
Passkeys in Microsoft 365
Are we there yet?
wpninjas.nl

Thank you Sponsors

Gold

liquidware

2Pint

PINK

RECAST SOFTWARE

Silver

PATCH MY PC

Technical Partners

CONSULTEQ

PROXSYS

Daalmans consulting

Secure At Work

About Jan Bakker

Focus

Fighting passwords and manual labor

From

The Netherlands

My Blog

JANBAKKER.TECH
sharing is caring

Certifications

Never not learning

Hobbies

Family
Music
F1

Contact

aka.ms/janbakker

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

FIDO2 (security)key

can store

passkeys

Yubikey

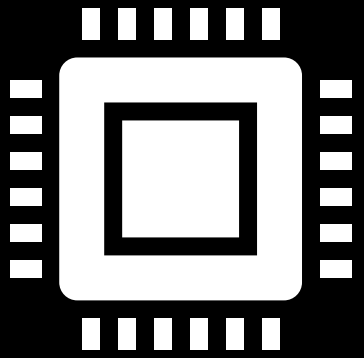

yubico

Passwords

keys

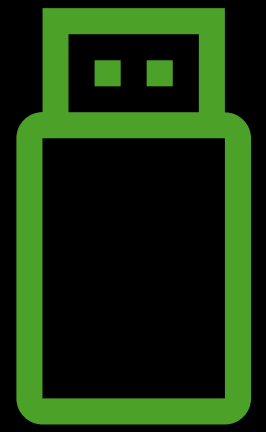
FIDO standard

Authenticator types



Platform Authenticator

Touch ID
Face ID
Windows Hello



Roaming Authenticator

Security keys
(USB/NFC/BTE)

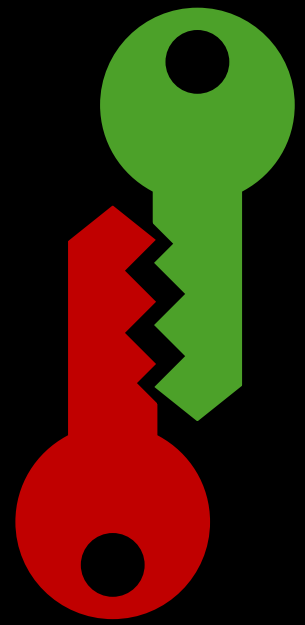
Platform authenticators can only authenticate the user on the device they are integrated with.

Roaming authenticators can be used with any compatible device.

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

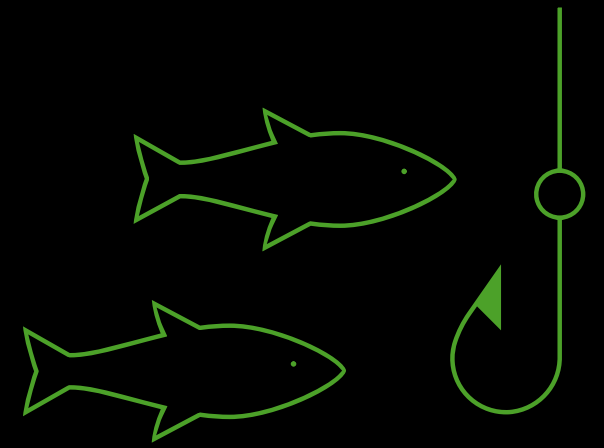
Faster & Easier

More Secure

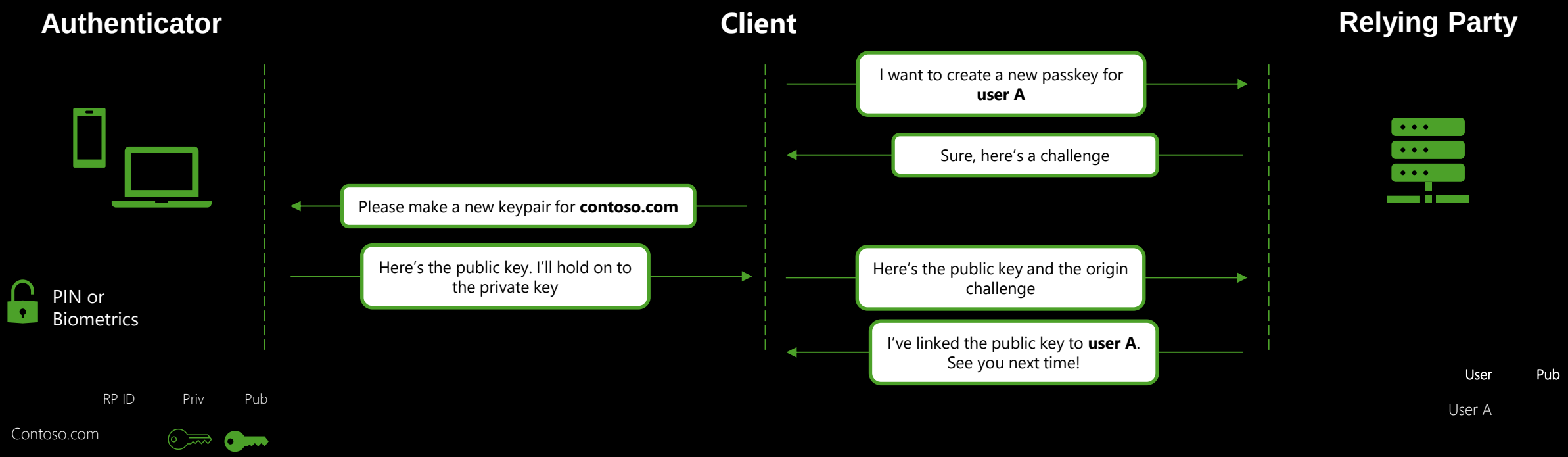


Passkey are built on PKI

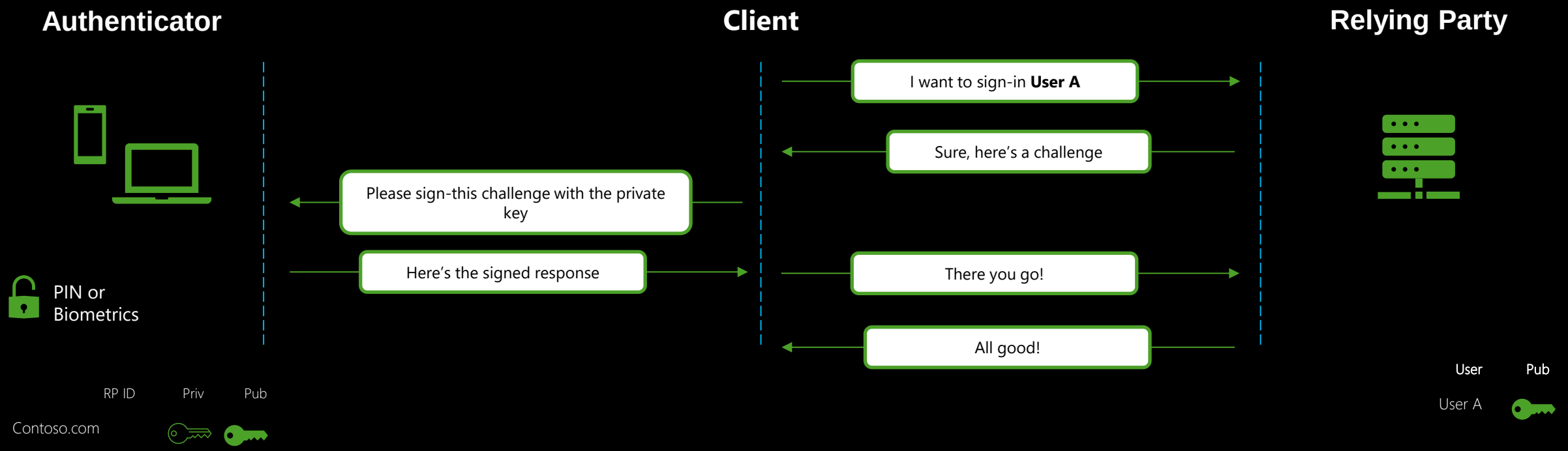
Phishing Resistant



How passkeys work (Registration)



How passkeys work (Subsequent Sign-in)



No more passwords
No more shared secrets
No more AiTM attacks

Where do we store our passkeys?


';--have i been pwned?
';--4935310

Device-bound passkeys

Bound to and used only on a single device

Synced passkeys

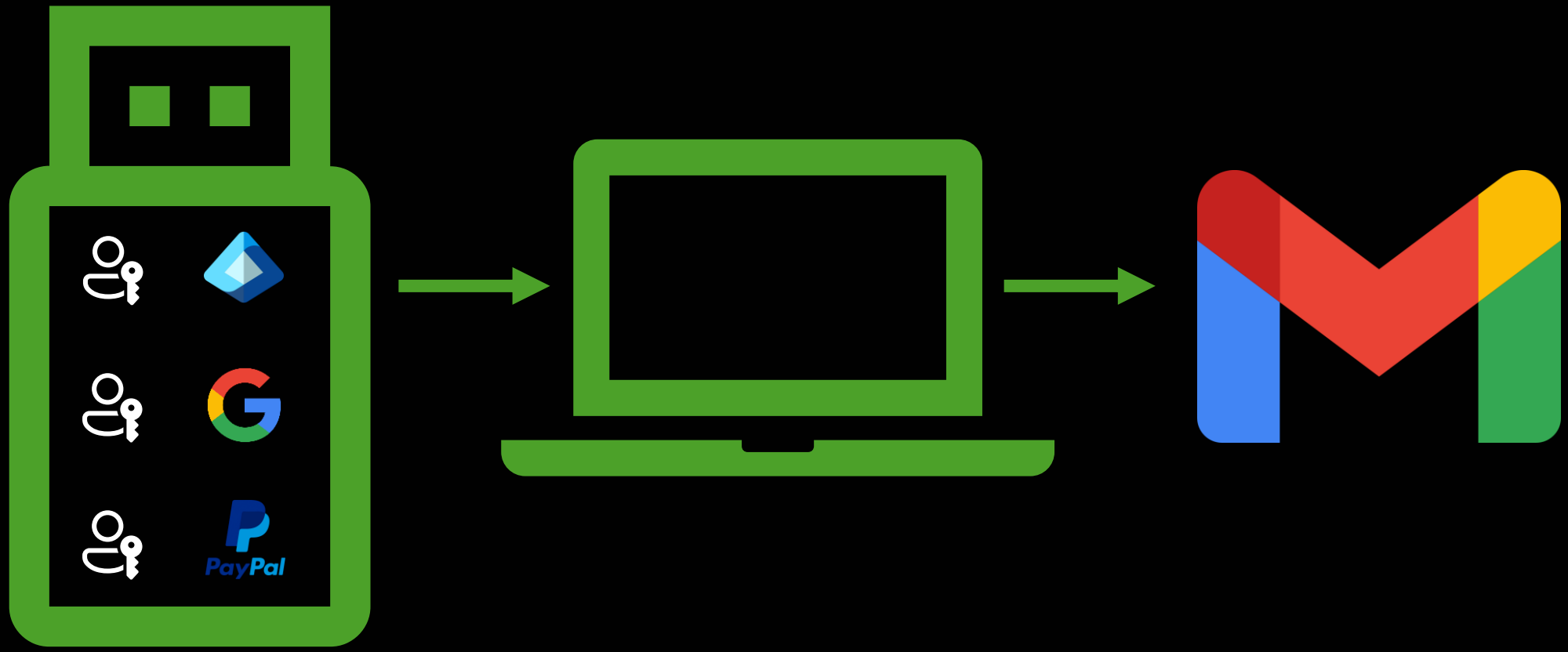
Stored securely in a credential manager and accessed across devices

Device-bound passkeys

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

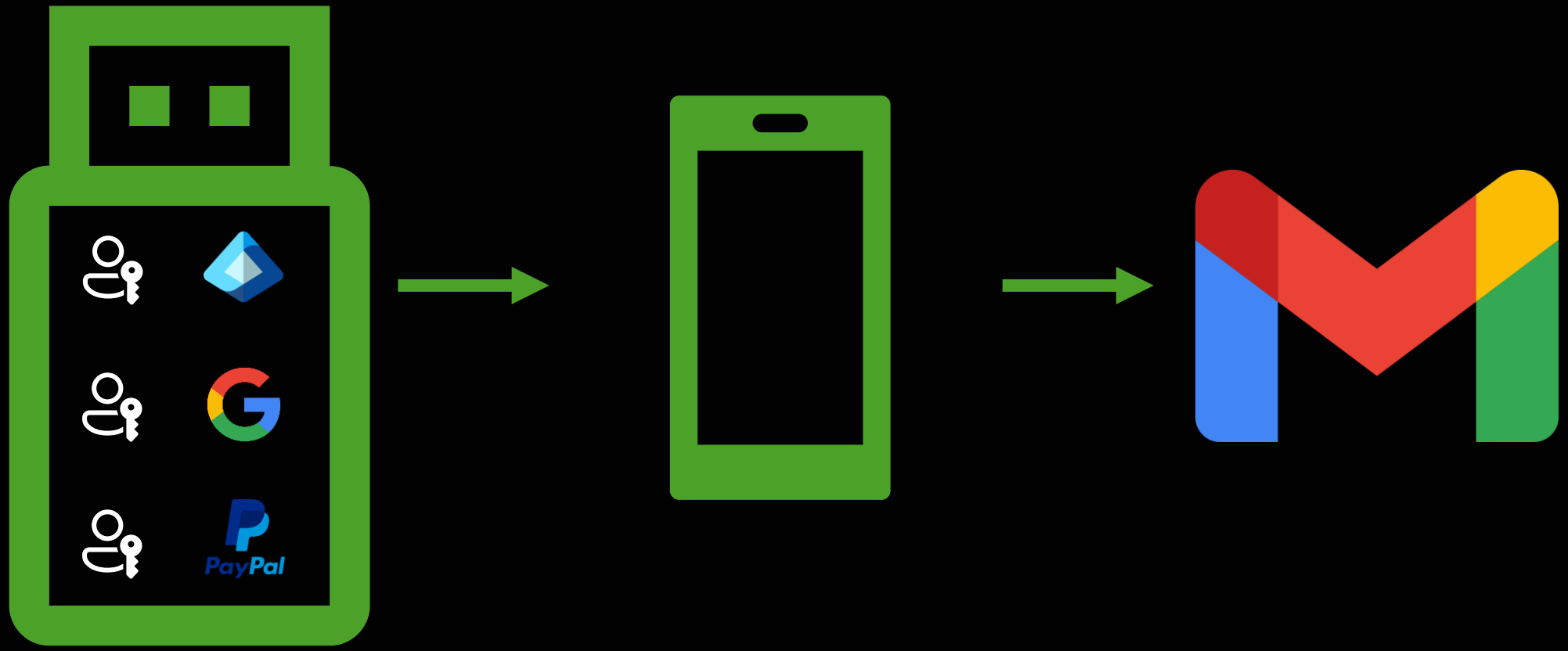
Device-bound passkeys

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



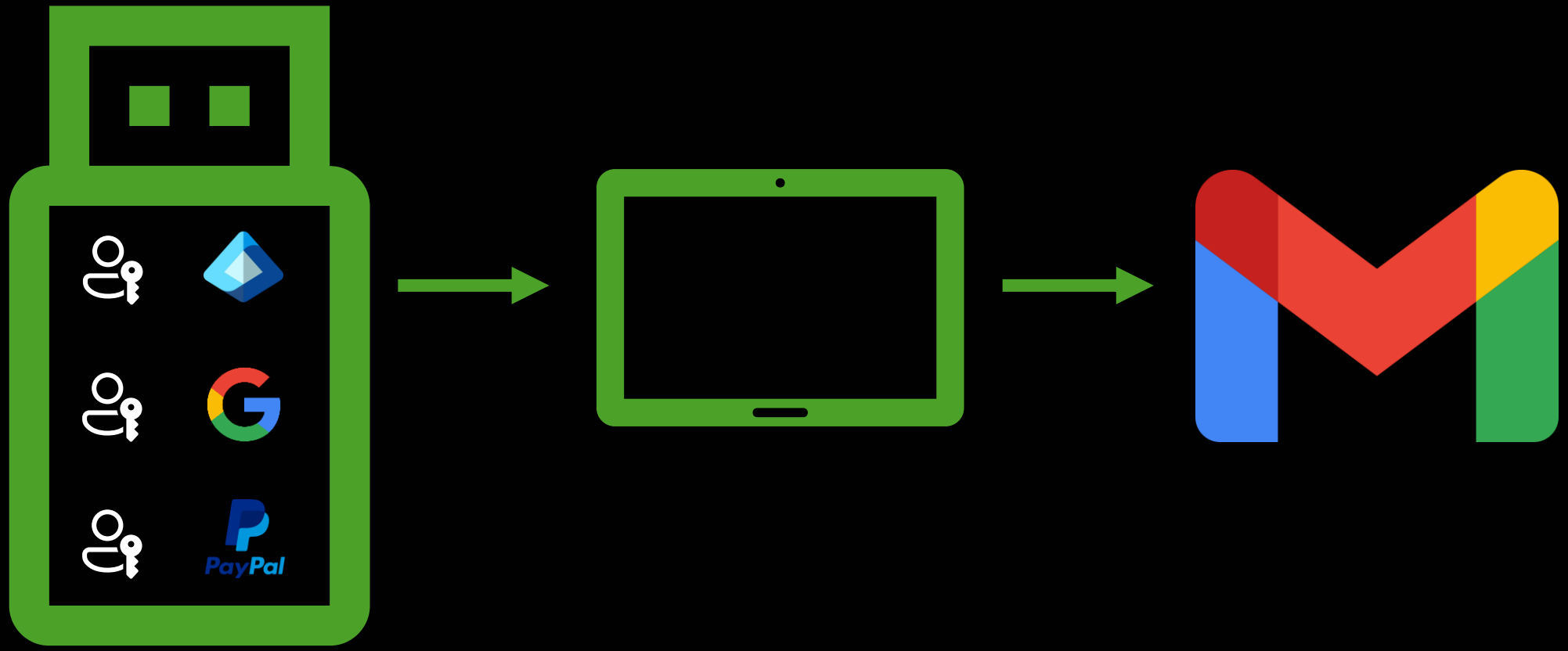
Device-bound passkeys

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.



Device-bound passkeys

Some examples

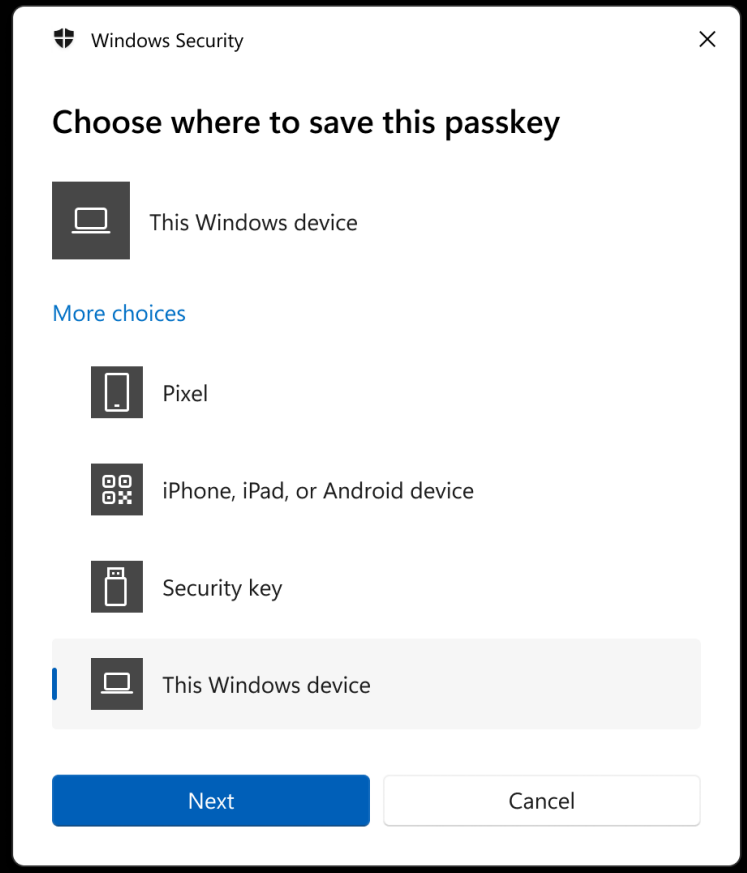
Windows Hello

Yubikey

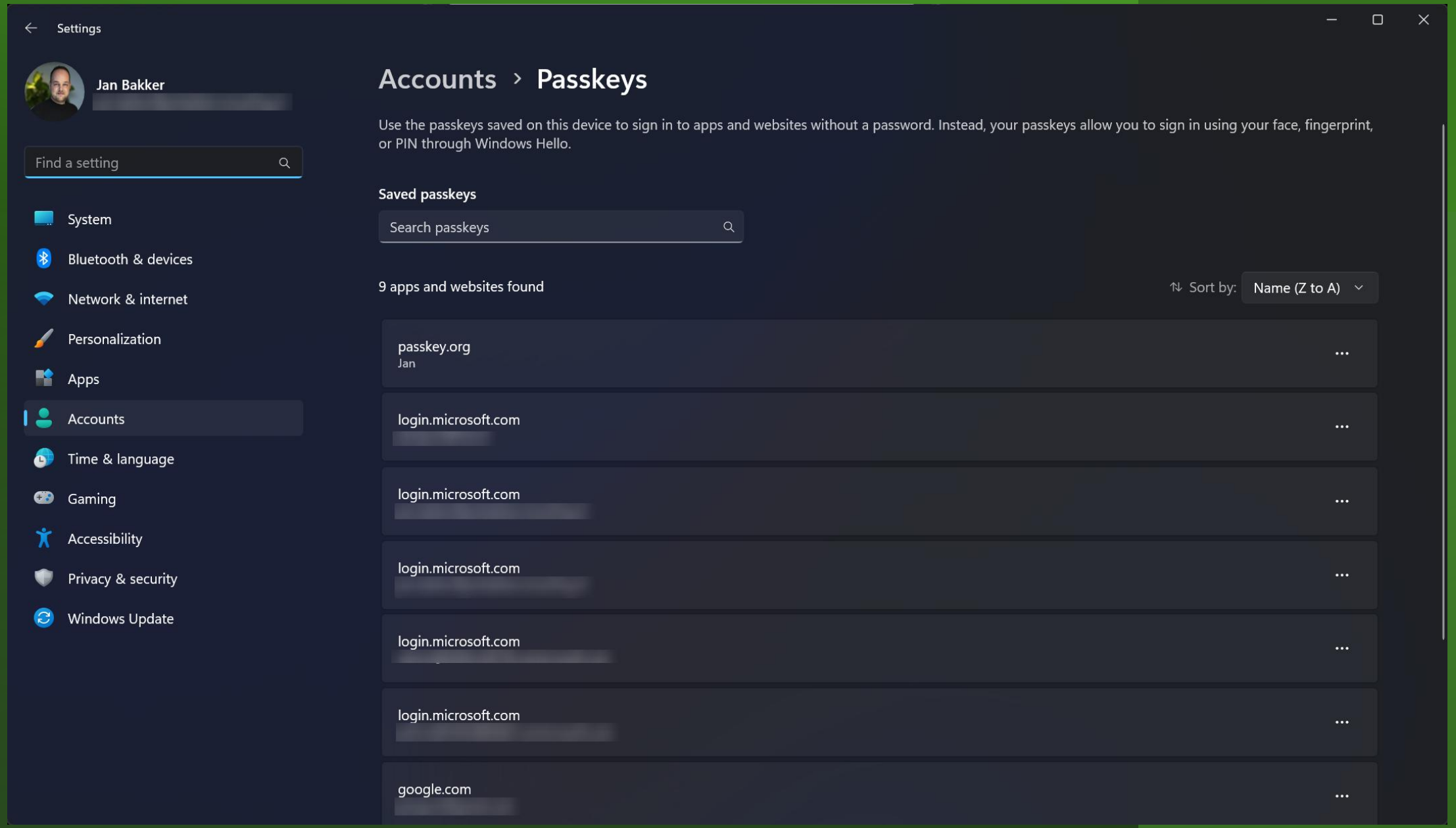
Microsoft Authenticator App

Support for passkeys in Windows

Local (Windows Hello)
Phone, iPad or Android device (QR code)
Linked device (Android only)
Security key (USB or NFC)



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

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 n 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

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

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

Passkeys Authenticator AAGUID Explorer

Exclude MDS authenticators

AAGUID	Name Yubikey 5 Series X	Icon light	Icon dark
c5ef55ff-ad9a-4b9f-b580-adebafe026d0	YubiKey 5 Series with Lightning		
fa2b99dc-9e39-4257-8f92-4a30d23c4118	YubiKey 5 Series with NFC		
4599062e-6926-4fe7-9566-9e8fb1aedaa0	YubiKey 5 Series (Enterprise Profile)		
b90e7dc1-316e-4fee-a25a-56a666a670fe	YubiKey 5 Series with Lightning (Enterprise Profile)		
a02167b9-ae71-4ac7-9a07-06432ebb6f1c	YubiKey 5 Series with Lightning		
3124e301-f14e-4e38-876d-fbeeb090e7bf	YubiKey 5 Series with Lightning Preview		
2fc0579f-8113-47ea-b116-bb5a8db9202a	YubiKey 5 Series with NFC		
20ac7a17-c814-4833-93fe-539f0d5e3389	YubiKey 5 Series (Enterprise Profile)		
d7781e5d-e353-46aa-afe2-3ca49f13332a	YubiKey 5 Series with NFC		

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

Authentication methods | User registration details

Contoso - Microsoft Entra ID Security

Download | Refresh | Columns | Got feedback?

Name or UPN starts with

Add filter

Multifactor authentication capable: All | Passwordless capable: All | SSPR capable: All | Methods registered: Passkey (Microsoft Authenticator),Passkey,... | User preferred method: All

Reset filters

UPN	Name	Methods Registered	Last Updated Time
[redacted]	[redacted]	Windows Hello for Business,Passkey (Microsoft Authenticator),Microsoft Passwordless phone	1/30/25, 7:48:51 PM UTC
[redacted]	[redacted]	Passkey (Microsoft Authenticator),Windows Hello for Business,Software OATH token	1/30/25, 7:48:51 PM UTC
[redacted]	[redacted]	Passkey (other device-bound),Mobile phone,Microsoft Authenticator app (push notification),S	1/30/25, 7:48:51 PM UTC
[redacted]	[redacted]	Passkey (other device-bound)	1/30/25, 7:48:51 PM UTC
[redacted]	[redacted]	Microsoft Passwordless phone sign-in,Passkey (Microsoft Authenticator),Passkey (other device	1/30/25, 7:48:51 PM UTC
[redacted]	[redacted]	Passkey (other device-bound)	1/30/25, 7:48:51 PM UTC
[redacted]	[redacted]	Passkey (other device-bound),Microsoft Passwordless phone sign-in,Passkey (Microsoft Authe	1/30/25, 7:48:51 PM UTC
[redacted]	[redacted]	Passkey (other device-bound),Mobile phone,Microsoft Authenticator app (push notification),S	1/30/25, 7:48:51 PM UTC
[redacted]	[redacted]	Email,Passkey (other device-bound),Microsoft Authenticator app (push notification),Software	1/30/25, 7:48:51 PM UTC
[redacted]	[redacted]	Passkey (other device-bound)	1/30/25, 7:48:51 PM UTC
[redacted]	[redacted]	Passkey (other device-bound)	1/30/25, 7:48:51 PM UTC
[redacted]	[redacted]	Microsoft Passwordless phone sign-in,Passkey (Microsoft Authenticator),Microsoft Authentica	1/30/25, 7:48:51 PM UTC
[redacted]	[redacted]	Passkey (Microsoft Authenticator),Microsoft Authenticator app (push notification),Software O	1/30/25, 7:48:51 PM UTC
[redacted]	[redacted]	Passkey (other device-bound)	1/30/25, 7:48:51 PM UTC

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

Gerhart Moller | Authentication methods

User

Search
Overview
Audit logs
Sign-in logs
Diagnose and solve problems
Custom security attributes
Assigned roles
Administrative units
Groups
Applications
Licenses
Devices
Azure role assignments
Authentication methods
New support request

Add authentication method | Reset password | Require re-

Authentication methods are the ways users sign into Microsoft Entra ID a
(SSPR). The user's "default sign-in method" is the first one shown
with a second factor - the user always can choose another
authenticate with. Learn more

Default sign-in method (Preview)

Usable authentication methods

Authentication method
Passkey
Passkey
Microsoft Authenticator

Non-usable authentication methods

Authentication method
No non-usable methods.

System preferred multifactor authentication method

Feature status	System preferred MFA method
Enabled	Fido2

Passkey details

ID
n4iWkUuq8bWqpreJOA9INGZNLifqGQFkEZ6W0NNNKBz9rGf2J4NPXlCetddslofL0

Model
YubiKey Bio FIDO Edition

AA Guid
dd86a2da-86a0-4cbe-b462-4bd31f57bc6f

Attestation Level
Attested

Graph Explorer

Tenant
Contoso

Sample queries | API Explorer | History

Search sample queries

See more queries in the Microsoft Graph API Reference docs.

- Getting Started (8)
  - GET my profile
  - GET my profile (beta)
  - GET my photo
  - GET my mail
  - GET list items in my drive
  - GET items trending around me
  - GET my manager
  - GET my To Do t
- Applications (8)
- Batching (2)
- Compliance (beta) (10)
- Edge (4)
- Excel (7)
- Extensions (7)

GET | beta | https://graph.microsoft.com/beta/users/GerhartM@M365x341716.OnMicrosoft.com/authentication/fido2Methods/n4iWkUuq8bWqpreJOA9INGZNLifqGQFkEZ6W0NNNKBz9rGf2J4NPXlCetddslofL0 | Run query

No resource was found matching this query

Request body | Request headers | Modify permissions | Access token

OK - 200 - 514 ms

Response preview | Response headers | Code snippets | Toolkit component | Adaptive cards | Expand


```
{
    "@odata.context": "https://graph.microsoft.com/beta/$metadata#users('GerhartM%40M365x341716.OnMicrosoft.com')/authentication/fido2Methods/$entity",
    "@microsoft.graph.tips": "Use $select to choose only the properties your app needs, as this can lead to performance improvements. For
...yName": "YubiKey BIO",
"createdDateTime": "2024-11-26T08:27:34Z",
"aaGuid": "dd86a2da-86a0-4cbe-b462-4bd31f57bc6f",
"model": "YubiKey Bio FIDO Edition",
"attestationCertificates": [
    "700c73b96ff5874c08d5eb85160
}
```

MichelvanVliet / Scripts Public

Notifications Fork 0 Star 1

Code Issues Pull requests Actions Projects Security Insights

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

```
<#
    .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 ";"
```

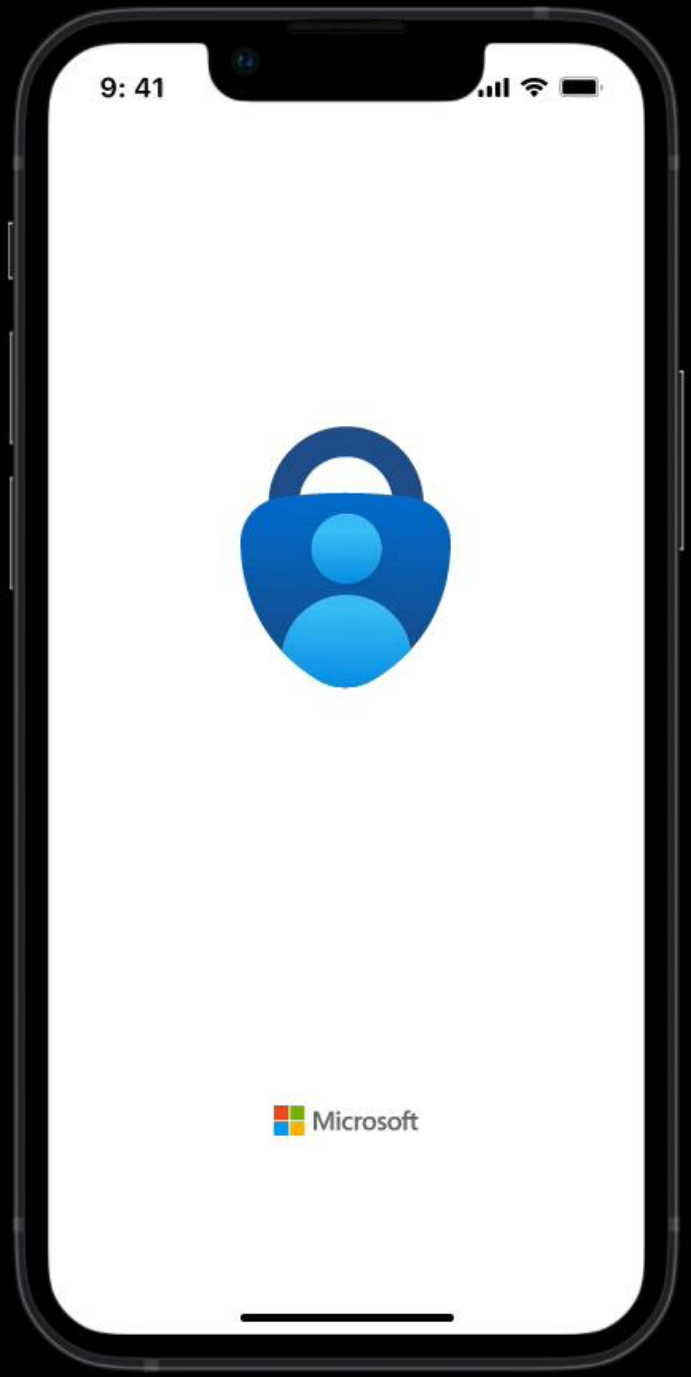
Passkey enrollment

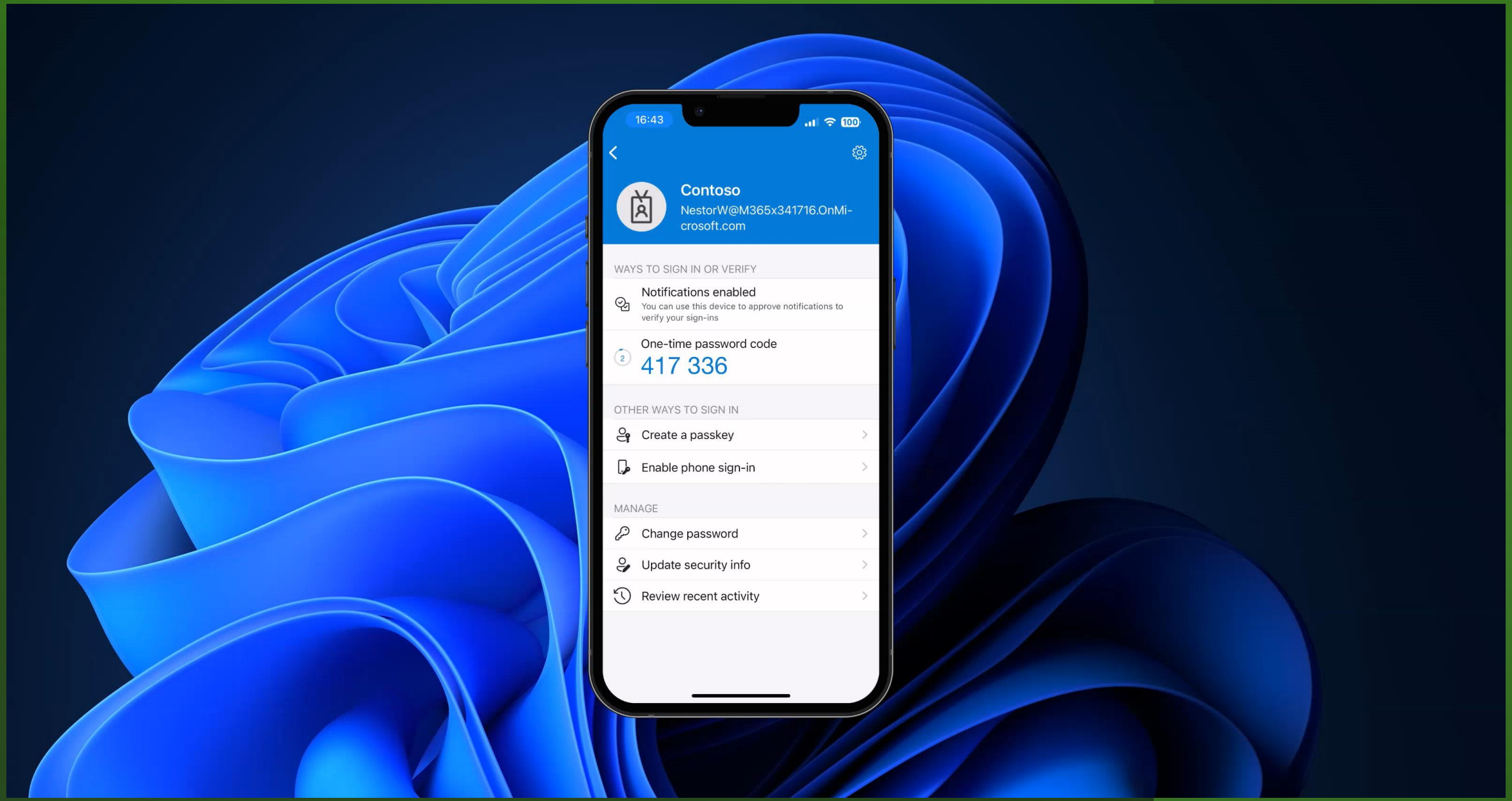
MFA is required for enrollment of strong auth methods

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

Temporary Access Pass

Register passkey in Authenticator App with Temporary Access Pass




16:43
100
Contoso
NestorW@M365x341716.OnMicrosoft.com
WAYS TO SIGN IN OR VERIFY
Notifications enabled
You can use this device to approve notifications to verify your sign-ins
One-time password code
417 336
OTHER WAYS TO SIGN IN
Create a passkey
Enable phone sign-in
MANAGE
Change password
Update security info
Review recent activity

Personal | Authentication methods - Micros | My Sign-Ins | Security Info | Micro

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

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.

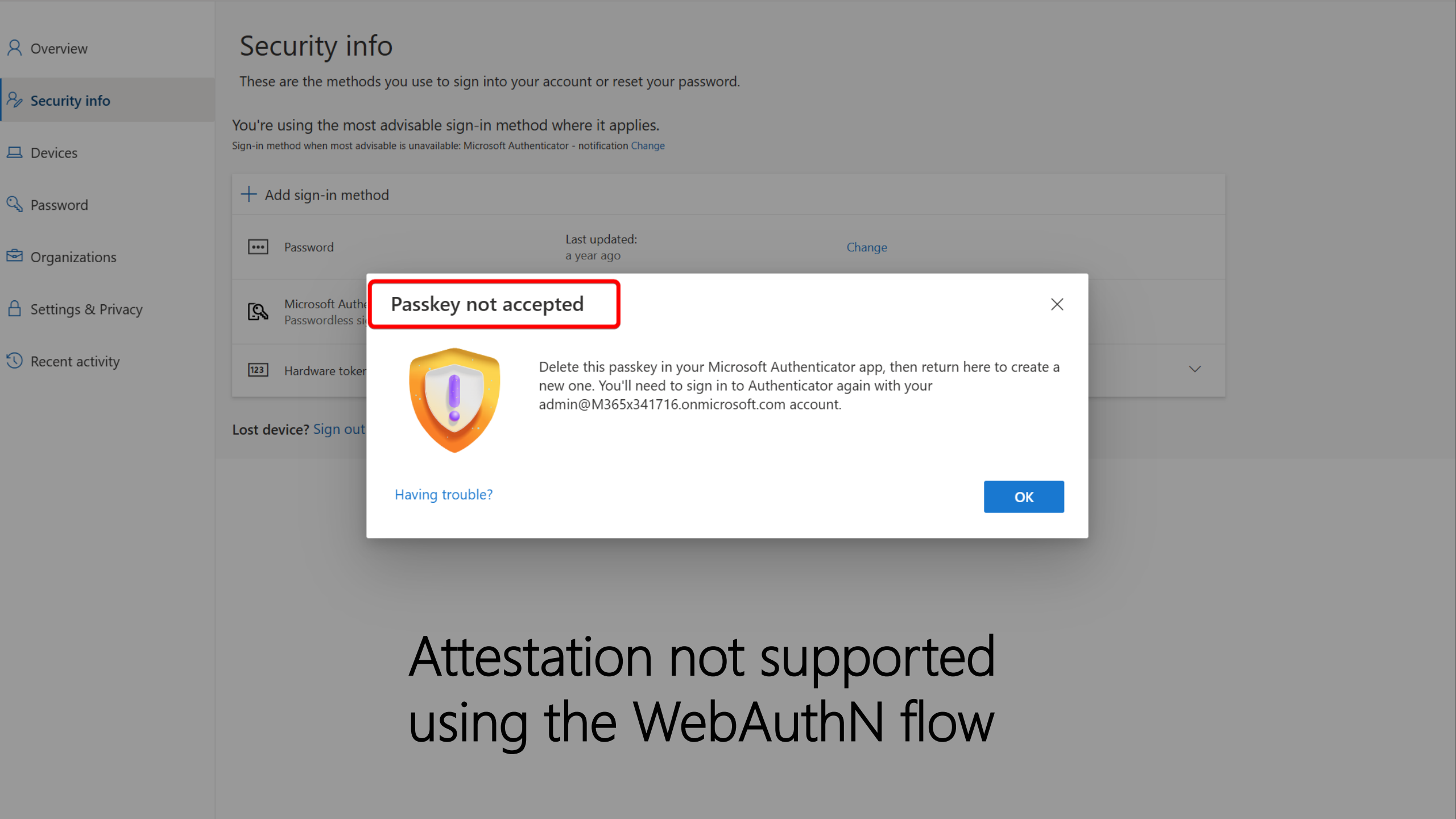
You're using the most advisable sign-in method where it applies.

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		Delete	
Hardware token	123456	Delete	

Lost device? Sign out everywhere

Register other types 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

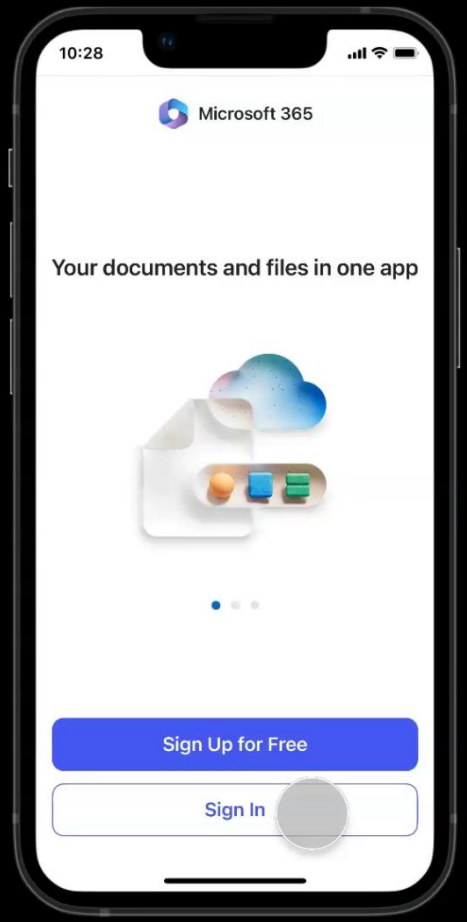
Request body | Request headers | Modify permissions | Access token

OK - 200 - 470 ms

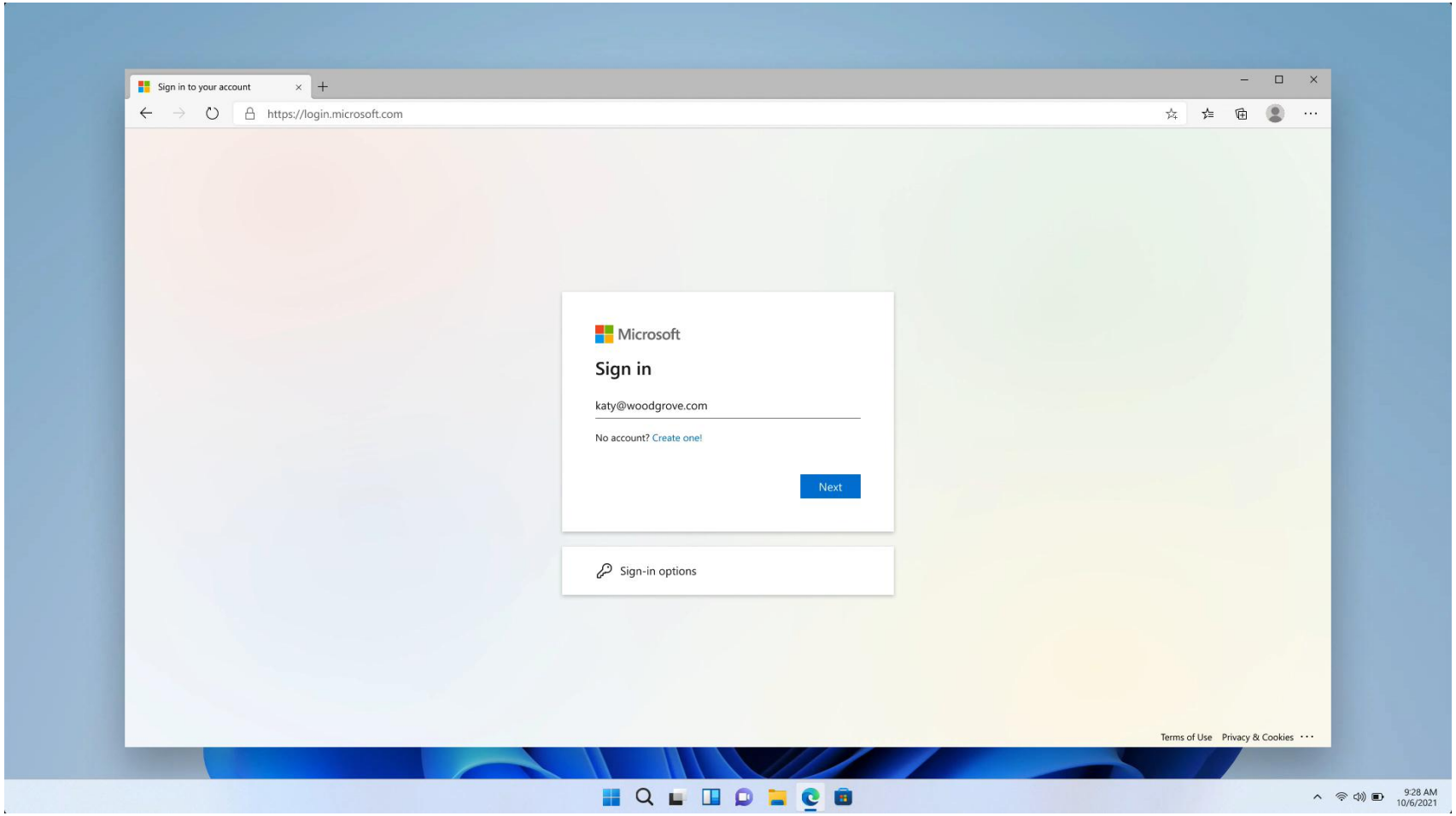
Response preview | Response headers | Code snippets | Toolkit component | Adaptive cards


```
{
    "@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"
        }
    ]
}
```


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

Cross device login also works with Windows Web Sign-in

Amanda Brady

Sign in

Sign-in options

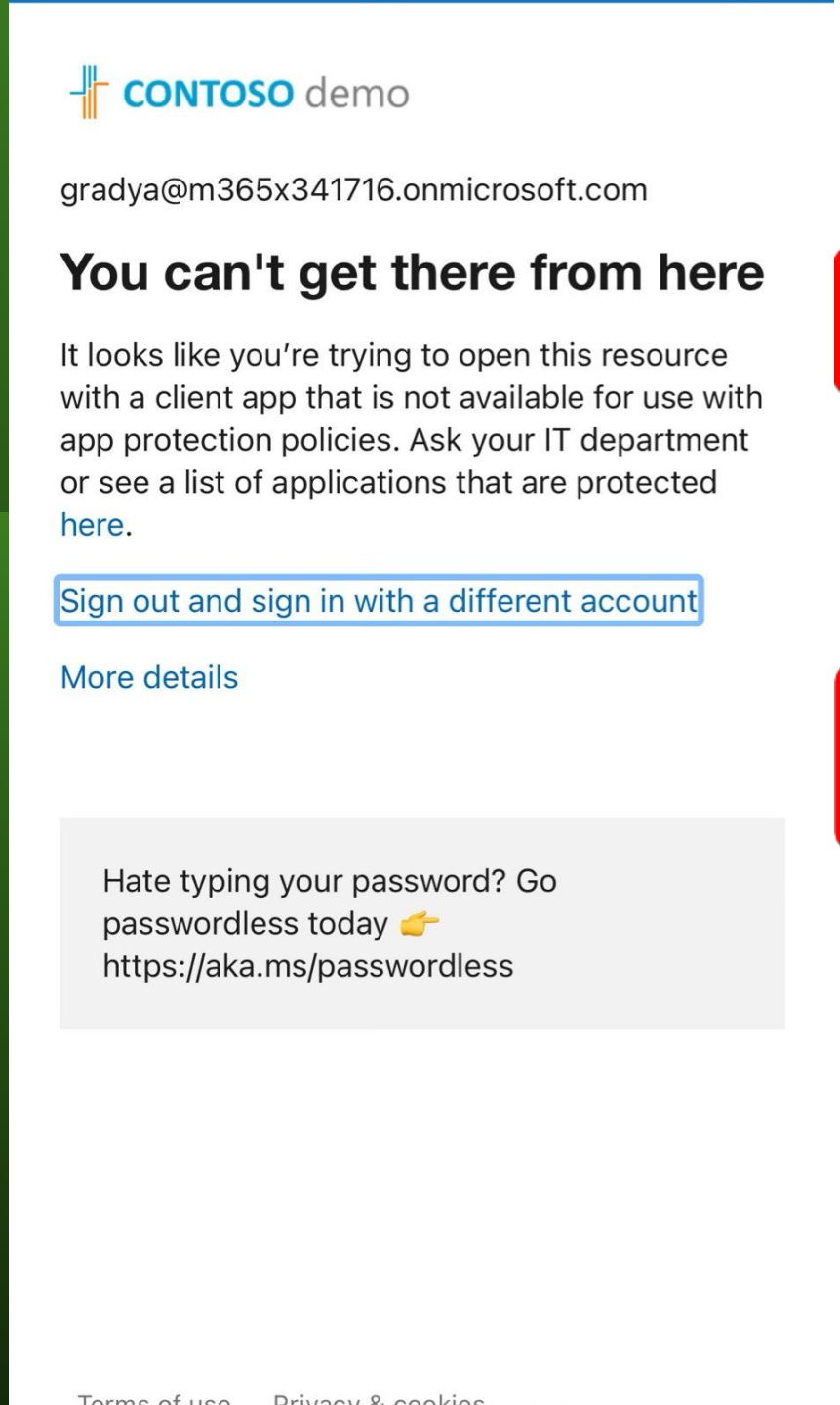
Amanda Brady

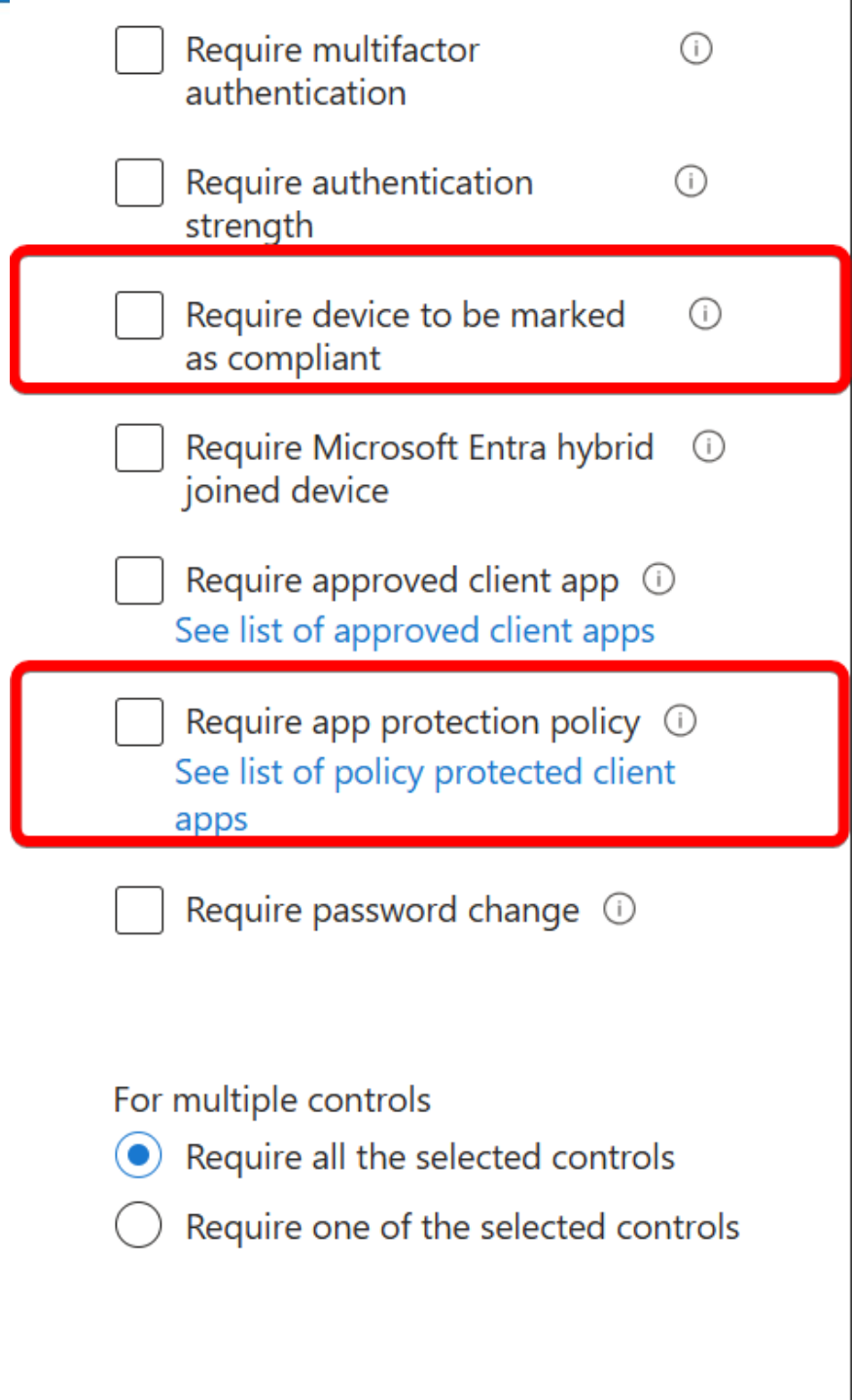
What does not work today?

- Store Entra ID passkeys in other credential providers like 1Passsword or Windows Hello
- Store 3rd party passkeys in Microsoft Authenticator
- Sync passkeys from Entra ID to other devices

Conditional Access doing its job

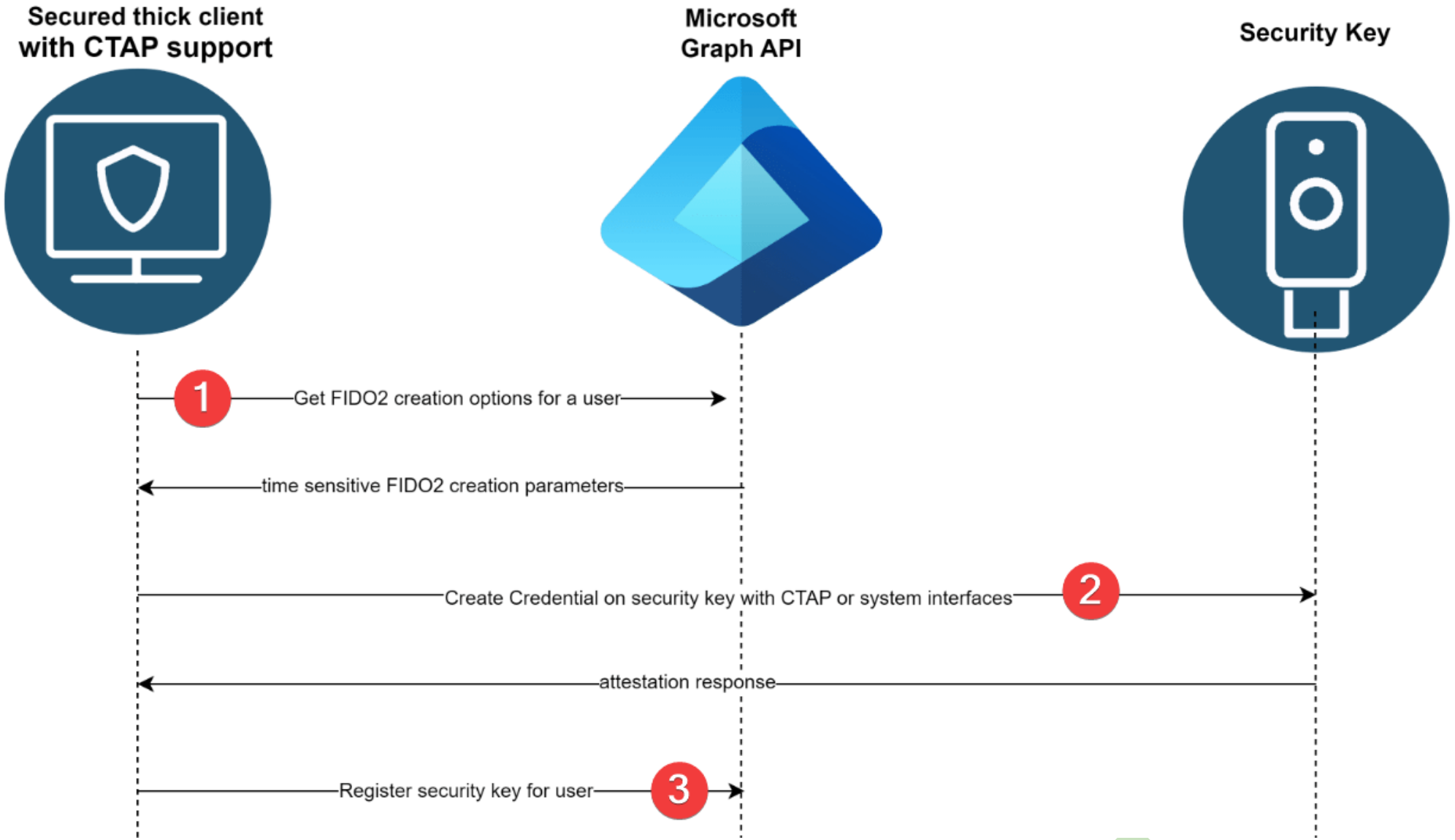
All resources (formerly 'All cloud apps')



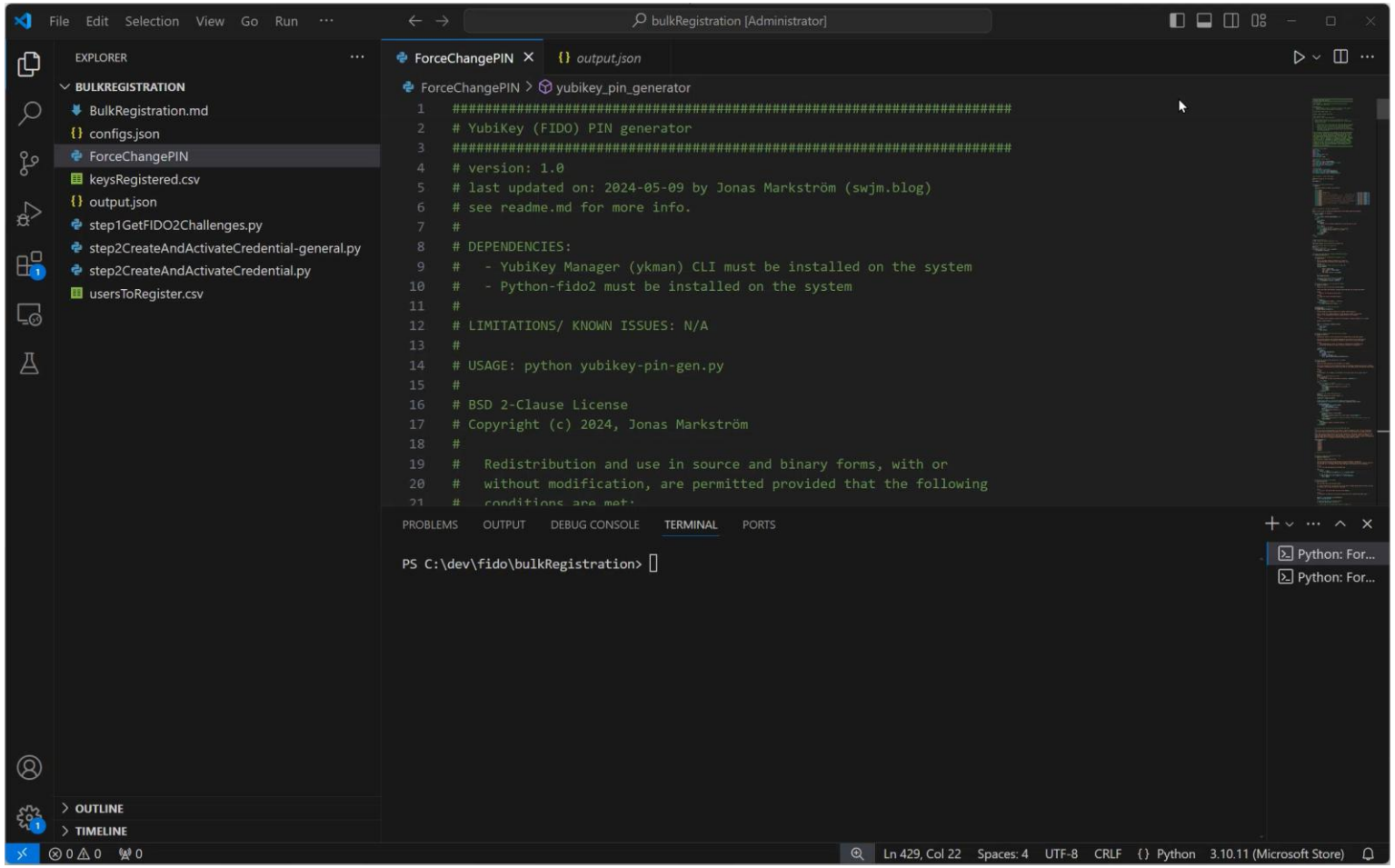


Passkey provisioning

(supported for hardware security keys)



https://janbakker.tech/register-yubikeys-on-behalf-of-your-users-with-microsoft-entra-id-fido2-provisioning-apis/

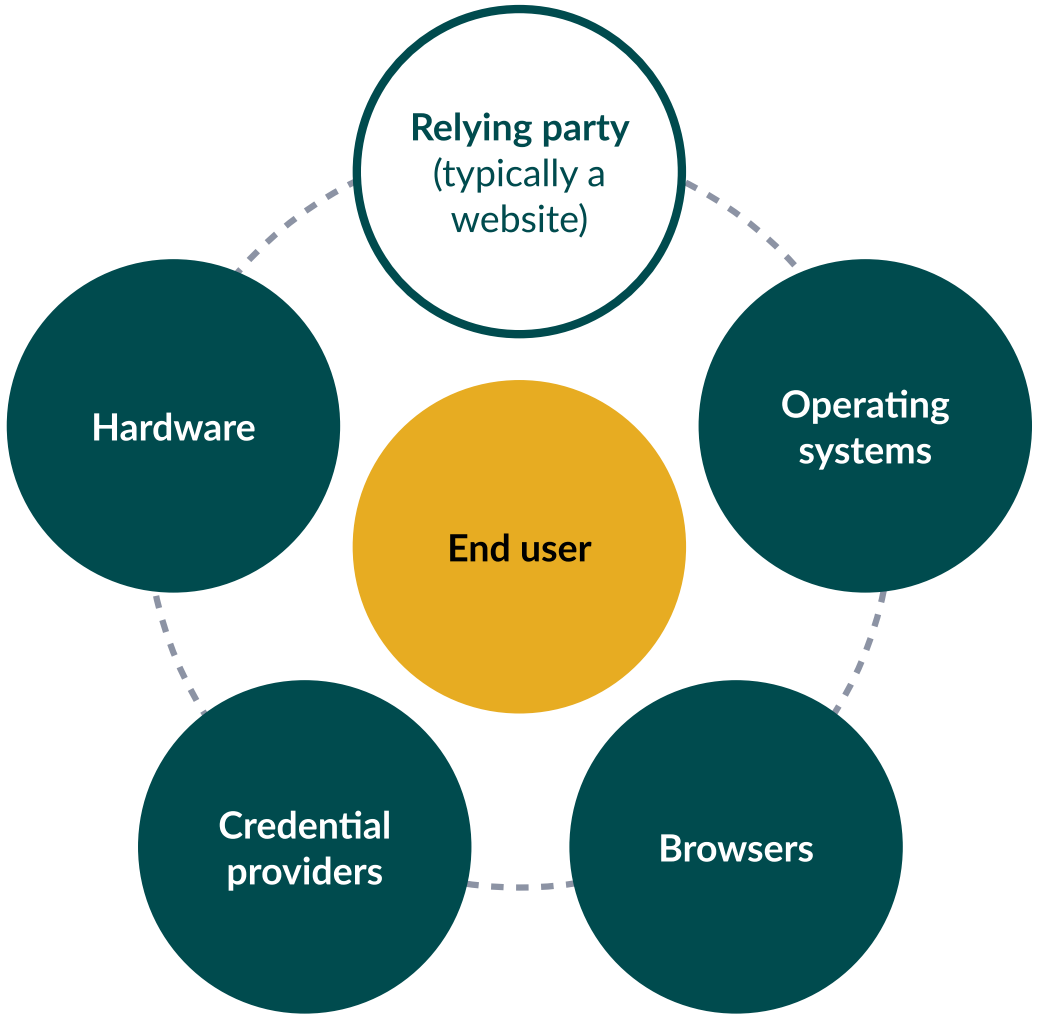


Enforce PIN complexity and change on first use

Are we there yet?


We are still in
the early stage
of passkeys

The API is there……



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

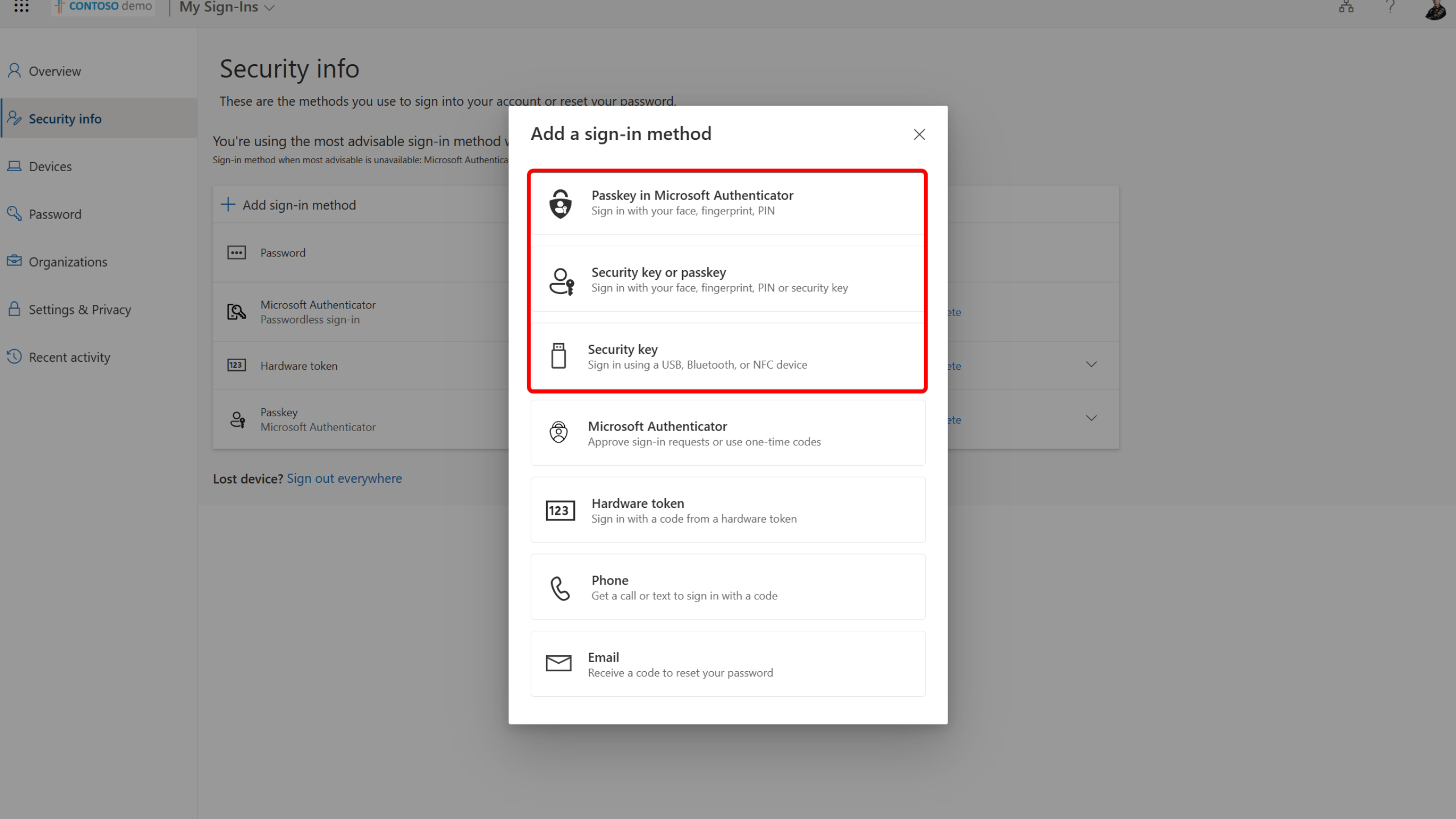
Store passkeys in Android profiles

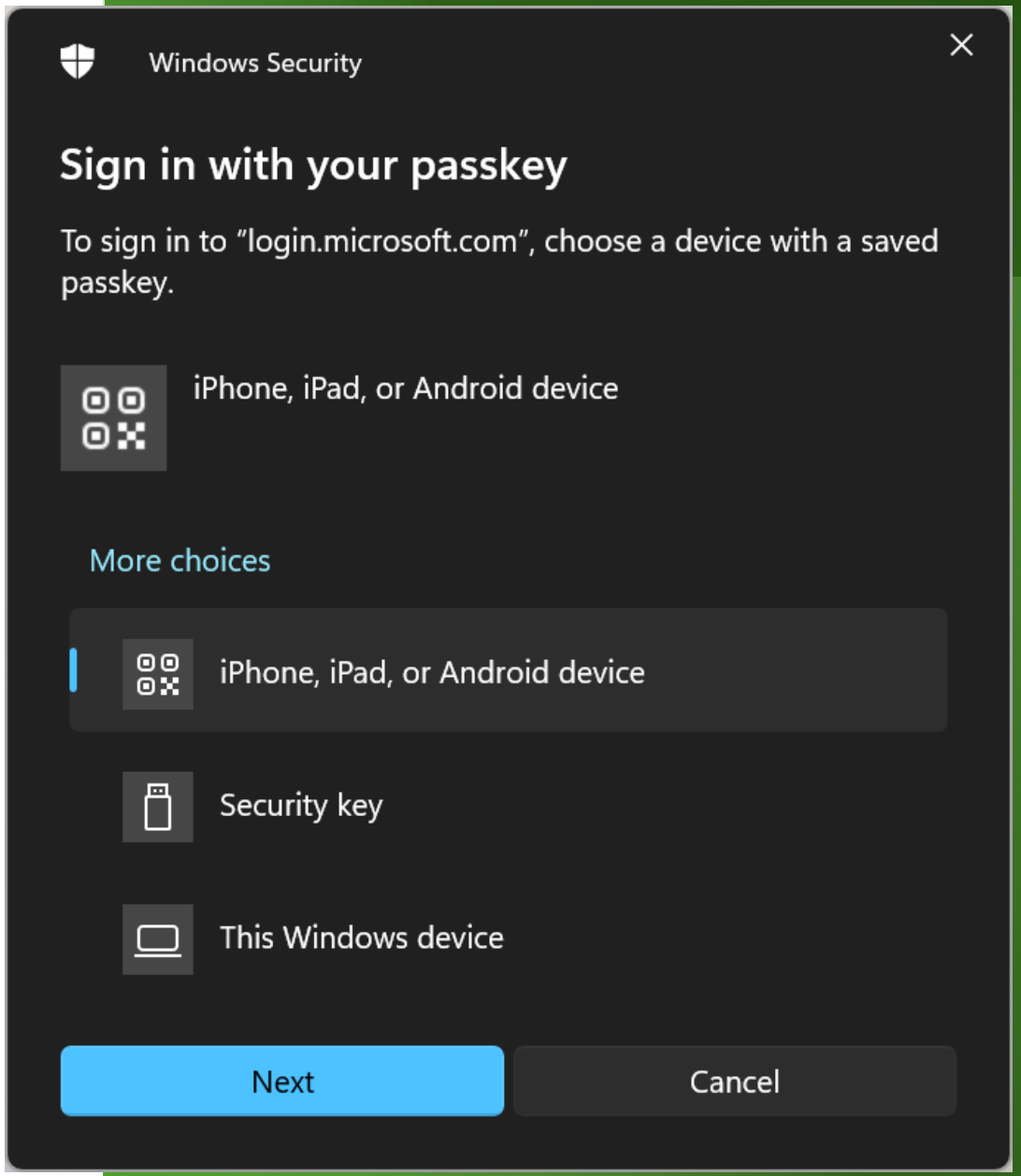
Passkeys on Android are used only from the profile where they're stored. If a passkey is stored in an Android Work profile, it's used from that profile. If a passkey is stored in an Android Personal profile, it's used from that profile. To make sure that users can access and use the passkey they need,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

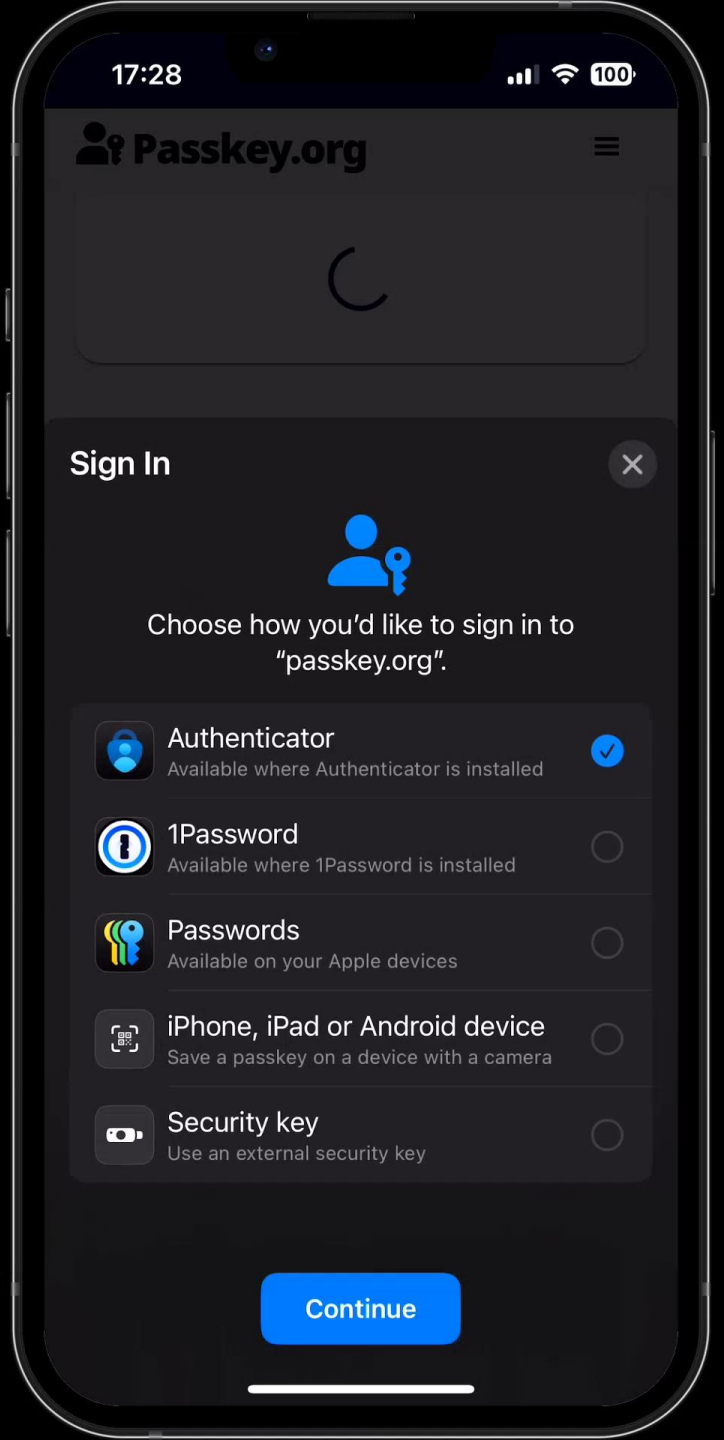
Android struggles PART 2

Lack of scoping for existing security key users

End-user confusion

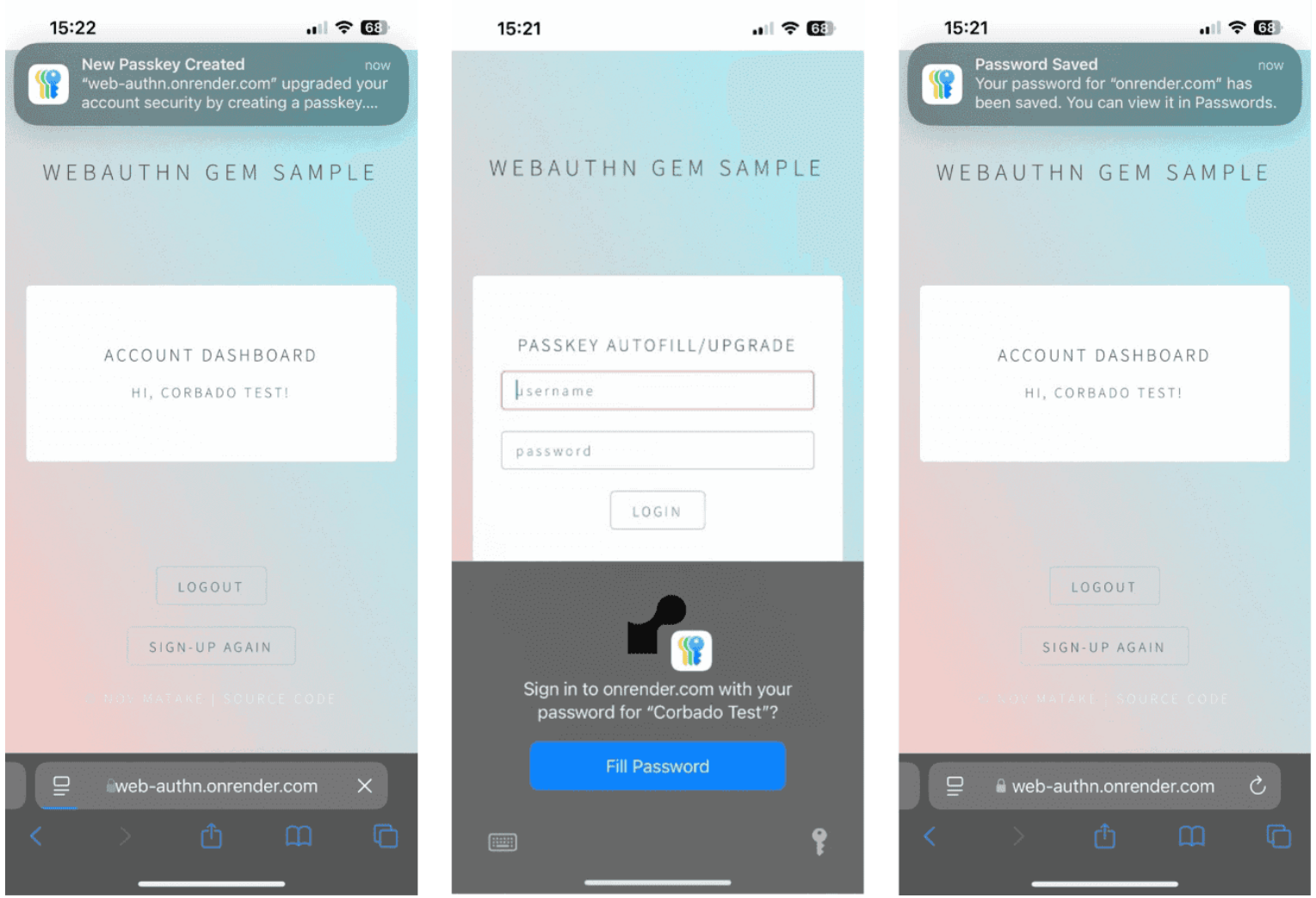

CONTOSO demo
My Sign-Ins
Overview
Security info
Devices
Password
Organizations
Settings & Privacy
Recent activity
Security info
These are the methods you use to sign into your account or reset your password.
You're using the most advisable sign-in method w
Sign-in method when most advisable is unavailable: 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

Automatic passkey upgrades

(as seen in iOS 18)




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

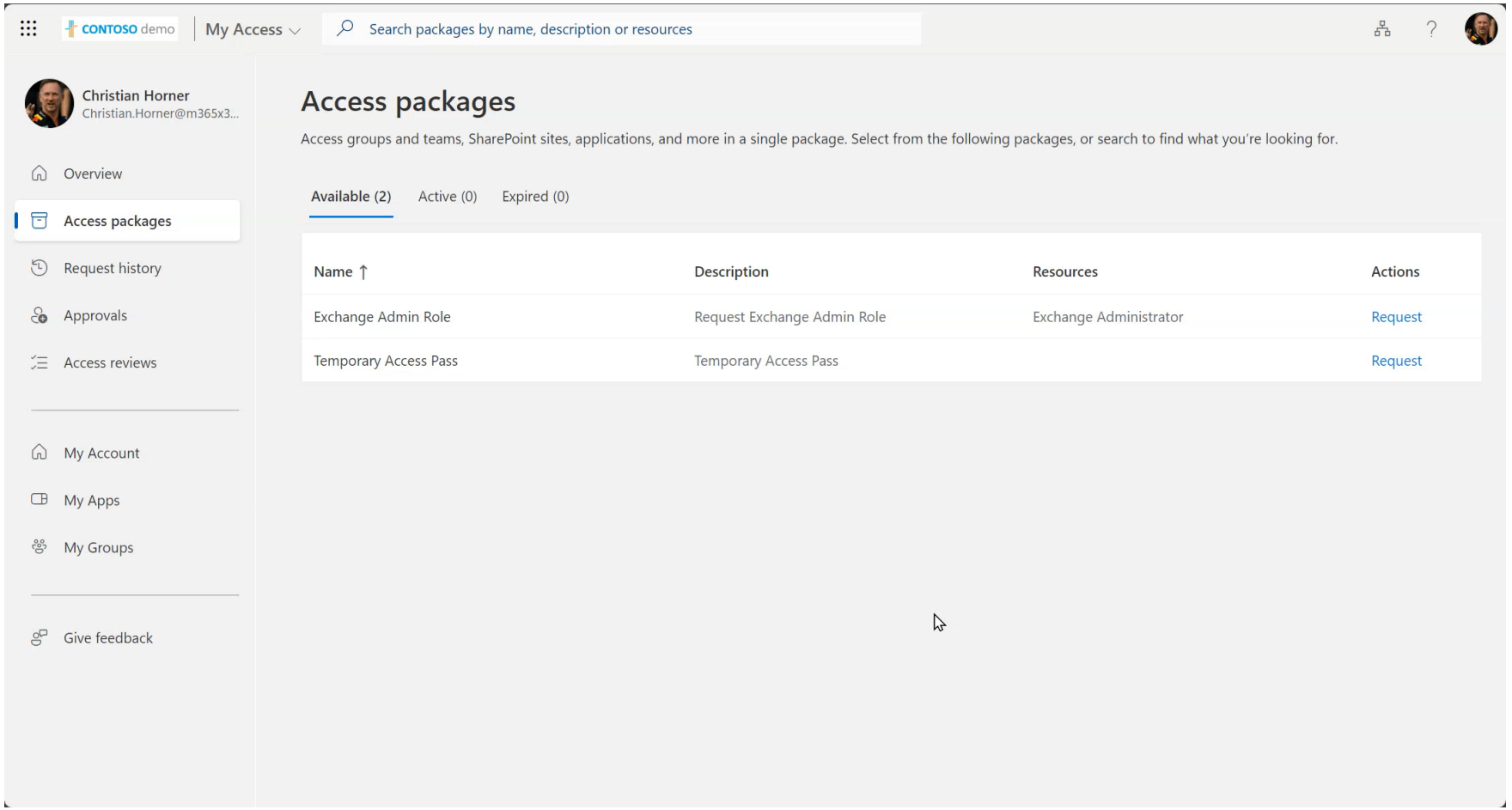
Strengthen onboarding & recovery process

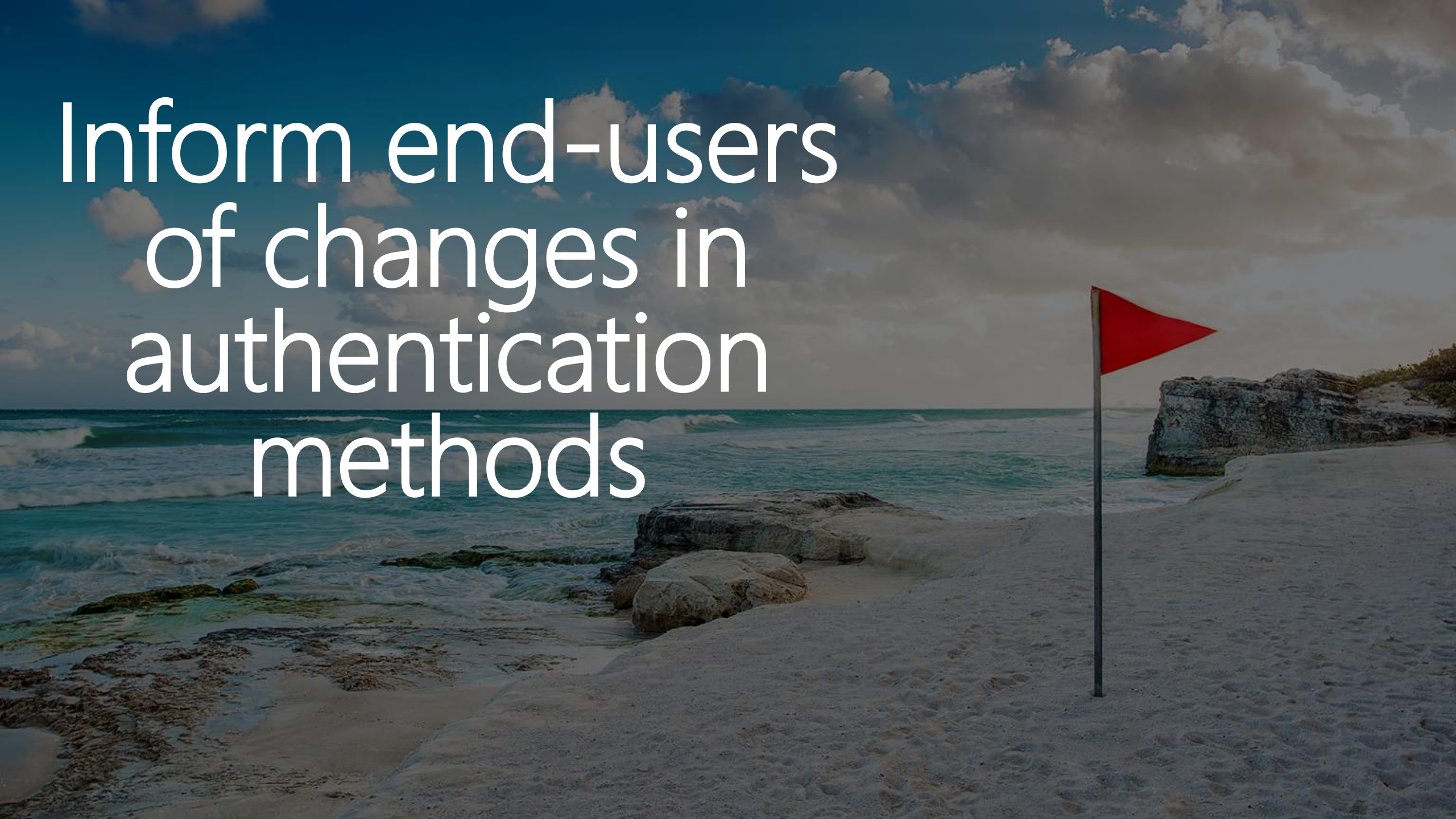
Trusted device

Trusted location

Temporary Access Pass

Request Temporary Access Pass on behalf of users




Inform end-users
of changes in
authentication
methods

Google

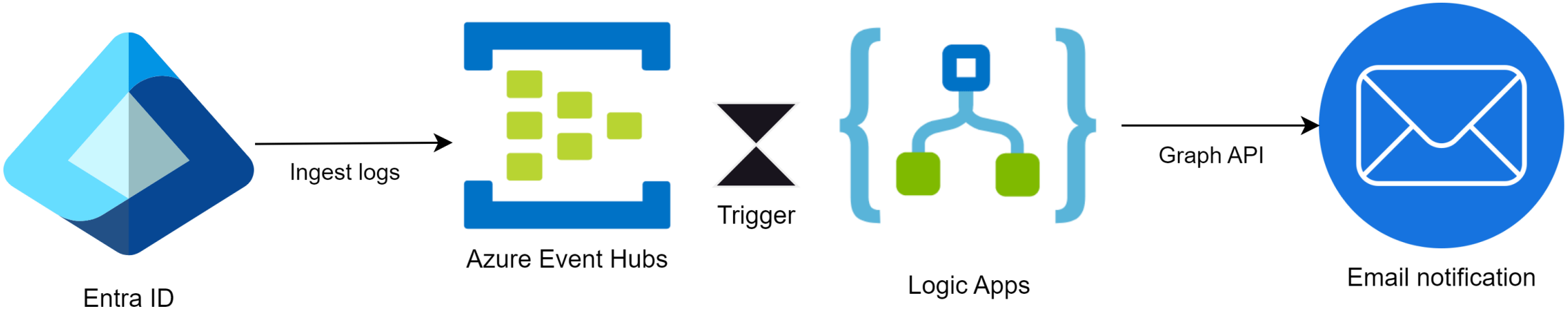
New passkey added to your account

[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: 3[redacted]

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

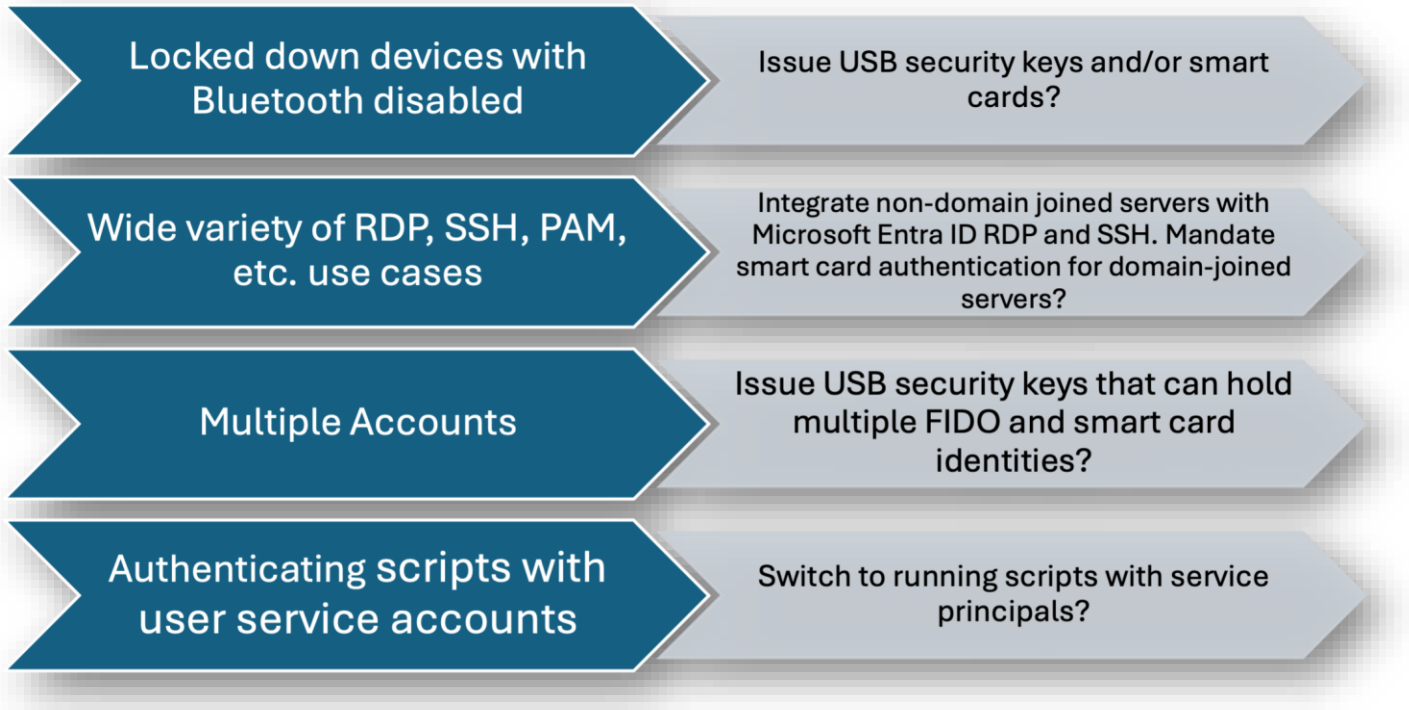
Events

Admin changed phone method for user
Admin registered phone method for user
Admin changed phone method for user
Admin registered phone method for user
Admin registered temporary access pass method for user
Admin deleted temporary access pass method for user
User deleted Mobile Phone Call and SMS
User registered Mobile Phone SMS
User deleted Authenticator App with Notification and Code
User registered Authenticator App with Notification and Code
User registered Fido
User deleted Fido

Start today!

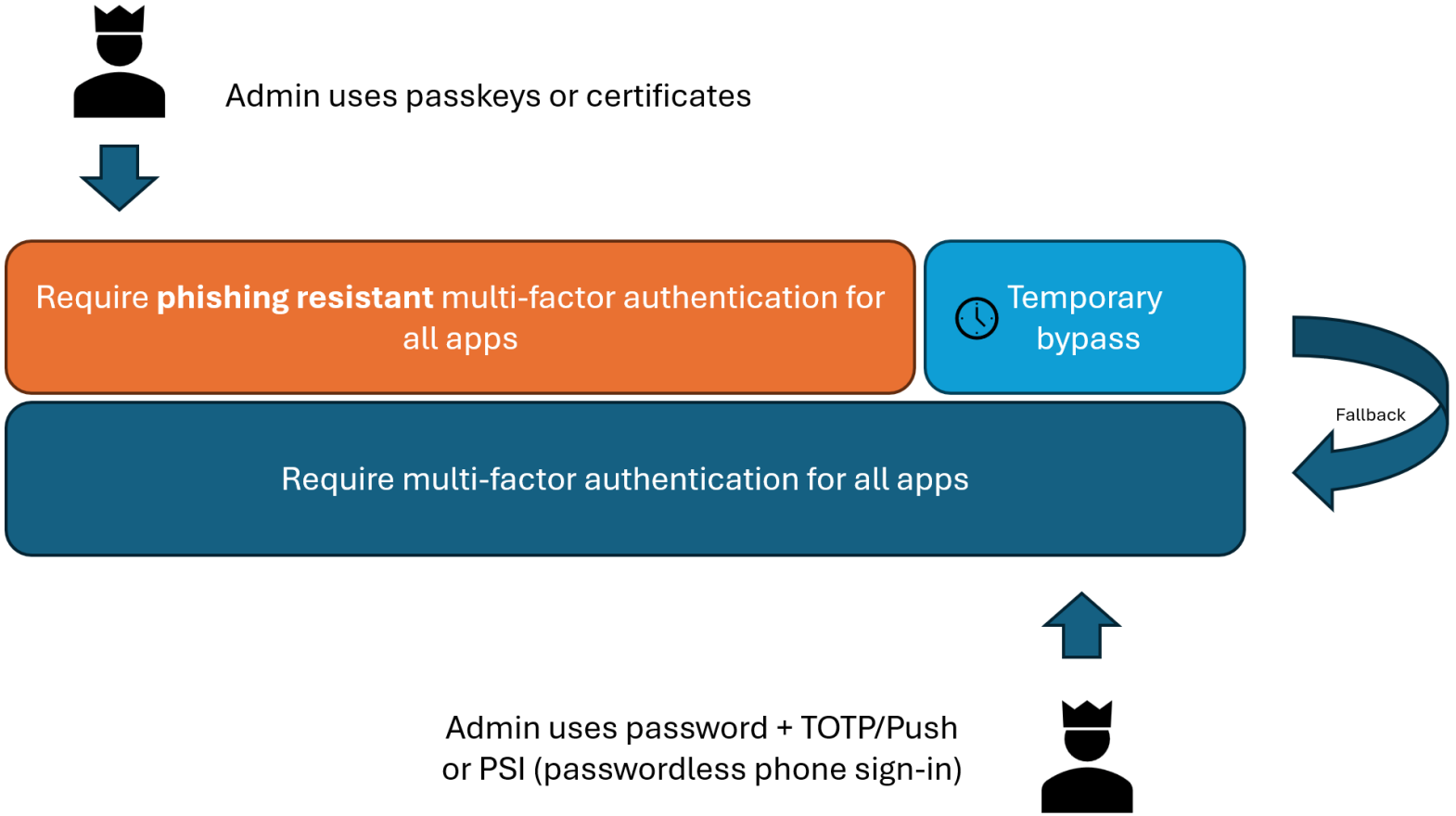
Considerations for specific personas in a phishing-resistant passwordless authentication deployment in Microsoft Entra ID

IT pros/DevOps workers



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

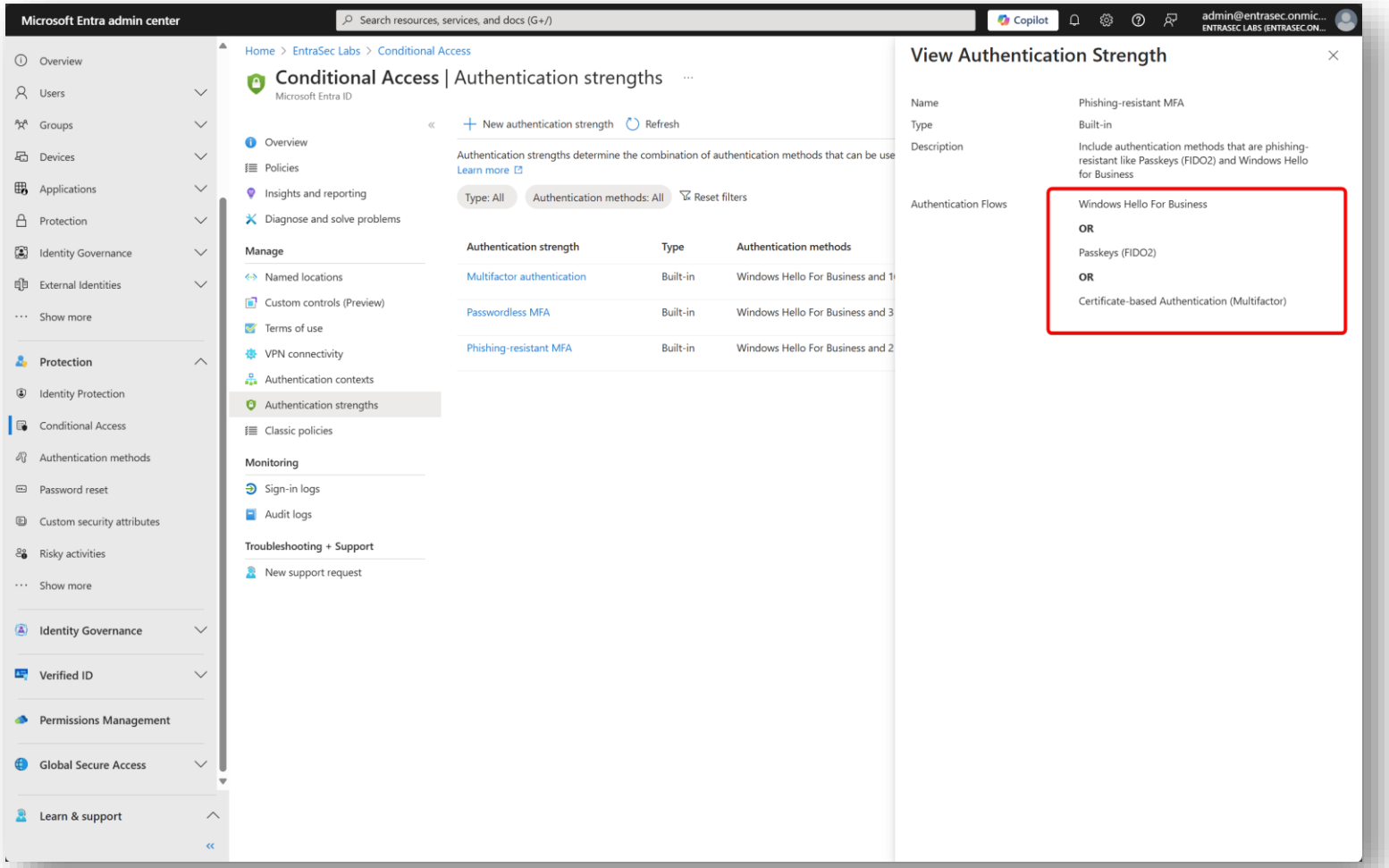
Entra/Azure Admins should be phishing resistant by now



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

Passkey enrolled?

Enforce it!



Avoid Authentication strength Conditional Access policy loops

Use different strengths for desktop and mobile

To avoid costs, first register, then enforce

Test all usecases, not just the happy flow

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
Hackers will go after tokens	Enrollment can be hard	End-users need guidance
Think persona-based	Have different passkeys for different platforms	Get started ASAP


Questions?