Passkeys in Microsoft 365

The Good, the Bad and the Ugly

Jan Bakker

Oktober 2025

aka.ms/janbakker

Find my contact details here

Jan Bakker

Solution Architect Security & IAM

MVP Microsoft® Most Valuable Professional

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

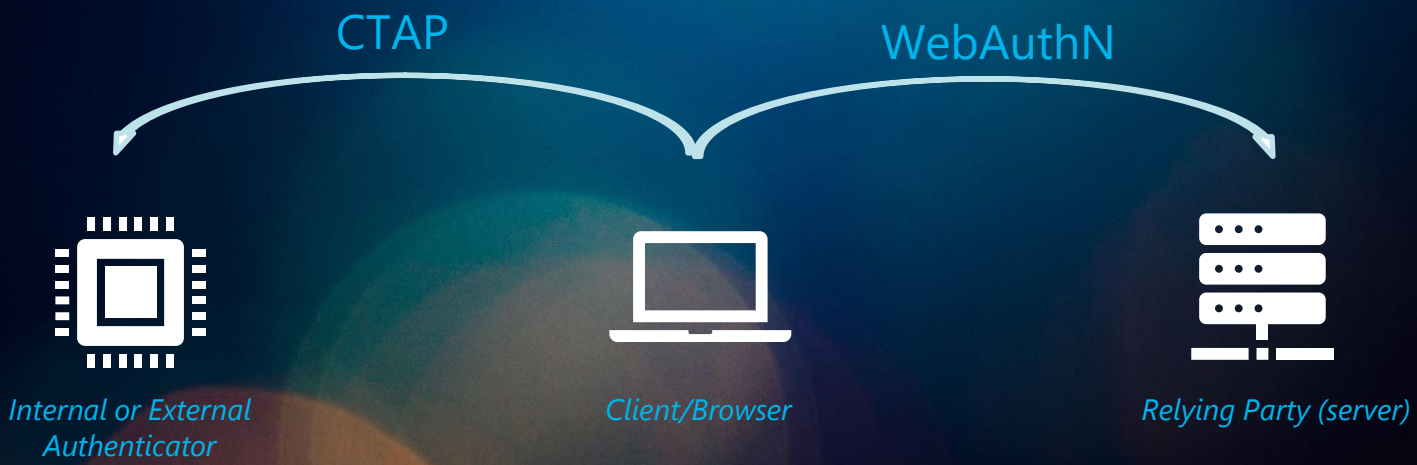
can store

passkeys

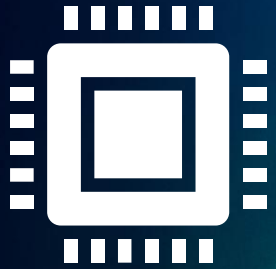
~~Passwords~~

keys

FIDO2 standard



Authenticator types



Platform Authenticator

Touch ID
Face ID
Windows Hello

Roaming Authenticator

Security keys
(USB/NFC/BTE)

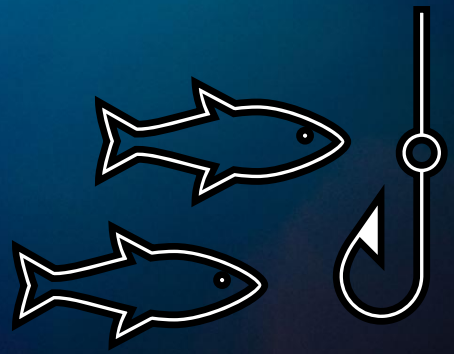
Most of your users already carry a platform authenticator in their pockets every day

Faster & Easier

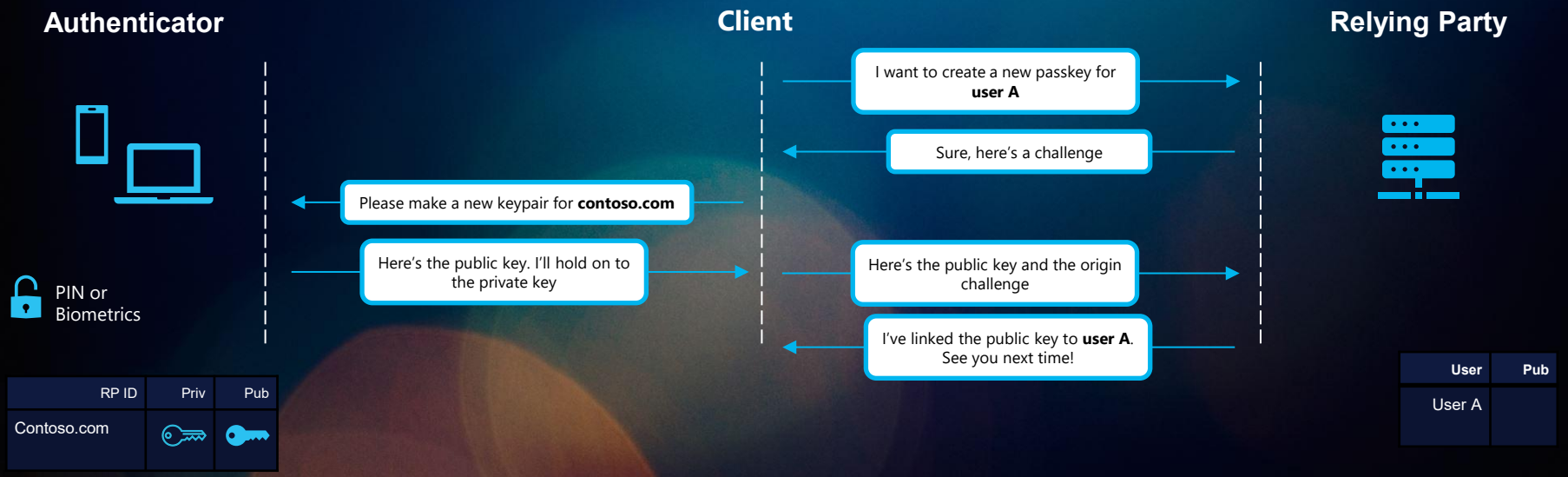
More Secure

Passkey are built on PKI

Phishing Resistant



How passkeys work (Registration)



No more **passwords**
No more **shared secrets**
No more **AiTM attacks**

Where do we store our passkeys?


';--have i been pwned?
';--493531n

Device-bound passkeys

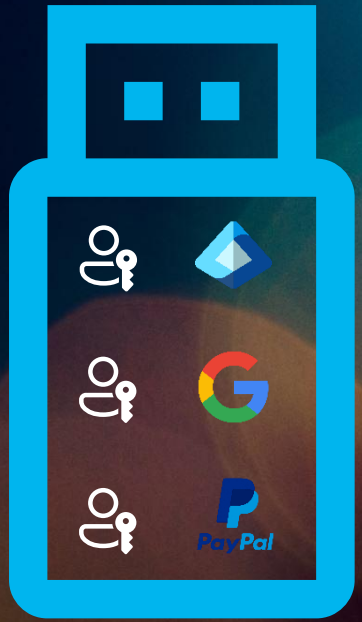
Bound to and used only on a single device

Synced passkeys

Stored securely in a credential manager and accessed across devices

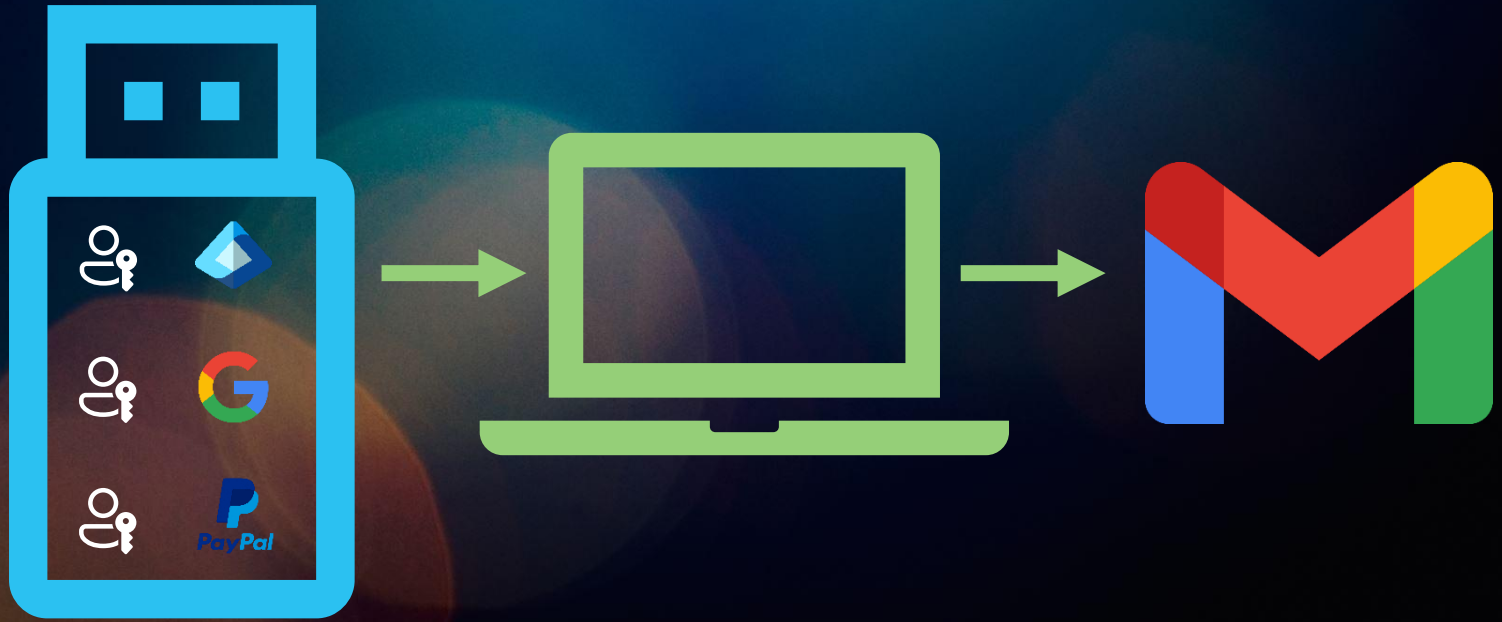
Device-bound passkeys

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



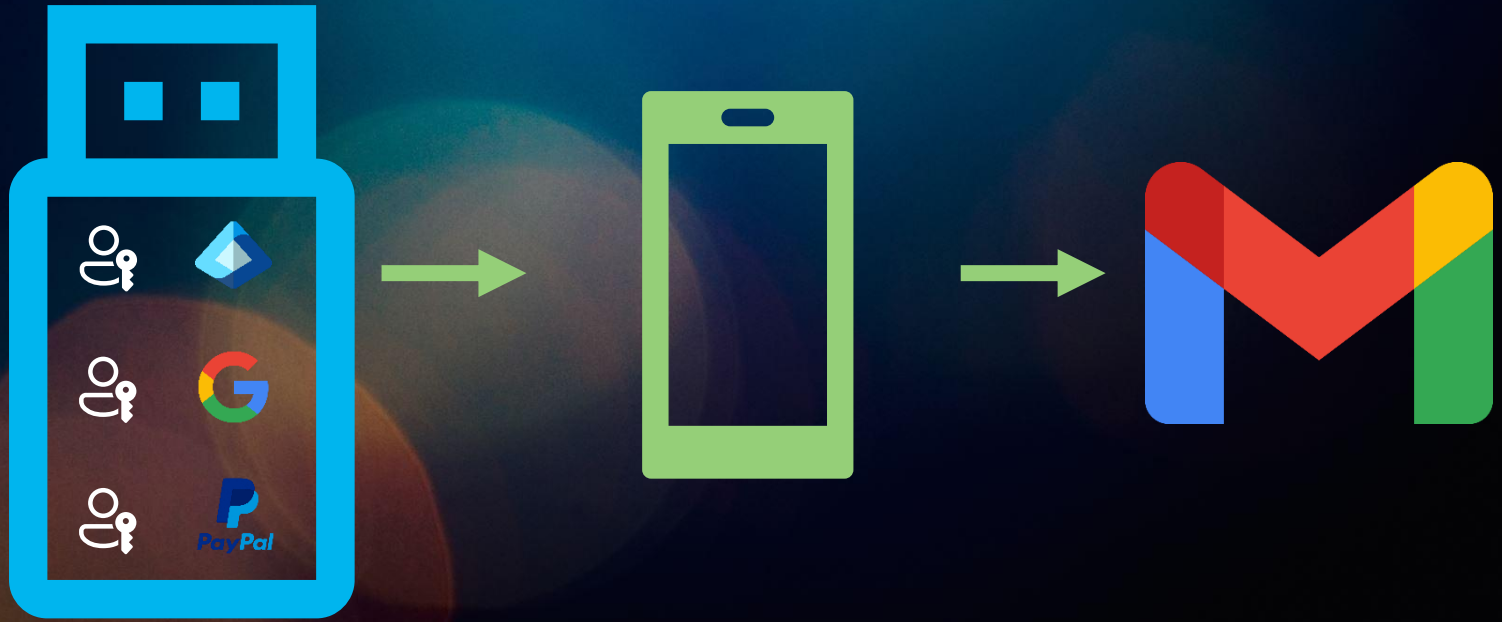
Device-bound passkeys

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



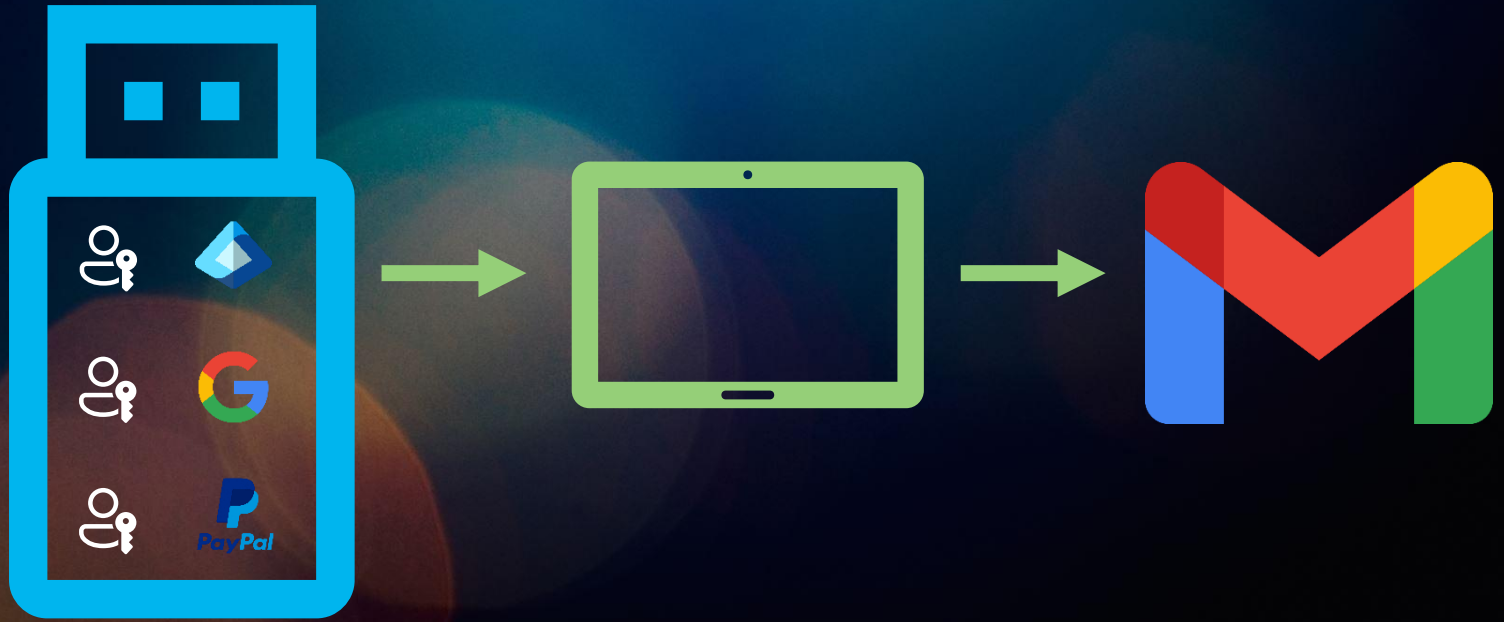
Device-bound passkeys

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



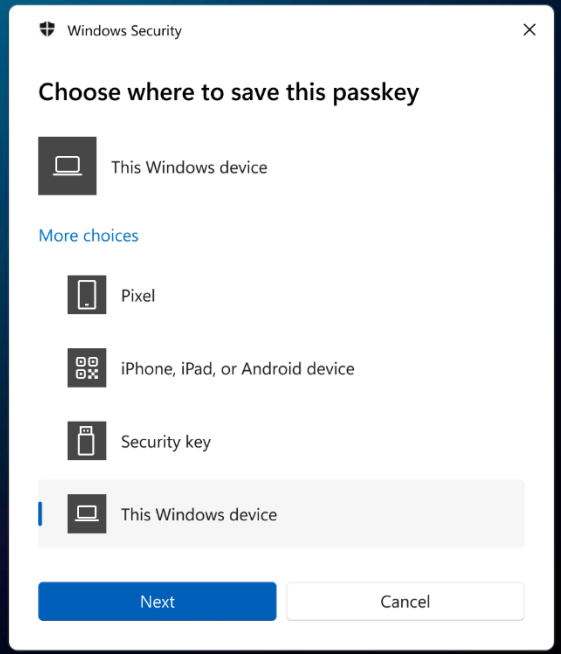
Device-bound passkeys

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

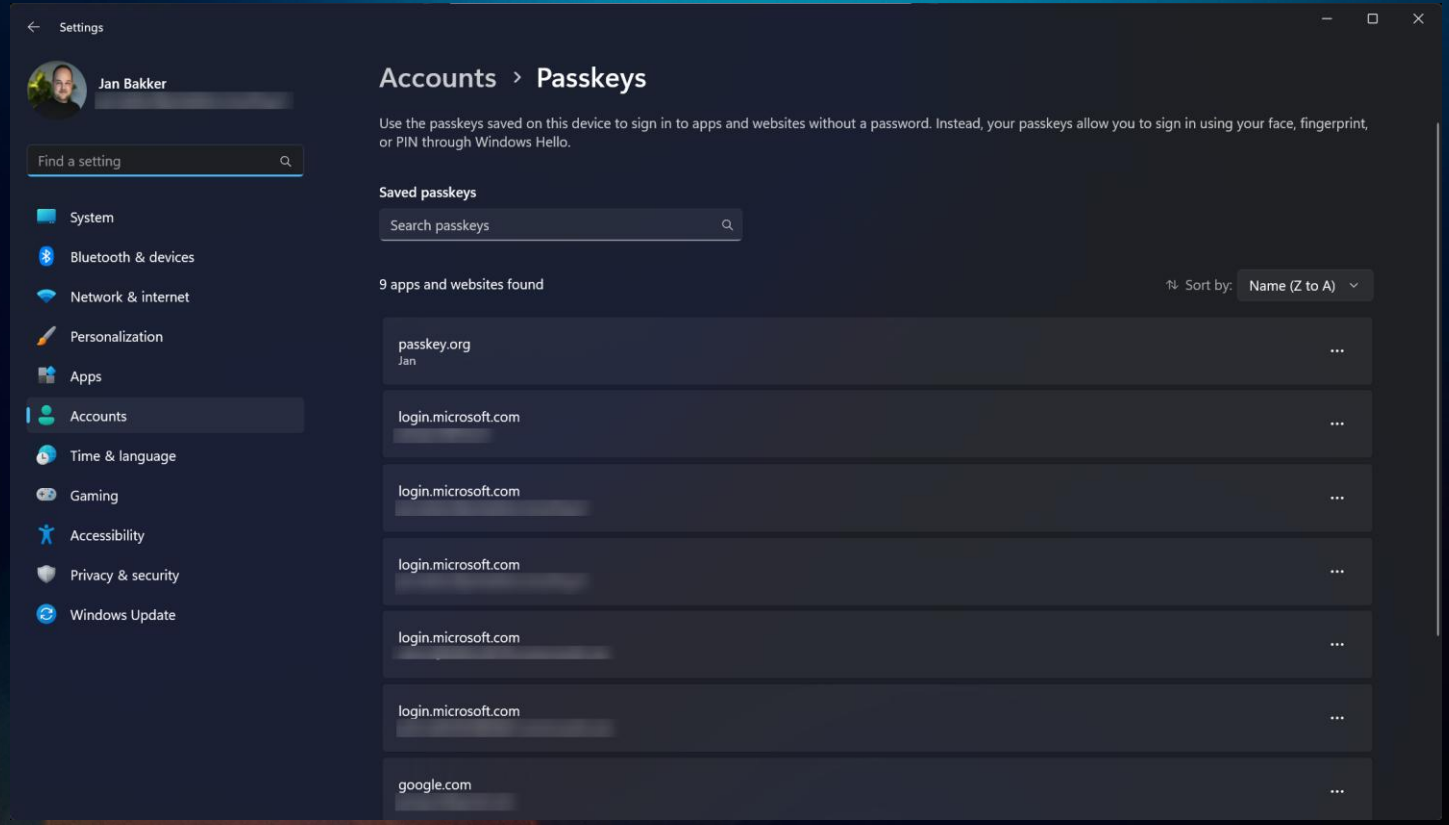


Support for passkeys in Windows

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
System
Bluetooth & devices
Network & internet
Personalization
Apps
Accounts
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
9 apps and websites found
Sort by: Name (Z to A)
passkey.org
Jan
login.microsoft.com
login.microsoft.com
login.microsoft.com
login.microsoft.com
login.microsoft.com
google.com

Microsoft Wallet

- Home
- Payment methods
- Passwords
- Personal info
- Order tracking
- Settings

Passwords

Add | Settings | Passkeys ...

Add or import passwords to your Wallet

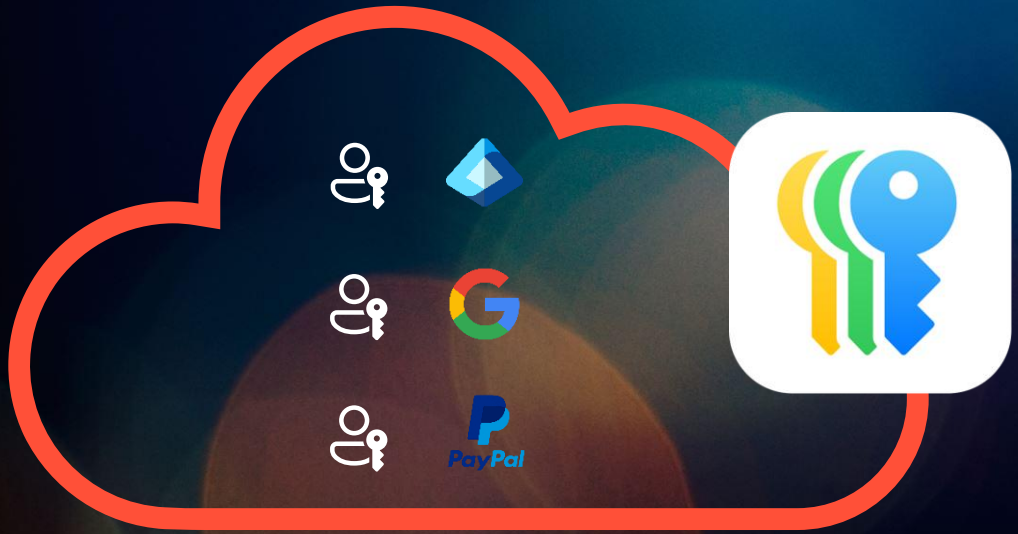
Improve your browsing and autofill experience when you add or import your passwords.

Import passwords

Satisfied with passwords?

Synced passkeys

Stored securely in a credential manager and accessed across devices.

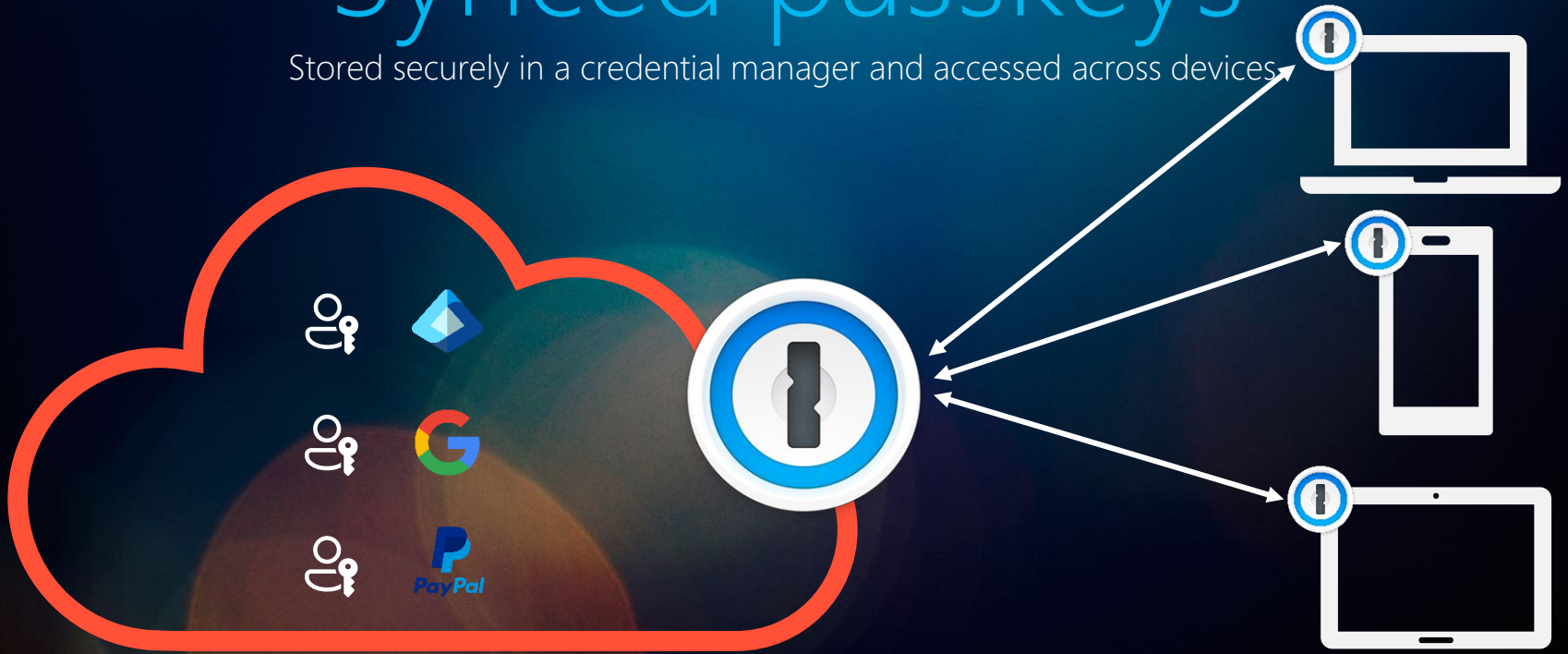


Synced passkeys

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	Service	Last Updated	Tag	Act by
MC920300 View in Message Center	Microsoft Entra	Jan 24, 2025 Published Oct 28, 2024	Major change Updated message Admin impact	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 & 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 & support

Home >

Authentication methods | Policies

Contoso - Microsoft Entra ID Security

Search
Manage
Policies
Password protection
Registration campaign
Authentication strengths
Settings
Monitoring
Activity
User registration details
Registration and reset events
Bulk operation results

Add external method (Preview) | Refresh | Got feedback?

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

Migration status: Complete (change)

Method	Target	Enabled
Passkey (FIDO2)	All users	Yes
	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 & 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 & support

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 & 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 & support

Home > Authentication methods | Policies >

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

YubiKey 4 (Series)	All	N/A	N/A
YubiKey FIPS (4 Series)	4.4	N/A	N/A
YubiKey 5 Series			
YubiKey 5 (USB-A, No NFC)	5.1	cb69481e-8ff7-4039-93ec-0a2729a154a8	Level 1
YubiKey 5 (USB-A, No NFC)	5.2, 5.4	ee882879-721c-4913-9775-3dfcce97072a	Level 1
YubiKey 5 NFC	5.1	fa2b99dc-9e39-4257-8f92-4a30d23c4118	Level 1
YubiKey 5 NFC	5.2, 5.4	2fc0579f-8113-47ea-b116-bb5a8db9202a	Level 1
YubiKey 5 NFC	5.7	a25342c0-3cdc-4414-8e46-f4807fca511c d7781e5d-e353-46aa-afe2-3ca49f13332a	Level 2
YubiKey 5C NFC	5.2, 5.4	2fc0579f-8113-47ea-b116-bb5a8db9202a	Level 1
YubiKey 5C NFC	5.7	a25342c0-3cdc-4414-8e46-f4807fca511c d7781e5d-e353-46aa-afe2-3ca49f13332a	Level 2
YubiKey 5 Nano	5.1	cb69481e-8ff7-4039-93ec-0a2729a154a8	Level 1
YubiKey 5 Nano	5.2, 5.4	ee882879-721c-4913-9775-3dfcce97072a	Level 1
YubiKey 5 Nano	5.7	19083c3d-8383-4b18-bc03-8f1c9ab2fd1b ff4dac45-ede8-4ec2-aced-cf66103f4335	Level 2
YubiKey 5C Nano	5.1	cb69481e-8ff7-4039-93ec-0a2729a154a8	Level 1
YubiKey 5C Nano	5.2, 5.4	ee882879-721c-4913-9775-3dfcce97072a	Level 1
YubiKey 5C Nano	5.7	19083c3d-8383-4b18-bc03-8f1c9ab2fd1b ff4dac45-ede8-4ec2-aced-cf66103f4335	Level 2
YubiKey 5C	5.1	cb69481e-8ff7-4039-93ec-0a2729a154a8	Level 1
YubiKey 5C	5.2, 5.4	ee882879-721c-4913-9775-3dfcce97072a	Level 1
YubiKey 5C	5.7	19083c3d-8383-4b18-bc03-8f1c9ab2fd1b ff4dac45-ede8-4ec2-aced-cf66103f4335	Level 2
YubiKey 5Ci	5.2, 5.4	c5ef55ff-ad9a-4b9f-b580-adebafe026d0	Level 1
YubiKey 5Ci	5.7	a02167b9-ae71-4ac7-9a07-06432ebb6f1c 24673149-6c86-42e7-98d9-433fb5b73296	Level 2

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

MichelvanVliet / Scripts Public

Scripts / Entra / Export-Fido2Info.ps1

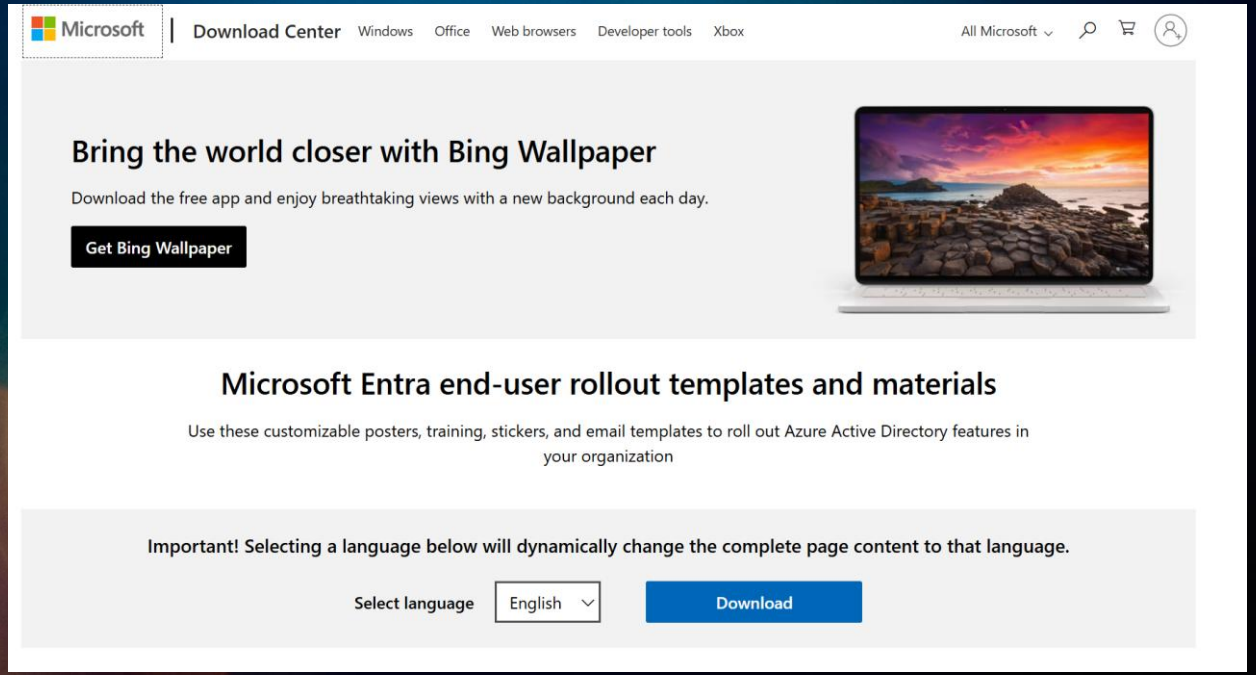
MichelvanVliet Update Export-Fido2Info.ps1 25d8d6c · 11 months ago History

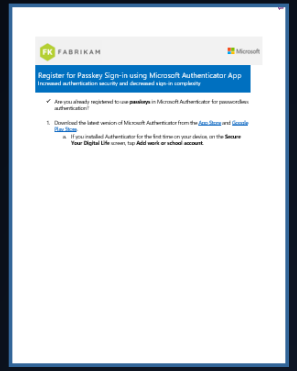
Code Blame 130 lines (110 loc) · 4.72 KB Raw

```
<#
    .SYNOPSIS
       Export all FIDO2 registration info for all users within an Entra OD tenant

    .DESCRIPTION
        PowerShell script to gather and export all FIDO2 registration information for all users to a .CSV file.

    .NOTES
        Requirements:
        - Microsoft Graph Powershell SDK (will be installed if not present)
        - Graph permissions:
                User.Read.All
                UserAuthenticationMethod.Read.All
                UserAuthMethod-Passkey.Read.All

    .PARAMETER CsvFile
        Specify the full output path and filename for the CSV report file.
        If not specified, the script will produce an report in the current folder using the following file name: "Fido2Registration_Report.csv".

    .PARAMATER Delimter
        Specify the delemiter character used for the CSV output file.
        If not specified, ";" will be used as delimiter.

    .EXAMPLE
        PS> .\Export-Fido2Info.ps1 -CsvFile "C:\Temp\Fido2Registration_Report.csv" -Delimiter ";"
```

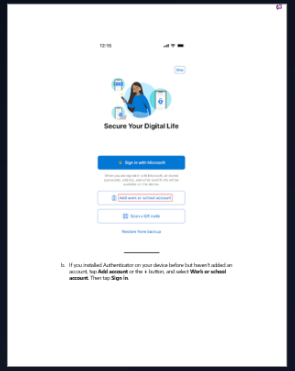
Passkey enrollment

Microsoft Entra end-user rollout templates and materials

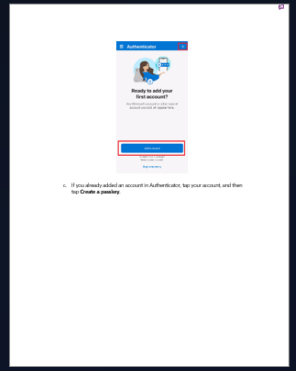




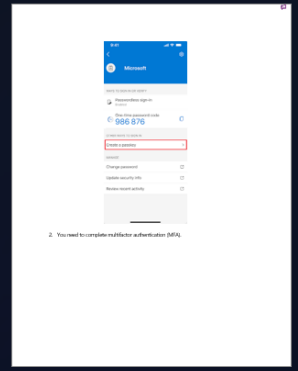
1



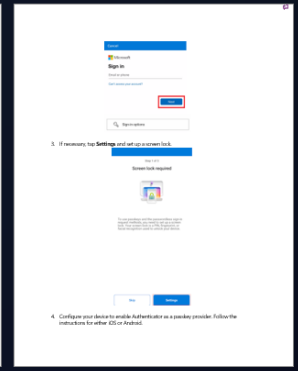
2



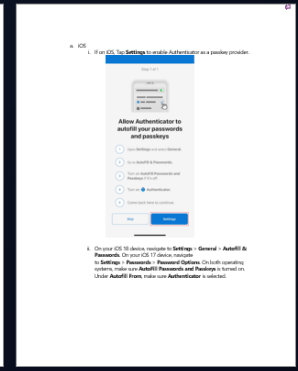
3



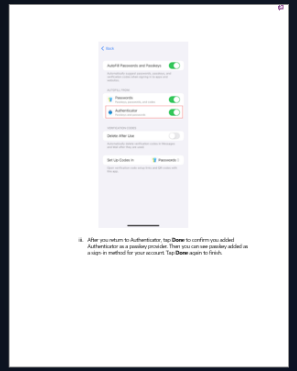
4



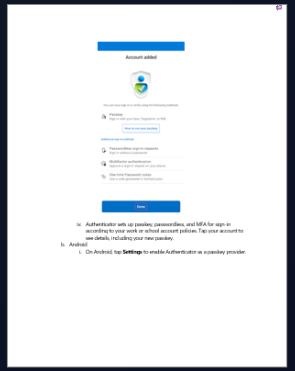
5



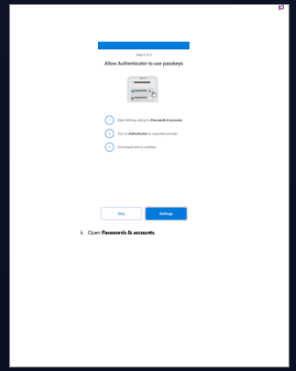
6



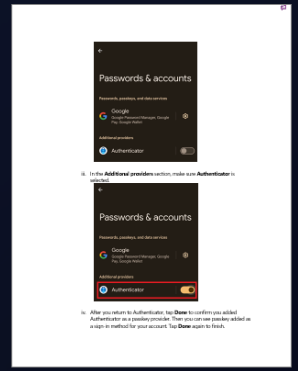
7



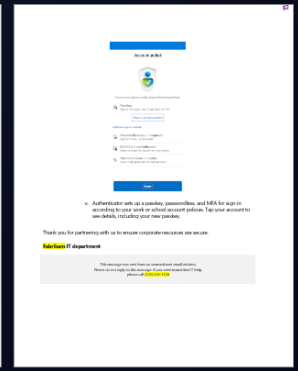
8



9



10



11

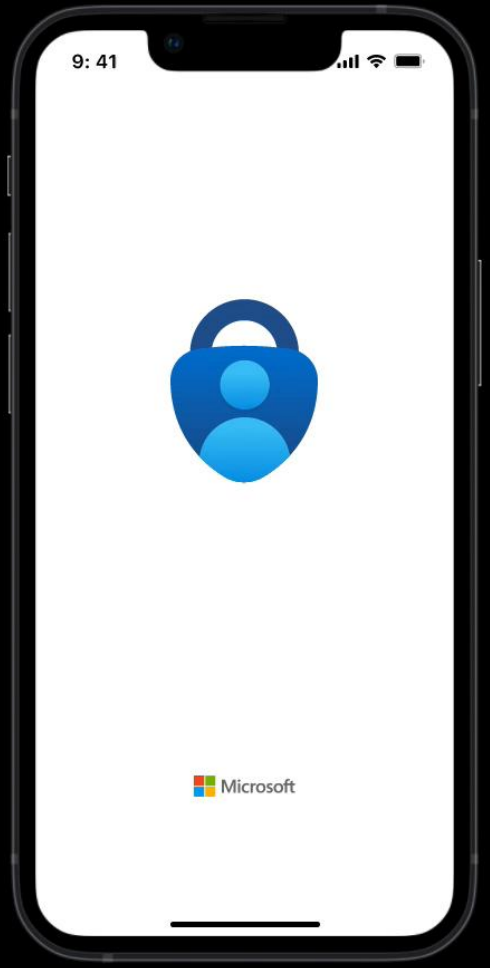
MFA is required for enrollment of strong auth methods

- Security key
- Windows Hello for Business
- Passkey in Auth App

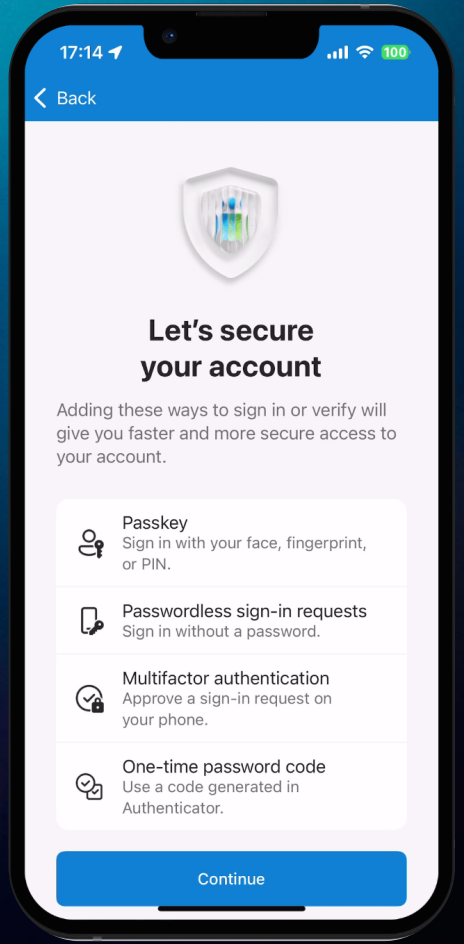
Temporary Access Pass

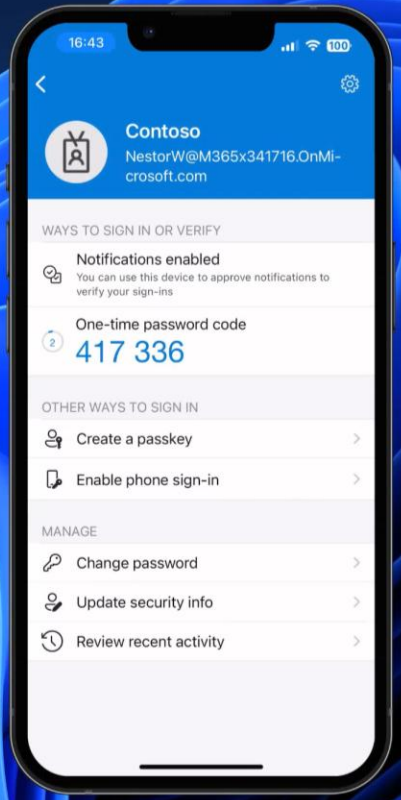
"The easiest and fastest way to add a passkey is to add it directly in the Authenticator app."

Register passkey in Authenticator App with Temporary Access Pass



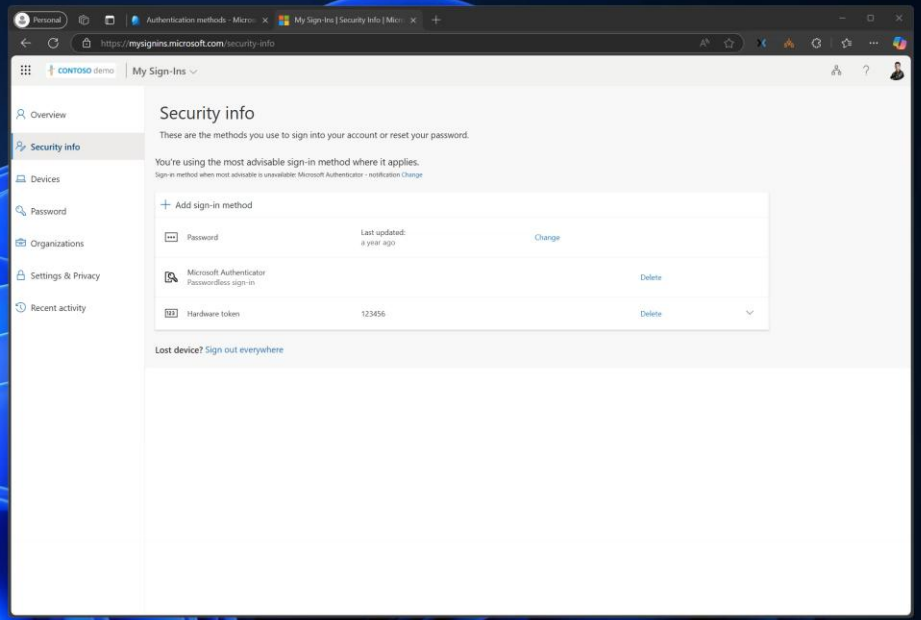
All the methods!

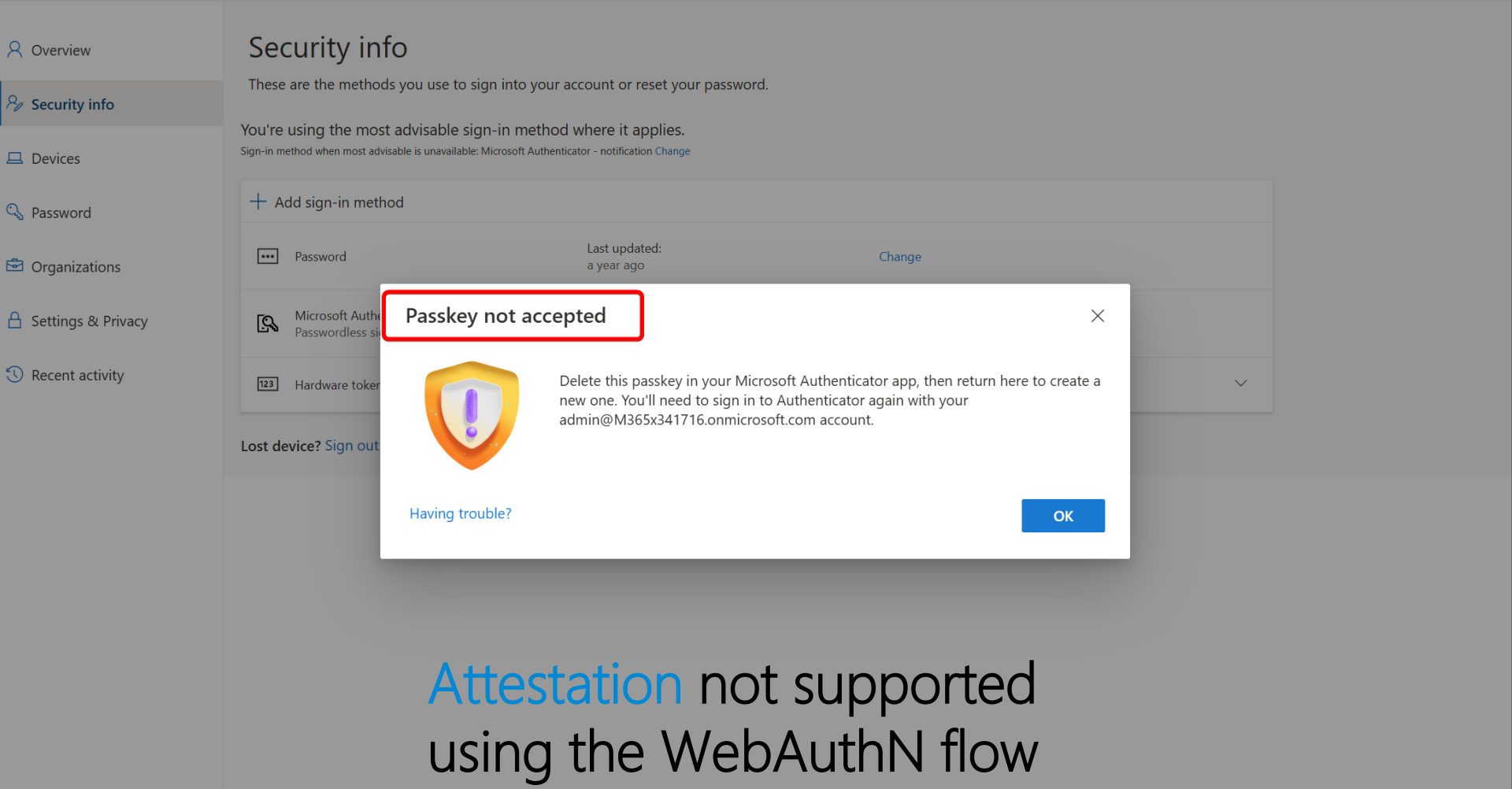




Register passkey for existing users with MFA

Cross-device registration of passkeys





Attestation not supported using the WebAuthN flow

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

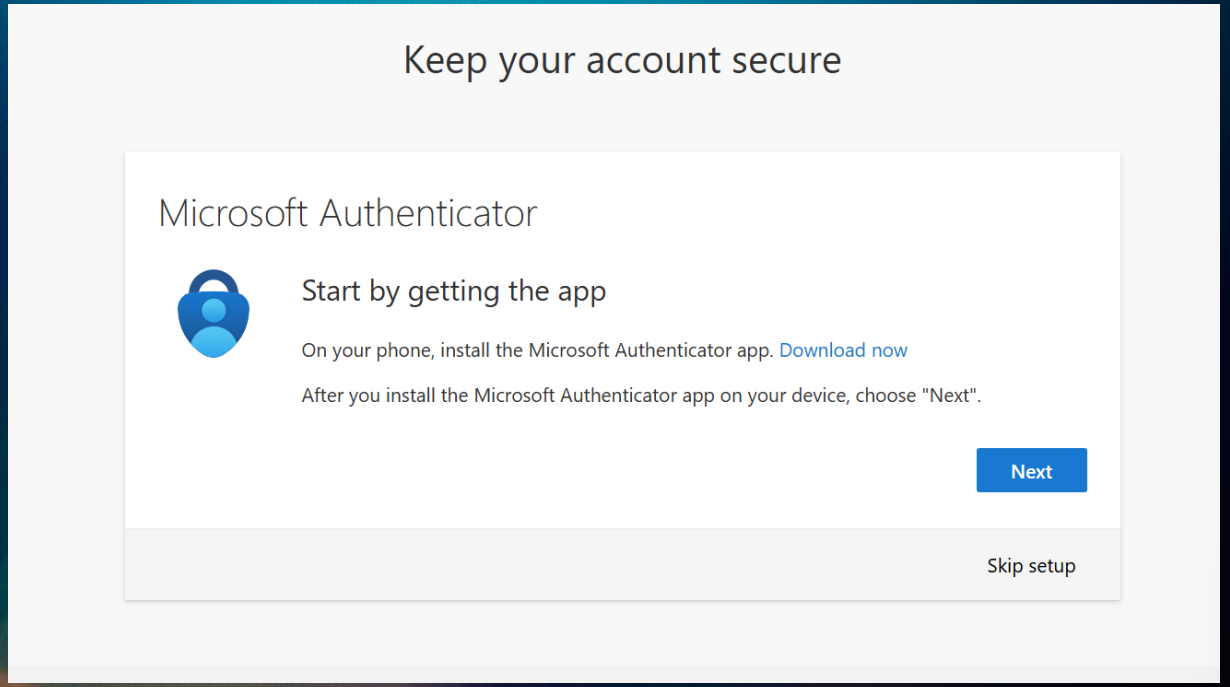
No resource was found matching this query

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": "4IHwPDQyTkO0C6t7DT9B7A2",
            "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"
        }
    ]
}
```



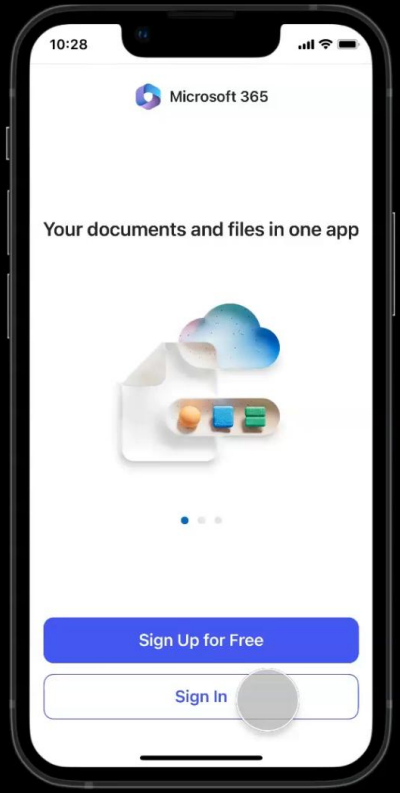
SelfServicePasswordReset

Self Service Password Reset

Method	Primary authentication	Secondary authentication
Windows Hello for Business	Yes	MFA[1]
Microsoft Authenticator push	No	MFA and SSPR
Microsoft Authenticator passwordless	Yes	No[2]
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

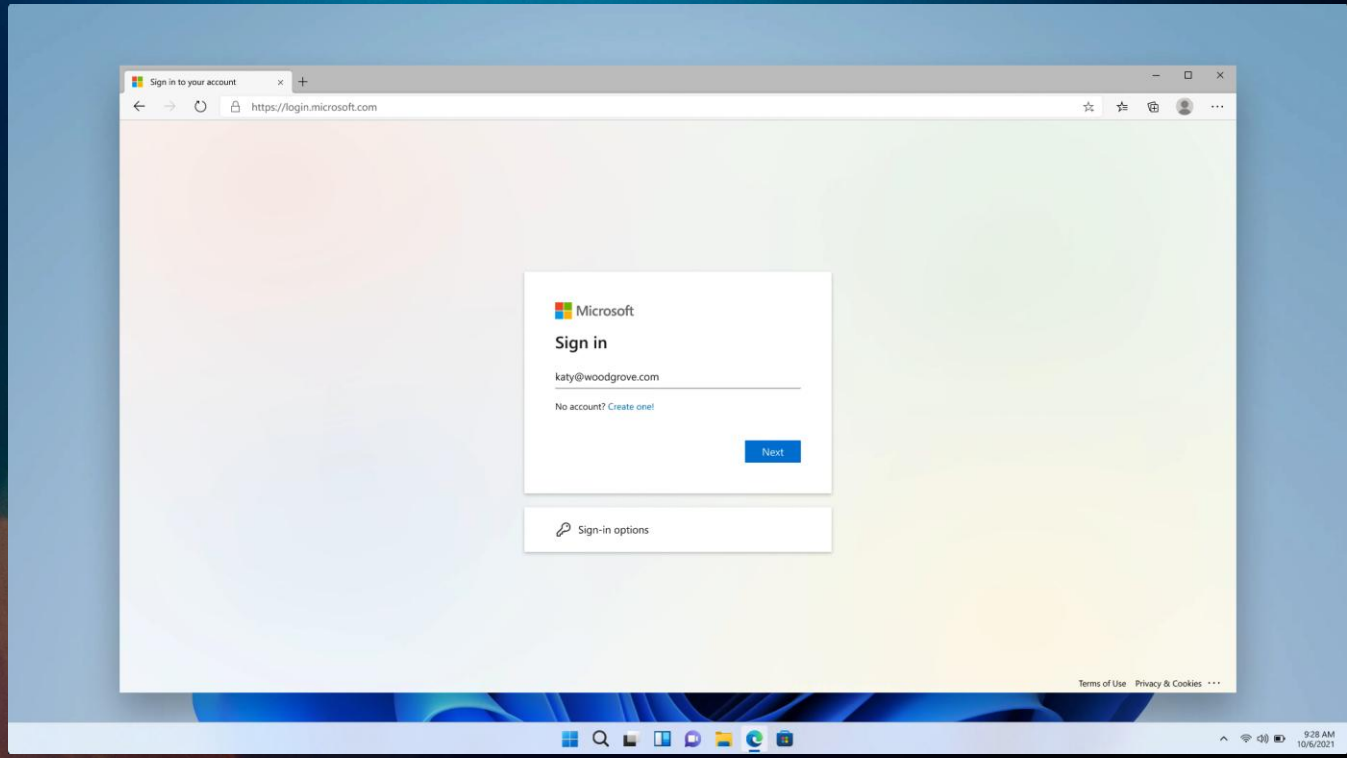

All set. Now let's use it!

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?

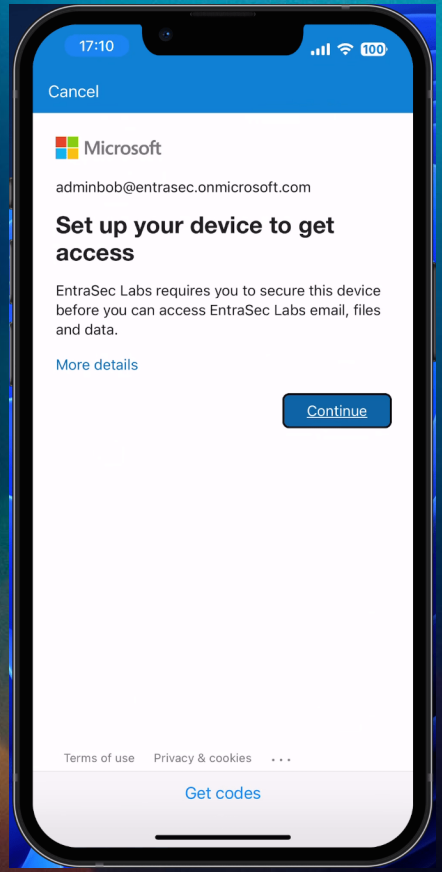
Store Entra ID passkeys in other credential providers like 1Passsword or Google Authenticator

Store 3rd 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
- [ ] Require authentication strength
- [ ] Require device to be marked as compliant
- [ ] Require Microsoft Entra hybrid joined device
- [ ] Require approved client app
  See list of approved client apps
- [ ] Require app protection policy
  See list of policy protected client apps
- [ ] Require password change

For multiple controls

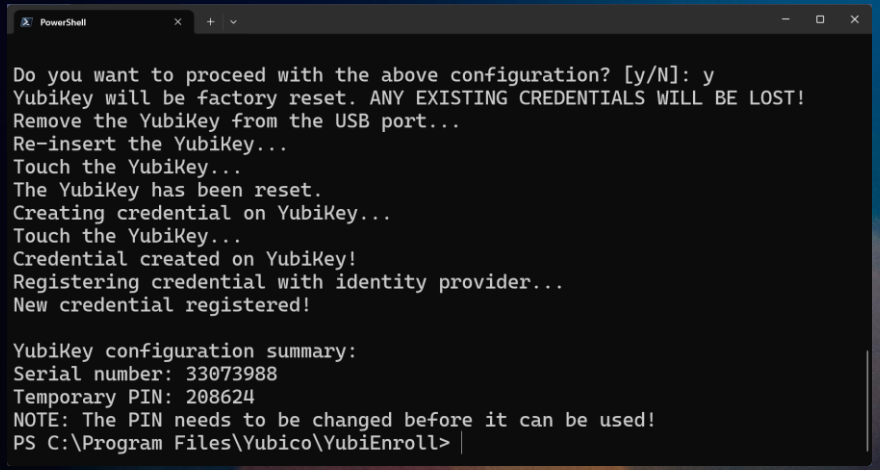
- (•) Require all the selected controls
- ( ) Require one of the selected controls

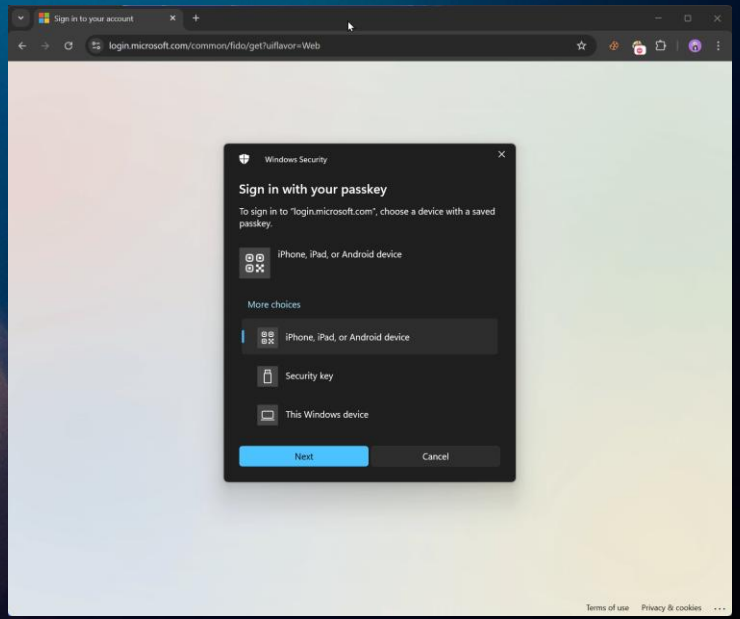
Passkey provisioning

(only supported for hardware security keys)

Learn how!

Enforce PIN complexity and change on first use

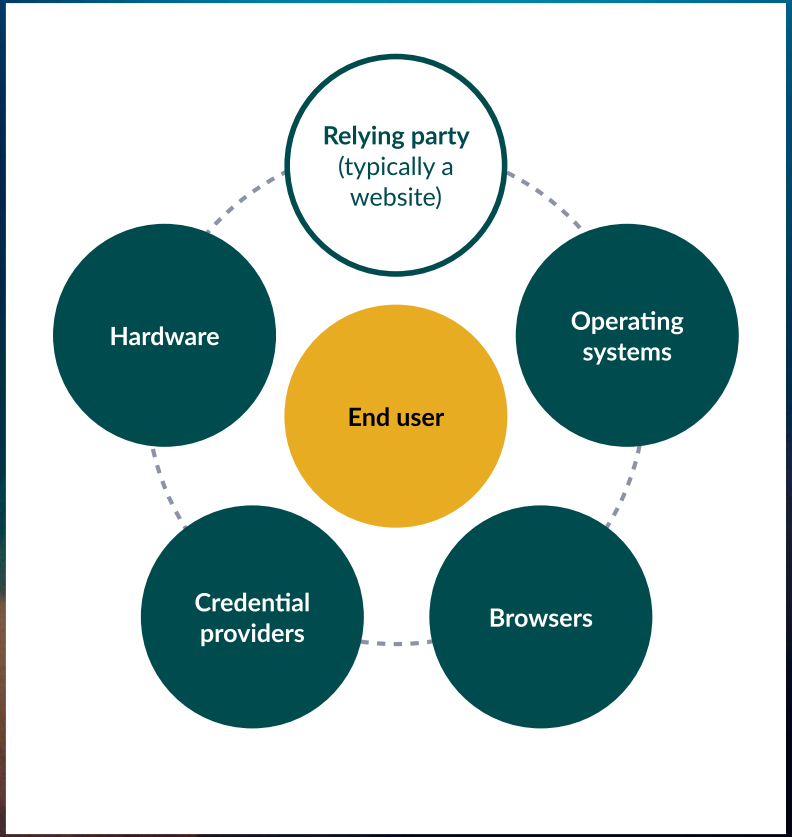




Are we there yet?

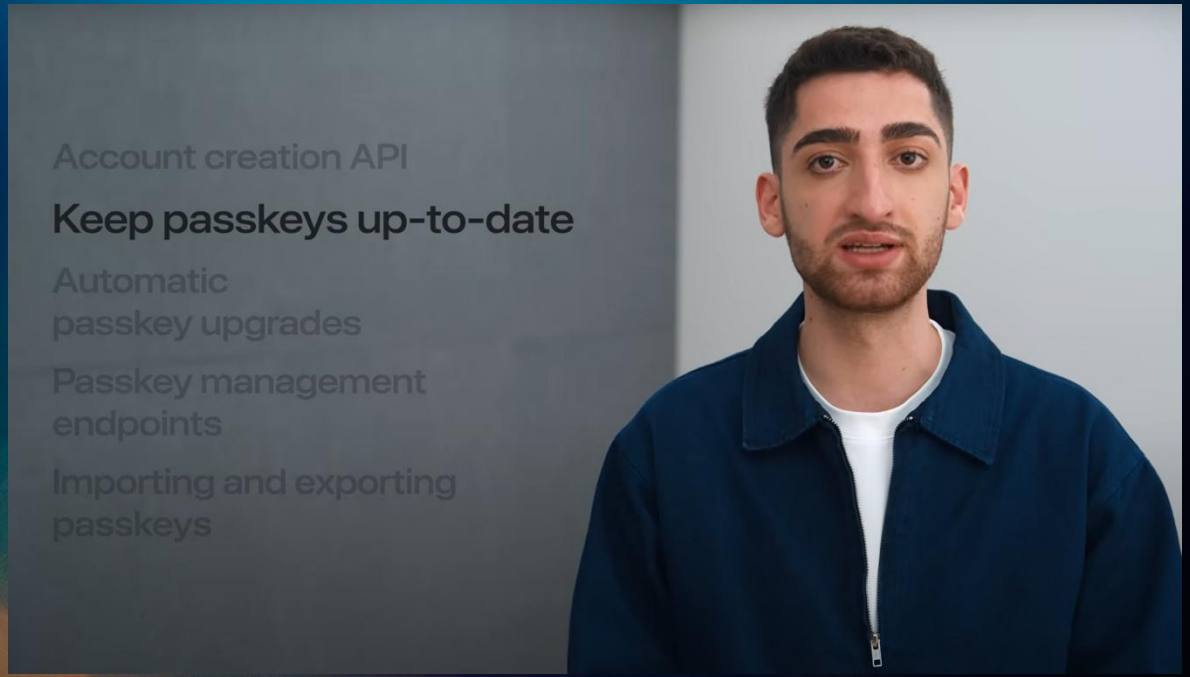

We are still in
the early stage
of passkeys

The API is there.....



WWDC25

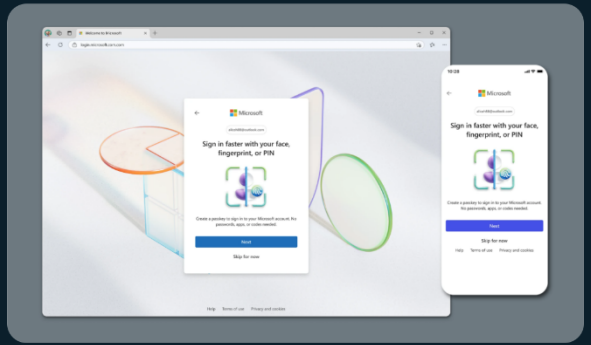
Passkey improvements by Apple



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.[3]
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

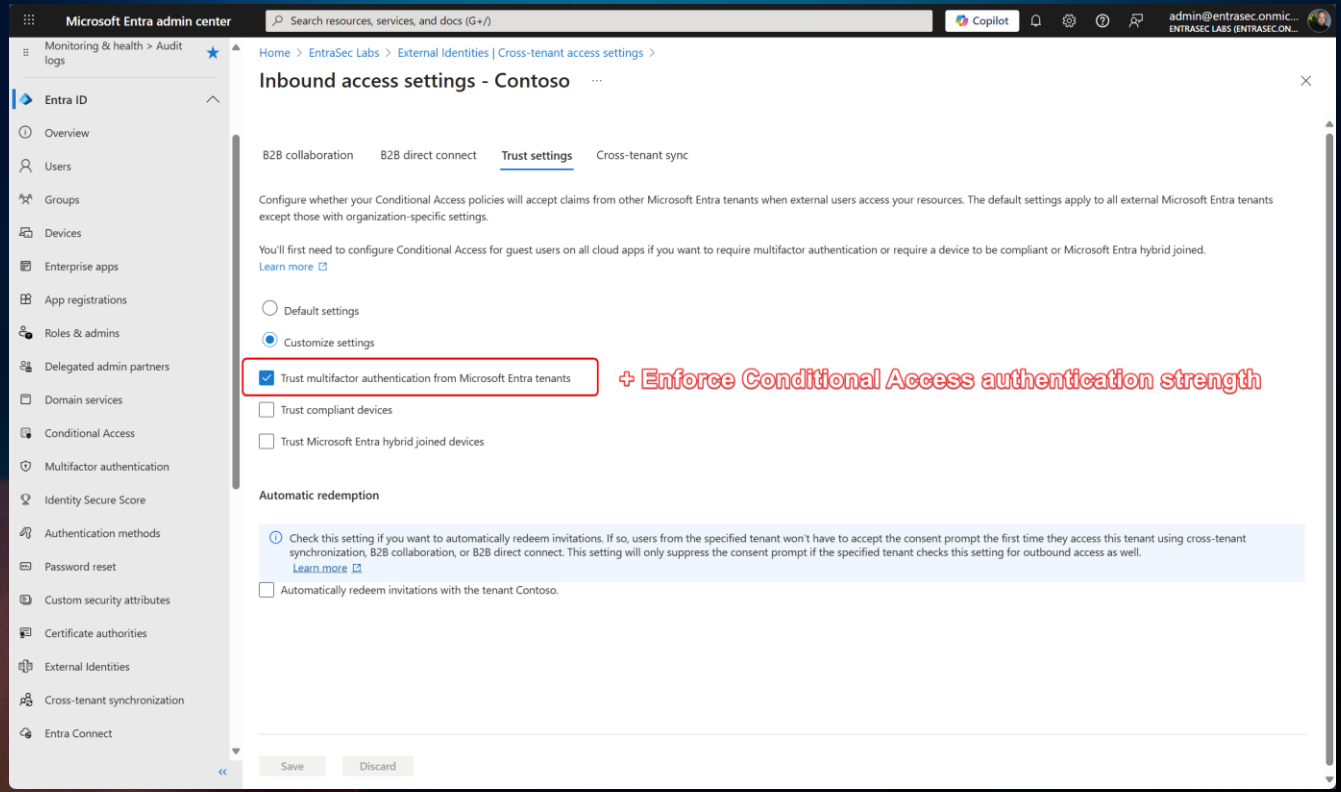
Why do I get prompted for PIN instead of biometric sign-in on my Android device?

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.

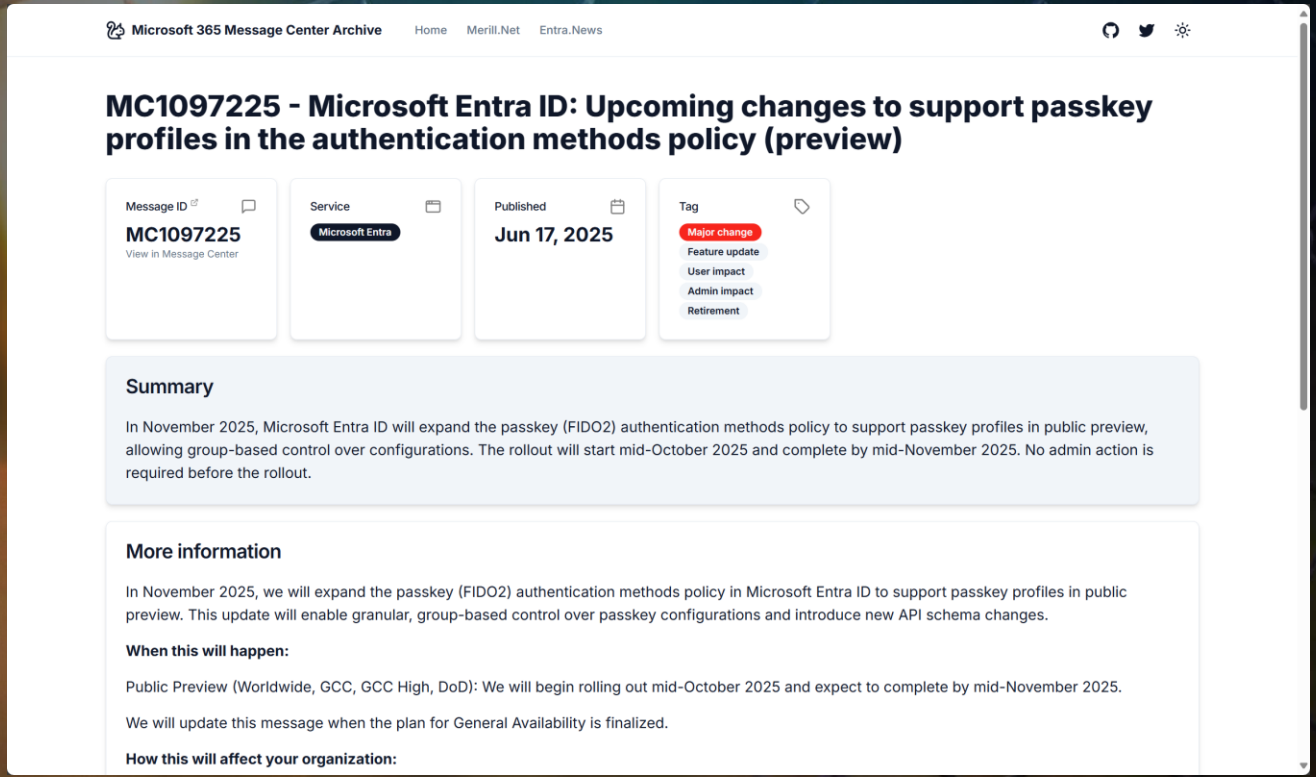
Does it work for External Guest Accounts?



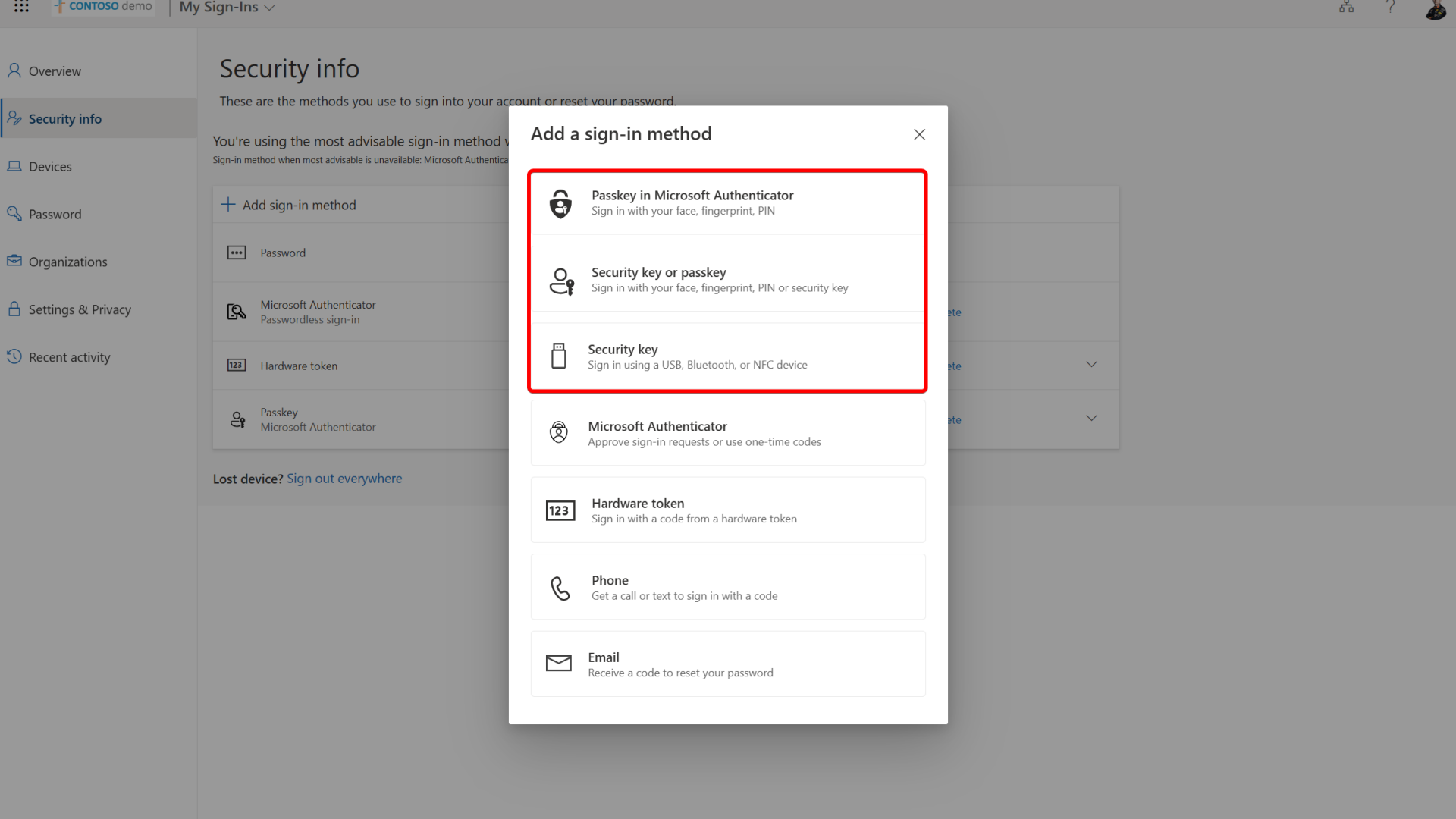
Lack of scoping and profiles

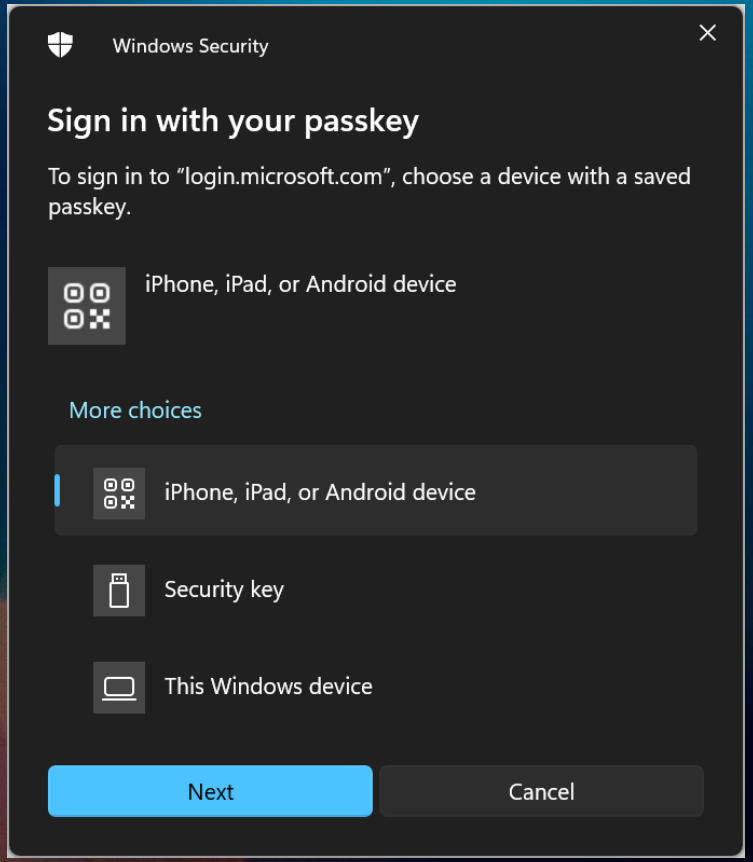
Currently one policy to rule them all.....

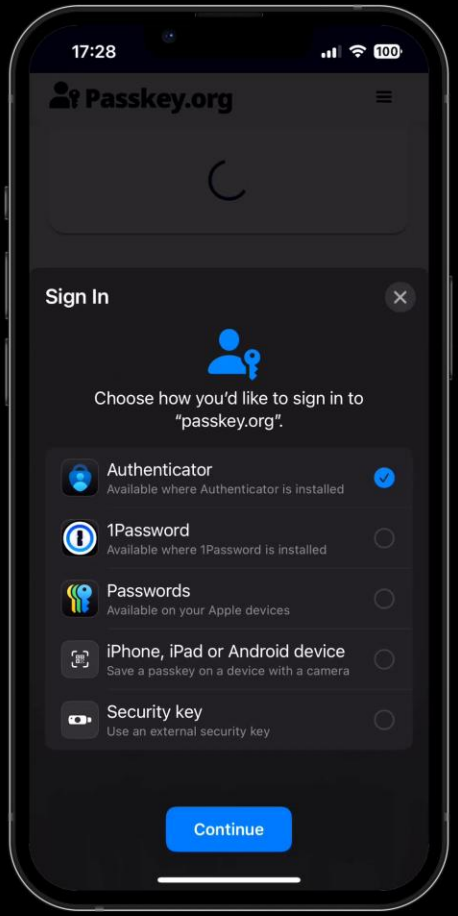
Passkey profiles soon in public preview!

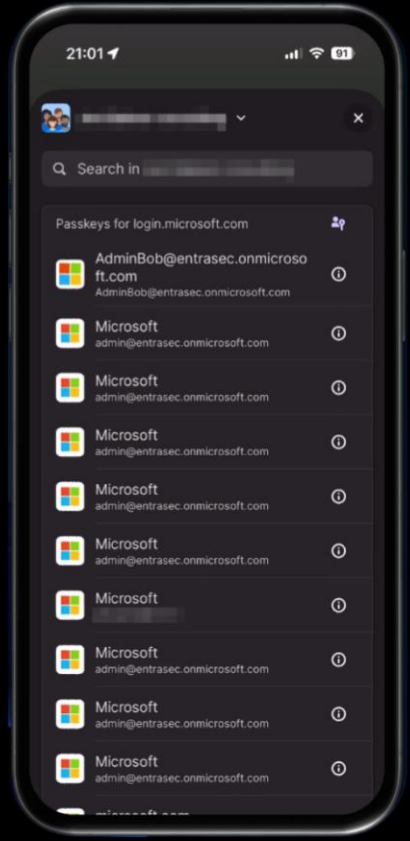



End-user
confusion


CONTOSO demo
My Sign-Ins
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
Sign-in method when most advisable is unavailable: Microsoft Authentica
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

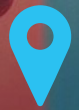

17:28
100
Passkey.org
Sign In
Choose how you'd like to sign in to "passkey.org".
Authenticator
Available where Authenticator is installed
1Password
Available where 1Password is installed
Passwords
Available on your Apple devices
iPhone, iPad or Android device
Save a passkey on a device with a camera
Security key
Use an external security key
Continue


21:01
91
Search in
Passkeys for login.microsoft.com
AdminBob@entrasec.onmicrosoft.com
AdminBob@entrasec.onmicrosoft.com
Microsoft
admin@entrasec.onmicrosoft.com
Microsoft
admin@entrasec.onmicrosoft.com
Microsoft
admin@entrasec.onmicrosoft.com
Microsoft
admin@entrasec.onmicrosoft.com
Microsoft
admin@entrasec.onmicrosoft.com
Microsoft
Microsoft
admin@entrasec.onmicrosoft.com
Microsoft
admin@entrasec.onmicrosoft.com
Microsoft
admin@entrasec.onmicrosoft.com


• Device-code phishing
• Malware
• Abuse onboard & recovery process
Hackers will go after tokens instead
(post-auth attacks)

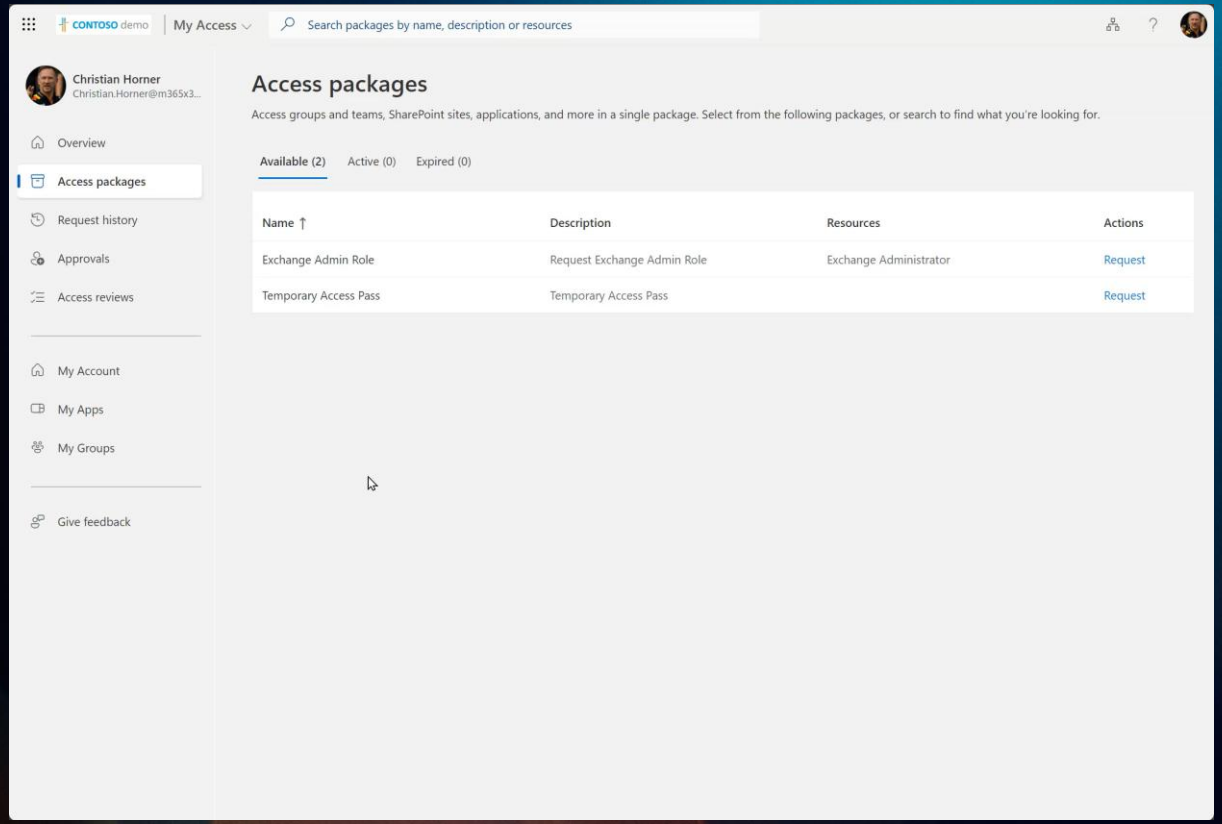
Strengthen onboarding & recovery process

Trusted device

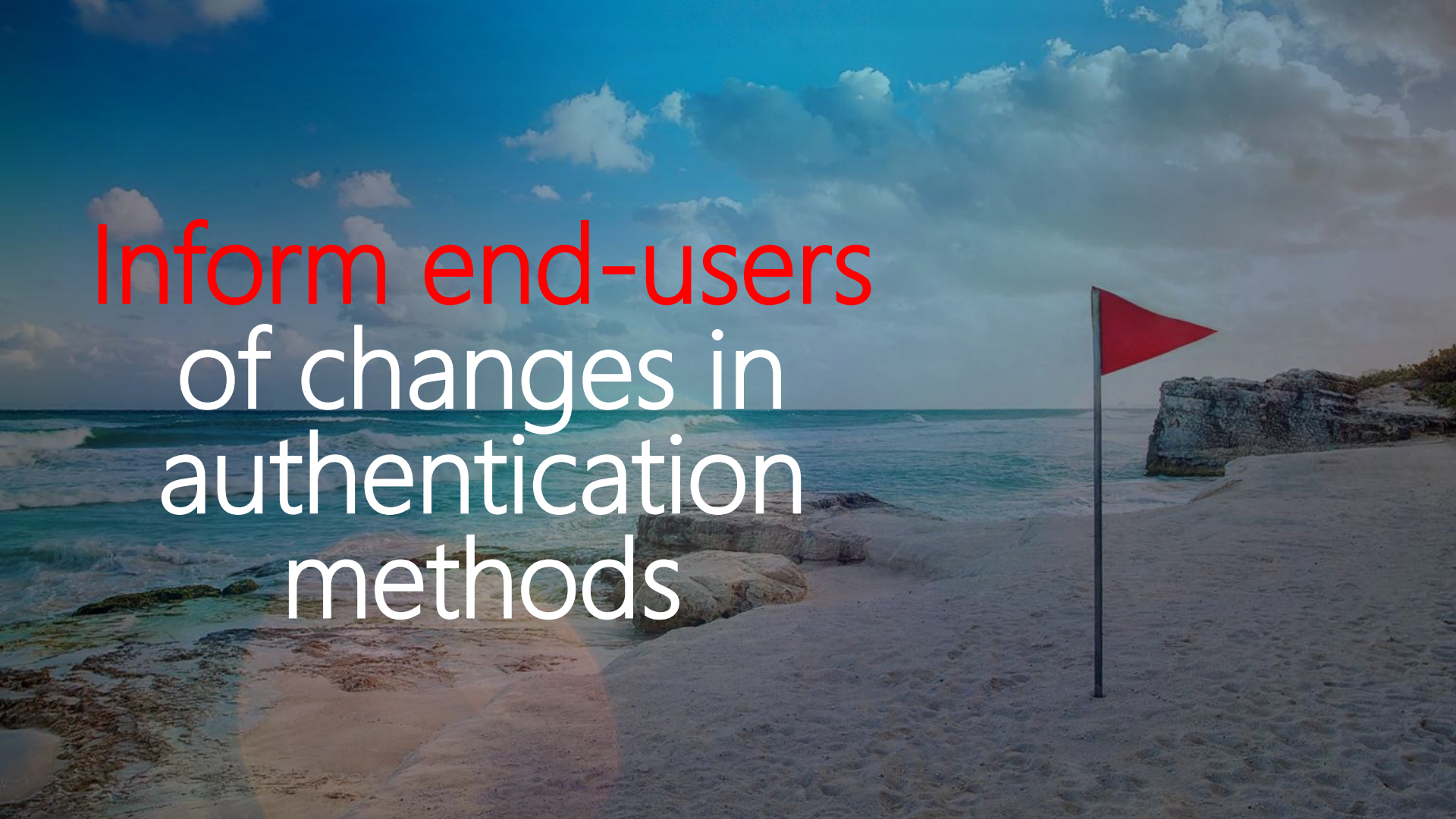


Trusted location

Temporary Access Pass



Request Temporary Access Pass on behalf of users


Inform end-users
of changes in
authentication
methods

Google

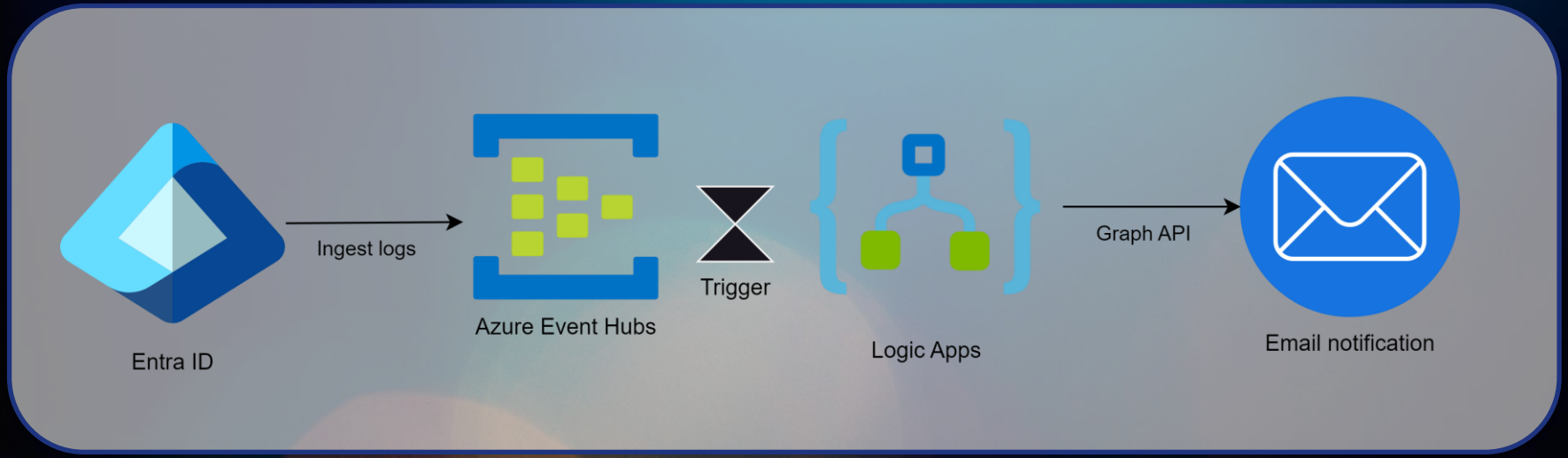
New passkey added to your account

[redacted]

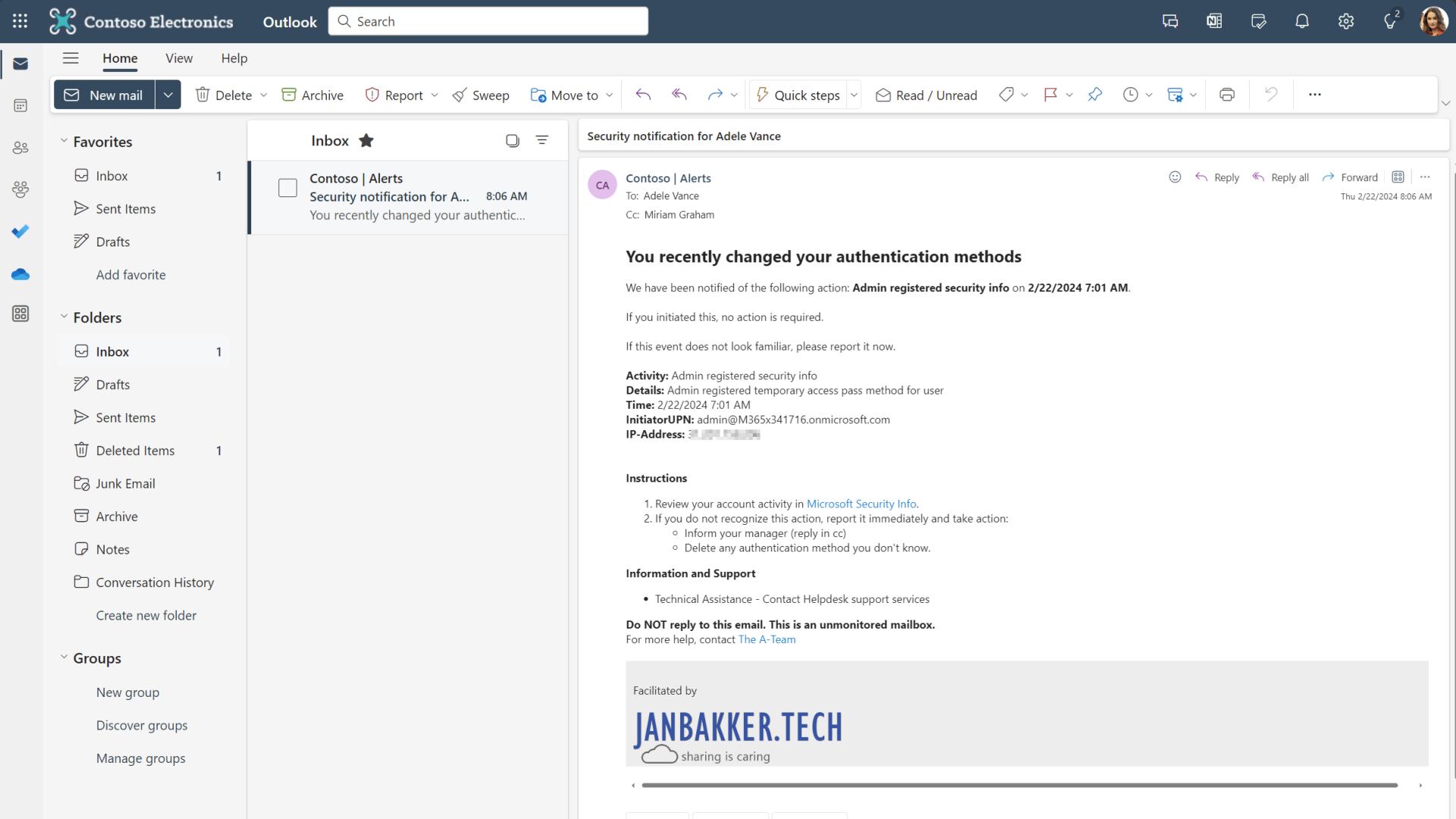
If you didn't add a passkey, someone might be using your account. Check and secure your account now.

Check activity

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



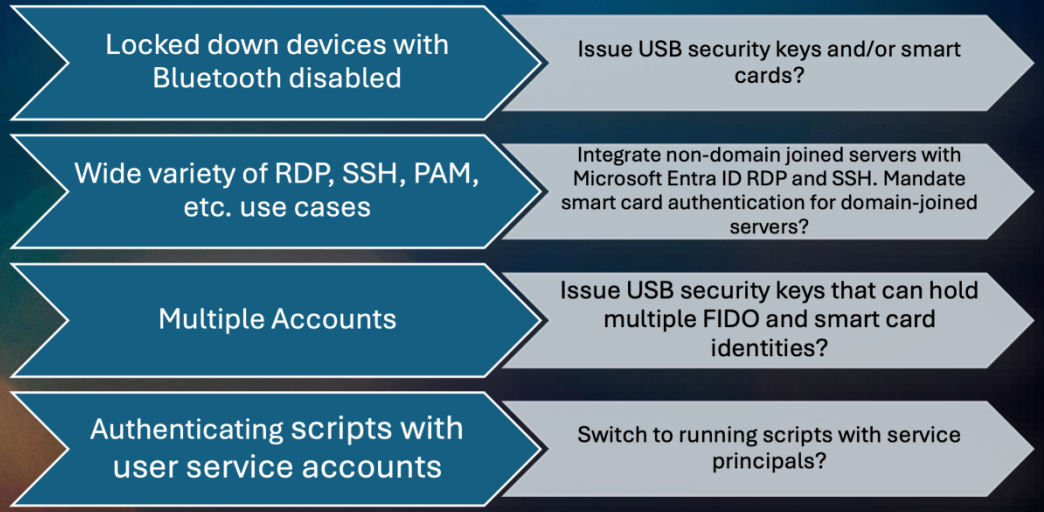
https://janbakker.tech/microsoft-365-end-user-notifications-for-changes-in-authentication-methods/


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
Folders
Inbox 1
Drafts
Sent Items
Deleted Items 1
Junk Email
Archive
Notes
Conversation History
Create new folder
Groups
New group
Discover groups
Manage groups
Inbox
Contoso | Alerts
Security notification for A... 8:06 AM
You recently changed your authentic...
Security notification for Adele Vance
CA
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:
Instructions
1. Review your account activity in Microsoft Security Info.
2. 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!

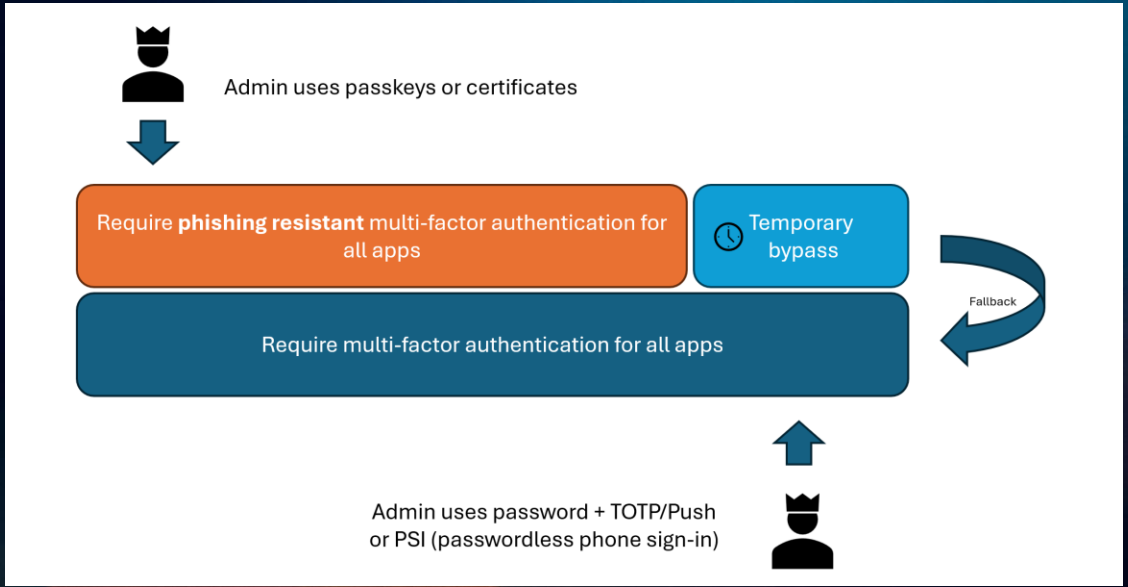
IT pros/DevOps workers

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



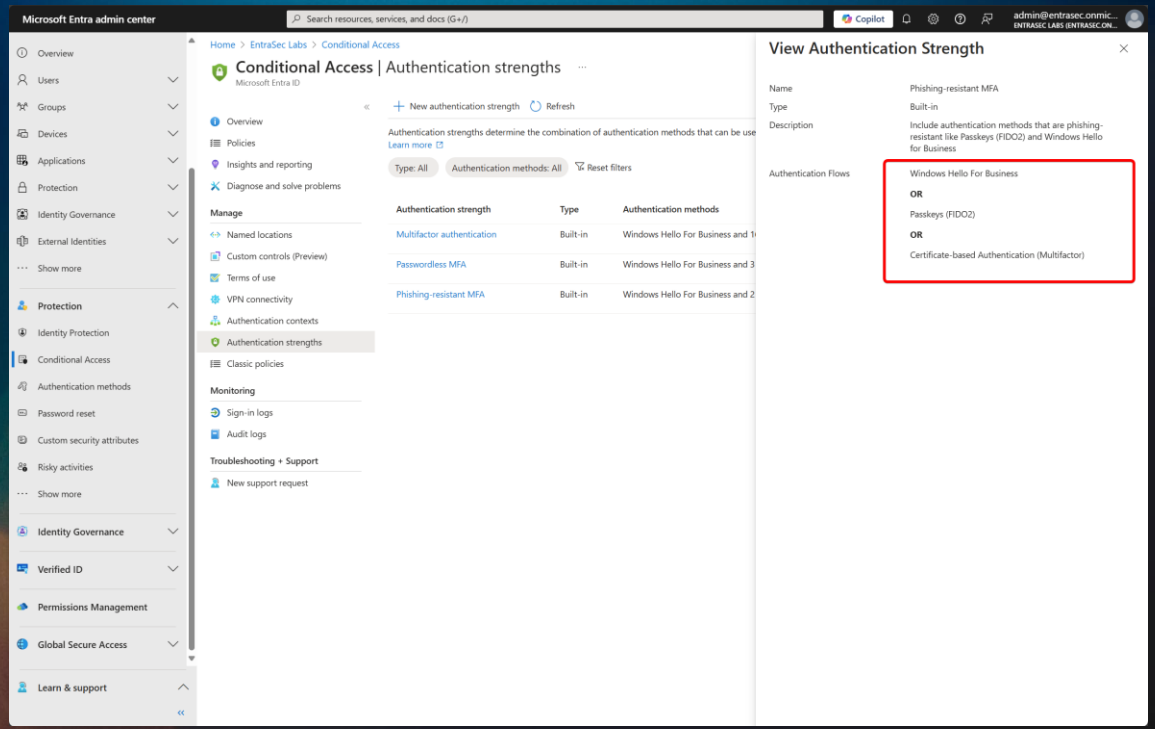
https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-plan-persona-phishing-resistant-passwordless-authentication#frontline-workers

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!



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) **OR** Temporary Access Pass (One-time use) **OR** Temporary Access Pass (Multi-use)	N/A.
Secure Desktop Apps	All resources	**Exclude:** iOS Android	Passkeys (FIDO2)*	Microsoft Authenticator (iOS) Microsoft Authenticator (Android)
Secure Mobile Apps	All resources	**Include:** iOS Android	Passkeys (FIDO2) **OR** Temporary Access Pass (One-time use) **OR** Temporary Access Pass (Multi-use)	Microsoft Authenticator (iOS) Microsoft Authenticator (Android)

https://janbakker.tech/you-shall-not-passkey/

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

https://janbakker.tech/you-shall-not-passkey/

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

https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-support-authenticator-passkey#workarounds-for-an-authentication-strength-conditional-access-policy-loop

What's next?

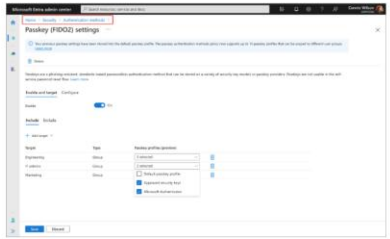
How this will affect your organization:

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

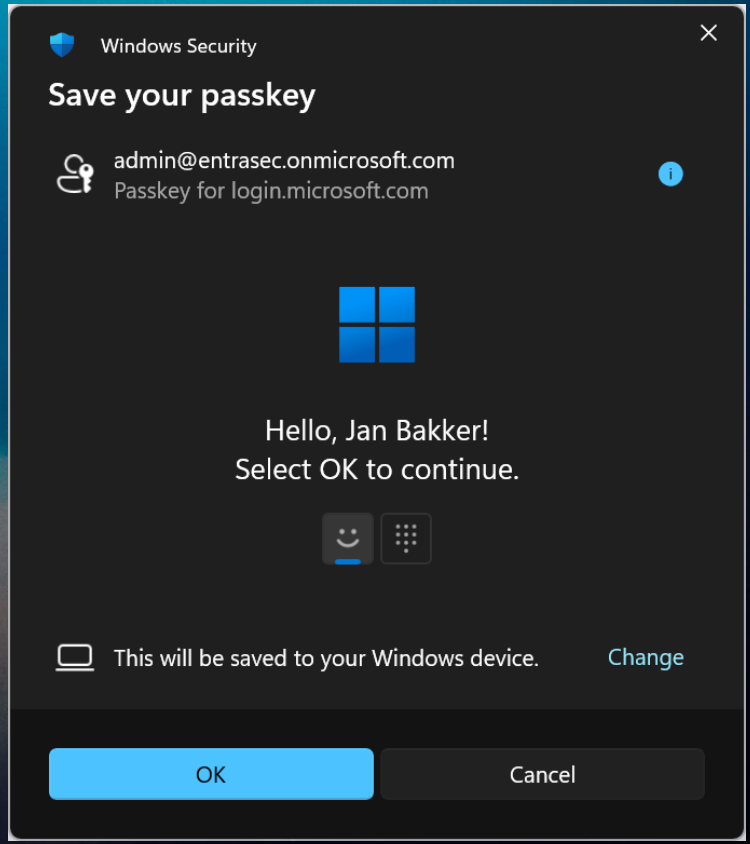
What you need to do to prepare:

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)

MC1097225 - Microsoft Entra ID: Upcoming changes to support passkey profiles in the authentication methods policy (preview) | Microsoft 365 Message Center Archive

What's next?



https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-support-authenticator-passkey#workarounds-for-an-authentication-strength-conditional-access-policy-loop

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
JANBAKKER.TECH
sharing is caring