

The state of passkey at the end of '25



Workplace Ninjas





Thank you Sponsors

Platinum Sponsors



SOFTWARE
CENTRAL

Gold Sponsors

Recast

 Microsoft

 **DEVICIE**

juriba 

 **numecent**
CLOUDPAGING DELIVERS



PATCH MY PC

inforcer 

 **LOGINVSI**



control^{UP} 

glueck  **kanja**

Silver Sponsors

Rimo3 

 **FERROQUE**
SYSTEMS

 **WEI**

About us

Fabian Bader



Chris Brumm



@fabian_bader ✉ @cbrhh

/in/fabianbader linkedin /in/christopherbrumm

cloudbrothers.info 🏠 chris-brumm.com

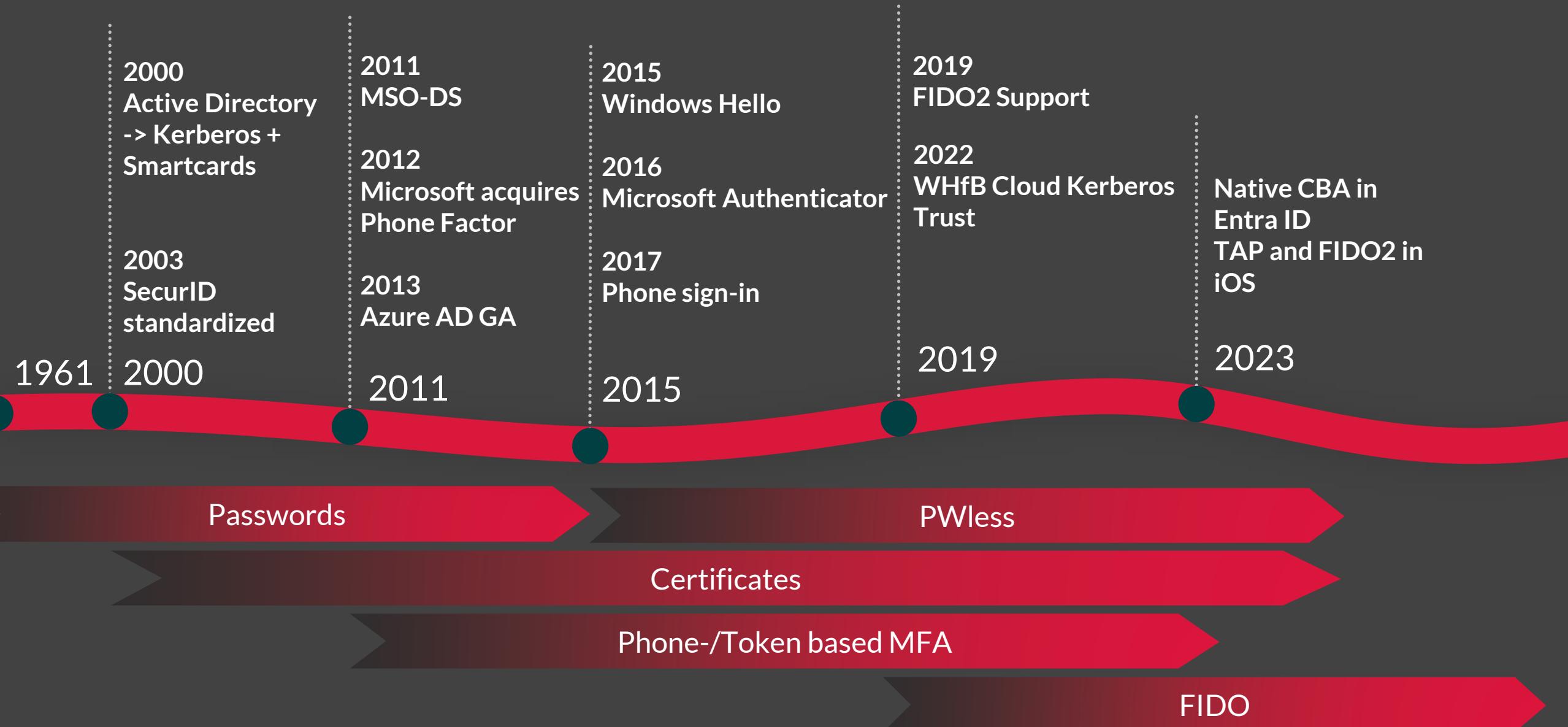
Cyber Security Architects

@
glueckkanja

Microsoft MVPs

www.workplacei

Evolution of Authentication at Microsoft



Evolution of Authentication at Microsoft

Passkey Support

- Entra ID
- Authenticator

FIDO2 on Android

GA @ Ignite 2024

2025



Passkey Support

- Syncable Passkeys
- Passkey Profiles

Preview @ Ignite 2025

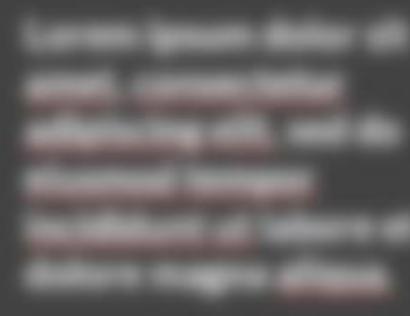
2025

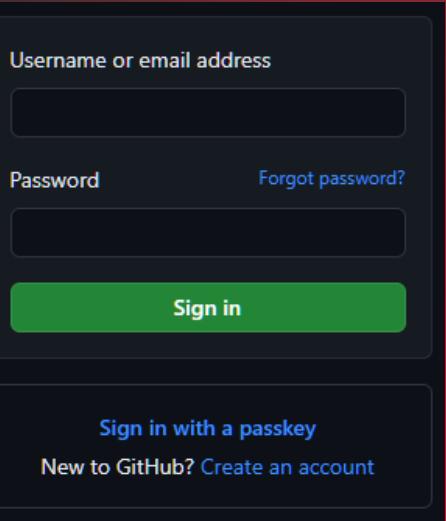


2026



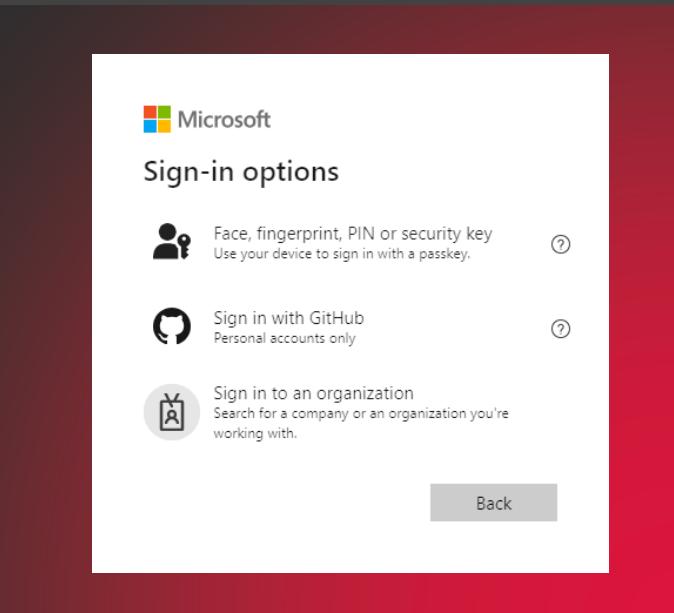
Passkeys





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



The screenshot shows the Amazon.de login page. At the top, there's a search bar with "Suche Amazon.de" and a magnifying glass icon. To the right are language and account selection buttons. Below the header, a navigation bar includes "Alle", "Angebote", "Erneut kaufen", "Browserverlauf", "Amazon Basics", "Christo...s Amazon", "Küche, Haushalt & Wohnen", "Kindle Bücher", and "Gutscheine". A "Passkey" link is visible in the "Mein Konto" dropdown. The main content area is titled "Passkey" and asks if the user wants to share their account with someone else using a passkey. It lists two existing passkeys: "Windows Hello" (created 16.08.2024) and "Google-Passwort-Manager" (created 16.08.2024). There are buttons for "Passkey hinzufügen" and "Wenn du einen Schlüsselbund hinzufügen möchtest, verwende ein anderes Cloud-Servicekonto (z. B.: Apple-ID oder Google-Konto.)".

This screenshot shows the "Google Passwortmanager" interface for creating a passkey. It features a large green "Erstelle einen Passkey" button. Below it, a note says: "Dein Passkey bietet eine sichere und einfache Möglichkeit, um dich wieder bei deinem Konto anzumelden." Another note says: "Verwende deinen Passkey mit deinem Fingerabdruck, der Gesichtserkennung oder der Displaysperre." A "Google Passwortmanager" logo is shown above a "Passkey zur Anmeldung in WhatsApp erstellen?" button. A "WhatsApp" icon and a placeholder "*****5910" are displayed. At the bottom are "Weiter" and "Anders speichern" buttons.

Passkeys used by Chris' family

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



DU HAST NUN ALLES EINGERICHTET

Nun kannst du diesen Passkey jedes Mal nutzen, wenn du dich auf diesem Gerät bei X anmeldest.

Fertig

E-Mail-Adresse oder Handynummer

Passwort Use a passkey

[Passwort vergessen?](#)

[Einloggen](#)

oder

[Neu anmelden](#)



Nintendo Account

[Passkey Sign-In](#)

Use a passkey to sign in to your account.

[Passkey Sign-In](#)



[Sign In](#)

[Cancel](#)

[Sign In Another Way](#)

[No Passkey Sign-In](#)

[Cancel](#)

[Sign In Another Way](#)

[No Passkey Sign-In](#)

Consumer
want **easy**
passkeys!

Synced
Keys 😊

Easy
Recovery

Easy Setup

Phishing-
resistance

Easy usage



Enterprises
want **secure**
passkeys!

Synced
Keys 😐

Secure
Recovery

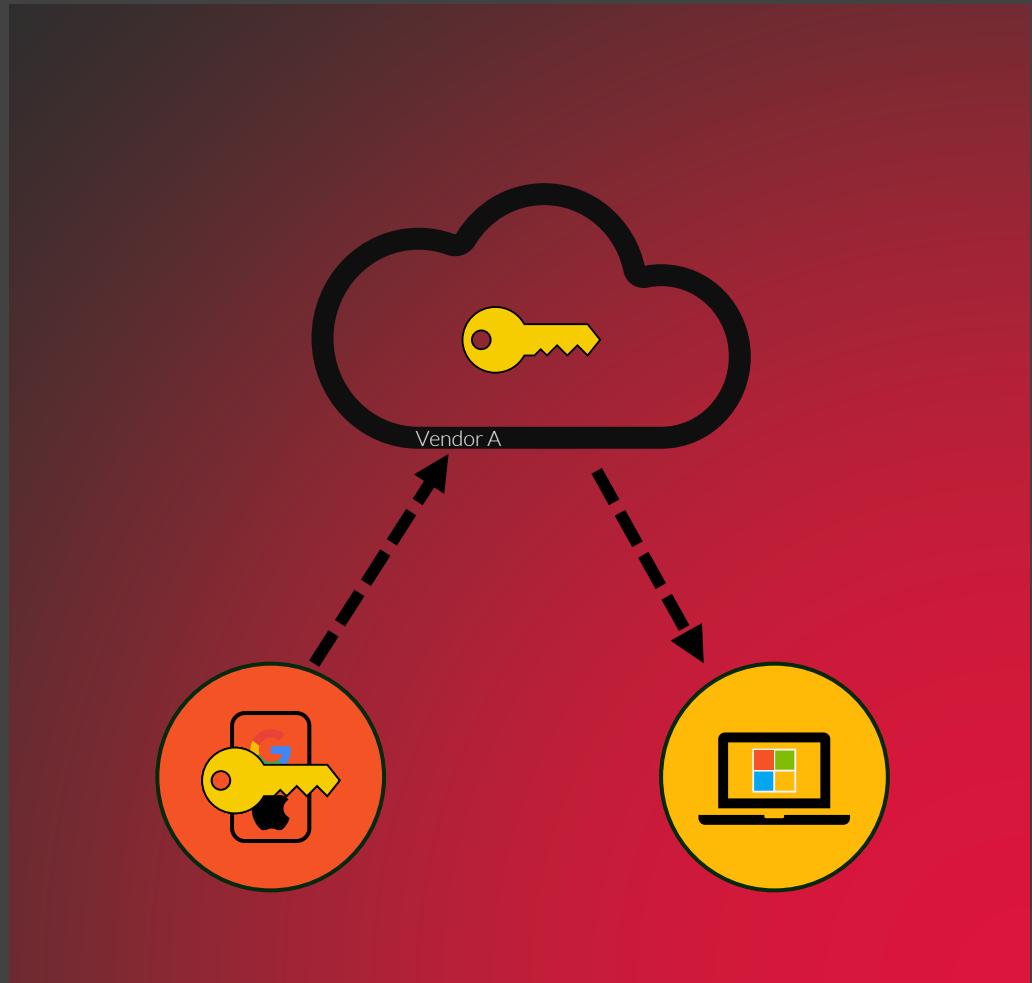
Controlled
Setup

Phishing-
resistance

Controlled
usage



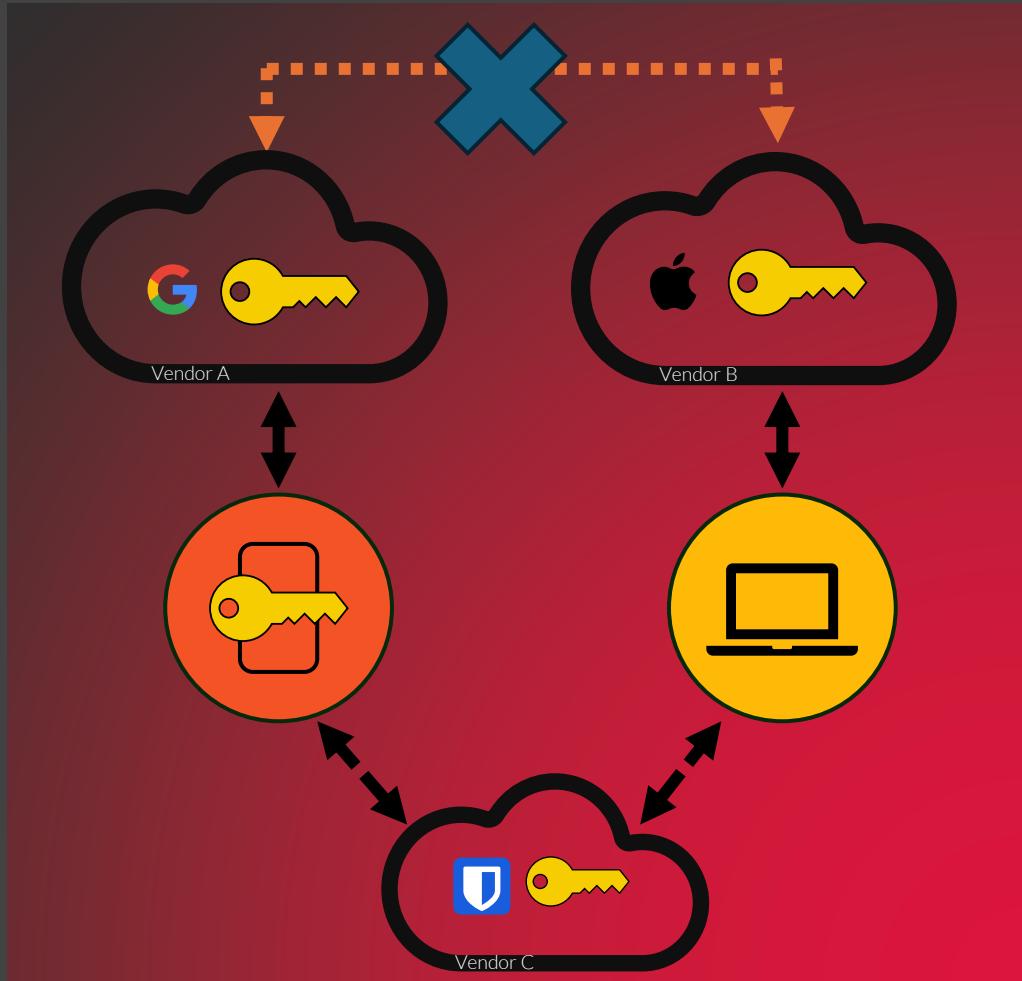
Synced vs. Device-bound passkeys



- 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



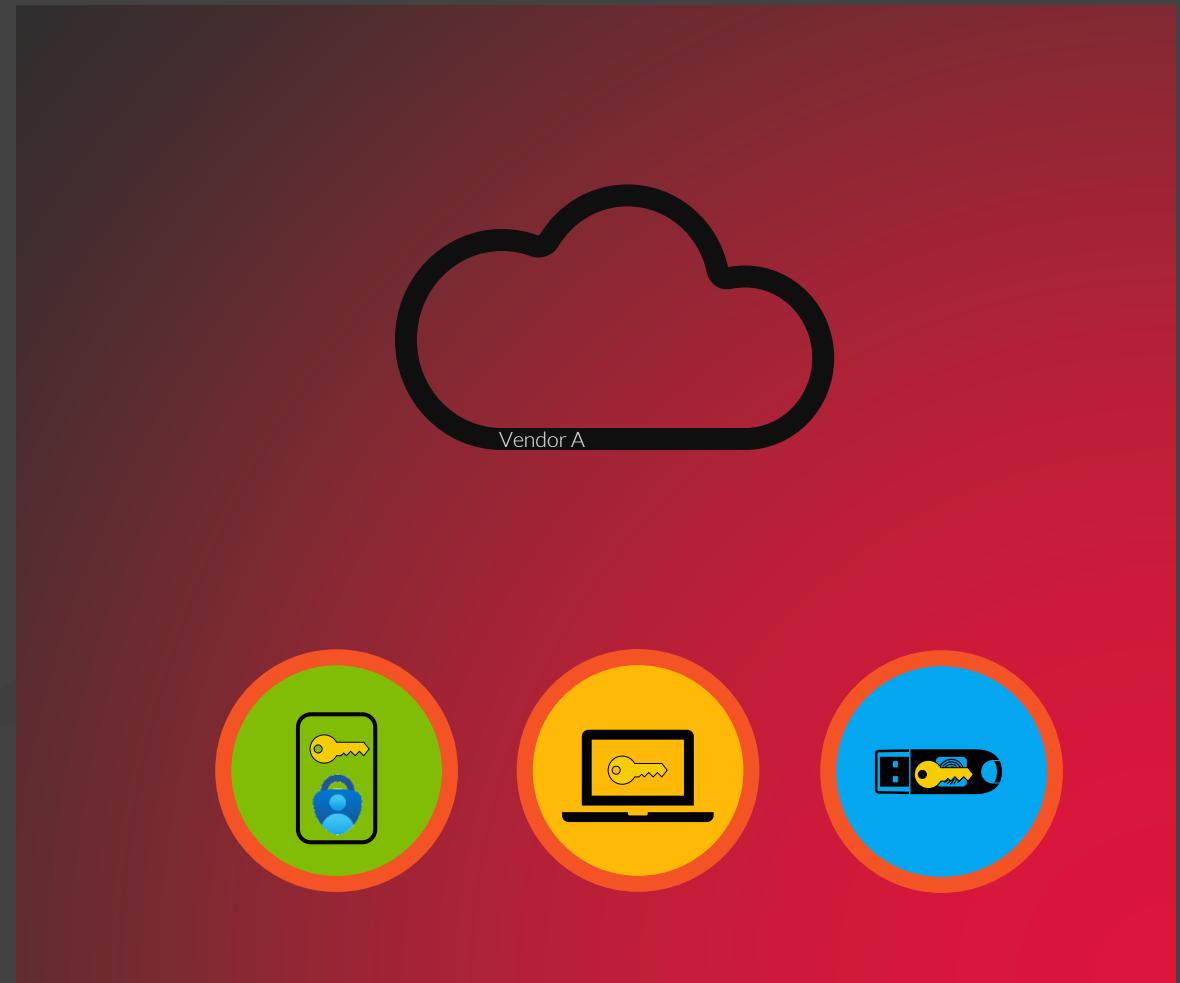
- Native cross vendor sync is not possible
- Workarounds
 - Cross-Device Authentication
 - Third-party passkey provider
 - Credential Exchange Protocol (CXP)



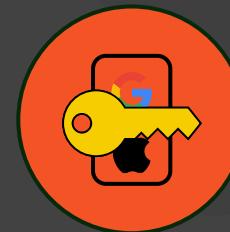
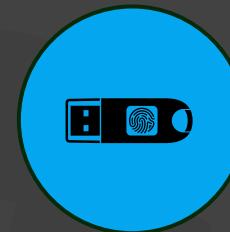
Synced vs. Device-bound passkeys



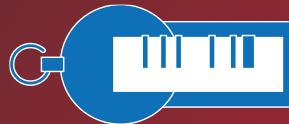
- The private key cannot leave the device
- FIDO2 security keys are device-bound passkeys
- Microsoft Authenticator creates a device-bound passkey
- Recovery = New Setup



Microsoft's 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 <> [+ Add external method \(Preview\)](#) [⟳ Refresh](#) | [👤 Got feedback?](#)

Manage

-  Policies
-  Password protection
-  Registration campaign
-  Authentication strengths
-  Settings

Monitoring

-  Activity
-  User registration details
-  Registration and reset events
-  Bulk operation results

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



+ Add external method (Preview)



Refresh



Got feedback?

Manage



Policies



Password protection



Registration campaign

Authentication strengths



Settings

Monitoring



Activity

User registration details

Registration and reset events

Bulk operation results

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)



i 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	<input type="text" value="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 [\(i\)](#)



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](#)
[\(i\)](#)

[+](#) Add profile (preview)

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

[Save](#)

[Discard](#)

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 [\(i\)](#)

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	Type
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 [\(i\)](#)Target types [*](#)

Device-bound

Target specific AAGUIDs [\(i\)](#)[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 [\(i\)](#)



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](#)
[\(i\)](#)

[+](#) Add profile (preview)

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

[Save](#)[Discard](#)

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 [i](#)

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	Type
Default passkey profile	Yes	Dev

[Save](#)

[Discard](#)

Add passkey profile

X

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 [i](#)

Target types *

Synced (preview), Device-bound

Target specific AAGUIDs [i](#)

[Save](#)

[Discard](#)

Passkey (FIDO2) settings

Passkeys (FIDO2) Authentication Methods (Preview)



i 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 i



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)



i 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	<input type="text" value="Default passkey profile"/> ▾

[Save](#)

[Discard](#)

Passkey (FIDO2) settings

X

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

X

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

Search

 cfg - Syncable Passkeys X

1 result found

Groups

	Name	Email
<input checked="" type="checkbox"/>	C- cfg - Syncable Passkeys	

Selected directory members (1)

⟲ Reset

C-	cfg - Syncable Passkeys	trash
-----------------	-------------------------	--------------------

Select

Passkey (FIDO2) settings

X

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

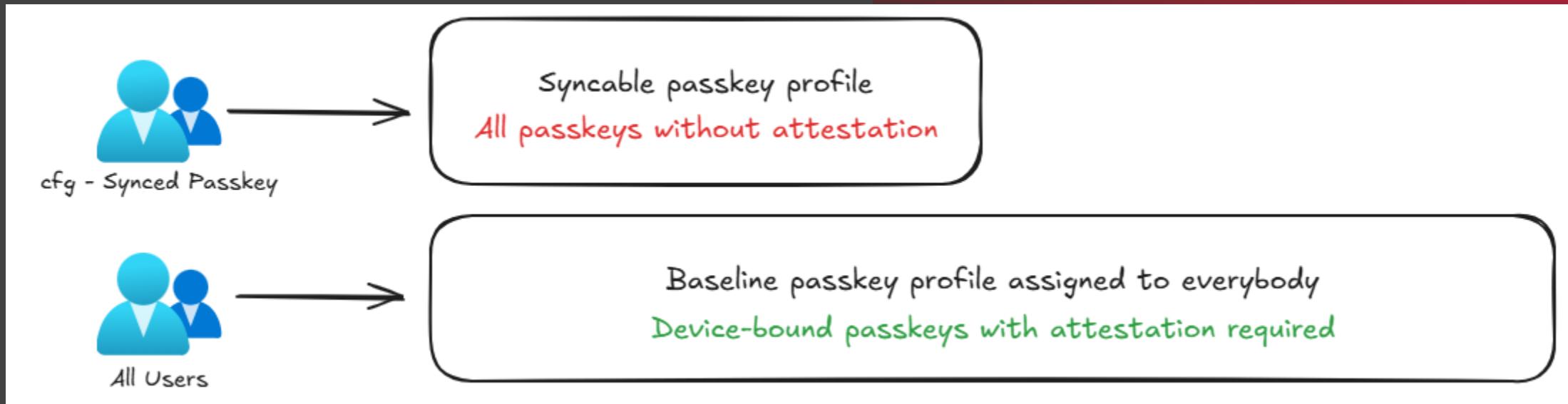
[Include](#)[Exclude](#)[+ Add target](#) ▾

Name	Type	Passkey profiles (preview)
All users	Group	<input type="button" value="Default passkey profile"/>
cfg - Syncable Passkeys	Group	<input type="button" value="Select passkey profiles"/> <input type="checkbox"/> All <input type="checkbox"/> Default passkey profile <input checked="" type="checkbox"/> Syncable passkeys

[Save](#)[Discard](#)

Recommendation

Authentication Methods allowed for the user
Configured through Authentication Policies



Authentication methods registered by the user

Home > Groups | Overview > cfg - Synced Passkey | Members > Quellcrist Falconer

Quellcrist Falconer | Authentication methods

User

Search < Add authentication method | Reset password | Require re-register multifactor authentication | Revoke multifactor authentication sessions | ...

Authentication methods are the ways users sign into Microsoft Entra ID and perform self-service password reset (SSPR). The user's "default sign-in method" is the first one shown to the user when they are required to authenticate with a second factor - the user always can choose another registered, enabled authentication method to authenticate with. [Learn more](#)

Default sign-in method (Preview) Microsoft Authenticator notification

Usable authentication methods

Authentication method	Detail	...
Passkey	Google Password Manager	...
Passkey	Bitwarden	...
Passkey	Black	...
Windows Hello for Business		...
Microsoft Authenticator	Pixel 6	...
Microsoft Authenticator	iPhone (2)	...

Non-usuable authentication methods

Authentication method	Detail	...
Temporary Access Pass	TAP expired	...

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

Authentication methods registered by the user

Home > Groups | Overview > cfg - Synced Passkey | Members > Quellcrist Falconer

Quellcrist Falconer | Authentication methods

Search < Add authentication method | Reset password | Require re-register multifactor authentication

Authentication methods are the ways users sign into Microsoft Entra ID and perform self-service password reset. The "default sign-in method" is the first one shown to the user when they are required to authenticate with a second factor. Users can always choose another registered, enabled authentication method to authenticate with. [Learn more](#)

Default sign-in method (Preview) Microsoft Authenticator notification

Usable authentication methods

Authentication method	Detail
Passkey	Google Password Manager
Passkey	Bitwarden
Passkey	Black
Windows Hello for Business	
Microsoft Authenticator	Pixel 6
Microsoft Authenticator	iPhone (2)

Non-usuable authentication methods

Authentication method	Detail
Temporary Access Pass	TAP exp

Passkey details

ID: 3cEjaXOnTnRy8uX5obUizQ2

Display name: Black

Created: 8/14/2022, 7:35:53 PM

Model: YubiKey 5 Series with NFC

AA Guid: 2fc0579f-8113-47ea-b116-bb5a8db9202a

Attestation Level: Attested

Attestation Certificates: 372ef74b6ea41a96e556d2c8fa1907efa51c1c70

Ok

Authentication methods registered by the user

Home > Groups | Overview > cfg - Synced Passkey | Members > Quellcrist Falconer

Quellcrist Falconer | Authentication methods

User

Search

Add authentication method | Reset password | Require re-register multifactor authentication

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

Default sign-in method (Pre) Usable authentication methods

Authentication method

- Passkey
- Passkey
- Passkey
- Windows Hello for Business
- Microsoft Authenticator
- Microsoft Authenticator
- iPhone (2)

You've reached your passkey limit

You can have a maximum of 10 passkeys. To add a new one, delete an old one first.

Having trouble? OK

Non-usable authentication methods

Authentication method	Detail
Temporary Access Pass	TAP exp

Passkey details

ID: 6Ynughkhuv0T7QLKkovKJQ2

Display name: Google Password Manager

OK

Define which Passkeys can be used in specific situations

Home >

EPA 1 - Require YubiKey for Admin Access

Conditional Access policy

[Delete](#) [View policy information](#)

Name *

EPA 1 - Require YubiKey for Admin Access

Assignments

Users or workload identities [\(1\)](#)

Specific users included and specific users excluded

Target resources [\(1\)](#)

1 app included

Network [\(NEW\)](#) [\(1\)](#)

Not configured

Conditions [\(0\)](#)

0 conditions selected

Access controls

Grant [\(1\)](#)

1 control selected

Session [\(0\)](#)

0 controls selected

Enable policy

Report-only [On](#) [Off](#)

[Save](#)

Grant

Control access enforcement to block or grant access. [Learn more](#)

Block access

Grant access

Require multifactor authentication

⚠ "Require authentication strength" cannot be used with "Require multifactor authentication". [Learn more](#)

Require authentication strength

[YubiKey Only](#)

[View Authentication Strength](#)

To enable all authentication strengths, consider tenant access accept claims for external users. [Learn more](#)

Require device marked as compliant

Select

Authentication methods the user must use
Configured through authentication strengths

Name	YubiKey Only
Type	Custom
Description	
Creation Date	7/28/2024, 2:05 PM
Modified Date	7/28/2024, 2:05 PM
Authentication Flows	Passkeys (FIDO2)

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

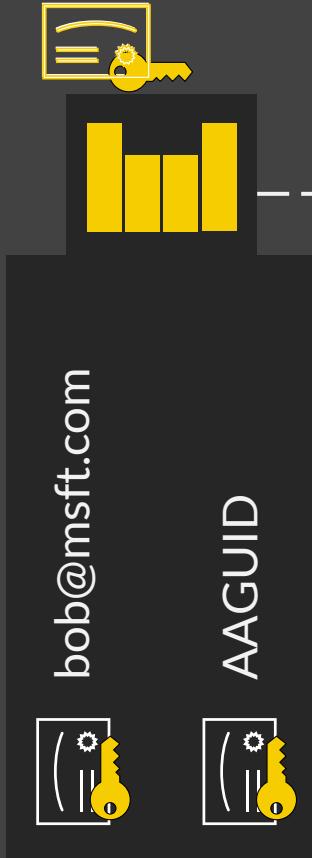




Attestation? AAGUID?

Authenticator Attestation GUID = AAGUID

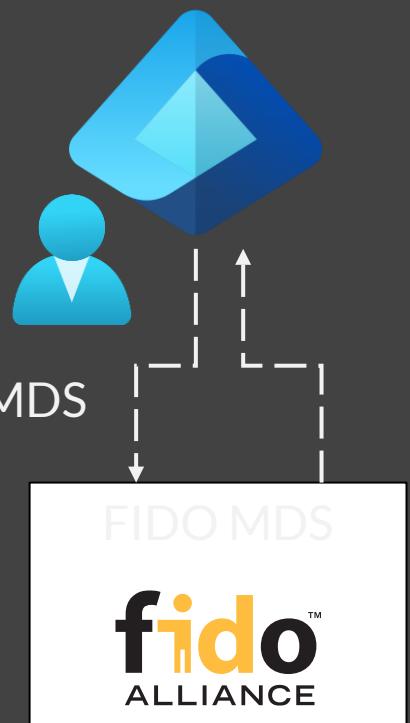
1. Credential key pair generated
2. Sign public with attestation private key



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



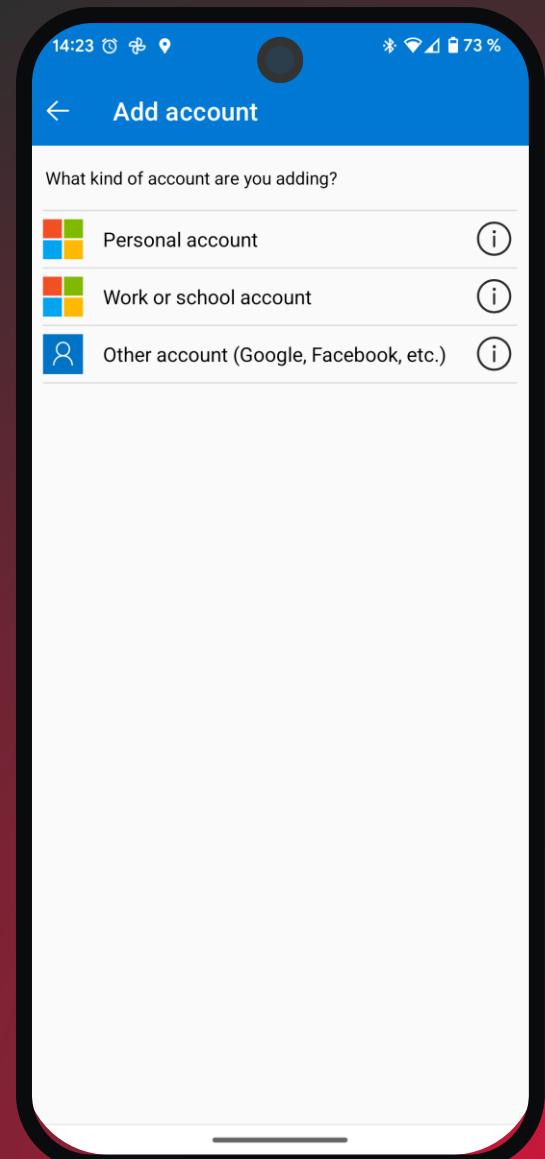
<https://aaguid.nicolasuter.ch/>

<https://fidoalliance.org/fido-technotes-the-truth-about-attestation/>

User experience in the lab



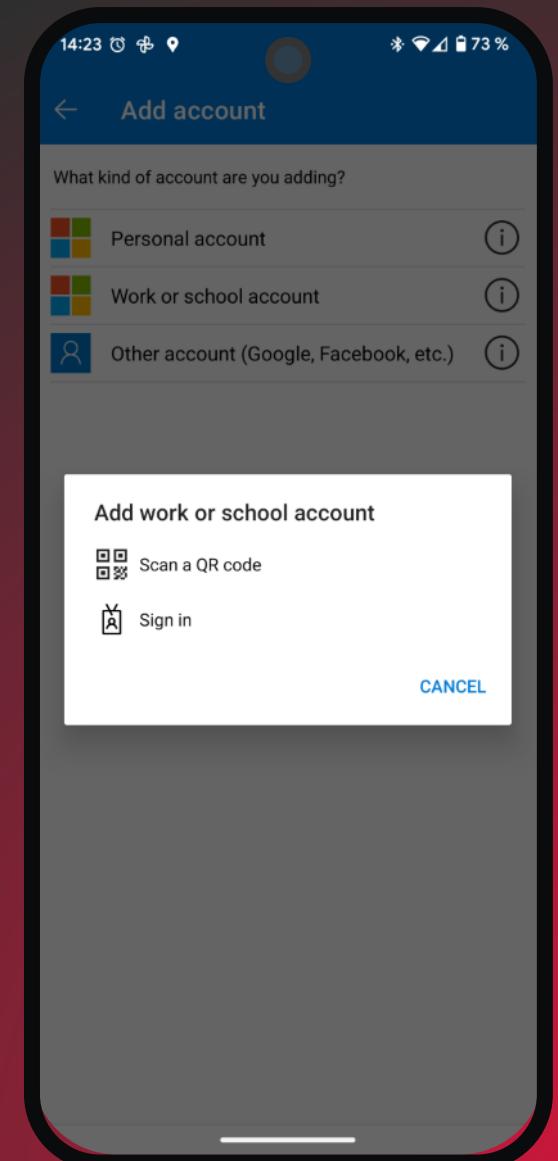
User experience in the lab



User experience in the lab



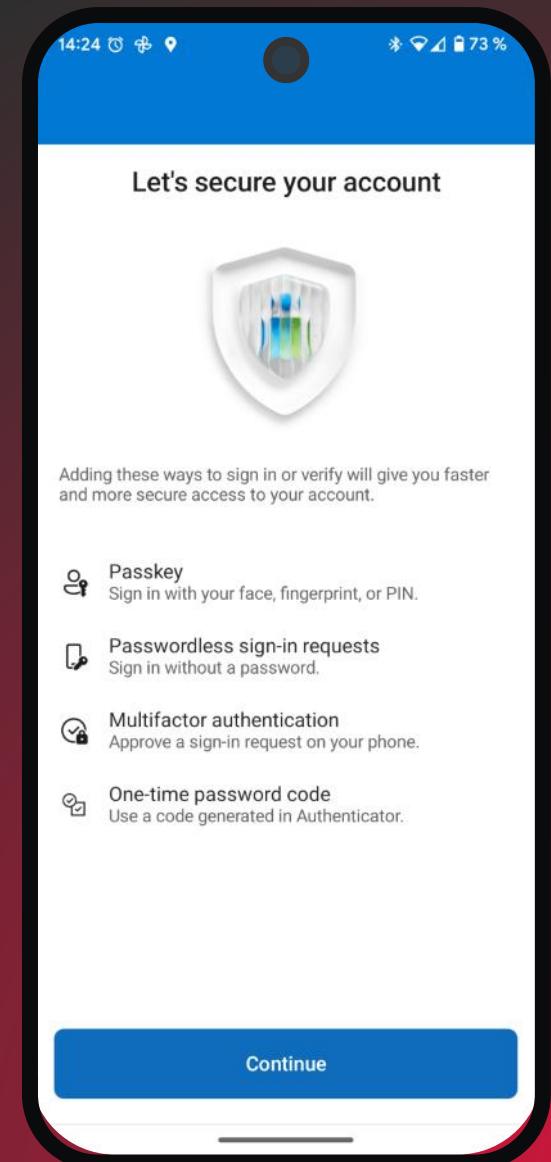
www.workplaceninjas.us



User experience in the lab



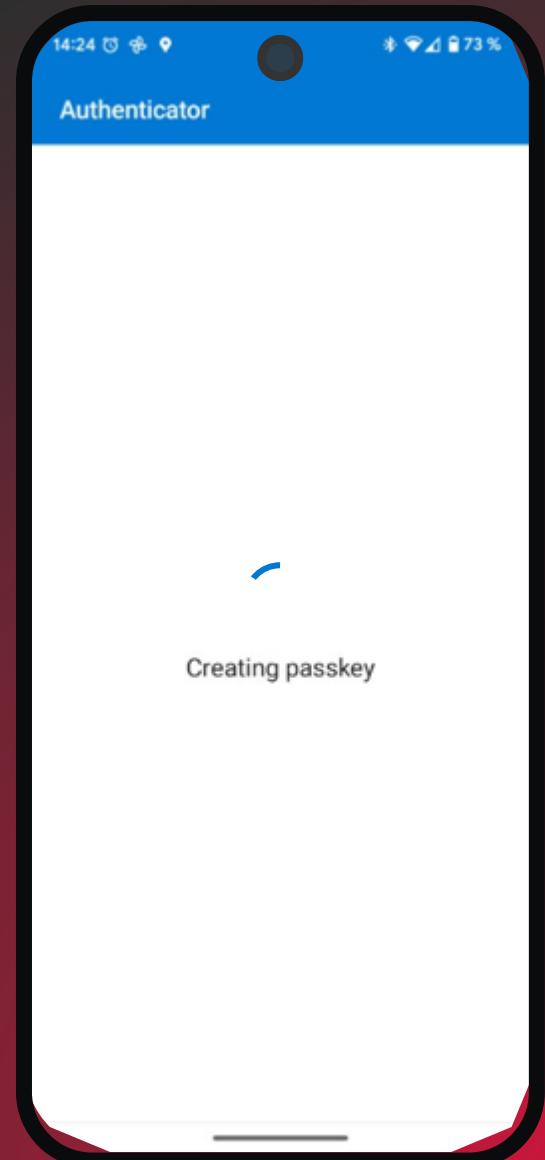
www.workplaceninjas.us



User experience in the lab



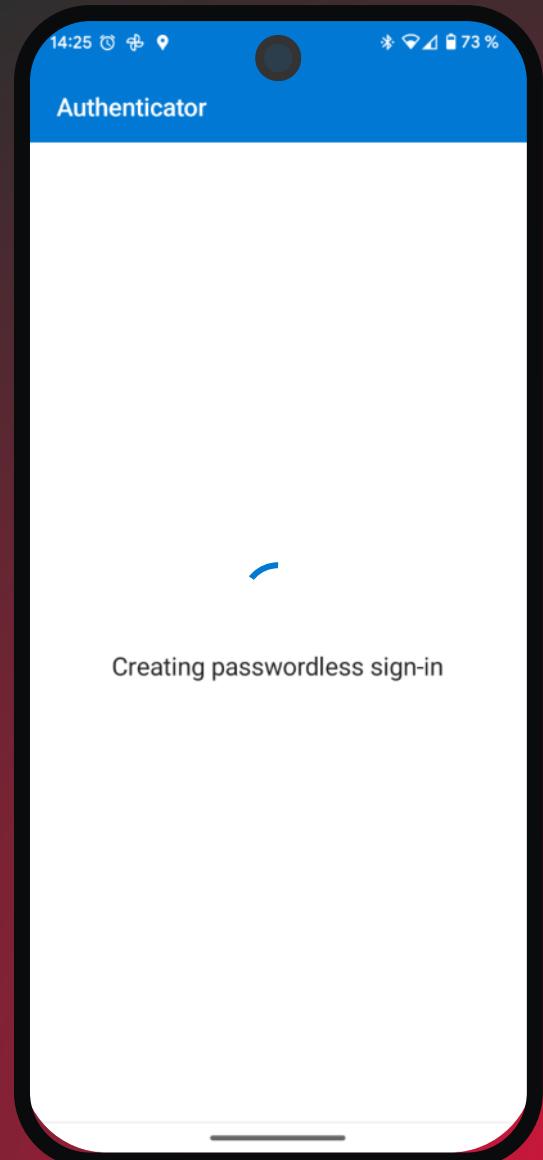
www.workplaceninjas.us



User experience in the lab



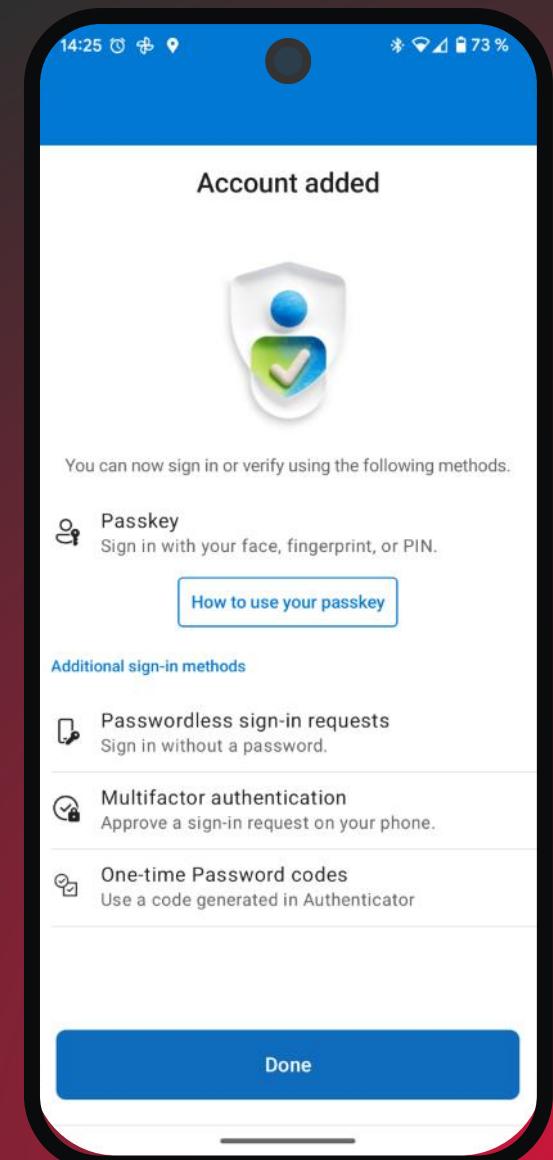
www.workplaceninjas.us



User experience in the lab



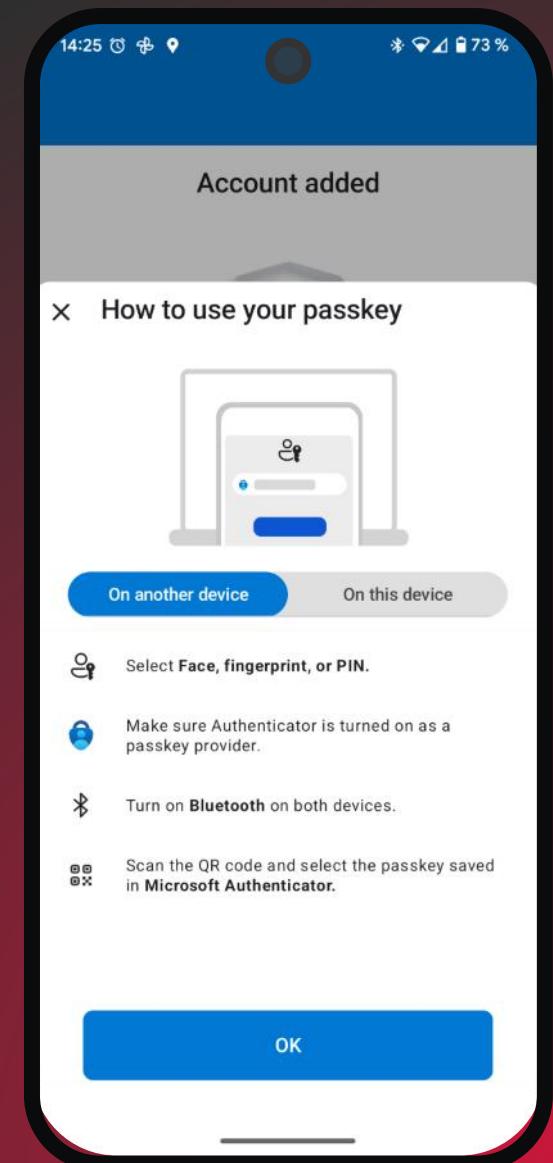
www.workplaceninjas.us



User experience in the lab



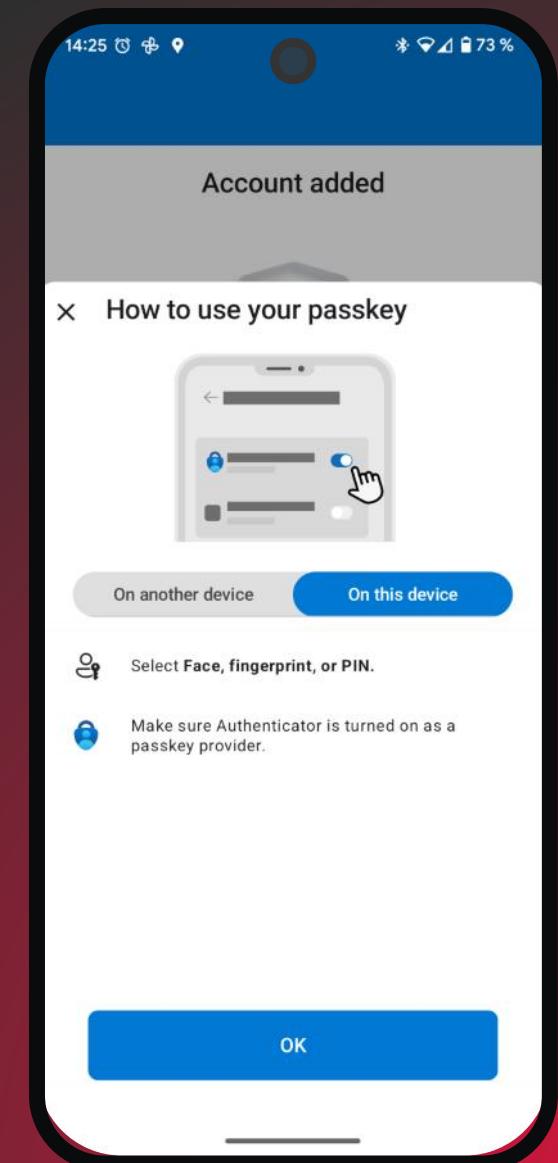
www.workplaceninjas.us



User experience in the lab



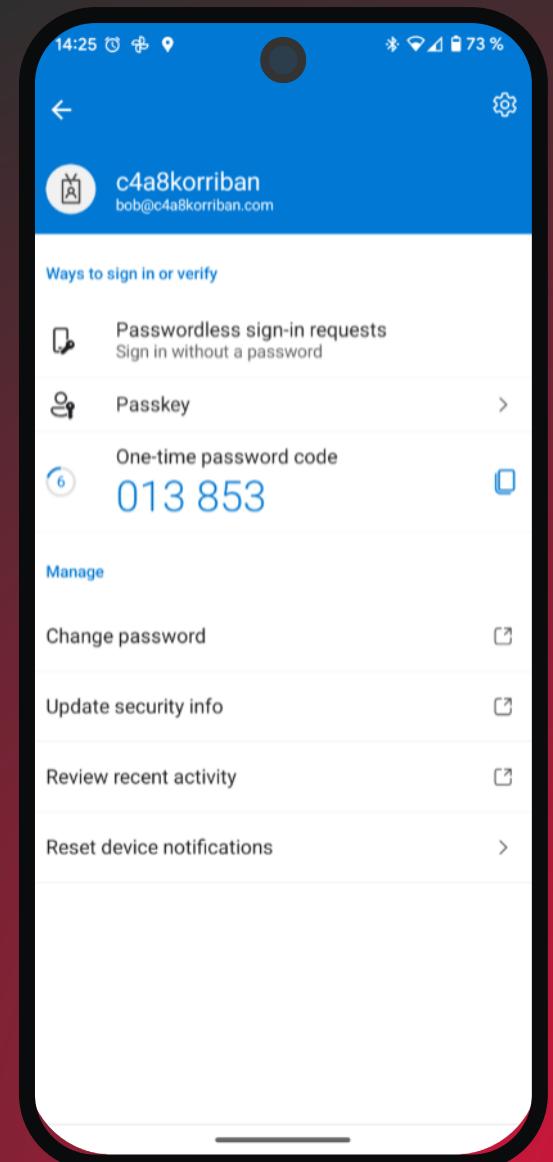
www.workplaceninjas.us



User experience in the lab



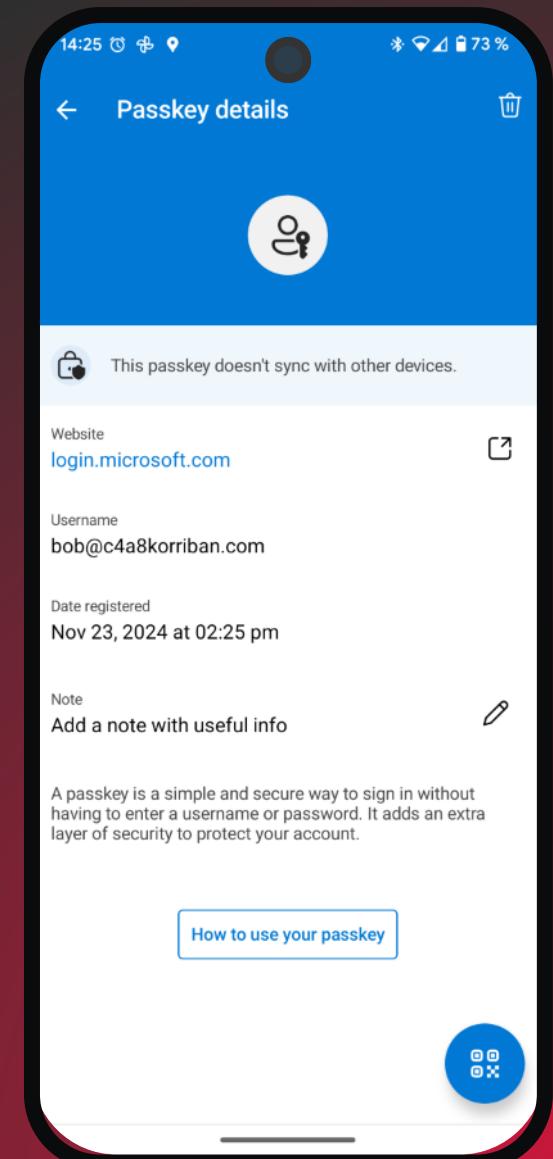
www.workplaceninjas.us



User experience in the lab



www.workplaceninjas.us

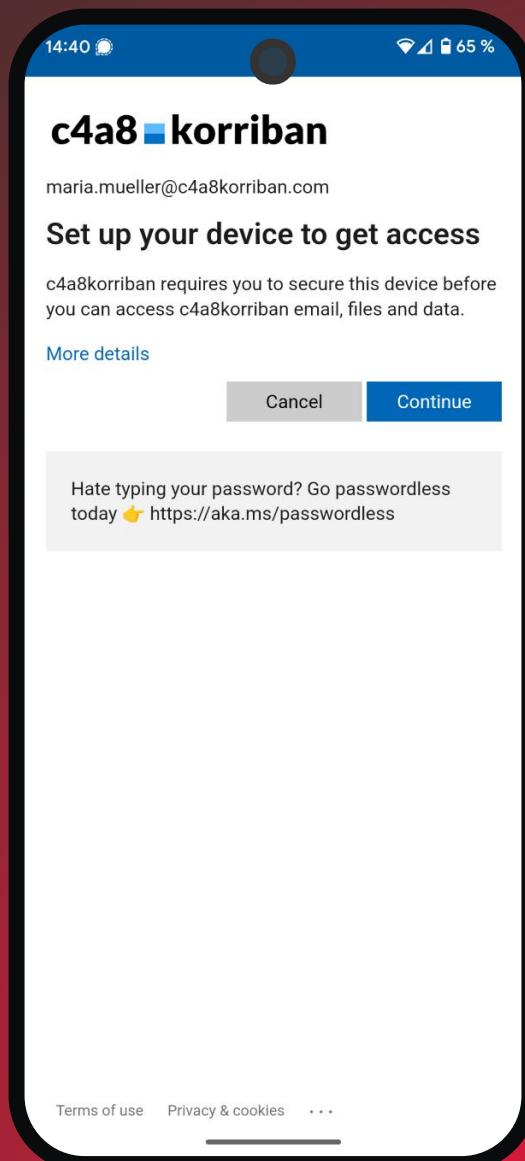


Experience in the real world



www.workplaceninjas.us

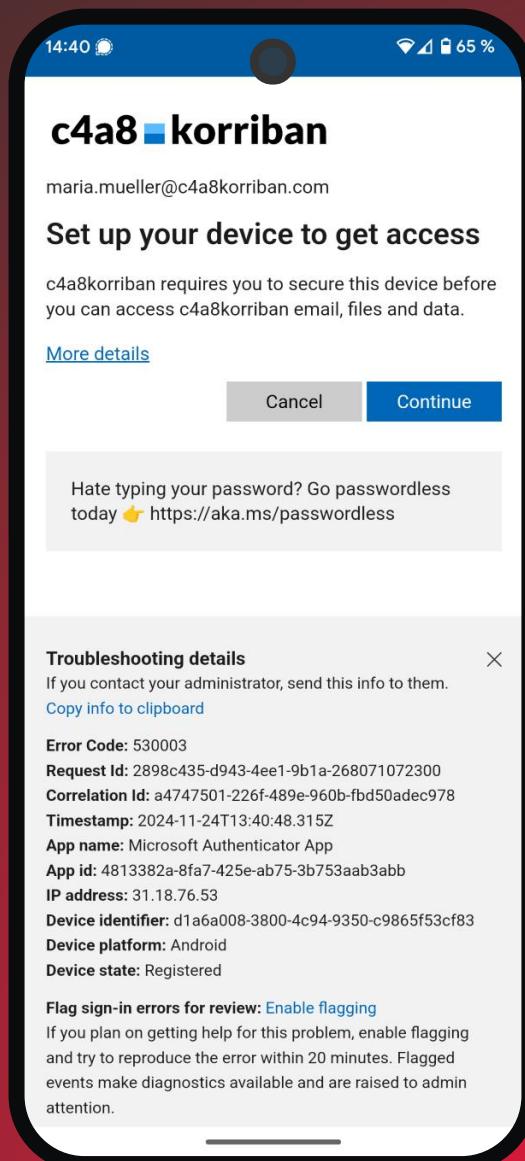




Experience in the
real world

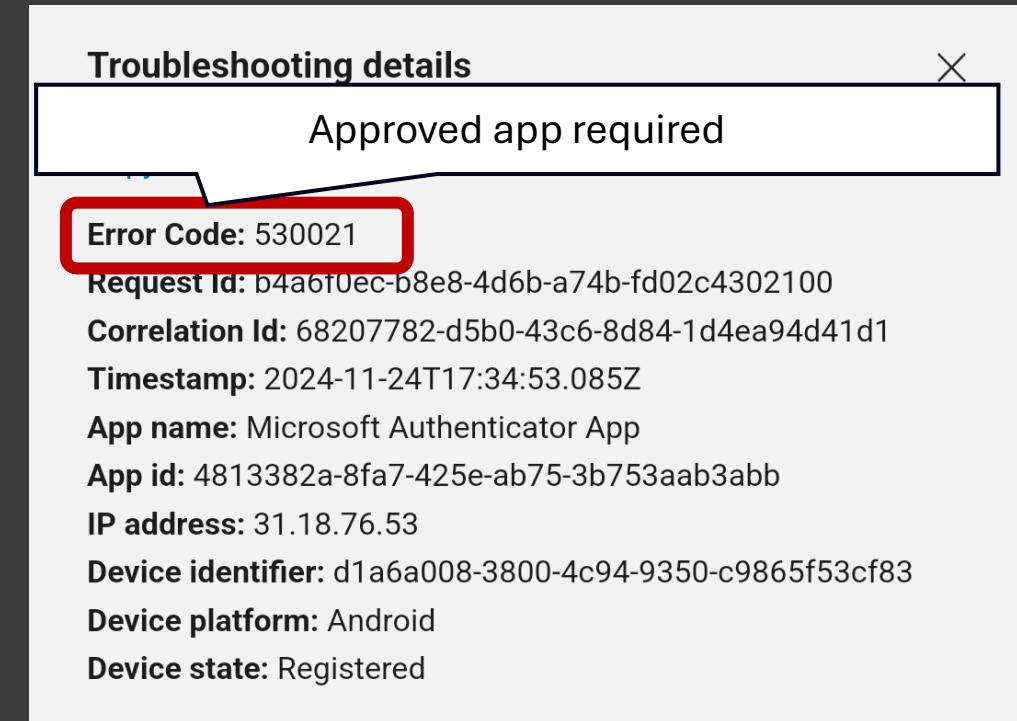
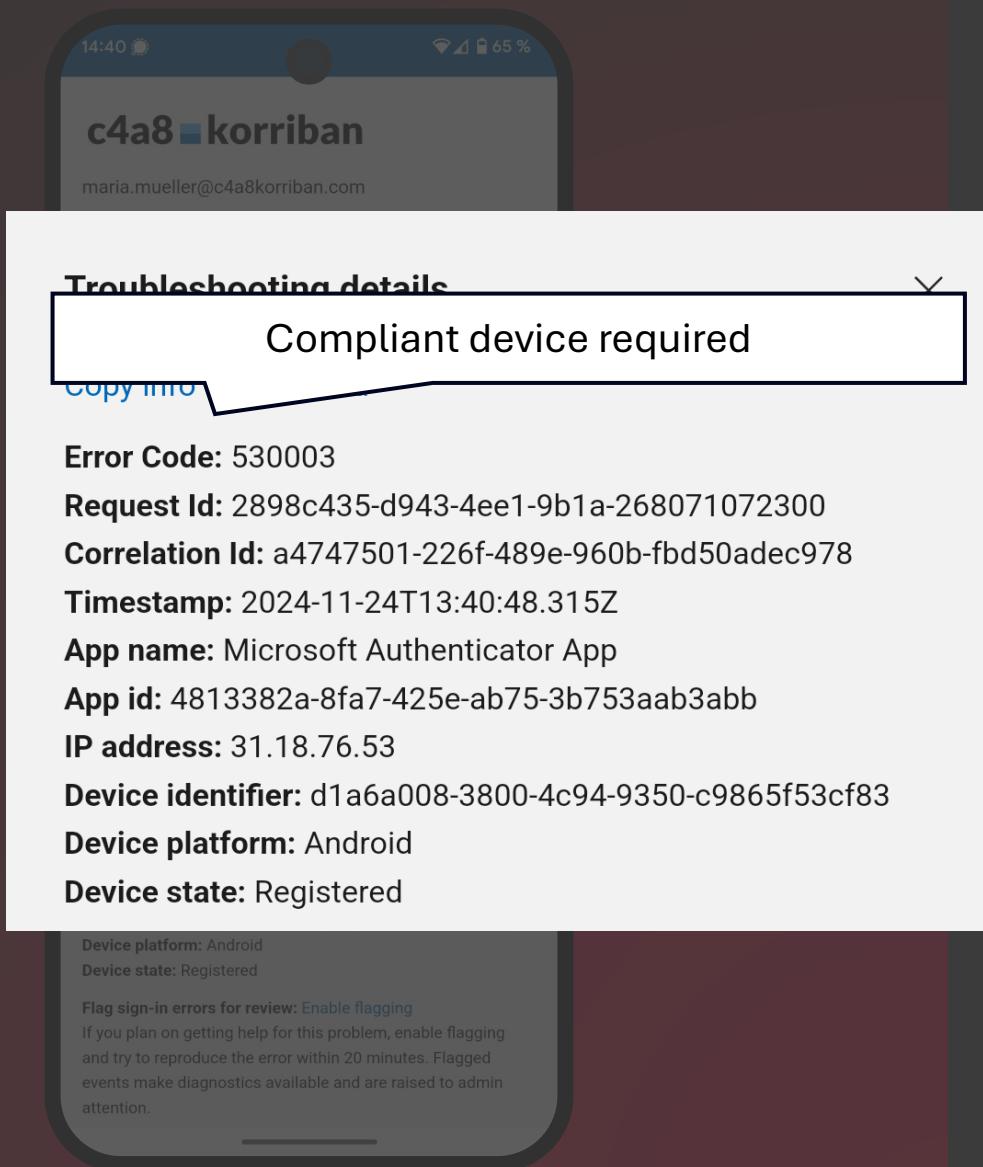
www.workplaceninjas.us





Experience in the real world





Cross Device Flow



InPrivate My Sign-Ins | Security Info | Micro + https://mysignins.microsoft.com/security-info c4a8 korriban My Sign-Ins Overview Security info Devices Password Organizations Settings & Privacy Recent activity

For security reasons, we recommend that you delete any sign-in methods that you no longer use.

Security info

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

Default sign-in method: Microsoft Authenticator - notification [Change](#)

Add sign-in method	Last updated	Action
>Password	a day ago	Change
Microsoft Authenticator Passwordless sign-in		Delete
Passkey Microsoft Authenticator	Authenticator - Android	Delete
Passkey Microsoft Authenticator	Authenticator - Android	Delete
Temporary access pass	Expires 11/24/2024, 7:34:32 PM	Delete

Lost device? [Sign out everywhere](#)



Cross Device Flow



InPrivate My Sign-Ins | Security Info | Micro X + https://mysignins.microsoft.com/security-info c4a8 korriban My Sign-Ins Overview Security info Devices Password Organizations Settings & Privacy Recent activity Default sign-in method: Microsoft Authenticator Add sign-in method + Password Microsoft Authenticator Passkey Microsoft Authenticator Passkey Microsoft Authenticator Temporary access pass Expires 11/24/2024, 7:34:32 PM Lost device? Sign out everywhere

For security reasons, we recommend that you delete any sign-in methods that you no longer use.

Security info

These are the methods you can use to sign in to your account.

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

Delete **Delete** **Delete**



Cross Device Flow



InPrivate My Sign-Ins | Security Info | Micro X https://mysignins.microsoft.com/security-info

c4a8 korriban My Sign-Ins

For security reasons, we recommend that you delete any sign-in methods that you no longer use.

Security info

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

Create your passkey in Microsoft Authenticator

A passkey lets you sign in more easily and securely with your face, fingerprint, or PIN.

Make sure your device has at least Android 14 or iOS 17, and that Authenticator is updated to the latest version.

Need to add your account in Authenticator? [Add it now](#)

[Having trouble?](#)

Back Next

Method	Details	Action
Passkey Microsoft Authenticator	Authenticator - Android	Delete
Temporary access pass	Expires 11/24/2024, 7:34:32 PM	Delete

Lost device? Sign out everywhere

Cross Device Flow



InPrivate My Sign-Ins | Security Info | Micro X + https://mysignins.microsoft.com/security-info c4a8 korriban My Sign-Ins Overview Security info Devices Password Organizations Settings & Privacy Recent activity Default Having Trouble? Can't sign in to Microsoft Authenticator? You can still [create your passkey a different way](#) using your browser and mobile device. This requires Bluetooth on both devices. For more information, go to our [support page](#). If you still need help, contact your admin. Close Lost device? Sign out everywhere

The screenshot shows a Microsoft Edge browser window with an InPrivate tab open. The URL is https://mysignins.microsoft.com/security-info. The main content is the 'Security info' section under 'My Sign-Ins'. On the left, there's a sidebar with links like Overview, Security info (which is selected), Devices, Password, Organizations, Settings & Privacy, and Recent activity. A modal window titled 'Having Trouble?' is displayed in the center. It contains text about troubleshooting Microsoft Authenticator sign-in issues using a browser and mobile device, with a link to a support page. At the bottom of the modal is a 'Close' button. The background shows a list of security methods: 'Passkey Microsoft Authenticator' (Authenticator - Android), 'Temporary access pass' (Expires 11/24/2024, 7:34:32 PM), and a 'Delete' button for each. A red horizontal bar is at the bottom of the slide.

Cross Device Flow



InPrivate My Sign-Ins | Security Info | Micro + https://mysignins.microsoft.com/security-info c4a8 korriban My Sign-Ins Overview Security info Devices Password Organizations Settings & Privacy Recent activity Default sign-in method: Microsoft Authenticator - notification Change Which device do you want to use? X Add sign-in method Android Passkeys require at least Android 14 iPhone or iPad Passkeys require at least iOS 17 or iPad OS 17 Delete Delete Lost device? Sign out everywhere

For security reasons, we recommend that you delete any sign-in methods that you no longer use.

Security info

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

Default sign-in method: Microsoft Authenticator - notification [Change](#)

[+ Add sign-in method](#)

Method	Description	Action
Android	Passkeys require at least Android 14	
iPhone or iPad	Passkeys require at least iOS 17 or iPad OS 17	
Passkey Microsoft Authenticator	Authenticator - Android	
Temporary access pass	Expires 11/24/2024, 7:34:32 PM	

Lost device? Sign out everywhere



Cross Device Flow



InPrivate My Sign-Ins | Security Info | Micro + https://mysignins.microsoft.com/security-info c4a8 korriban My Sign-Ins Overview Security info Devices Password Organizations Settings & Privacy Recent activity Step 1 of 3 Turn on Microsoft Authenticator as a passkey provider Default Having trouble? Back Continue Passkey Microsoft Authenticator Authenticator - Android Lost device? Sign out everywhere

For security reasons, we recommend that you delete any sign-in methods that you no longer use.

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

Step 1 of 3

Turn on Microsoft Authenticator as a passkey provider

Having trouble?

Back Continue

Passkey Microsoft Authenticator Authenticator - Android

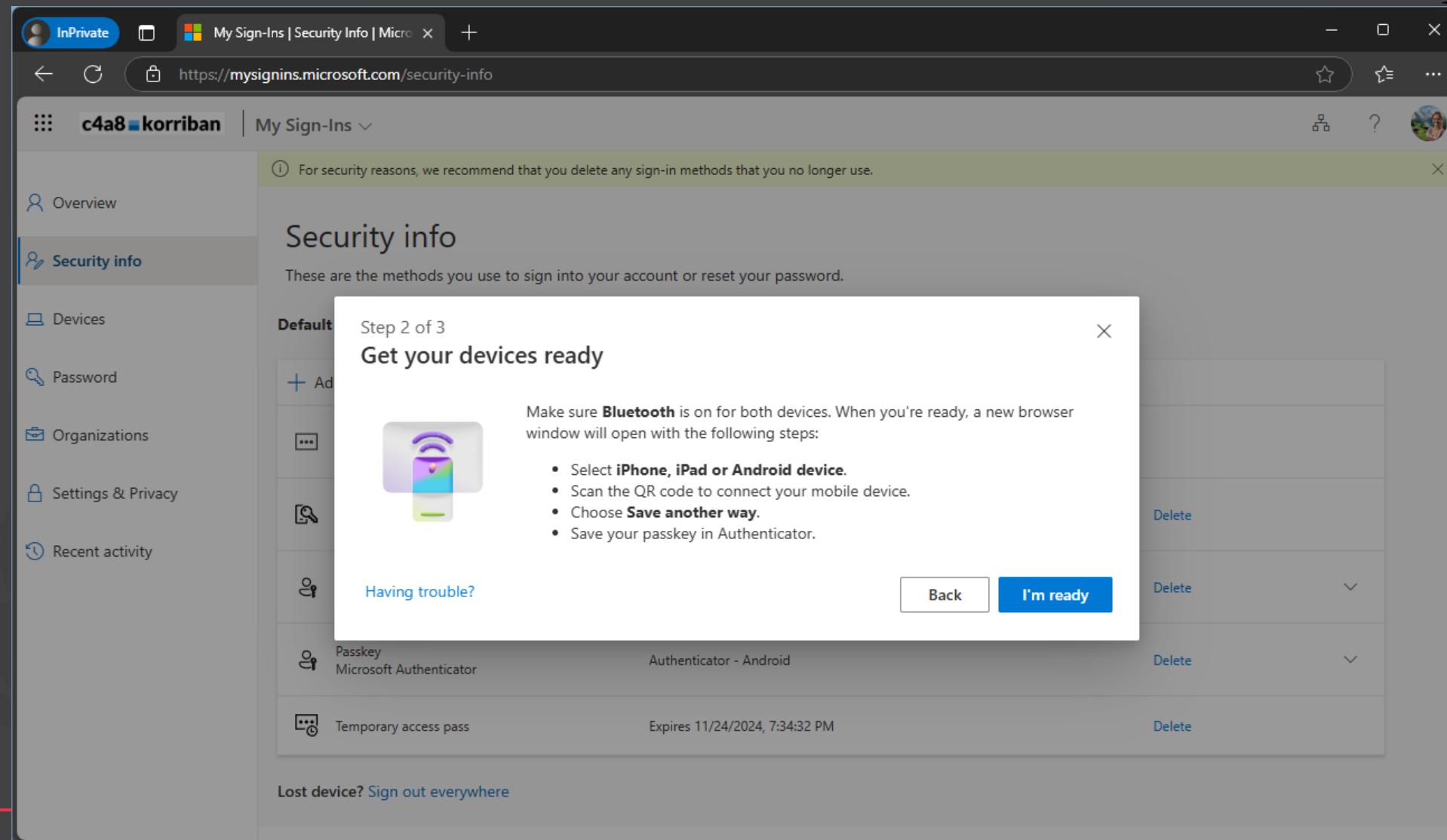
Temporary access pass Expires 11/24/2024, 7:34:32 PM Delete

Lost device? Sign out everywhere

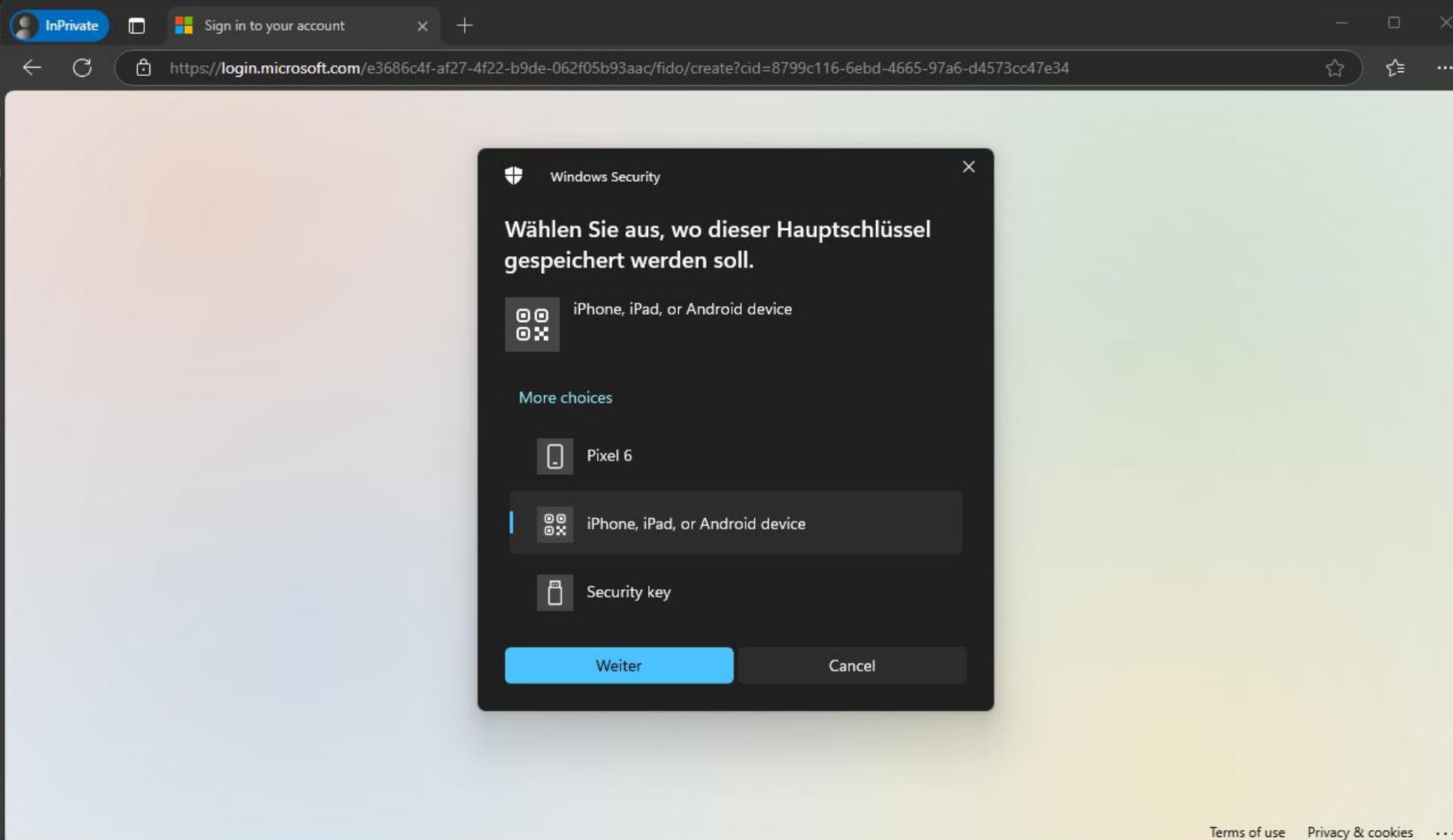
A screenshot of a Microsoft Edge browser window showing the "Security info" page. A modal dialog box titled "Step 1 of 3" is displayed, instructing the user to turn on Microsoft Authenticator as a passkey provider. The dialog includes a "Having trouble?" link, a "Back" button, and a "Continue" button. Below the dialog, there are sections for "Passkey Microsoft Authenticator" and "Authenticator - Android", along with a "Temporary access pass" that expires on November 24, 2024, at 7:34:32 PM. A "Delete" link is also present next to the temporary access pass. At the bottom of the page, there is a link to "Lost device? Sign out everywhere".



Cross Device Flow

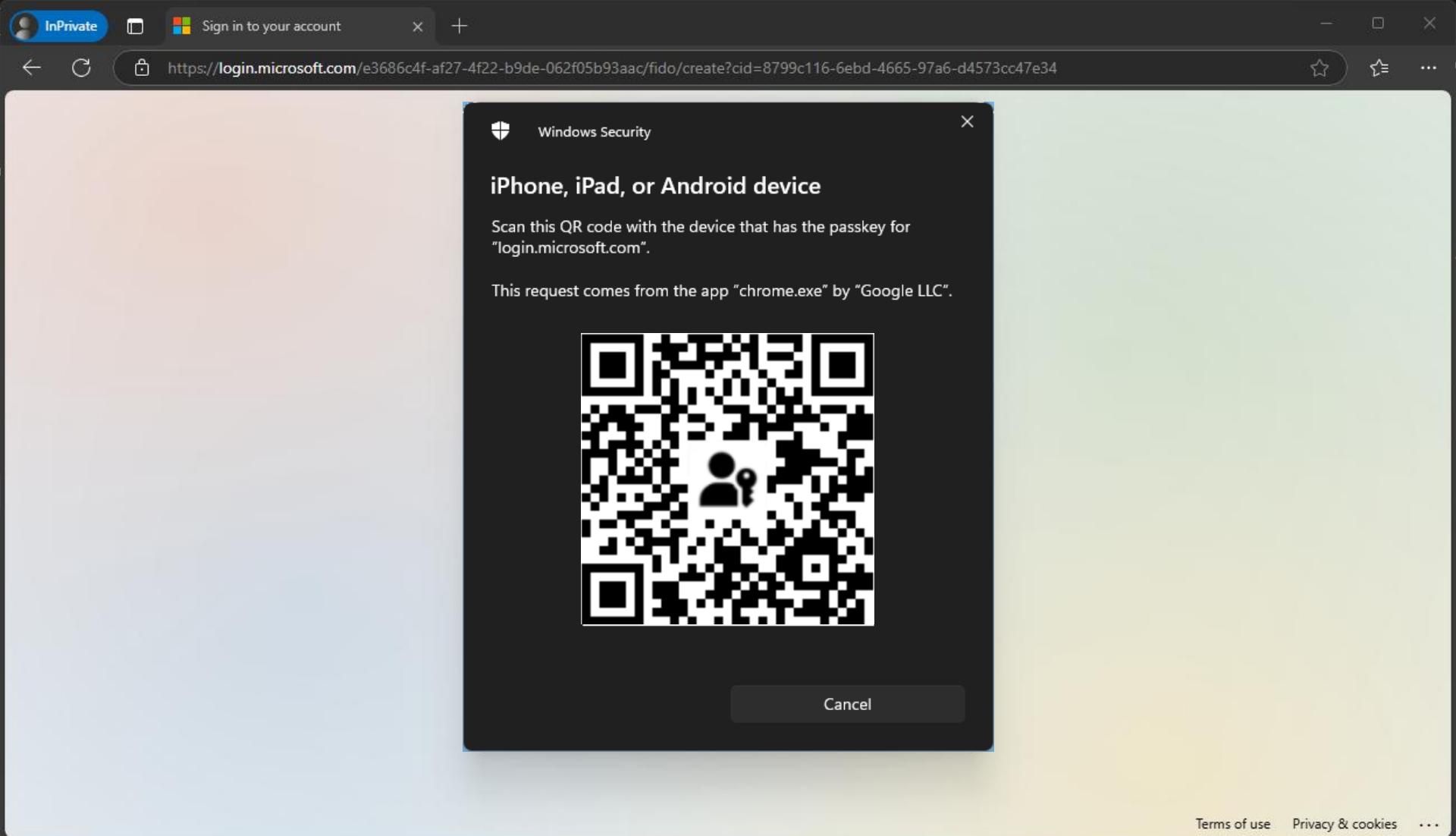


Cross Device Flow



A screenshot of a Microsoft Edge browser window in InPrivate mode. The address bar shows the URL <https://login.microsoft.com/e3686c4f-af27-4f22-b9de-062f05b93aac/fido/create?cid=8799c116-6ebd-4665-97a6-d4573cc47e34>. A modal dialog box titled "Windows Security" is displayed, asking the user to choose where to store the primary key. The options listed are "iPhone, iPad, or Android device" (selected), "Pixel 6", and "Security key". At the bottom are "Weiter" and "Cancel" buttons. The page footer includes links for "Terms of use", "Privacy & cookies", and an ellipsis.

Cross Device Flow



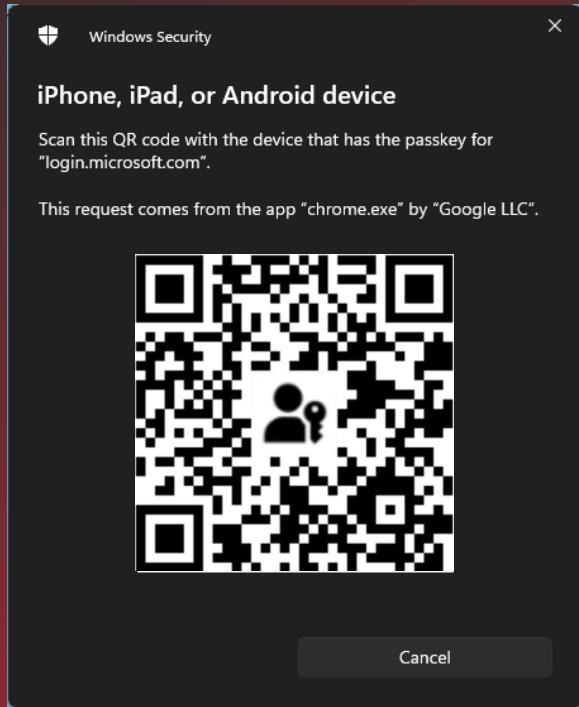
A screenshot of a Microsoft Edge browser window showing the FIDO2 passkey setup process. The address bar shows the URL <https://login.microsoft.com/e3686c4f-af27-4f22-b9de-062f05b93aac/fido/create?cid=8799c116-6ebd-4665-97a6-d4573cc47e34>. A modal dialog box titled "Windows Security" is displayed, instructing the user to scan a QR code with an iPhone, iPad, or Android device. The dialog also states that the request comes from the app "chrome.exe" by "Google LLC". A large QR code is centered in the dialog. At the bottom right of the dialog is a "Cancel" button. The browser interface includes tabs for "InPrivate", "Sign in to your account", and a "+" sign. The bottom right corner of the browser window contains links for "Terms of use", "Privacy & cookies", and an ellipsis.

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

QR Code Deep Dive

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

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

QR Code Deep Dive

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

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

QR Code Deep Dive

A6	00	58	21	02	73	1F
00	0E	75	37	28	D1	39
97	00	CD	91	98	8A	EA
85	12	00	2D	B4	16	91
2E	D5	38	00	7A	17	FF
52	2B	56	31	00	5F	C4
01	50	7A	F8	FB	00	59
60	2E	FD	4F	8C	38	00
48	AF	DA	C4	B5	27	02
00	02	03	1A	67	4B	14
84	00	04	F5	05	62	67
61	00	00				

```
// 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
Android Apple MAM	Compliant device: All resources		Same-Device	Yes/No	i
Android MAM	Compliant device: All resources	Bluetooth icon	Cross-Device	Yes	✓
Android Apple MAM	Compliant device: All resources	Bluetooth icon	Cross-Device	No	✓
Android Apple All	Approved apps: All resources		Same-Device	Yes/No	i
Android MAM	Approved apps: All resources	Bluetooth icon	Cross-Device	Yes	✓
Android Apple MAM	Approved apps: All resources	Bluetooth icon	Cross-Device	No	✓
Android Apple Work Profile/MDM	Compliant device: All resources		Same-Device	Yes/No	✓
Apple All	n/a	Bluetooth icon	Cross-Device	Yes	i



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.

Compliant Device required with Passkey exclusion

Conditional Access policy

Delete View policy information View policy impact

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.

[Learn more](#)

Name *

Compliant Device required with Passkey exc...

Assignments

Users, agents or workload identities

Specific users included and specific users excluded

Target resources

All resources (formerly 'All cloud apps') included and 1 resource excluded

Network

Not configured

Conditions

0 conditions selected

Access controls

Grant

1 control selected

Session

Enable policy

Report-only On Off

Save

Control access based on all or specific apps, agents, internet resources, actions, or authentication context. [Learn more](#)

Select what this policy applies to

Resources (formerly cloud apps)

Include

Select the resources to exempt from the policy

- None
- All internet resources with Global Secure Access
- All agent resources (Preview)
- Select resources

Select resources based on attributes

None

Select specific resources

Azure Credential Configuration Endpoint Service

AC Azure Credential Configuratio...

To create a Conditional Access policy targeting members in your tenant with Global Secure Access (GSA) as a

Passkey "support" matrix + workaround



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



Remediate risk for all users

Conditional Access policy

[Delete](#) [View policy information](#) [View policy impact](#)[Remediate risk for all users](#)

Assignments

Users, agents or workload identities [\(i\)](#)[Specific users included and specific users excluded](#)

Target resources [\(i\)](#)

[All resources \(formerly 'All cloud apps'\)](#)

Network [\(NEW\)](#) [\(i\)](#)

[Not configured](#)

Conditions [\(i\)](#)

[1 condition selected](#)

Access controls

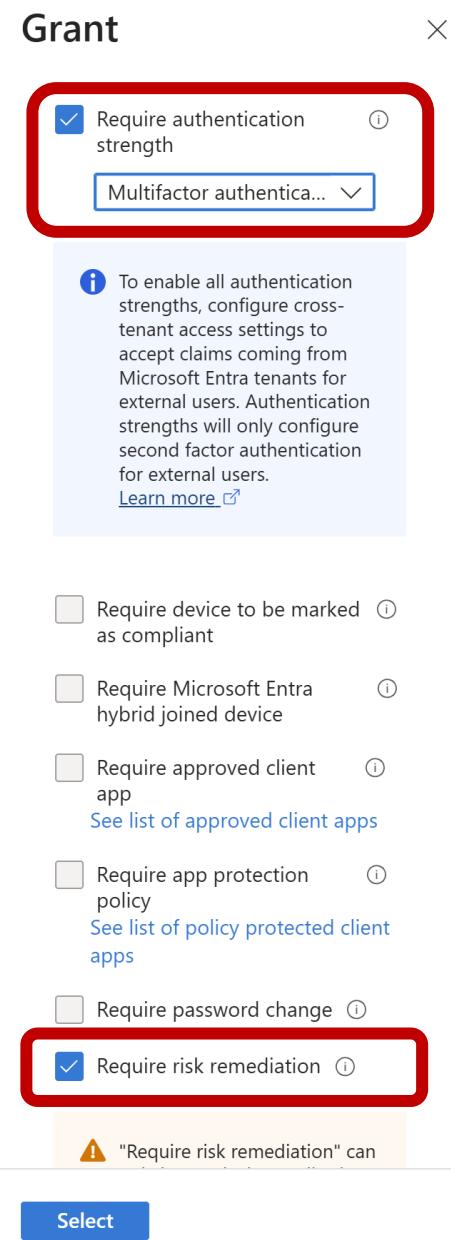
Grant [\(i\)](#)

[2 controls selected](#)

Session [\(i\)](#)

[Sign-in frequency - Every time](#)

Enable policy

[Report-only](#) [On](#) [Off](#)[Save](#)

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**

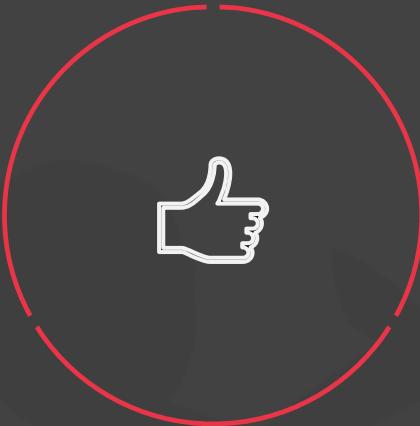




Every passkey is better than a password even with MFA!

www.workplaceninjas.us





Thank You!

