The state of passkey at the end of '25

Workplace Ninjas

Thank you Sponsors

www.workplaceninjas.us

Platinum Sponsors

robopack

SOFTWARE CENTRAL

Gold Sponsors

Recast

PATCH MY PC

Microsoft

inforcer

controlUP

DEVICIE

LOGINVSI

glueck kanja

Silver Sponsors

juriba

liquidware

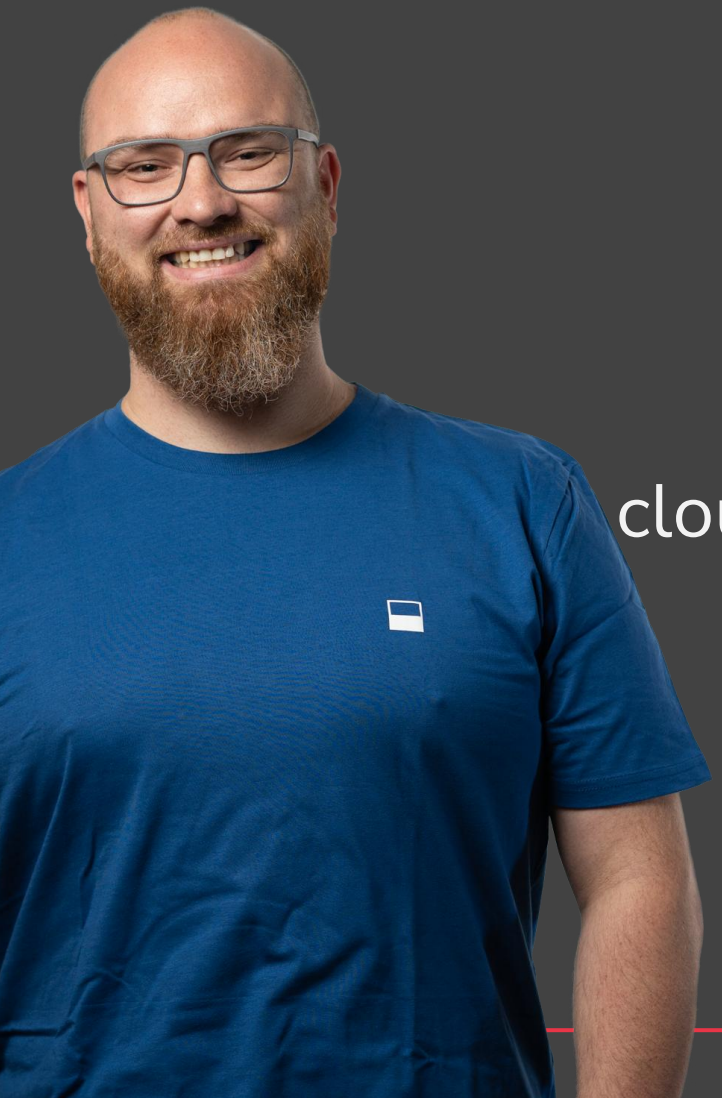
Rimo3

numecent
CLOUDPAGING DELIVERS

FERROQUE SYSTEMS

WEI

About us



Fabian Bader **Chris Brumm**

@fabian_bader @cbrhh

/in/fabianbader /in/christopherbrumm

cloudbrothers.info chris-brumm.com

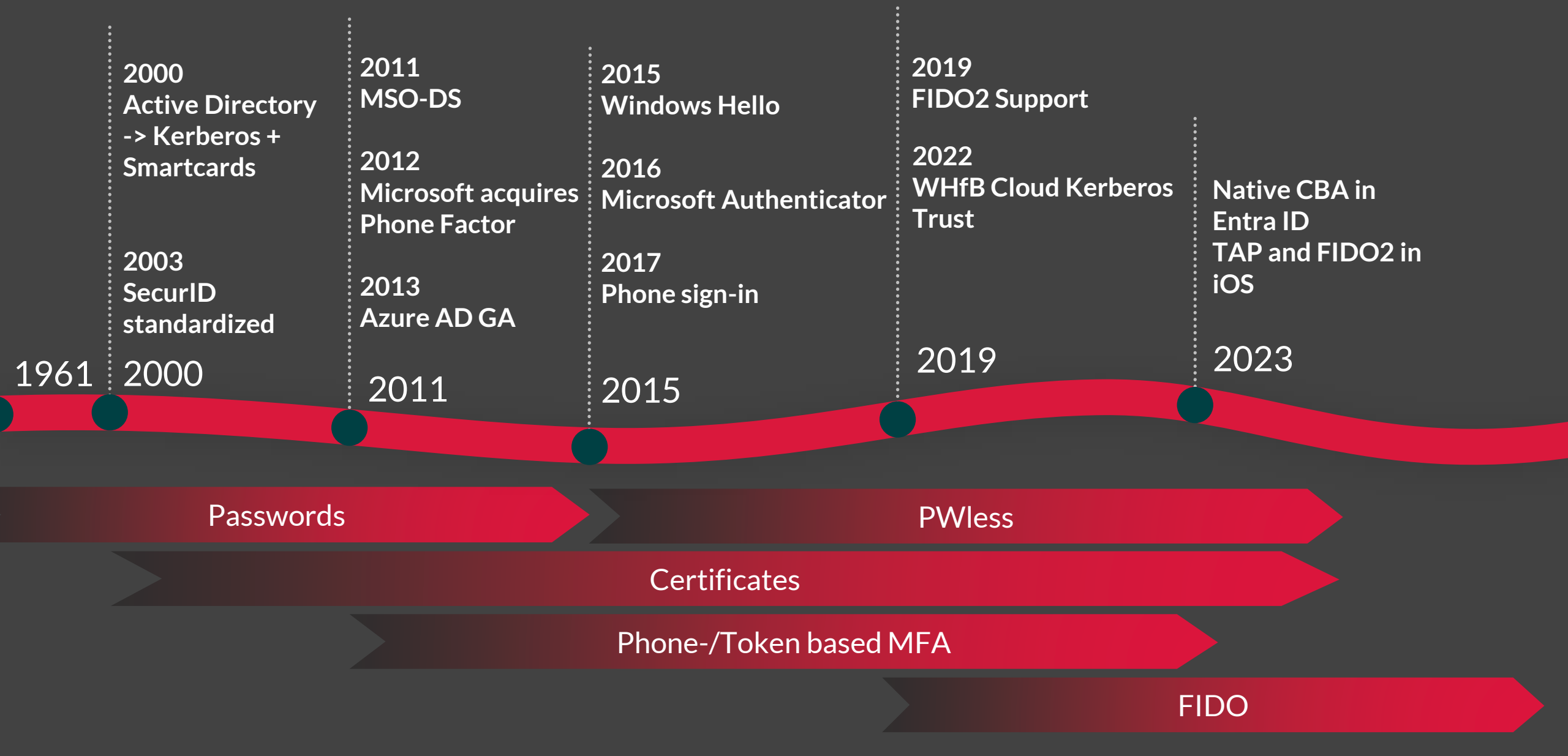
Cyber Security Architects

@

glueck kanja

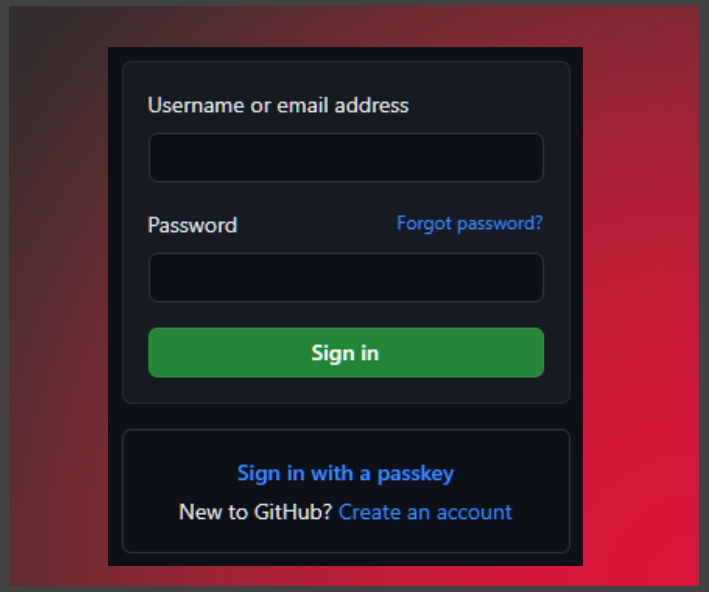
Microsoft MVPs

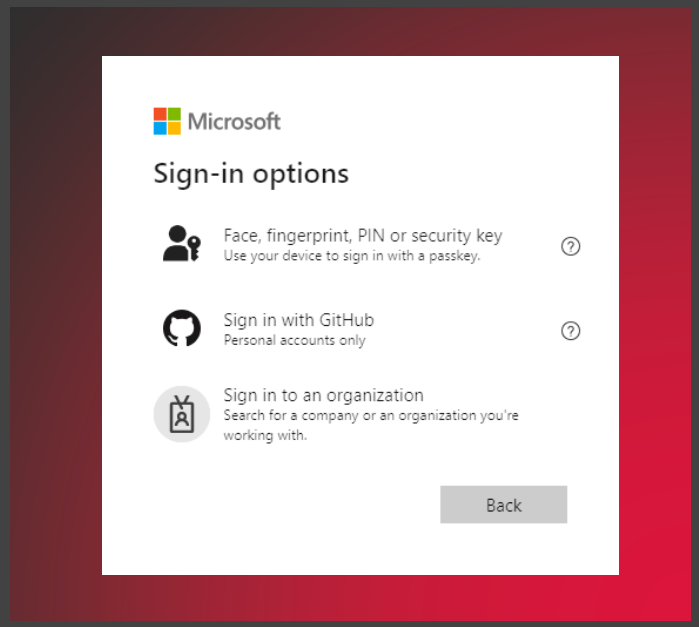
Evolution of Authentication at Microsoft



Evolution of Authentication at Microsoft

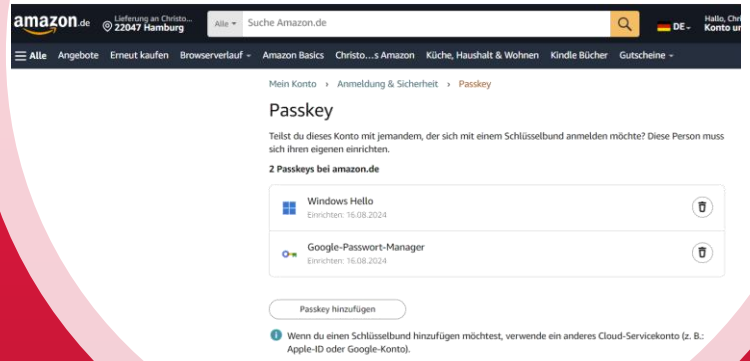
🎉 🎉 🎉 **Passkeys** 🎉 🎉 🎉

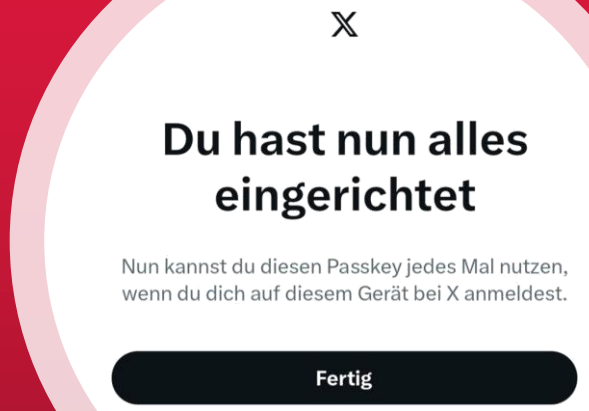


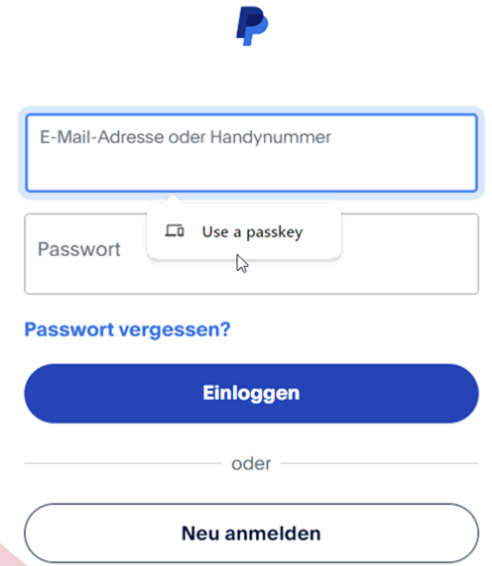


What's a passkey?

- A passkey is a FIDO2/WebAuthn Discoverable Credential
- "Discoverable Credential" means you don't have to enter your username
- Password-less
- Phishing resistant
- Based on cryptographic public and private keys

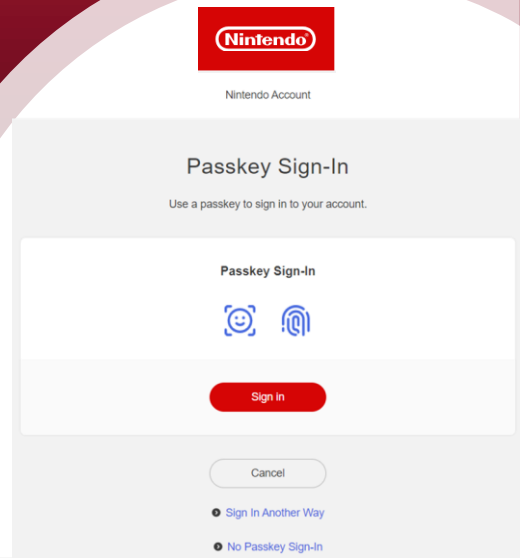






Passkeys used by Chris' family

https://www.passkeys.io/who-supports-passkeys



Consumer want **easy** passkeys!

Synced Keys 🤗

Easy Recovery

Easy Setup

Phishing-resistance

Easy usage

Enterprises want **secure** passkeys!

Synced Keys 🧐

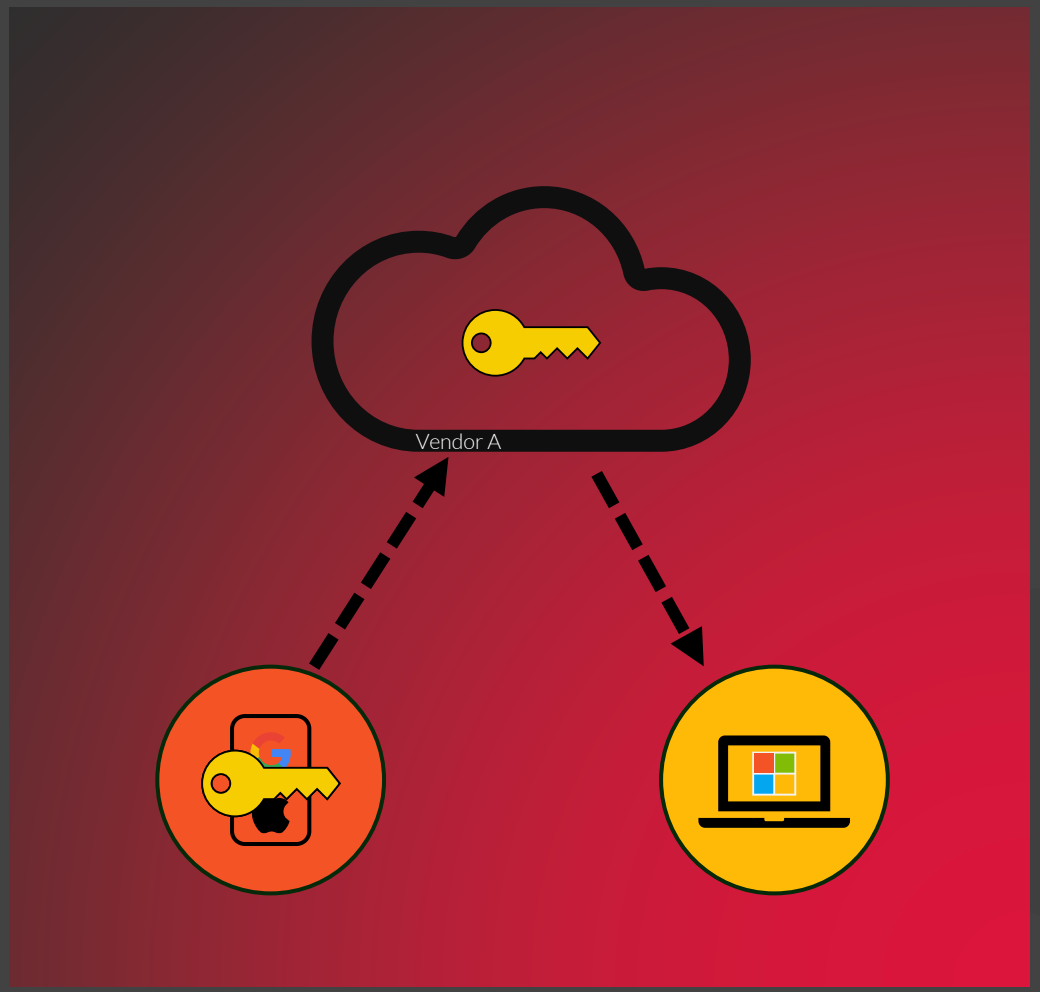
Secure Recovery

Controlled Setup

Phishing-resistance

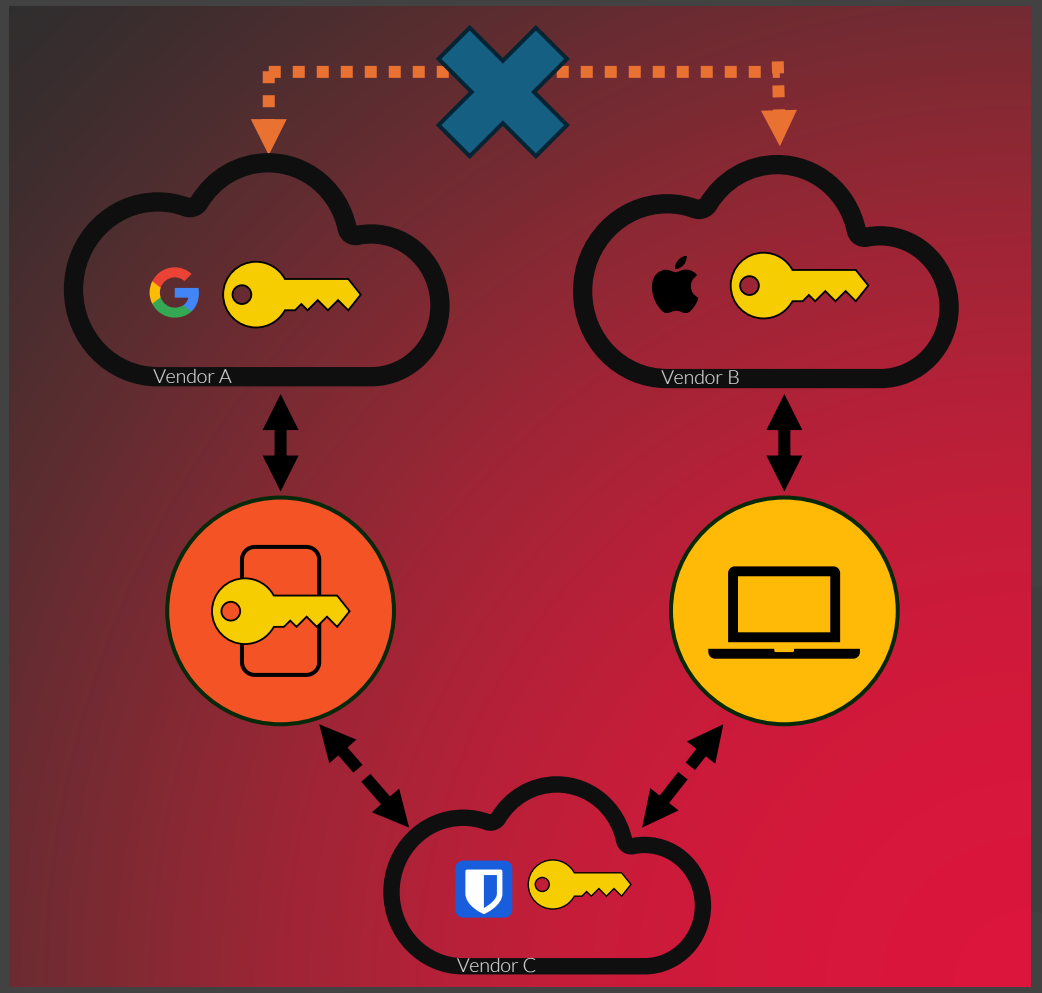
Controlled usage

Synced vs. Device-bound passkeys



- Passkeys are synced by default
- Private key is sent to your provider
- Restore security is based on the account recovery mechanism of the provider
- Hard to track or secure for enterprises
- Backup to vendor or third-party passkey provider

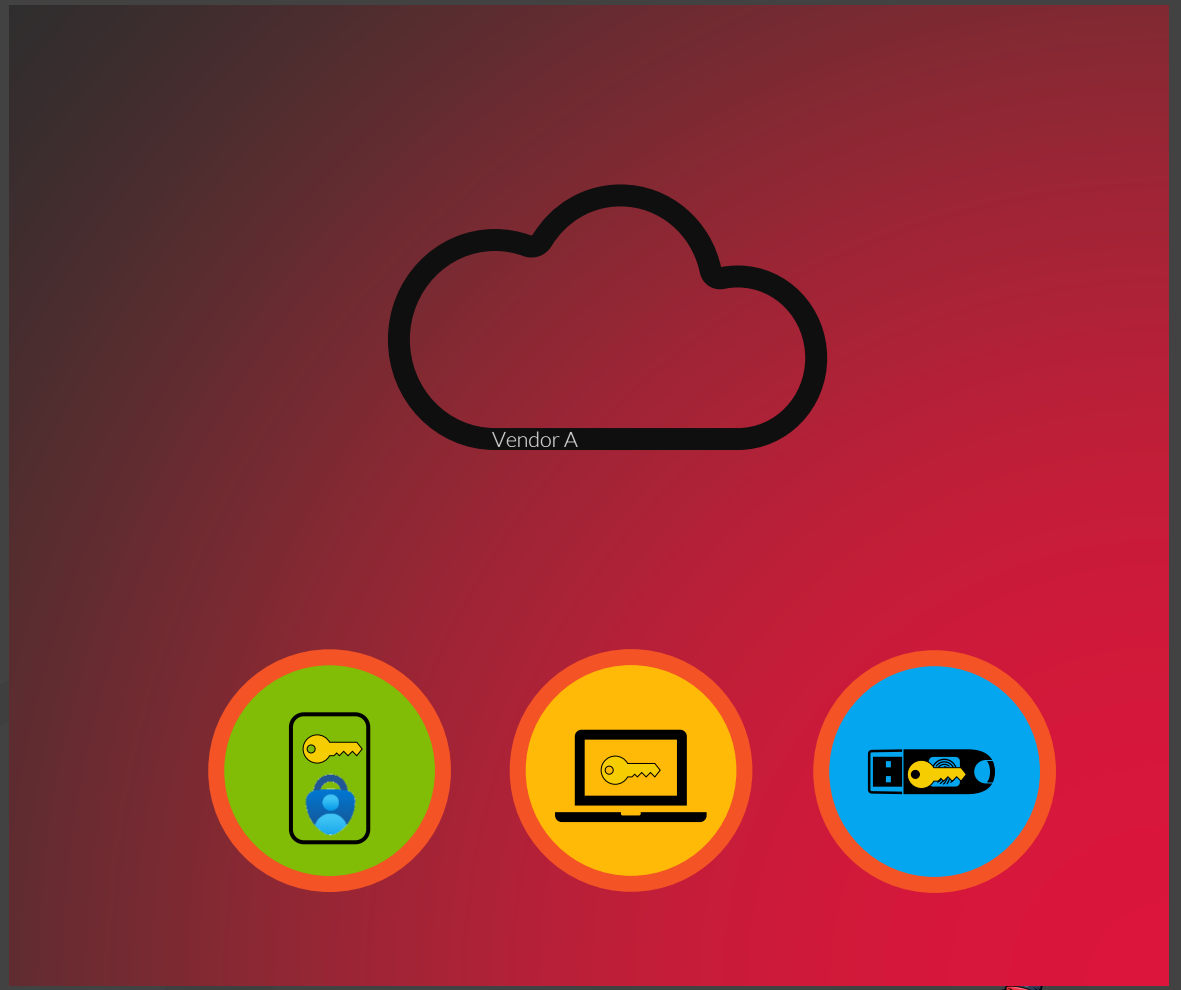
Synced vs. Device-bound passkeys



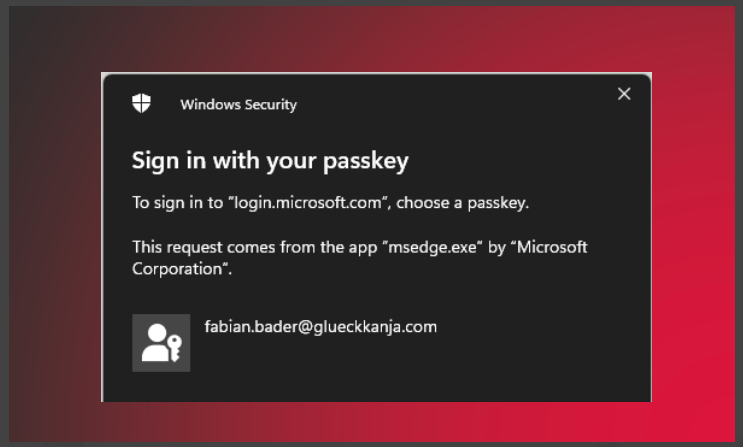
- Native cross vendor sync is not possible
- Workarounds
  - Cross-Device Authentication
  - Third-party passkey provider
  - Credential Exchange Protocol (CXP)

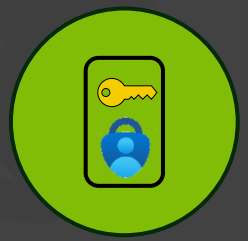
Synced vs. Device-bound passkeys

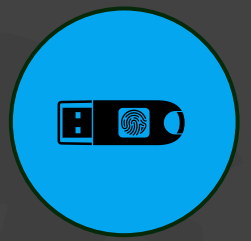
- The private key cannot leave the device
- FIDO2 security keys are device-bound passkeys
- Microsoft Authenticator creates a device-bound passkey
- Recovery = New Setup



Microsofts current implementation







Auth Funnel - Thanks @merill

Authentication Methods available

Authentication Methods allowed for the user
Configured through Authentication Policies

Authentication methods registered by the user

Authentication methods the user must use
Configured through authentication strengths

Authentication Methods allowed for the user
Configured through Authentication Policies

Authentication methods | Policies

dev.bader.cloud - 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
Built-In		
Passkey (FIDO2)	All users	Yes
Microsoft Authenticator	All users	Yes
SMS		No
Temporary Access Pass	All users	Yes
Hardware OATH tokens (Preview)		No
Software OATH tokens		No
Voice call		No
Email OTP		Yes
Certificate-based authentication		No
QR code		No

Authentication methods | Policies

dev.bader.cloud - 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
Built-In		
Passkey (FIDO2)	All users	Yes
Microsoft Authenticator	All users	Yes
SMS		No
Temporary Access Pass	All users	Yes
Hardware OATH tokens (Preview)		No
Software OATH tokens		No
Voice call		No
Email OTP		Yes
Certificate-based authentication		No
QR code		No

Passkey (FIDO2) settings

Passkeys (FIDO2) Authentication Methods (Preview)

Your organization has opted into public preview for synced passkeys and passkey profiles. Your previous passkey settings have been moved into ...

Opt-out of public preview

Passkeys are a phishing-resistant, standards-based passwordless authentication method that can be stored on a variety of security key models or passkey providers. Passkeys are not usable in the self-service password reset flow. Learn more

Enable and target | Configure

Enable: On

Include | Exclude

Add target

Name	Type	Passkey profiles (preview)
All users	Group	Default passkey profile

Save | Discard

Passkey (FIDO2) settings

Passkeys (FIDO2) Authentication Methods (Preview)

Your organization has opted into public preview for synced passkeys and passkey profiles. Your previous passkey settings have been moved into ...

Opt-out of public preview

Passkeys are a phishing-resistant, standards-based passwordless authentication method that can be stored on a variety of security key models or passkey providers. Passkeys are not usable in the self-service password reset flow. Learn more

Enable and target | Configure

General

Allow self-service set-up

Passkey profiles

At least one passkey profile must be applied to each target in this policy. The default passkey profile cannot be deleted or renamed. Up to 3 passkey profiles are supported.

Learn more

Add profile (preview)

Name	Enforce attestation	Type	Key restrictions
Default passkey profile	Yes	Device-bound	No

Save | Discard

Home > Authentication methods | Policies >

Passkey (FIDO2) settings

Passkeys (FIDO2) Authentication Methods (Preview)

Your organization has opted into public preview for synced passkeys and passkey p

Passkeys are a phishing-resistant, standards-based passwordless authentication me
usable in the self-service password reset flow. Learn more

Enable and target | Configure

General

Allow self-service set-up

Passkey profiles

At least one passkey profile must be applied to each target in this policy. The defau
supported.

Add profile (preview)

Name	Enforce attestation	Typ
Default passkey profile	Yes	Dev

Save Discard

Edit passkey profile

Certain combinations of these settings could target passkeys that may not exist. This can prevent your users from registering and signing in with a passkey.
View compatibility documentation

Name *: Default passkey profile

Enforce attestation

Target types *: Device-bound

Target specific AAGUIDs

Save Discard

Passkey (FIDO2) settings

Passkeys (FIDO2) Authentication Methods (Preview)

Your organization has opted into public preview for synced passkeys and passkey profiles. Your previous passkey settings have been moved into ...

Opt-out of public preview

Passkeys are a phishing-resistant, standards-based passwordless authentication method that can be stored on a variety of security key models or passkey providers. Passkeys are not usable in the self-service password reset flow. Learn more

Enable and target | Configure

General

Allow self-service set-up

Passkey profiles

At least one passkey profile must be applied to each target in this policy. The default passkey profile cannot be deleted or renamed. Up to 3 passkey profiles are supported.

Learn more

Add profile (preview)

Name	Enforce attestation	Type	Key restrictions
Default passkey profile	Yes	Device-bound	No

Save | Discard

Home > Authentication methods | Policies >

Passkey (FIDO2) settings

Passkeys (FIDO2) Authentication Methods (Preview)

Your organization has opted into public preview for synced passkeys and passkey p

Passkeys are a phishing-resistant, standards-based passwordless authentication me
usable in the self-service password reset flow. Learn more

Enable and target | Configure

General

Allow self-service set-up

Passkey profiles

At least one passkey profile must be applied to each target in this policy. The defau
supported.

+ Add profile (preview)

Name	Enforce attestation	Typ
Default passkey profile	Yes	Dev

Save | Discard

Add passkey profile

Certain combinations of these settings could target passkeys that may not exist. This can prevent your users from registering and signing in with a passkey.
View compatibility documentation

Name * Syncable passkeys

Enforce attestation

Target types * Synced (preview), Device-bound

Target specific AAGUIDs

Save | Discard

Home > Authentication methods | Policies >

Passkey (FIDO2) settings

Passkeys (FIDO2) Authentication Methods (Preview)

Your organization has opted into public preview for synced passkeys and passkey profiles. Your previous passkey settings have been moved into ...

Opt-out of public preview

Passkeys are a phishing-resistant, standards-based passwordless authentication method that can be stored on a variety of security key models or passkey providers. Passkeys are not usable in the self-service password reset flow. Learn more

Enable and target | Configure

General

Allow self-service set-up

This profile configuration includes type restrictions but attestation is not enforced, so we cannot guarantee the syncability of the security key model or passkey provider.

Syncable passkeys	No	Device-bound, Synced (preview)	No

Save | Discard

Passkey (FIDO2) settings

Passkeys (FIDO2) Authentication Methods (Preview)

Your organization has opted into public preview for synced passkeys and passkey profiles. Your previous passkey settings have been moved into ...

Opt-out of public preview

Passkeys are a phishing-resistant, standards-based passwordless authentication method that can be stored on a variety of security key models or passkey providers. Passkeys are not usable in the self-service password reset flow. Learn more

Enable and target | Configure

Enable: On

Include | Exclude

Add target

Name	Type	Passkey profiles (preview)
All users	Group	Default passkey profile

Save | Discard

Passkey (FIDO2) settings

Passkeys (FIDO2) Authentication Methods (Preview)

Your organization has opted into public preview for synced passkeys and passkey profiles. Your previous passkey settings have been moved into ...

Opt-out of public preview

Passkeys are a phishing-resistant, standards-based passwordless authentication method that can be stored on a variety of security key models or passkey providers. Passkeys are not usable in the self-service password reset flow. Learn more

Enable and target | Configure

Enable: On

Include | Exclude

+ Add target

- All users
- Select targets

	Type	Passkey profiles (preview)
All users	Group	Default passkey profile

Save | Discard

Add directory members

Try changing or adding filters if you don't see what you're looking for.

Search

cfg - Syncable Passkeys

1 result found

Groups

	Name	Email
☑	C- cfg - Syncable Passkeys	

Selected directory members (1)

Reset

C- cfg - Syncable Passkeys

Select

Passkey (FIDO2) settings

Passkeys (FIDO2) Authentication Methods (Preview)

Your organization has opted into public preview for synced passkeys and passkey profiles. Your previous passkey settings have been moved into ...

Opt-out of public preview

Passkeys are a phishing-resistant, standards-based passwordless authentication method that can be stored on a variety of security key models or passkey providers. Passkeys are not usable in the self-service password reset flow. Learn more

Enable and target | Configure

Enable: On

Include | Exclude

Add target

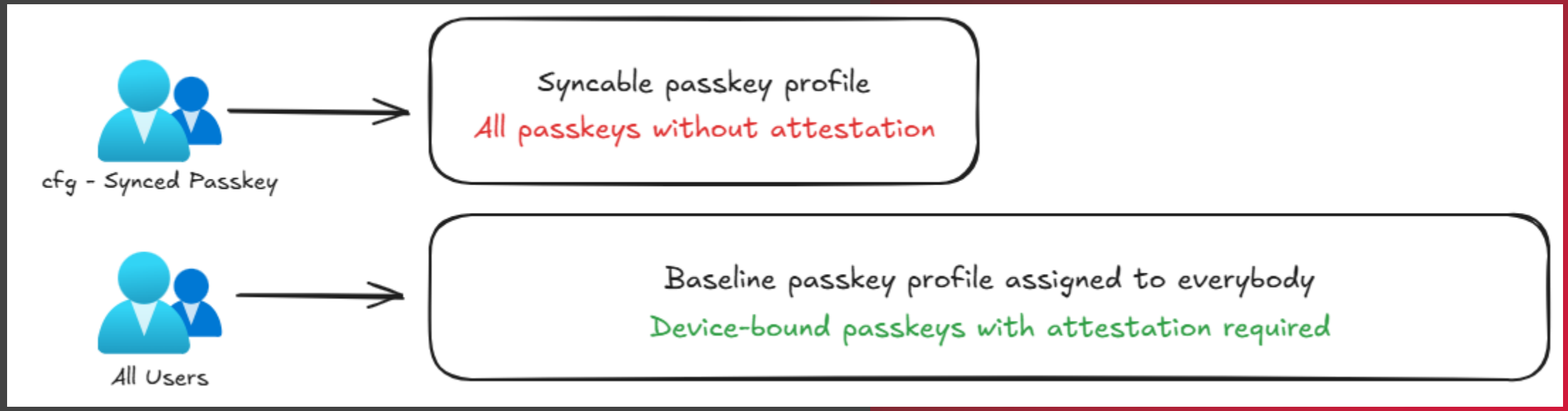
Name	Type	Passkey profiles (preview)
All users	Group	Default passkey profile
cfg - Syncable Passkeys	Group	Select passkey profiles

- [ ] All
- [ ] Default passkey profile
- [x] Syncable passkeys

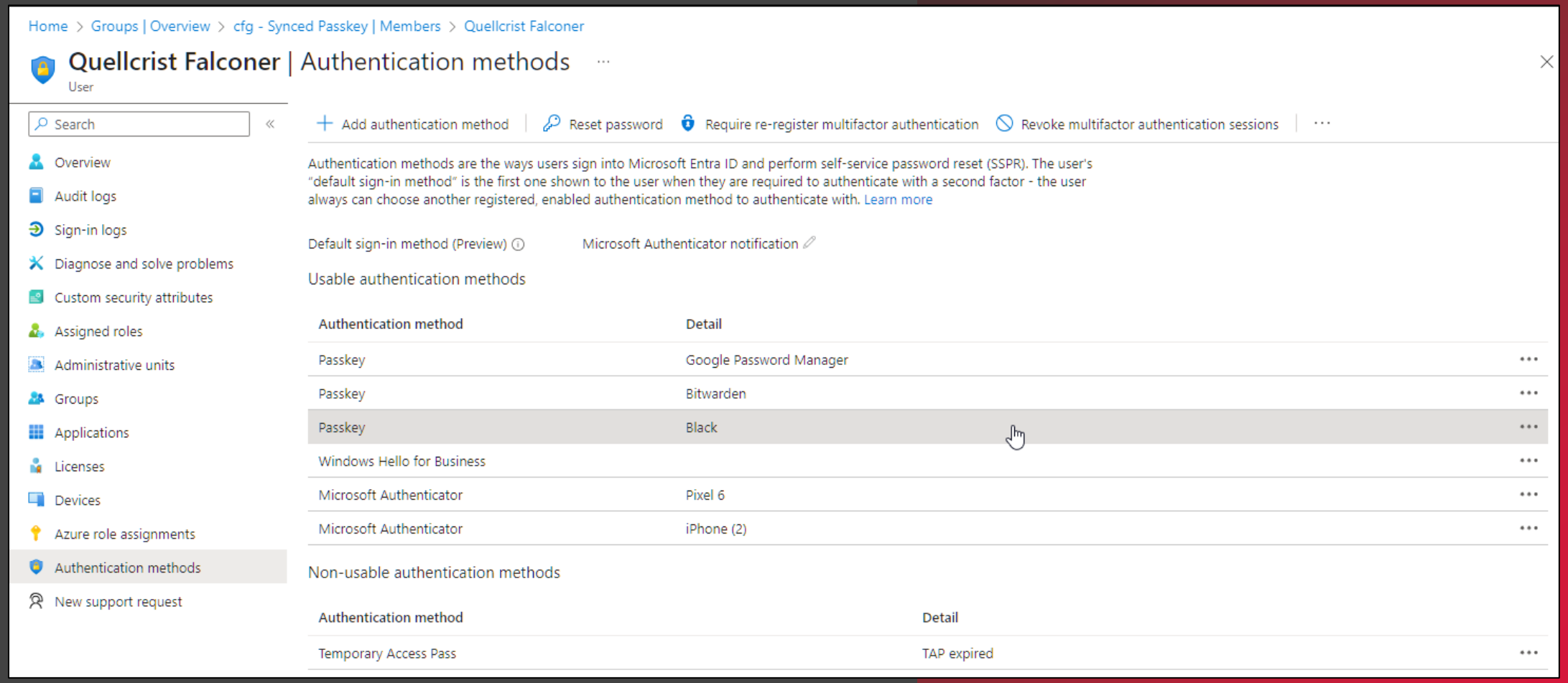
Save | Discard

Recommendation

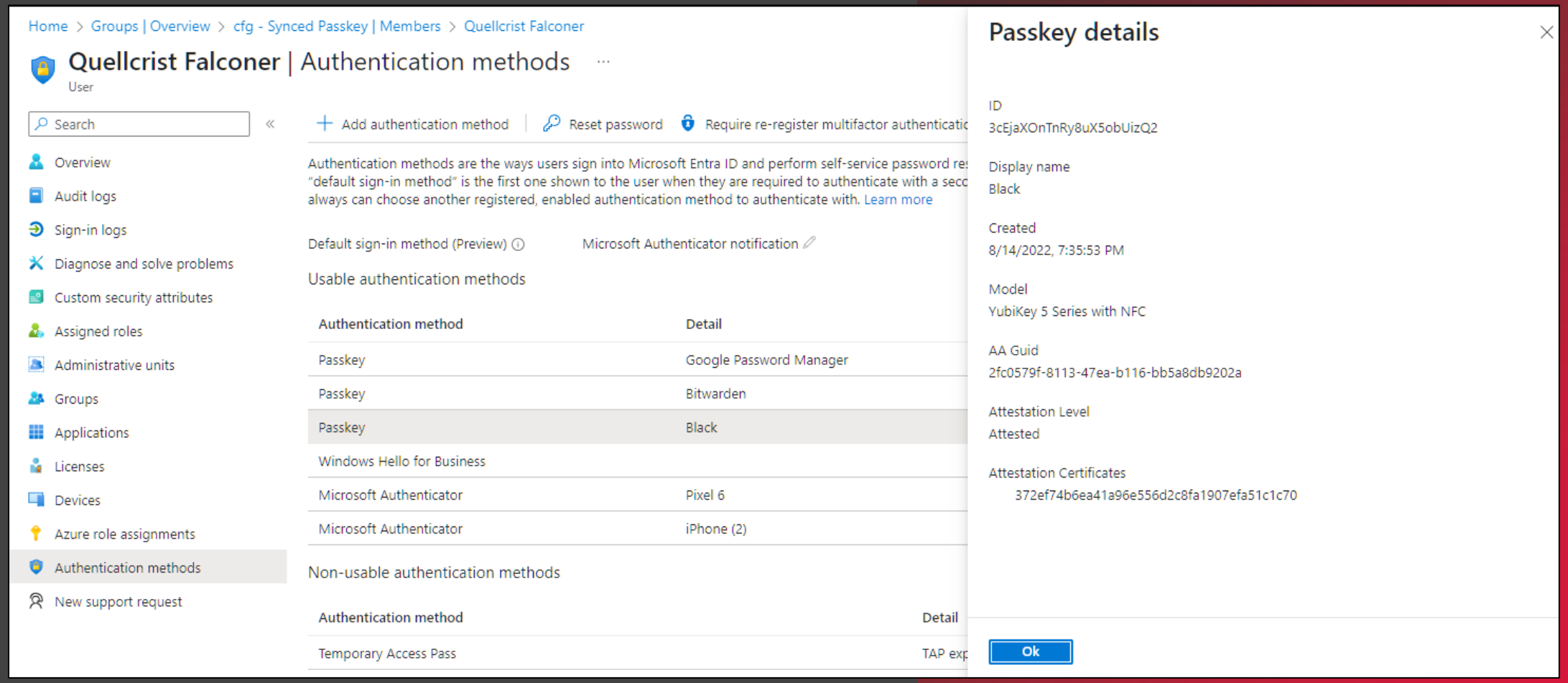
Authentication Methods allowed for the user
Configured through Authentication Policies



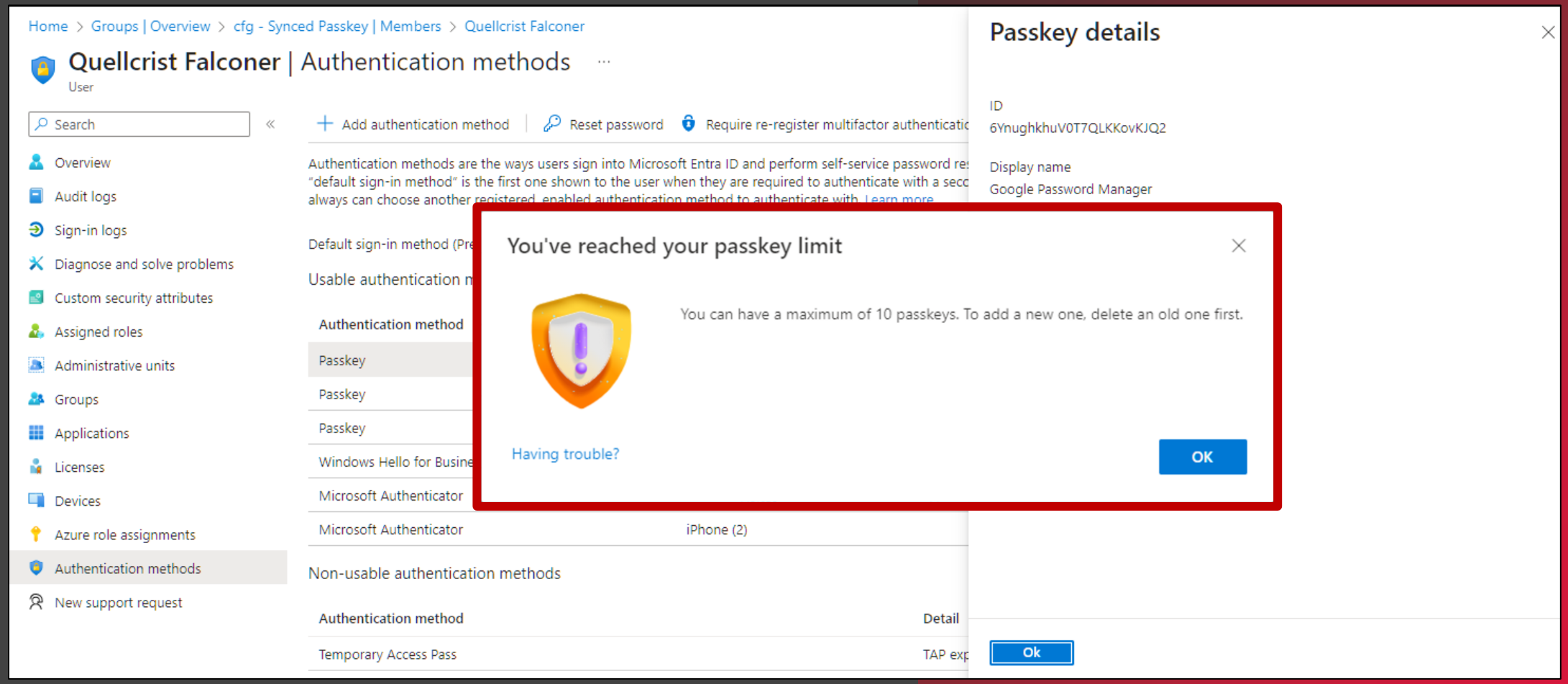
Authentication methods registered by the user



Authentication methods registered by the user

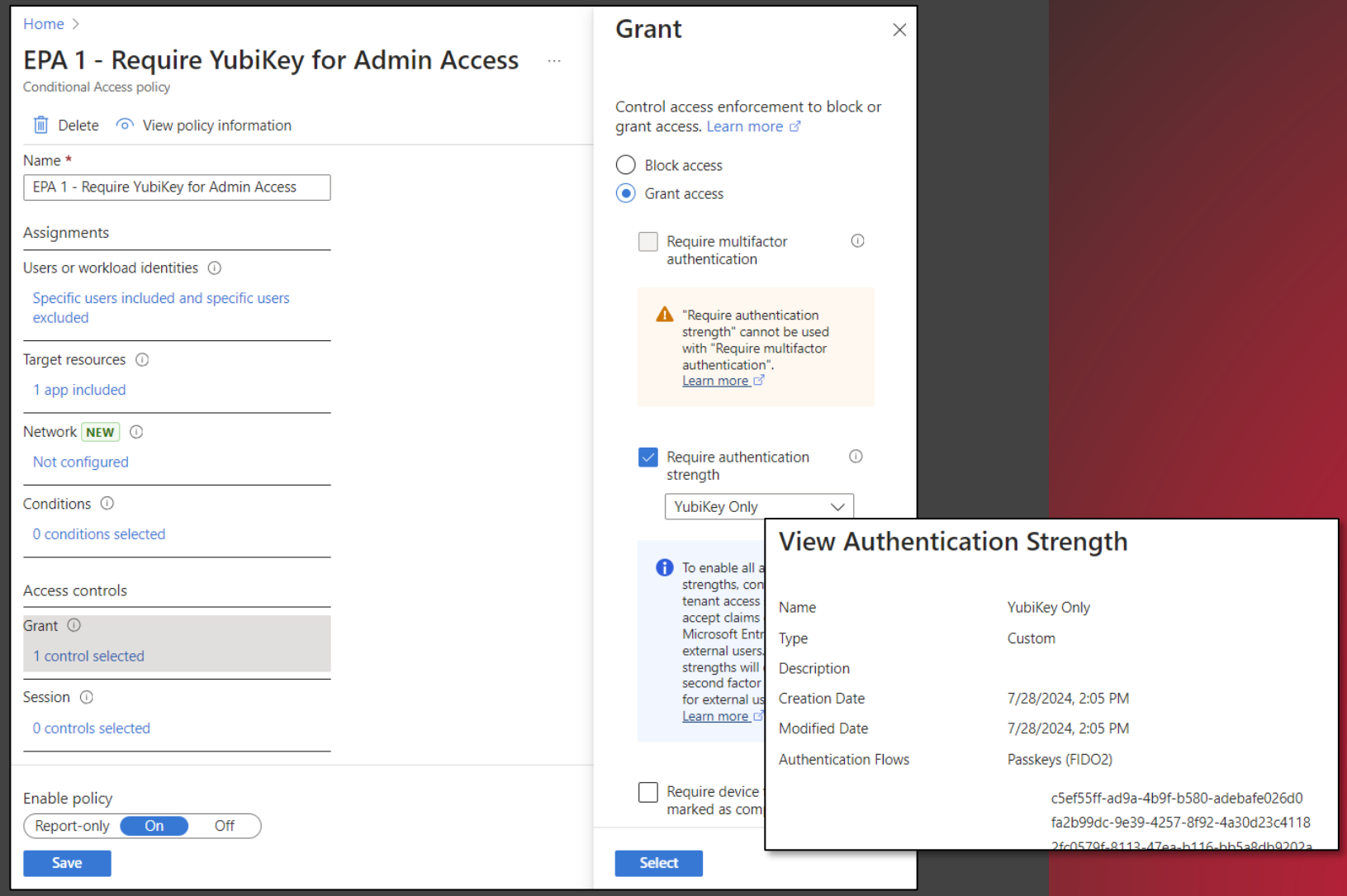


Authentication methods registered by the user



Define which Passkeys can be used in specific situations

Authentication methods the user must use
Configured through authentication strengths



Auth Funnel - Thanks @merill

Authentication Methods available

Authentication Methods allowed for the user
Configured through Authentication Policies

Authentication methods registered by the user

Authentication methods the user must use
Configured through authentication strengths

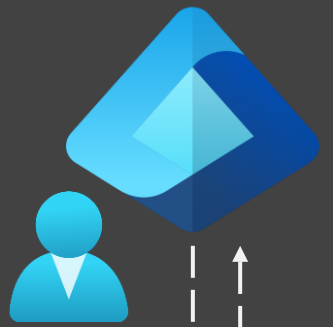
Attestation? AAGUID?

Authenticator Attestation **GUID** = **AAGUID**

1. Credential key pair generated
2. Sign public with attestation private key

3. Send signed public key to Entra ID

AAGUID: dd86a2da-86a0-4cbe-b462-4bd31f57bc6f
Vendor: Yubikey
Product: YubiKey Bio - FIDO Edition
Firmware: 5.7



4. Request Certificate information from MDS
5. Validate signed public key
6. Store public key with user object

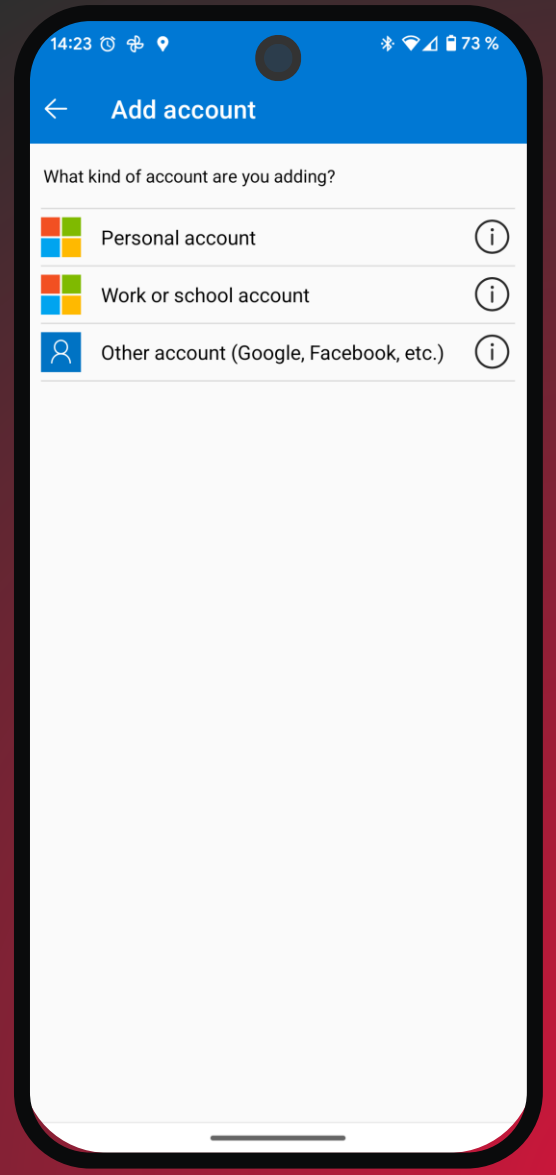
FIDO MDS

fido™ ALLIANCE

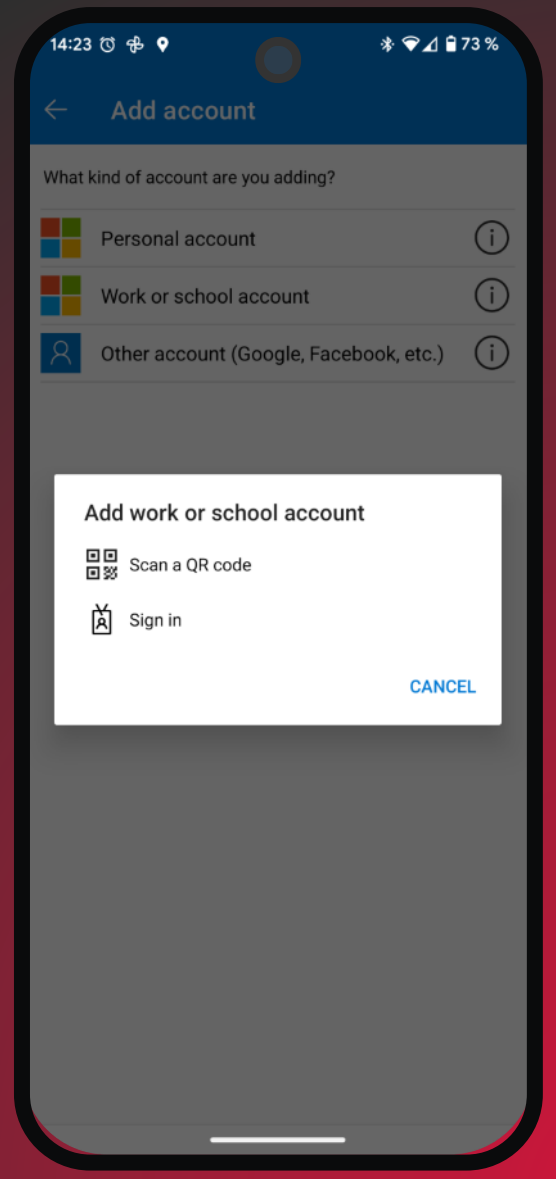
https://aaguid.nicolasuter.ch/
https://fidoalliance.org/fido-technotes-the-truth-about-attestation/

User experience in the lab

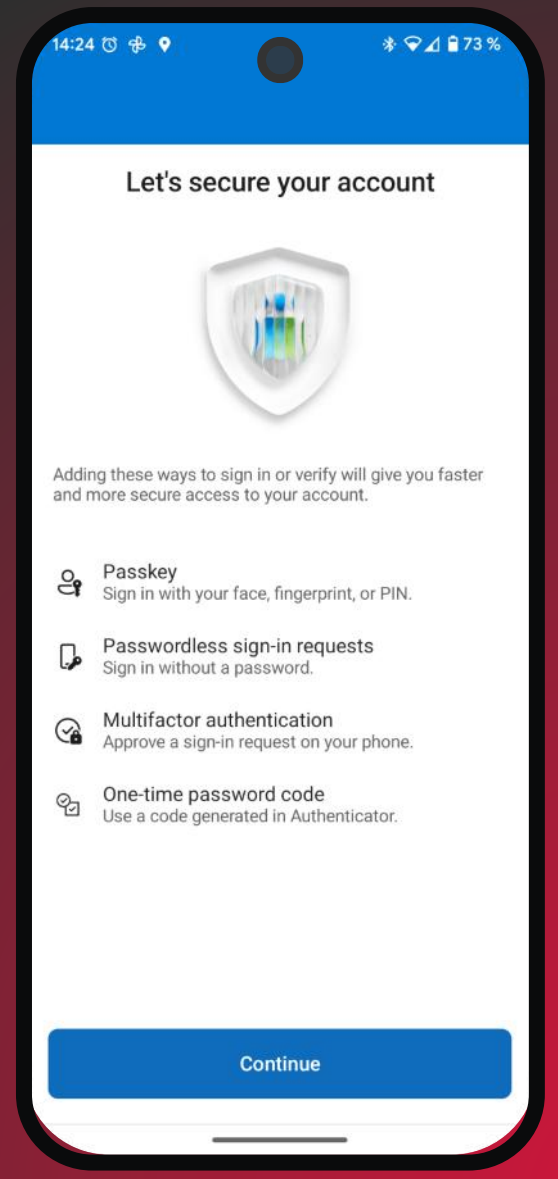
User experience in the lab



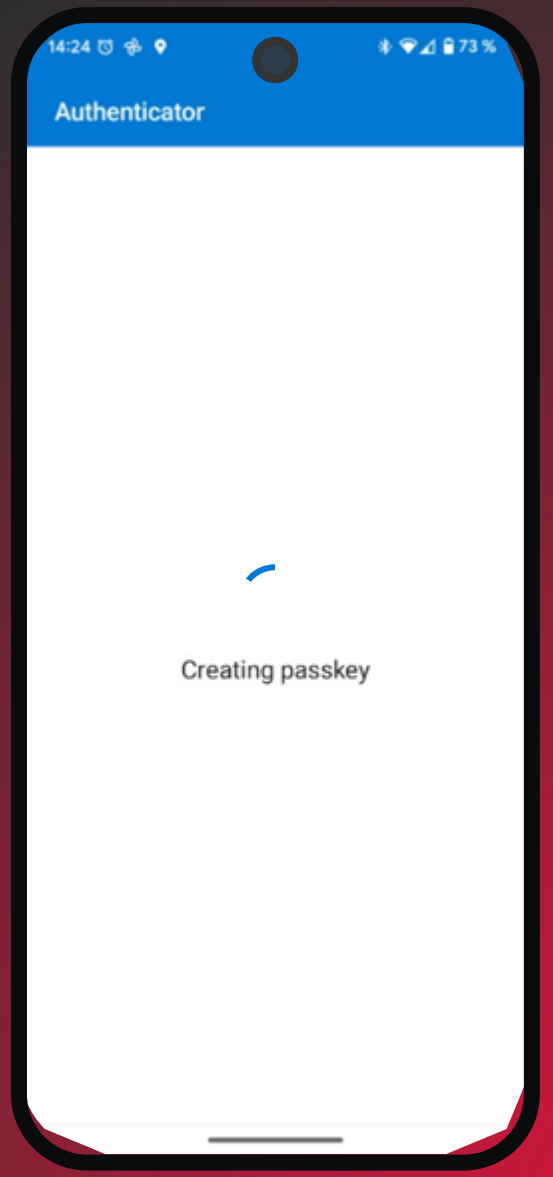
User experience in the lab



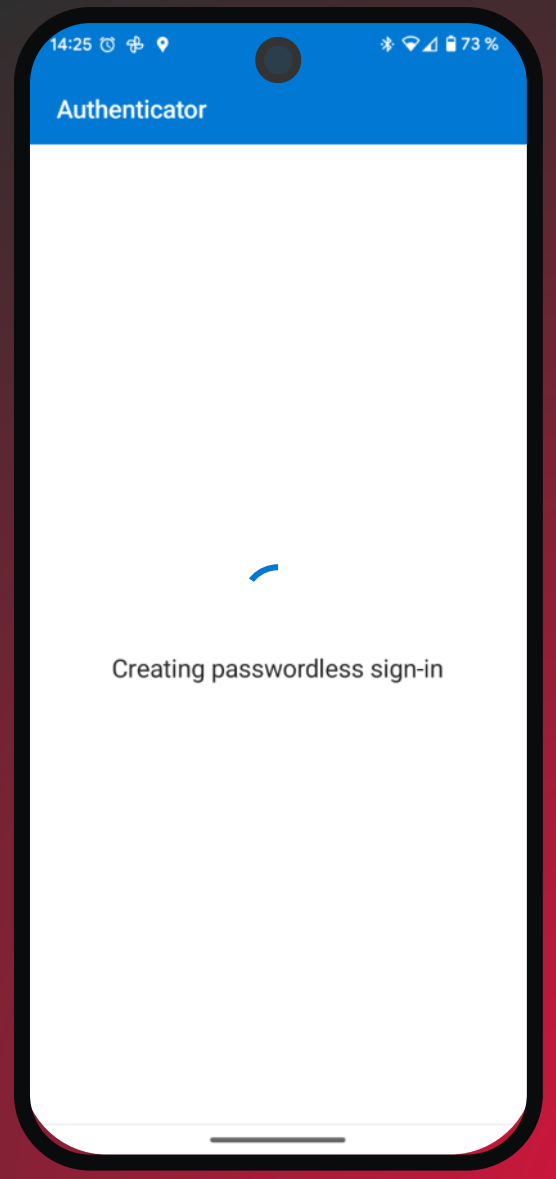
User experience in the lab



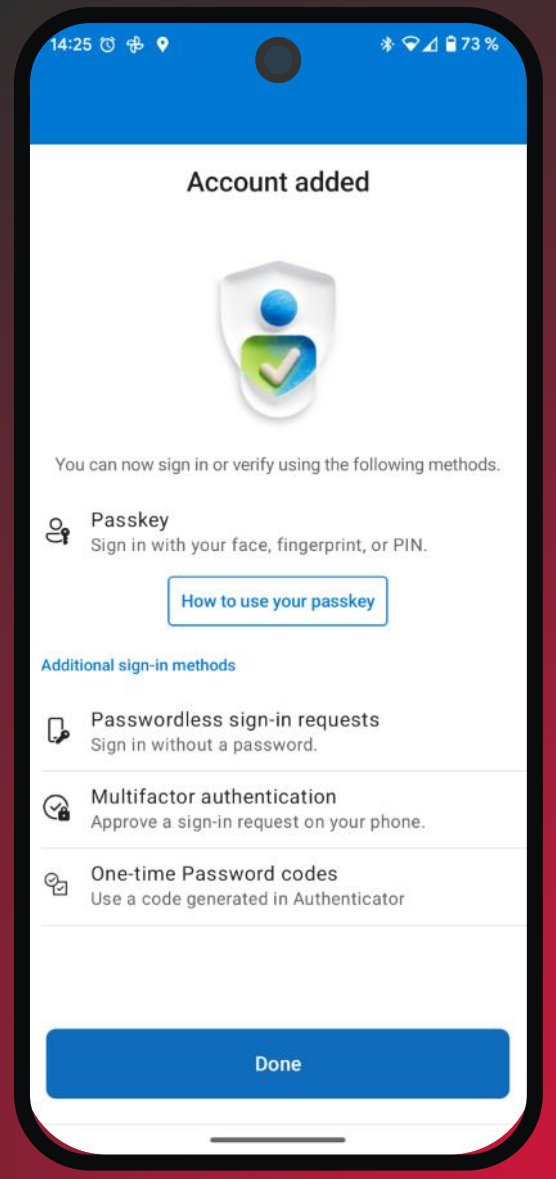
User experience in the lab



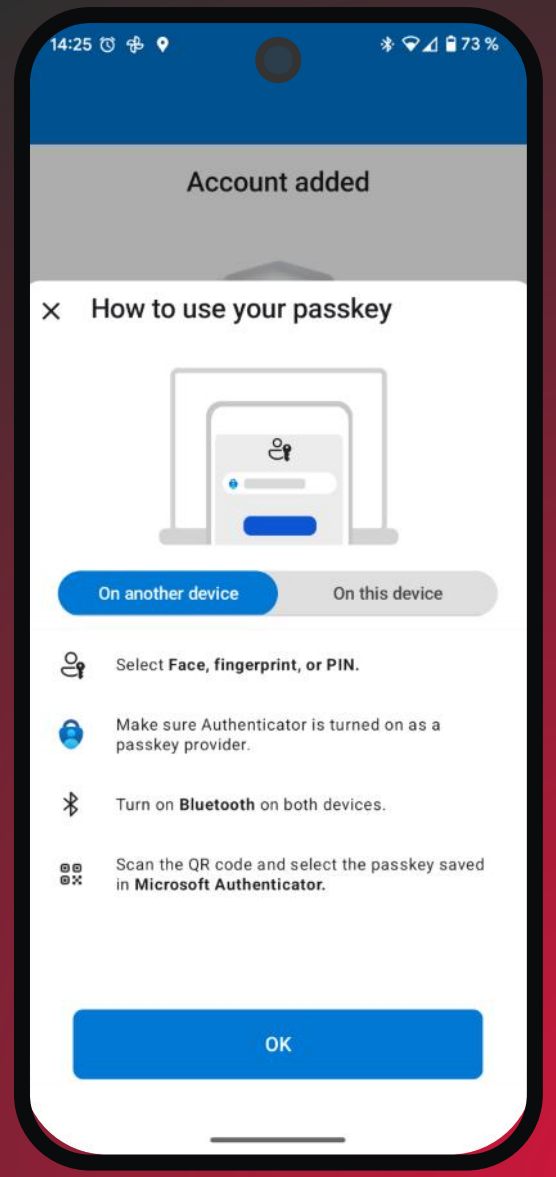
User experience in the lab



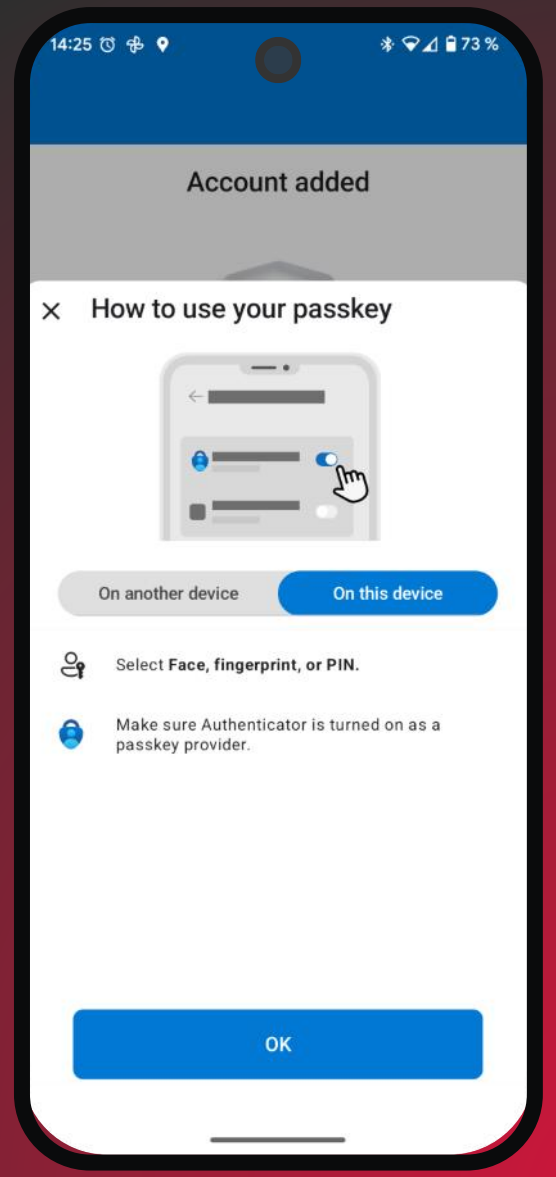
User experience in the lab



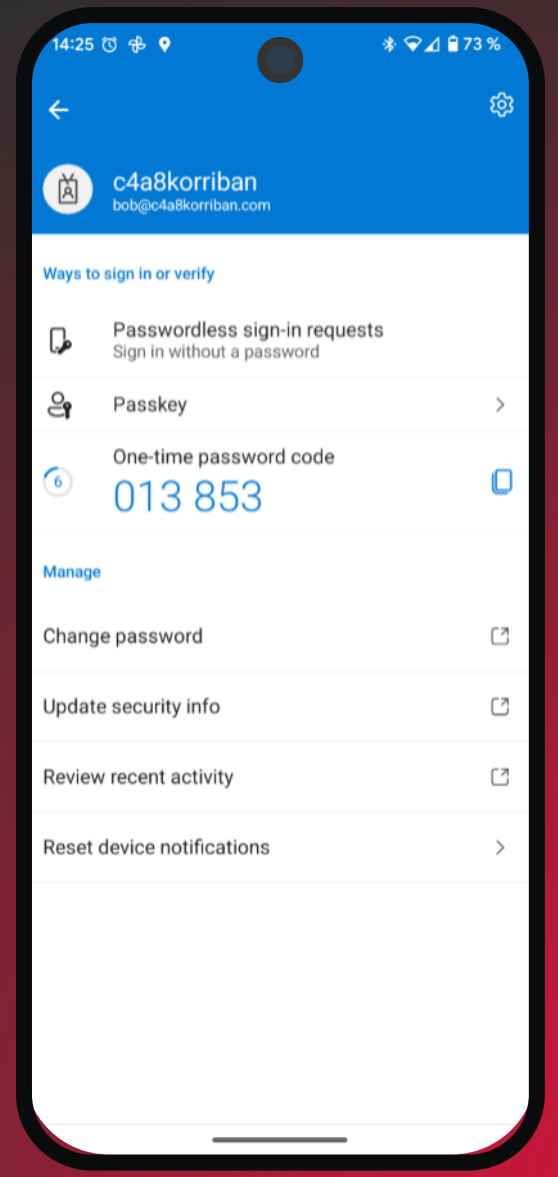
User experience in the lab



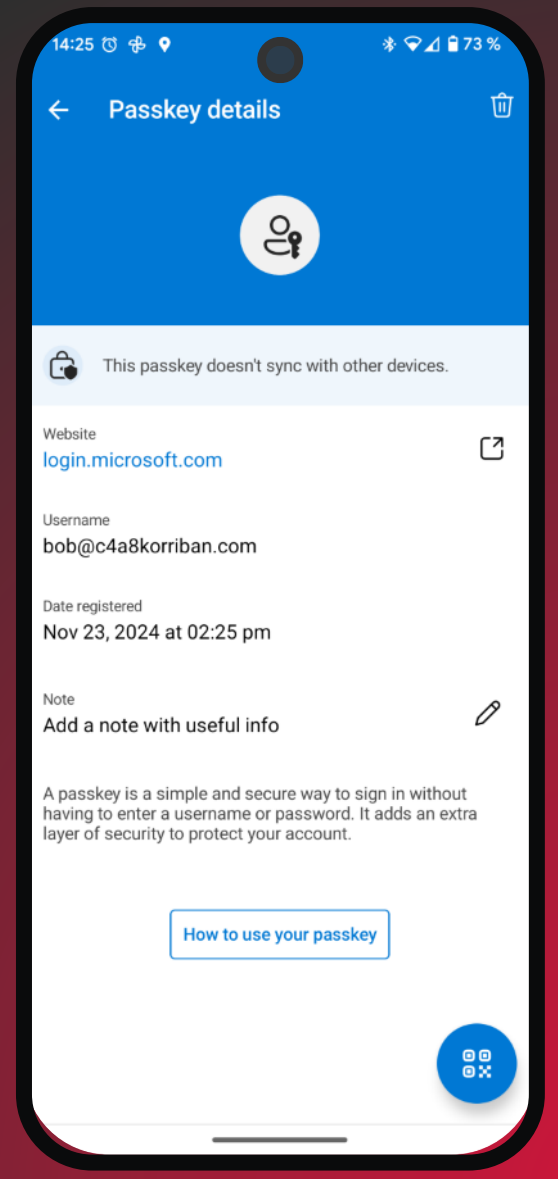
User experience in the lab



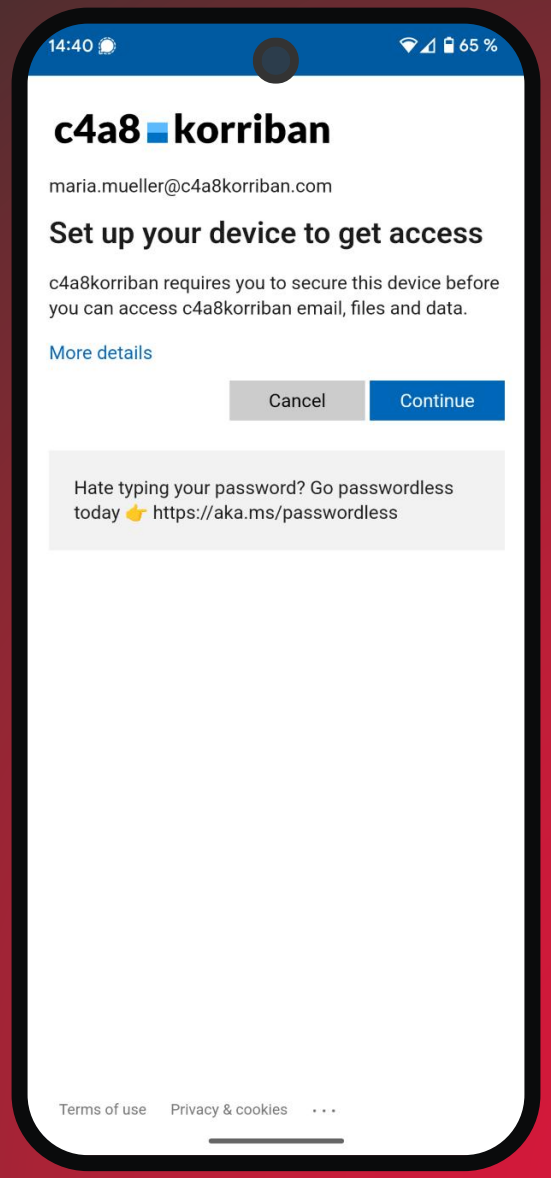
User experience in the lab



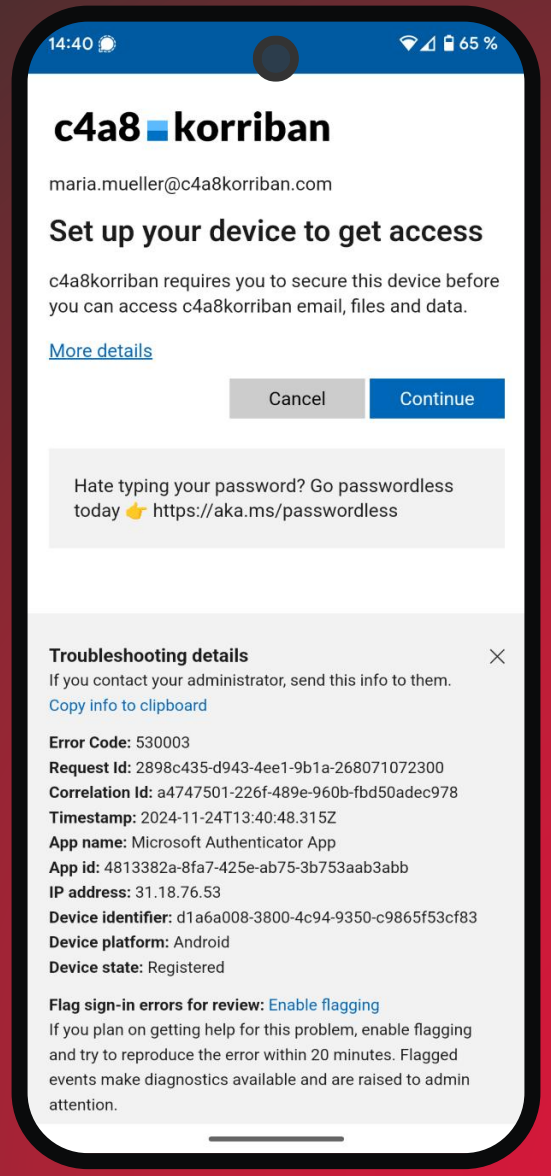
User experience in the lab



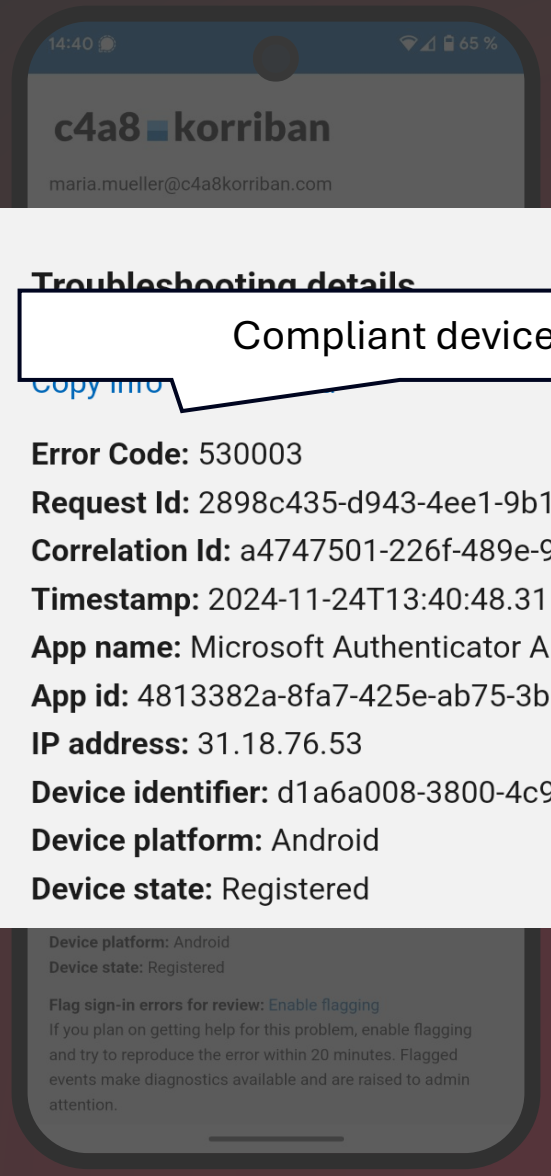
Experience in the real world



Experience in the real world



Experience in the real world

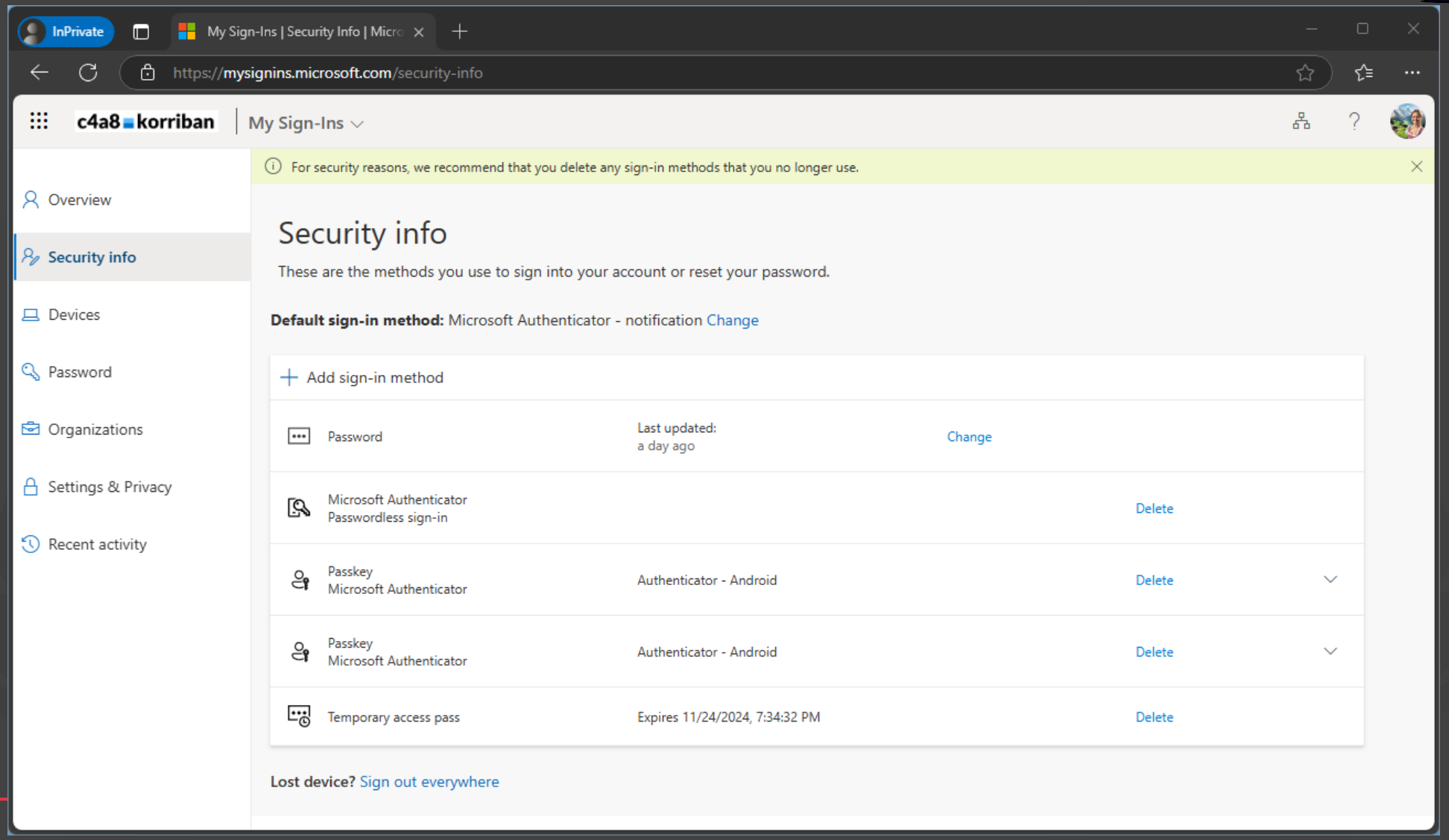


Troubleshooting details

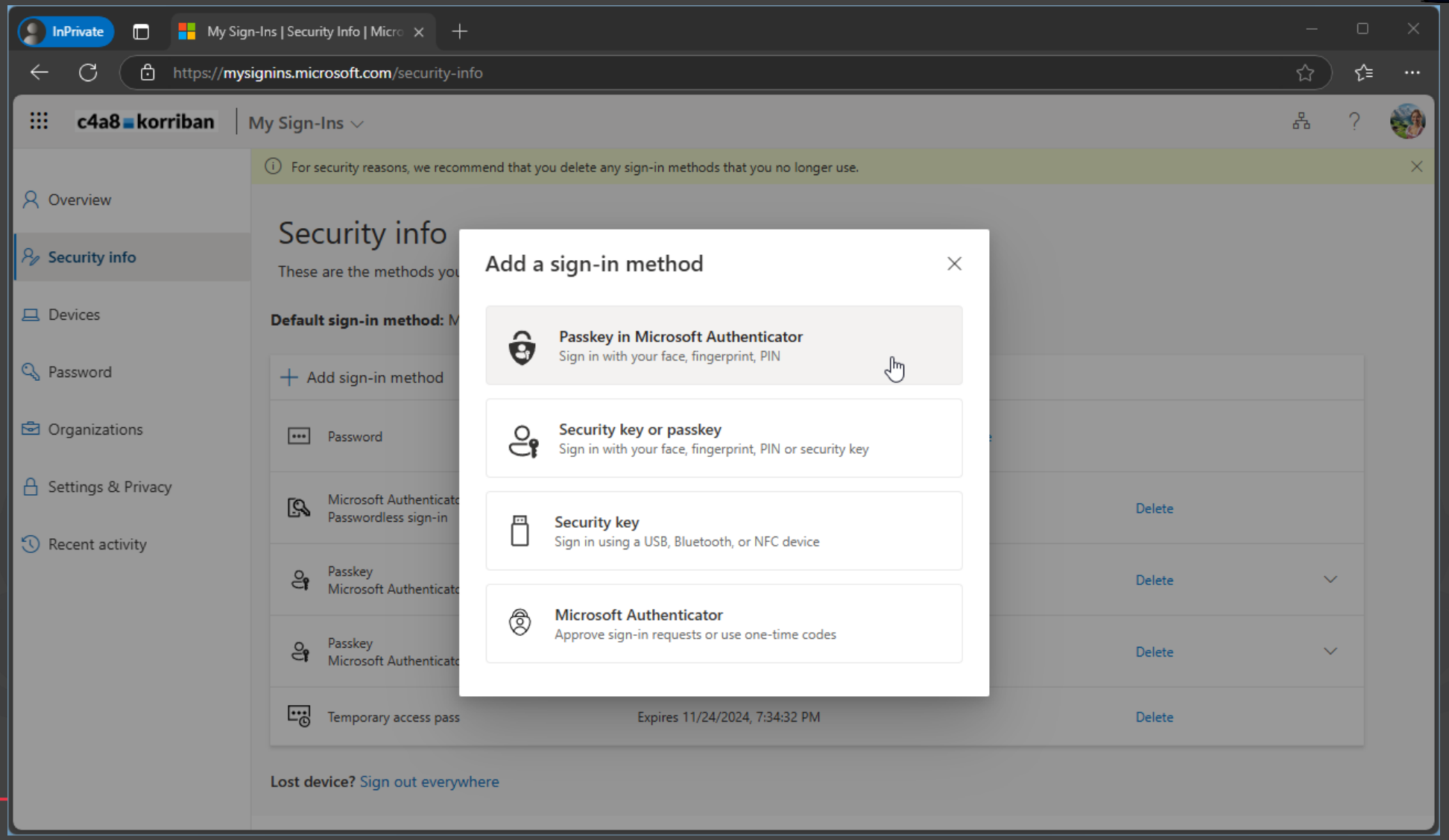
Approved app required

Error Code: 530021
Request Id: b4a6f0ec-b8e8-4d6b-a74b-fd02c4302100
Correlation Id: 68207782-d5b0-43c6-8d84-1d4ea94d41d1
Timestamp: 2024-11-24T17:34:53.085Z
App name: Microsoft Authenticator App
App id: 4813382a-8fa7-425e-ab75-3b753aab3abb
IP address: 31.18.76.53
Device identifier: d1a6a008-3800-4c94-9350-c9865f53cf83
Device platform: Android
Device state: Registered

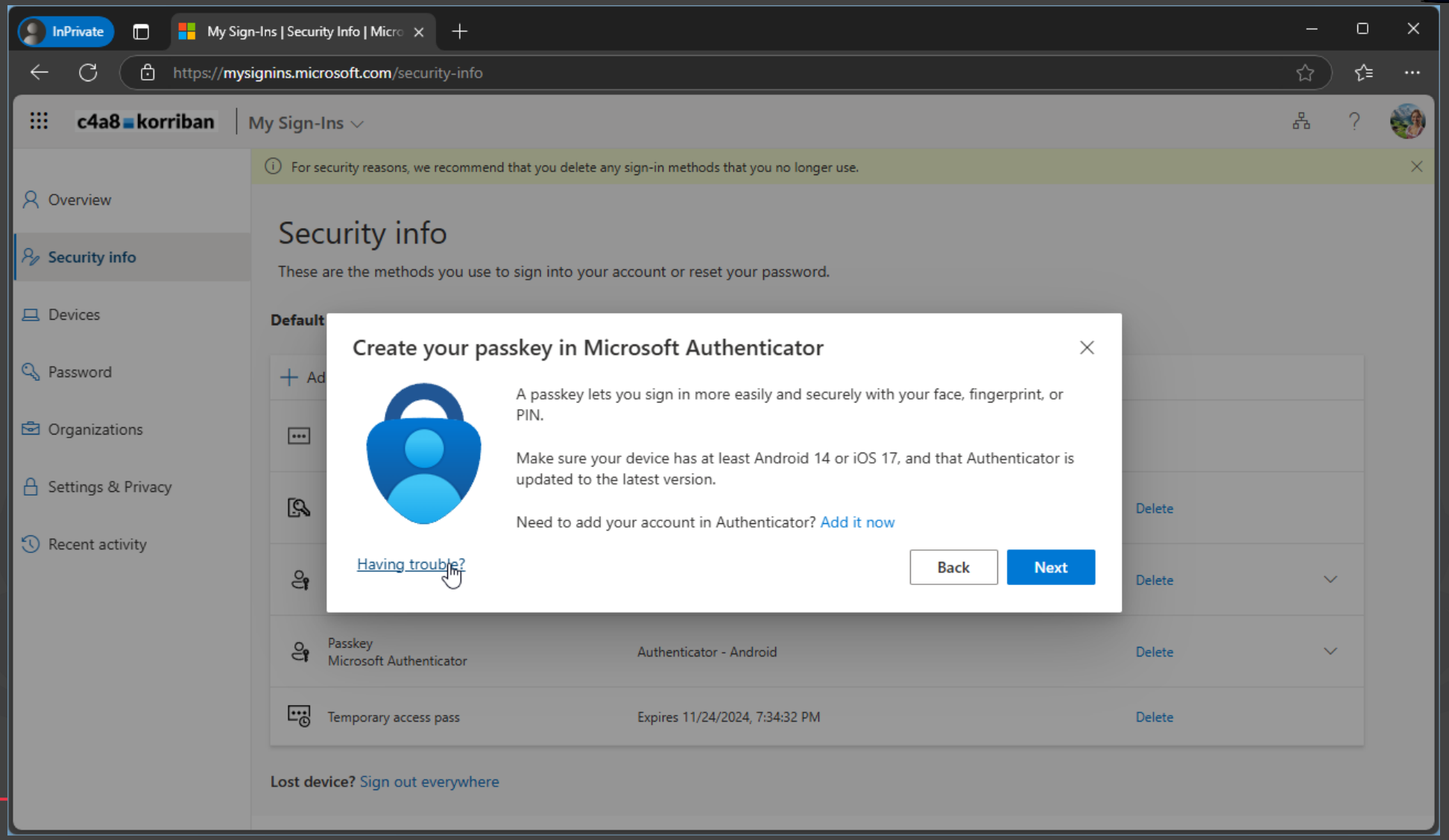
Cross Device Flow



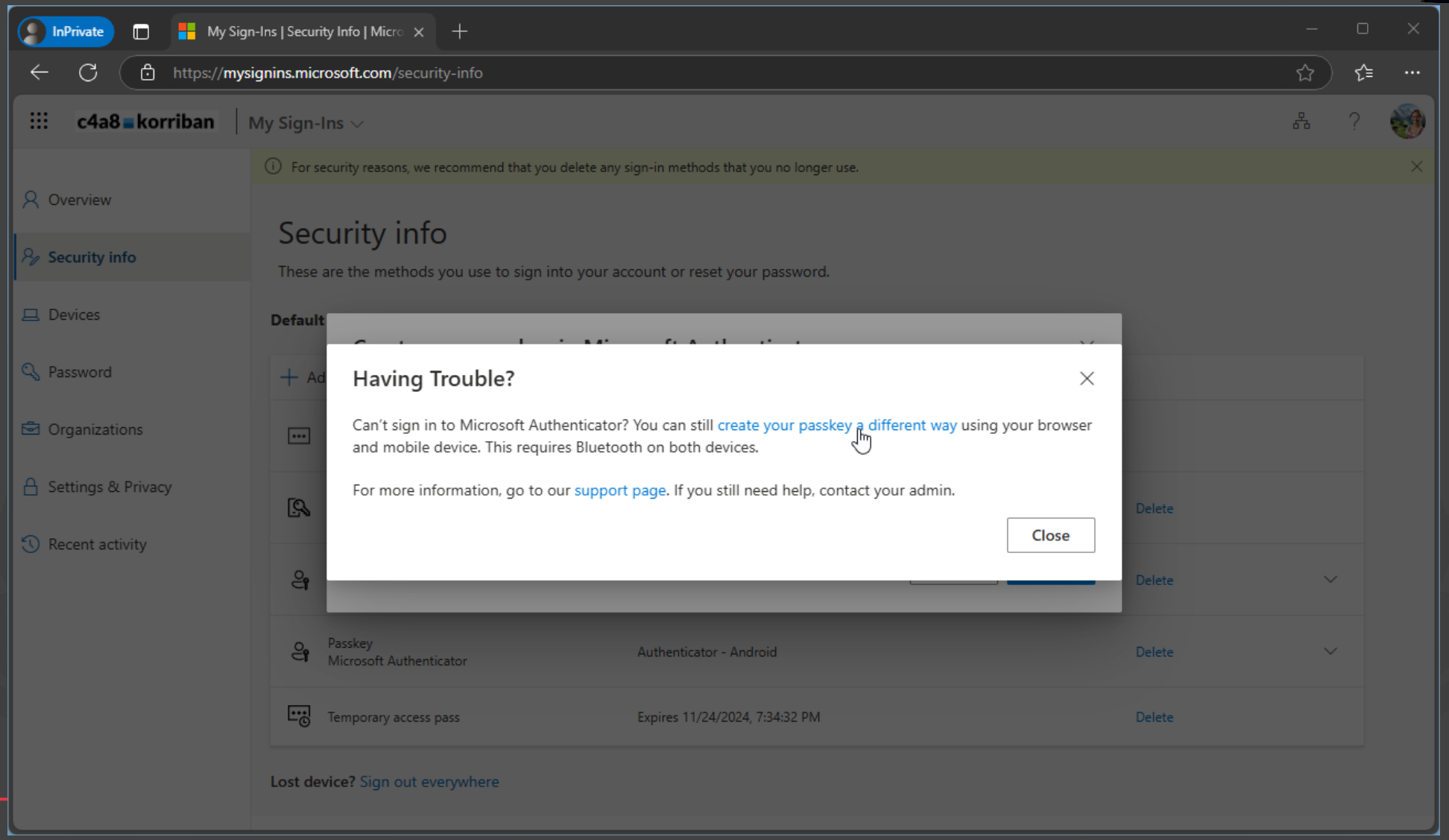
Cross Device Flow



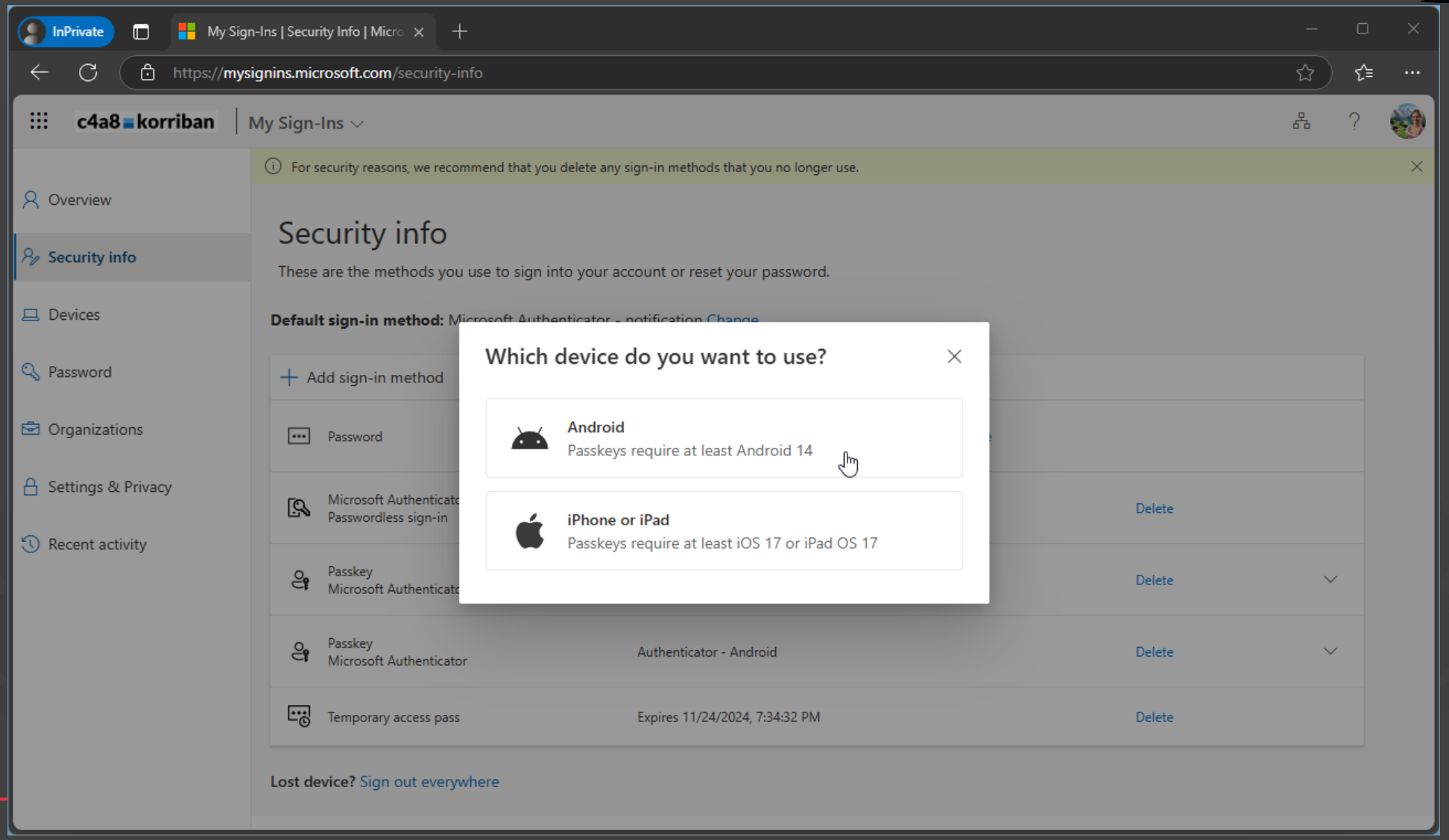
Cross Device Flow



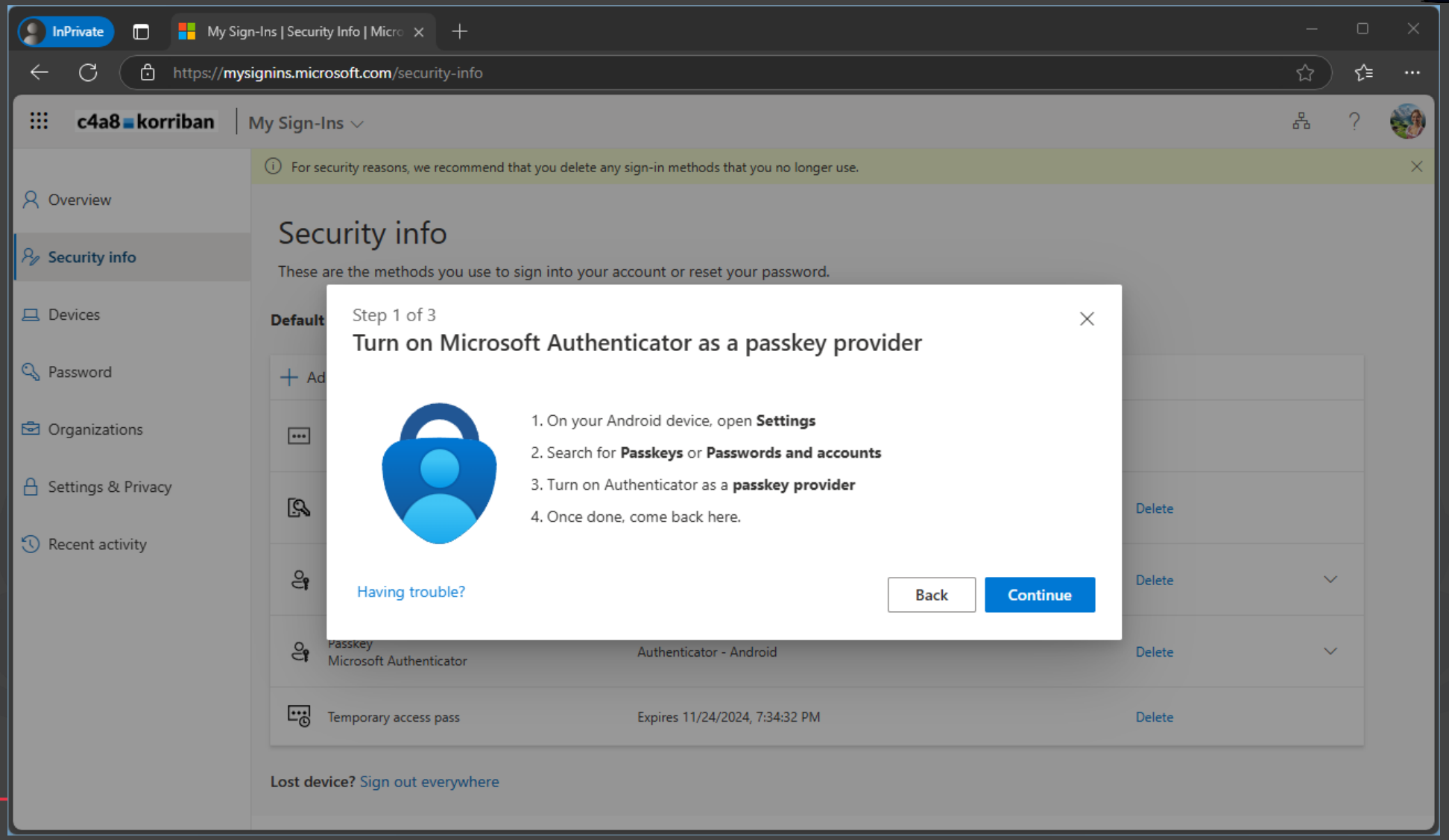
Cross Device Flow



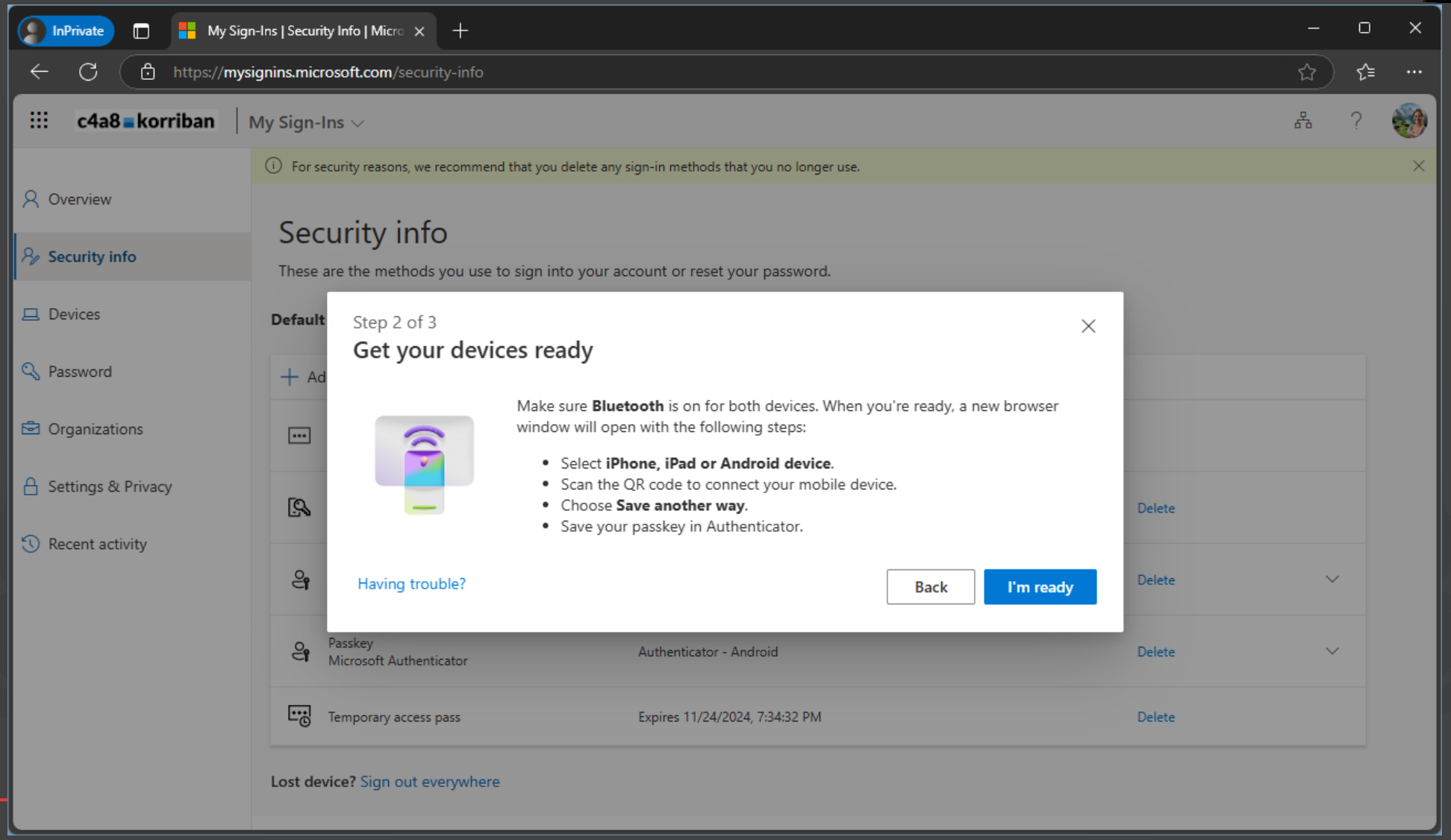
Cross Device Flow



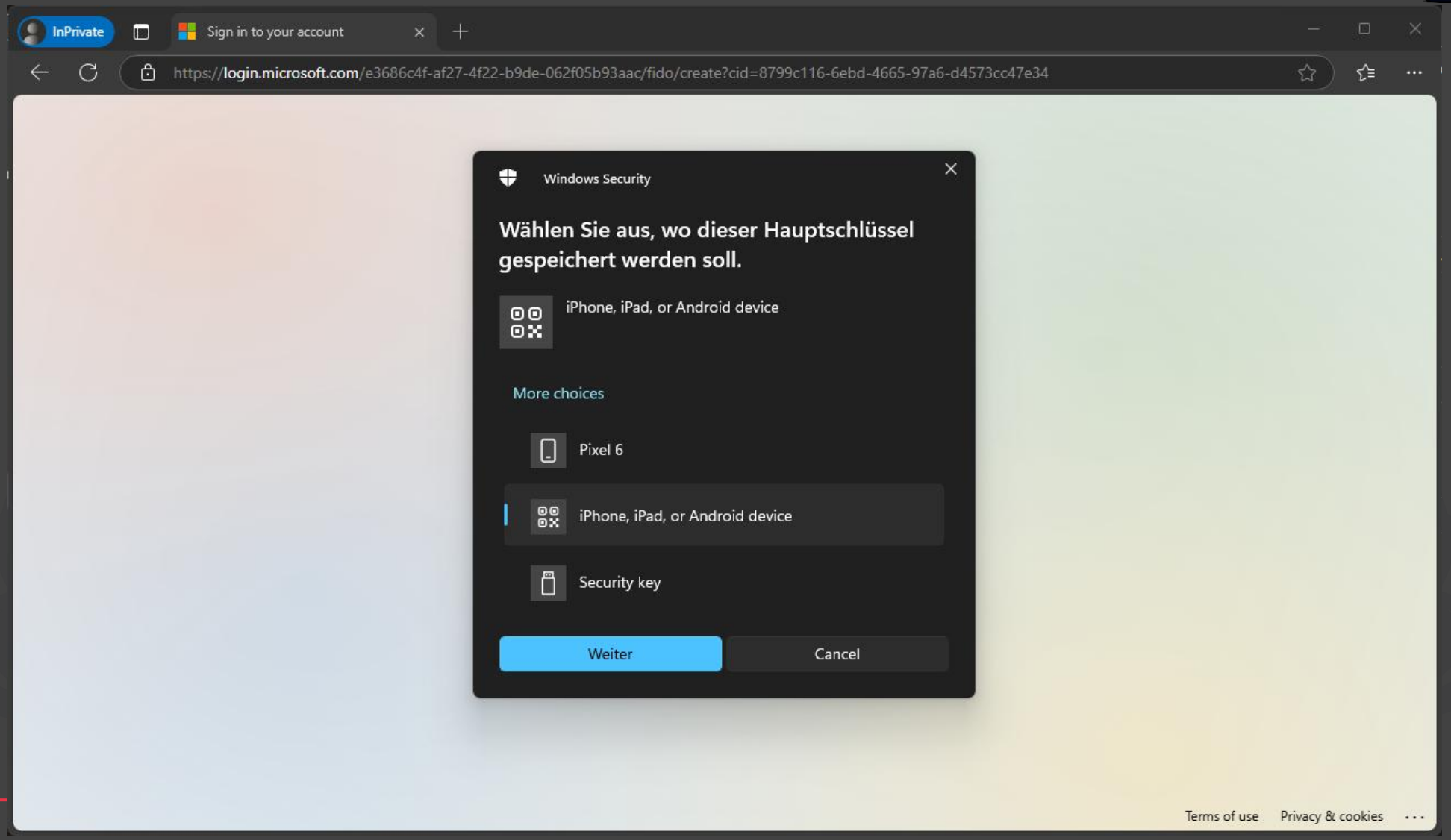
Cross Device Flow



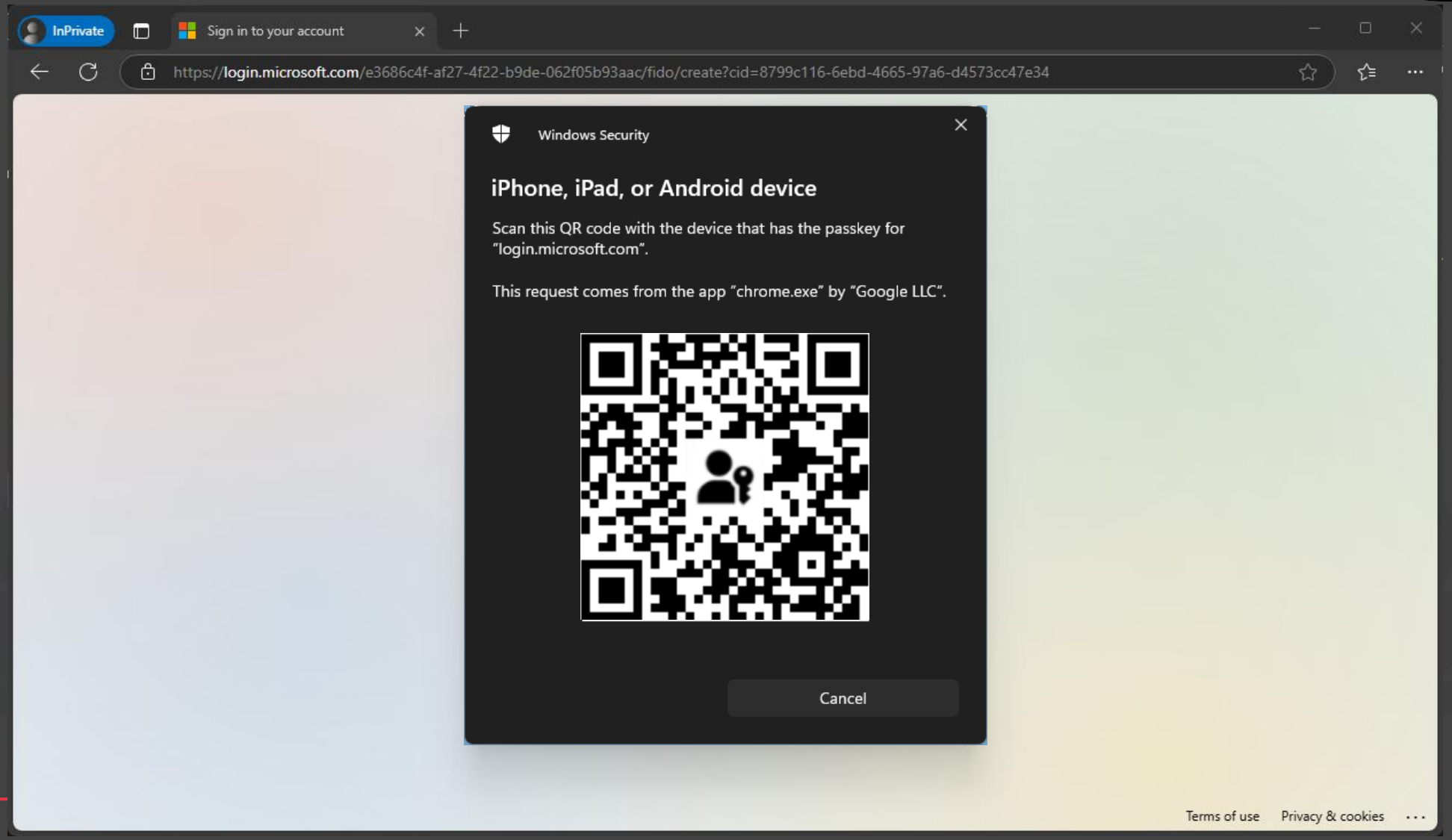
Cross Device Flow



Cross Device Flow



Cross Device Flow

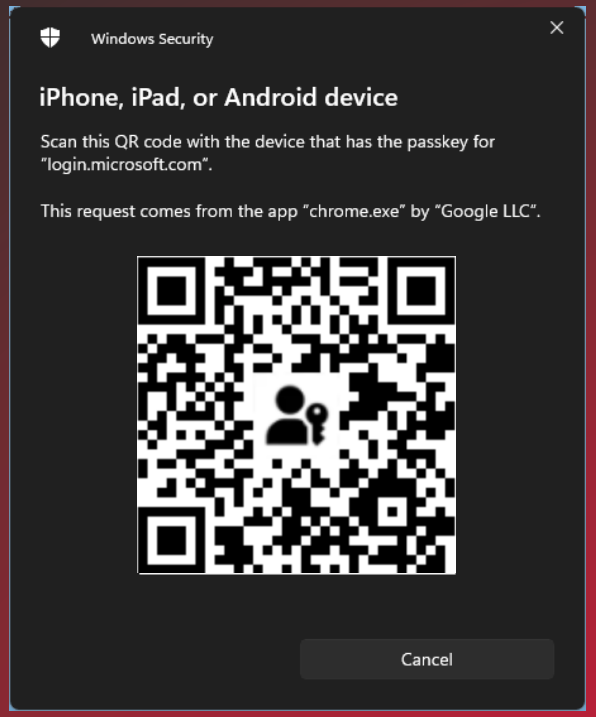


Maybe Cross-Device is not the answer…

Cross Device

- Requires Bluetooth on both devices for proximity check

- Requires internet access
  - https://cable.ua5v.com (Android)
  - https://cable.auth.com (Apple)



FIDO:/088521772645746
304256629196898023805
213791974887885159969
946751928771388701793
485401070923423366366
303159168738737767290
060661159865120837177

FIDO:/088521772645746
304256629196898023805
213791974887885159969
946751928771388701793
485401070923423366366
303159168738737767290
060661159865120837177
011010667266107096654
083332

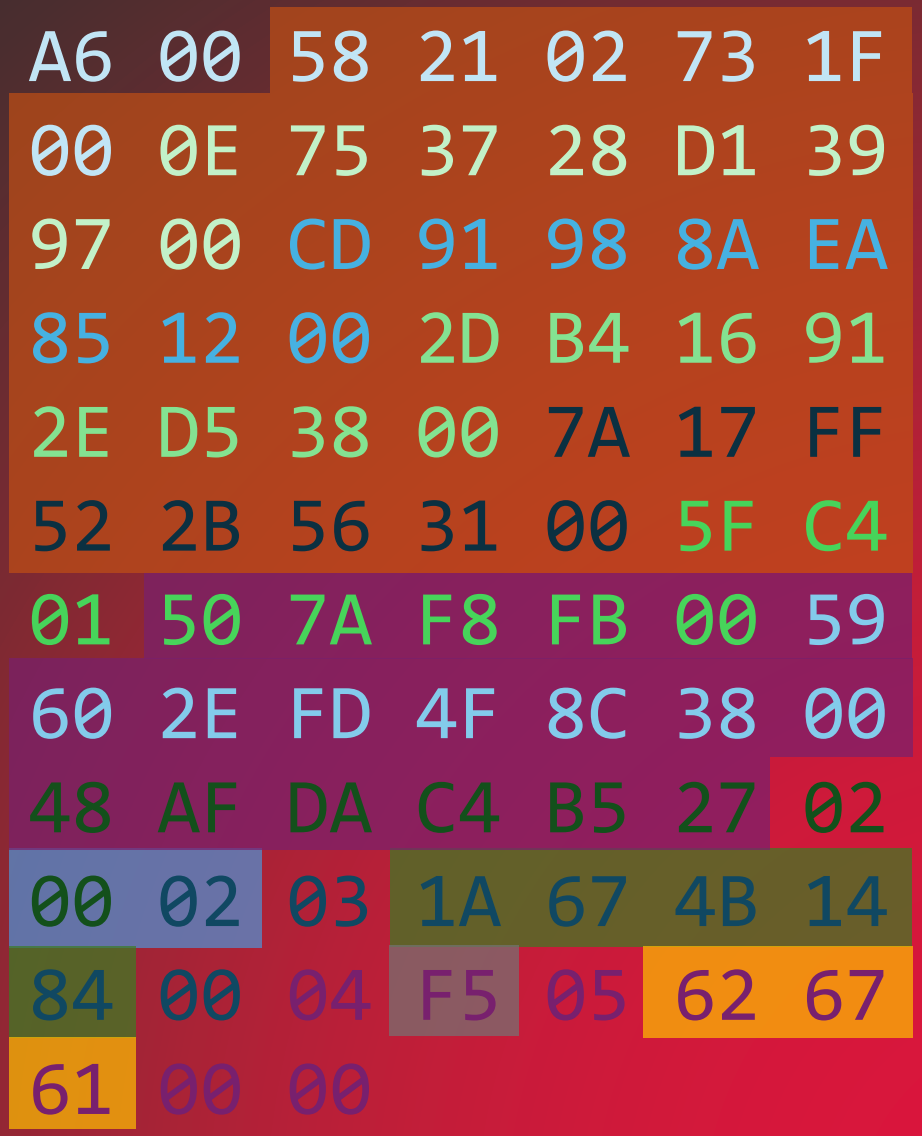
QR Code Deep Dive

- Base10 encoded string
- Concise Binary Object Representation (CBOR) data format

FIDO:/088521772645746
304256629196898023805
213791974887885159969
946751928771388701793
485401070923423366366
303159168738737767290
060661159865120837177
011010667266107096654
083332

QR Code Deep Dive

- Base10 encoded string
- Concise Binary Object Representation (CBOR) data format



QR Code Deep Dive

```
// Compressed public key
0: h'02731F0E7537[...]315FC4‘
// Random QR Code secret
1: h'7AF8FB59602E[...]C4B527‘
// decodeTunnelServerDomain
2: 2
// Current epoch time
3: 1732973700
// State-assisted transactions
4: true
// getAssertion or makeCredential
5: "ga"
```

Prepare for rollout

Passkey "support" matrix

Passkey "support" matrix

Management	Conditional Access	BT	Method	Attestation	Result
MAM	Compliant device: All resources		Same-Device	Yes/No	ⓘ
MAM	Compliant device: All resources	✱	Cross-Device	Yes	✓
MAM	Compliant device: All resources	✱	Cross-Device	No	✓
All	Approved apps: All resources		Same-Device	Yes/No	ⓘ
MAM	Approved apps: All resources	✱	Cross-Device	Yes	✓
MAM	Approved apps: All resources	✱	Cross-Device	No	✓
Work Profile/MDM	Compliant device: All resources		Same-Device	Yes/No	✓
All	n/a	✱	Cross-Device	Yes	ⓘ

The workaround

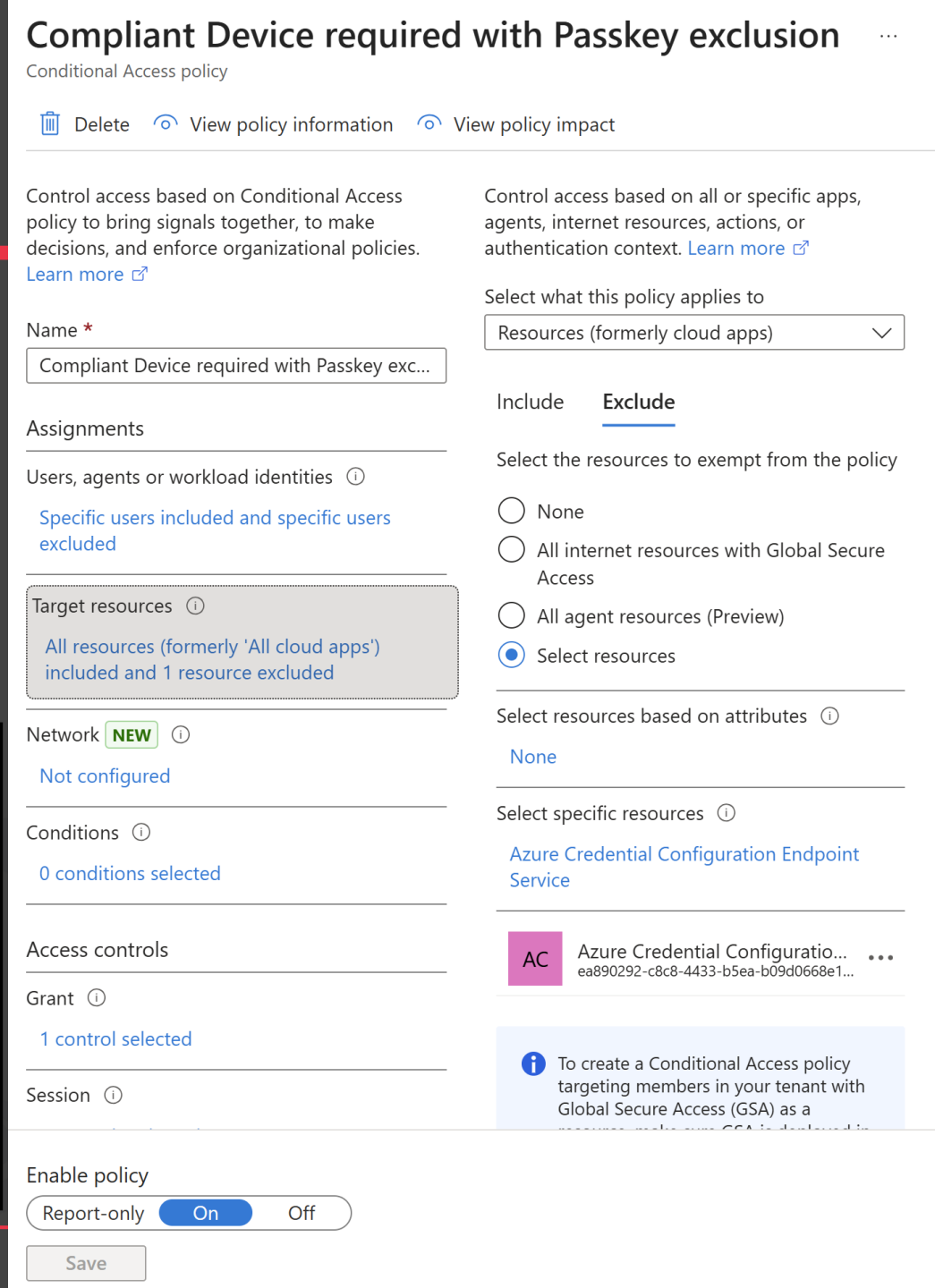
Azure Credential Configuration Endpoint Service

ea890292-c8c8-4433-b5ea-b09d0668e1a6

Disclaimer

Use at your own risk.

This excludes the AuthenticationMethodsPolicy.Read/Write permission from this Conditional Access policy. Ensure you have at least a “Require Authentication Strength” policy covering all resources, including this one.



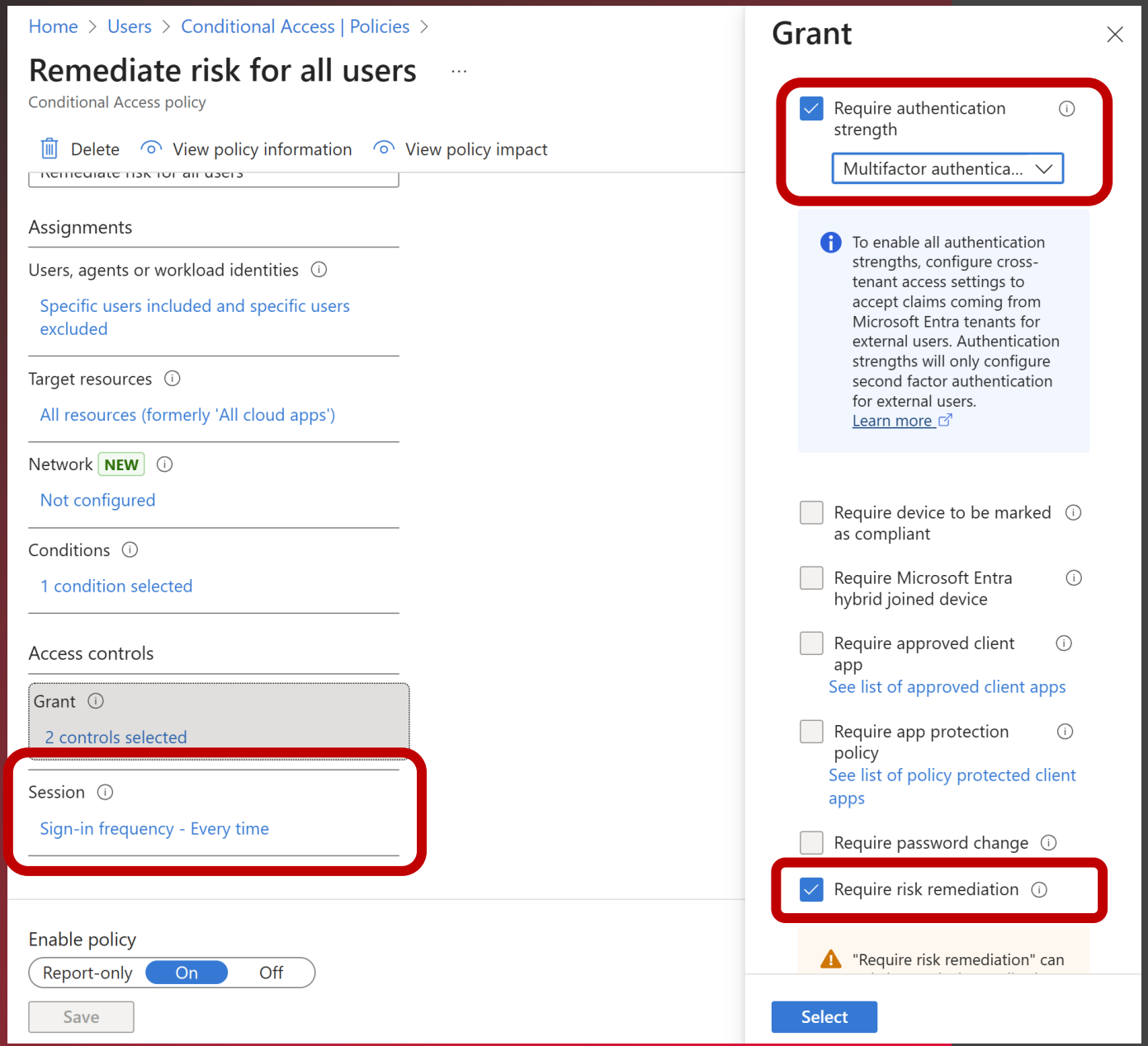
Passkey "support" matrix + workaround

	Management	Conditional Access	BT	Method	Attestation	Result
	MAM	Compliant device: All resources		Same-Device	Yes/No	✓
	MAM	Compliant device: All resources	✱	Cross-Device	Yes	✓
	MAM	Compliant device: All resources	✱	Cross-Device	No	✓
	All	Approved apps: All resources		Same-Device	Yes/No	✓
	MAM	Approved apps: All resources	✱	Cross-Device	Yes	✓
	MAM	Approved apps: All resources	✱	Cross-Device	No	✓
	Work Profile/MDM	Compliant device: All resources		Same-Device	Yes/No	✓
	All	n/a	✱	Cross-Device	Yes	ⓘ

Passkey "support" matrix caveats

- Update to the latest OS version
- On Android also update the Play Service
  Settings → About phone → Android version → Google play system update
- On Android 14 the device vendor third party passkeys are optional
  Not supported by e.g. Motorola, Fairphone, Oppo, Oneplus, Sony*

*List based on forums entries and responses to social media outreach.



Self-remediation for passwordless users

Our best practices and tips

Use **TAP** and **same device registration** for initial onboarding

Restrict Security Info Registration via **Conditional Access** and switch to new **risk remediation** option

On Windows devices use **WHfB** & **Cloud Kerberos Trust**

Enforce phishing resistant using **Authentication Strength** to prevent downgrade AiTM attacks

Enable **attestation** for **device bound** passkeys

No synced passkeys for **privileged identities**

Every passkey is better than a password even with MFA!

Thank You!