure Admins should be phishing resistant by now



<https://janbakker.tech/temporary-exclusions-for-conditional-access-using-pim-for-groups/>

# Passkey enrolled? Enforce it!

The screenshot shows the Microsoft Entra admin center interface. The left sidebar navigation includes Overview, Users, Groups, Devices, Applications, Protection, Identity Governance, External Identities, Show more, Protection, Identity Protection, Conditional Access, Authentication methods, Password reset, Custom security attributes, Risky activities, Show more, Identity Governance, Verified ID, Permissions Management, Global Secure Access, and Learn & support.

The main content area displays the "Conditional Access | Authentication strengths" page under "Microsoft Entra ID". The navigation bar at the top shows Home > EntraSec Labs > Conditional Access. The page title is "Conditional Access | Authentication strengths".

Key elements on the page include:

- A "New authentication strength" button and a "Refresh" button.
- A "Type: All" dropdown and a "Authentication methods: All" dropdown.
- A "Reset filters" link.
- A table with columns: Authentication strength, Type, and Authentication methods. It lists:
  - Multifactor authentication (Built-in, Windows Hello For Business and 1 other method)
  - Passwordless MFA (Built-in, Windows Hello For Business and 3 other methods)
  - Phishing-resistant MFA (Built-in, Windows Hello For Business and 2 other methods)
- A "Classic policies" section.
- A "Monitoring" section with "Sign-in logs" and "Audit logs" links.
- A "Troubleshooting + Support" section with a "New support request" link.

A modal window titled "View Authentication Strength" is open on the right side, listing authentication flows:

Name	Type	Description
Phishing-resistant MFA	Built-in	Include authentication methods that are phishing-resistant like Passkeys (FIDO2) and Windows Hello for Business
Windows Hello for Business	Built-in	
OR		
Passkeys (FIDO2)		
OR		
Certificate-based Authentication (Multifactor)		

# Chicken & egg problem



# Conditional Access Authentication Strengths

Policy	Target	Device Platforms	Grant control – Custom Authentication Strength	AAGUIDS
Bootstrap & Recovery policy	Register security information	N/A.	Password + Microsoft Authenticator (Push Notification) <b>OR</b> Temporary Access Pass (One-time use) <b>OR</b> Temporary Access Pass (Multi-use)	N/A.
Secure Desktop Apps	All resources	<b>Exclude:</b> iOS Android	Passkeys (FIDO2)*	Microsoft Authenticator (iOS) Microsoft Authenticator (Android)
Secure Mobile Apps	All resources	<b>Include:</b> iOS Android	Passkeys (FIDO2) <b>OR</b> Temporary Access Pass (One-time use) <b>OR</b> Temporary Access Pass (Multi-use)	Microsoft Authenticator (iOS) Microsoft Authenticator (Android)

# Conditional Access Authentication Strengths

## Assignments

### User

Admin Bob

✓ Matched



### Resource

Microsoft Graph

✓ Matched



All resources included

### Audience ⓘ

### Application Id

Azure Credential Configuration Endpoint Service

ea890292-c8c8-4433-b5ea-b09d0668e1a6

Windows Azure Active Directory

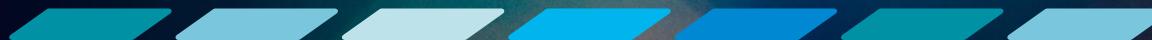
00000002-0000-0000-c000-000000000000

# Avoid Authentication strength Conditional Access policy loops

Use different strengths for desktop and mobile



To avoid costs, first register, then enforce



Test all use cases, not just the happy flow



Have proper guidance for your users



# What's next?

## How this will affect your organization:

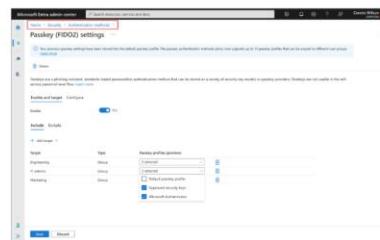
After this rollout, you'll be able to apply different passkey configurations per user group. For example, you will be able to:

Allow the use of specific FIDO2 security key models for user group A

Allow the use of passkeys in Microsoft Authenticator for user group B

**Important:** If your organization modifies the passkey policy via the Microsoft Azure or Entra portal during preview, the new schema will take effect. If you continue using Graph API or third-party tools to modify the policy, the schema will not change until General Availability.

These new settings will be available at Microsoft 365 admin center > Home > *Security* > *Authentication methods* > *Passkey (FIDO2) settings*:



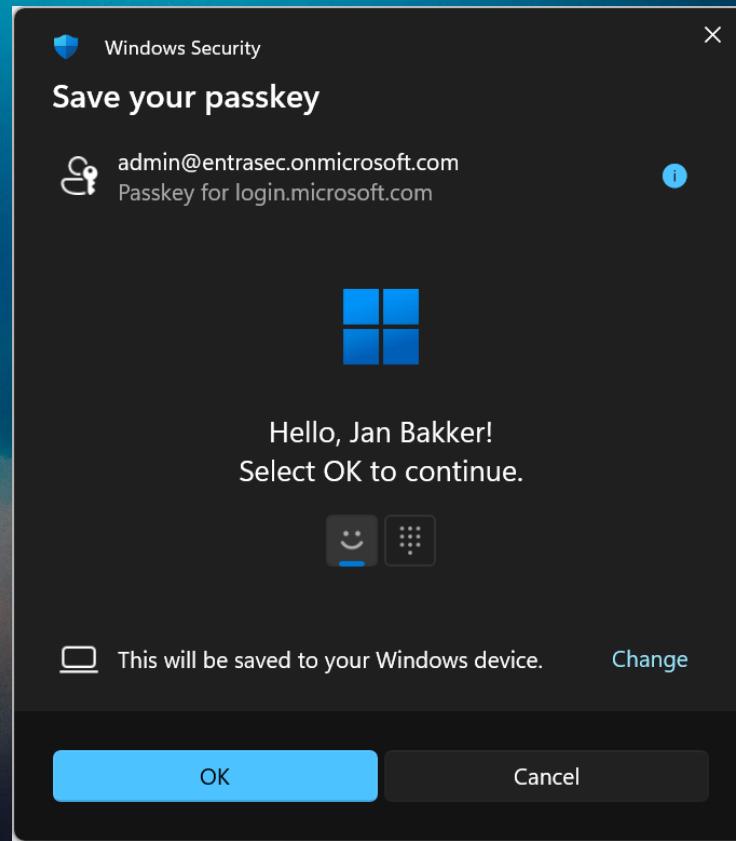
As part of this update in November 2025, we will start accepting any WebAuthn-compliant security key or passkey provider when *Enforce attestation* is disabled. This will allow a wider range of security keys and passkey providers to be accepted for registration and authentication in Microsoft Entra ID. To compare this upcoming update with the current behavior, refer to Microsoft Entra ID attestation for FIDO2 security key vendors.

## What you need to do to prepare:

This rollout will happen automatically by the specified dates with no admin action required before the rollout. You may want to review your current passkey configuration, notify your admins about this change, and update internal documentation.

Learn more about passkeys in Microsoft Entra ID: Enable passkeys for your organization - Microsoft Entra ID | Microsoft Learn (will be updated before rollout)

# What's next?



# What have we learned today?

Passkeys are not new

Passkey will replace passwords

We're just getting started

We really need passkey profiles!

Enrollment can be hard. Auth app first!

End-users need guidance

Think persona-based

Have different passkeys for different platforms

Get started ASAP

?

Questions?



# THANK YOU