CLOUD IDENTITY SUMMIT '24

Identity Security Track

The End of Passwords

An Introduction to Passkeys in Entra ID

Chris Brumm + Fabian Bader

from glueckkanja AG

Community Event by Azure Meetup BONN

About us...

Fabian Bader		Chris Brumm
old		very old
MVP		CISSP
@fabian_bader	𝕏	@cbrhh
/in/fabianbader	in	/in/christopherbrumm
cloudbrothers.info	🏠	chris-brumm.com

working at glueckkanja AG
as Cyber Security Architect
living in Hamburg, Germany

Evolution of Authentication at Microsoft

2000
Active Directory ->
Kerberos + Smartcards

2003
SecurID standardized

2011
MSO-DS

2012
Microsoft acquires
Phone Factor

2013
Azure AD GA

2015
Windows Hello

2016
Microsoft Authenticator

2017
Phone sign-in

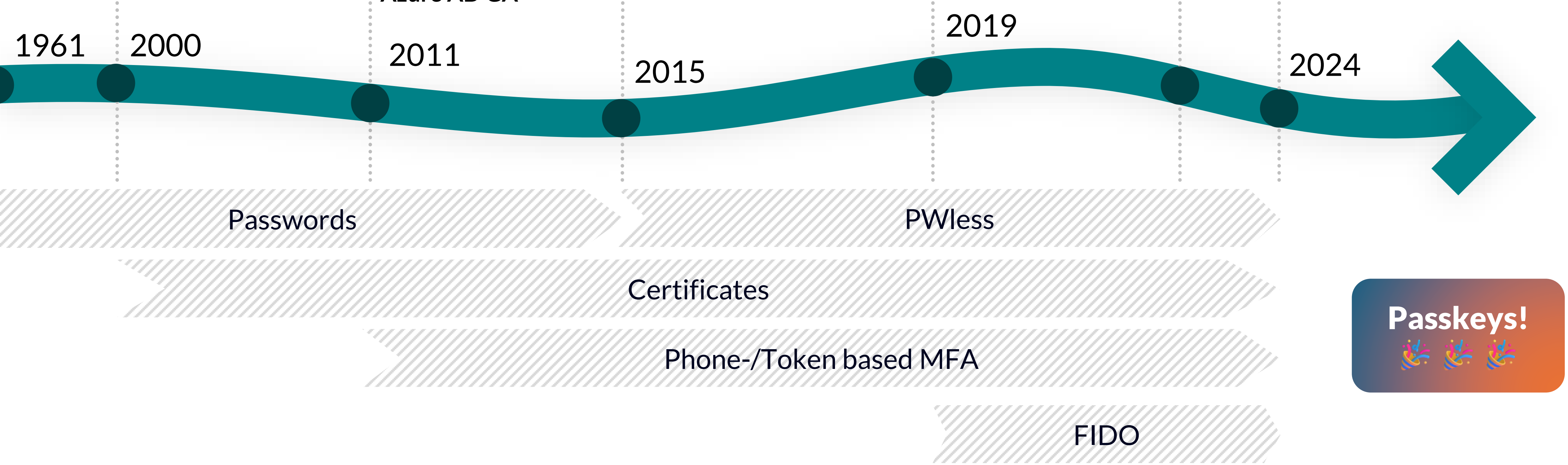
2019
FIDO2 Support

2022
WHfB Cloud Kerberos Trust

2023
Native CBA in Entra ID
TAP and FIDO2 in iOS

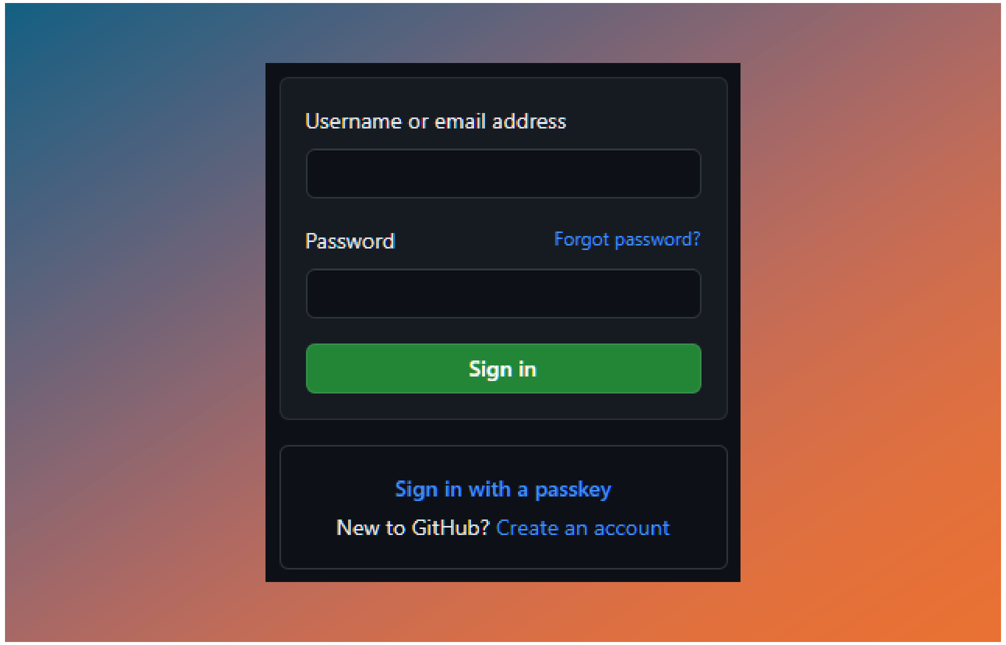
2024
Passkey Support
- Entra ID
- Authenticator

FIDO2 on Android



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



Username or email address

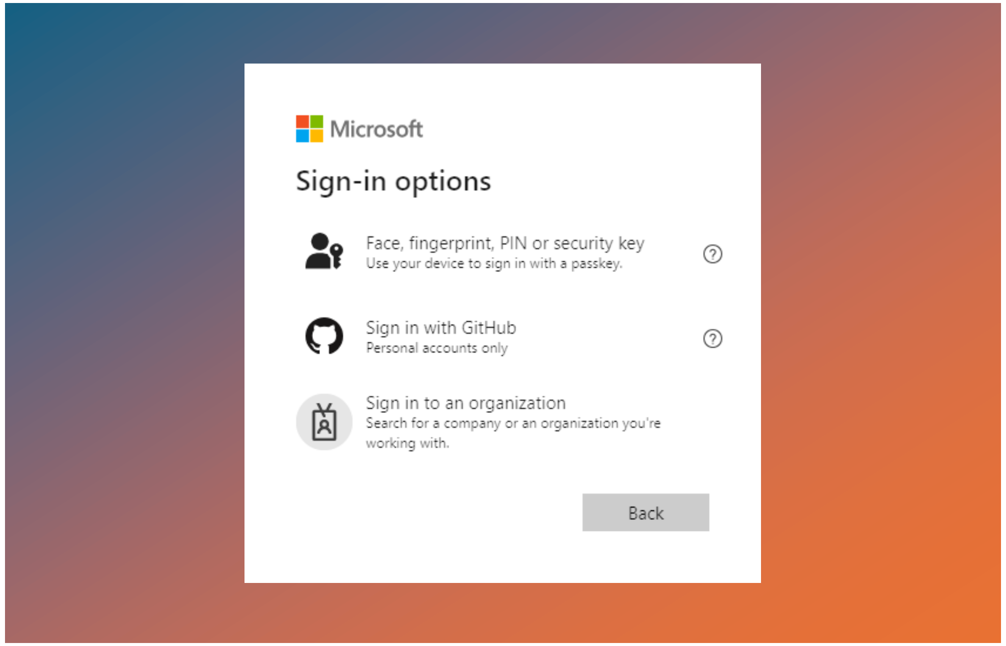
Password

Forgot password?

Sign in

Sign in with a passkey

New to GitHub? Create an account



Microsoft

Sign-in options

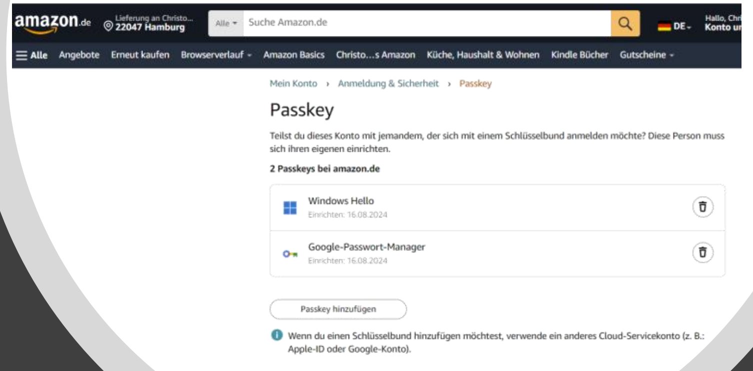
Face, fingerprint, PIN or security key
Use your device to sign in with a passkey.

Sign in with GitHub
Personal accounts only

Sign in to an organization
Search for a company or an organization you're working with.

Back

Passkeys used by Chris’ family



Passkey

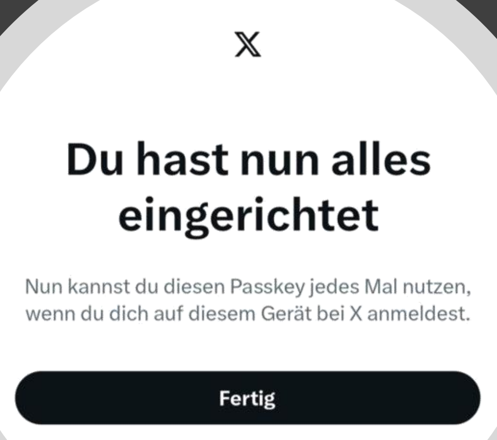
Teilst du dieses Konto mit jemandem, der sich mit einem Schlüsselbund anmelden möchte? Diese Person muss sich ihren eigenen einrichten.

2 Passkeys bei amazon.de

Windows Hello
Einrichten: 16.08.2024

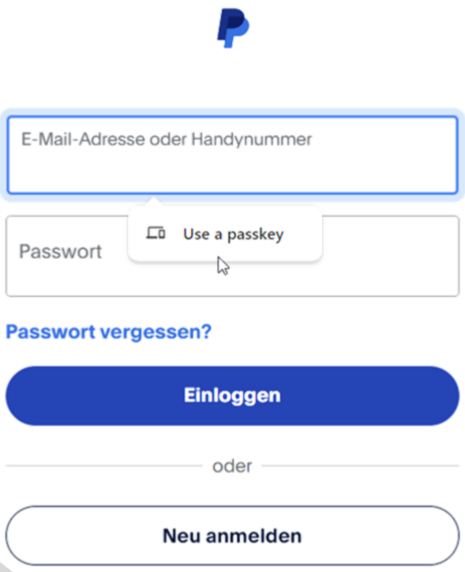
Google-Passwort-Manager
Einrichten: 16.08.2024

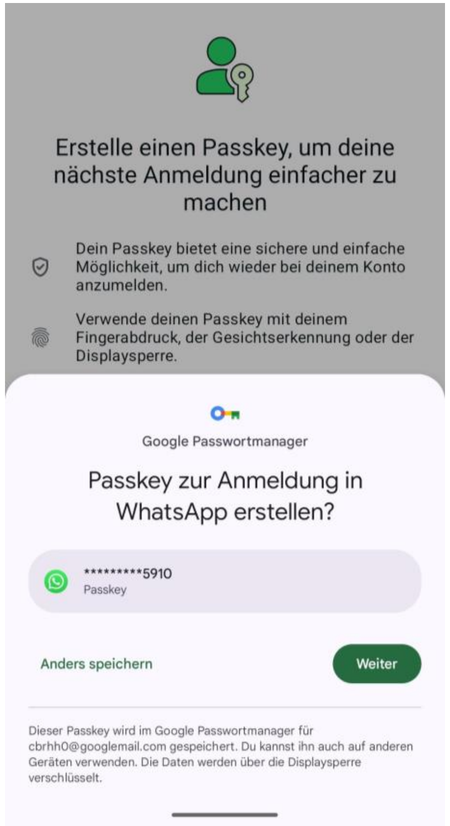
Wenn du einen Schlüsselbund hinzufügen möchtest, verwende ein anderes Cloud-Servicekonto (z. B.: Apple-ID oder Google-Konto).



Du hast nun alles eingerichtet

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




Erstelle einen Passkey, um deine nächste Anmeldung einfacher zu machen

Dein Passkey bietet eine sichere und einfache Möglichkeit, um dich wieder bei deinem Konto anzumelden.

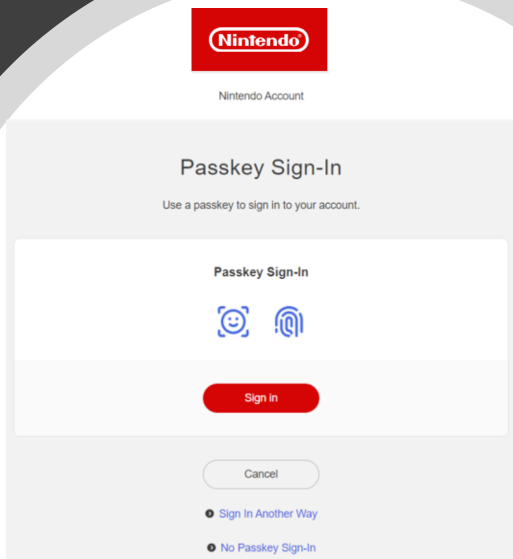
Verwende deinen Passkey mit deinem Fingerabdruck, der Gesichtserkennung oder der Displaysperre.

Google Passwortmanager

Passkey zur Anmeldung in WhatsApp erstellen?

*********5910
Passkey

Dieser Passkey wird im Google Passwortmanager für cbrhh0@googlemail.com gespeichert. Du kannst ihn auch auf anderen Geräten verwenden. Die Daten werden über die Displaysperre verschlüsselt.



Passkey Sign-In

Use a passkey to sign in to your account.

Passkey Sign-In

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 😳

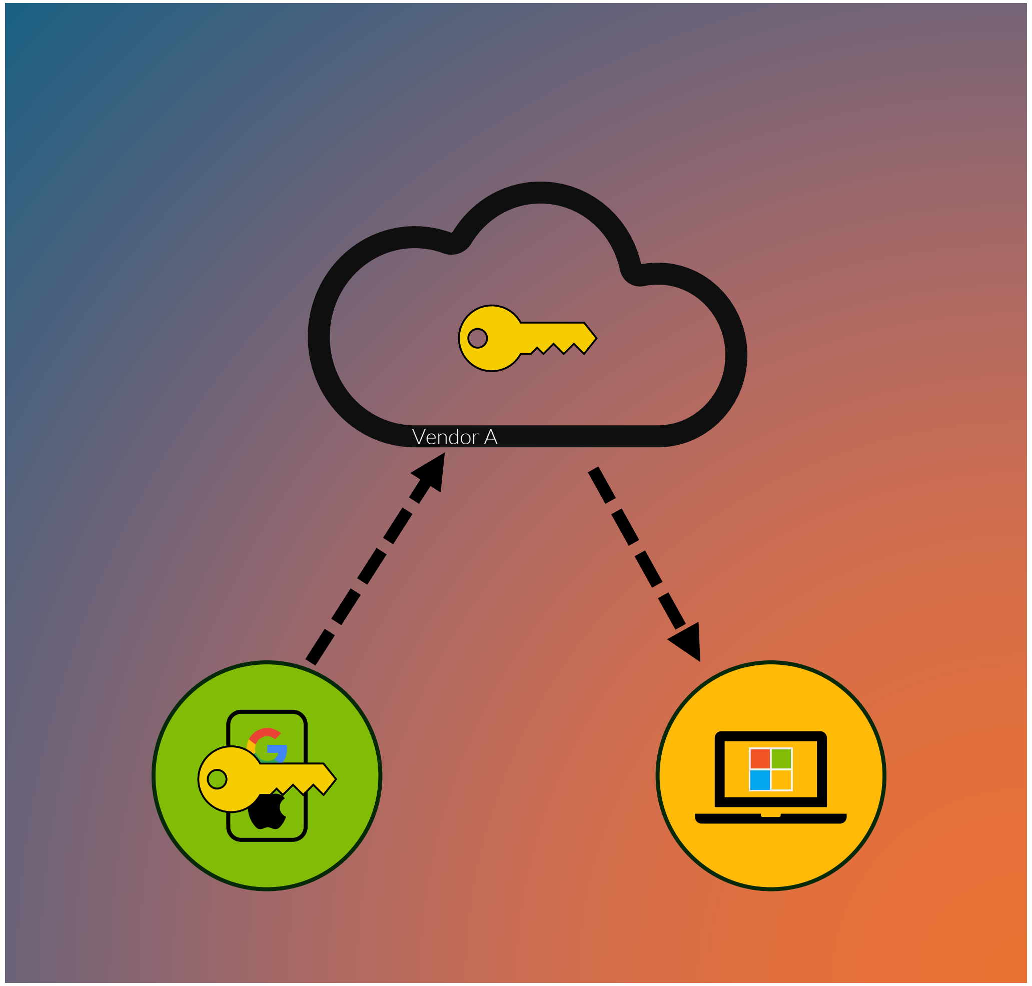
Secure Recovery

Controlled Setup

Phishing-resistance

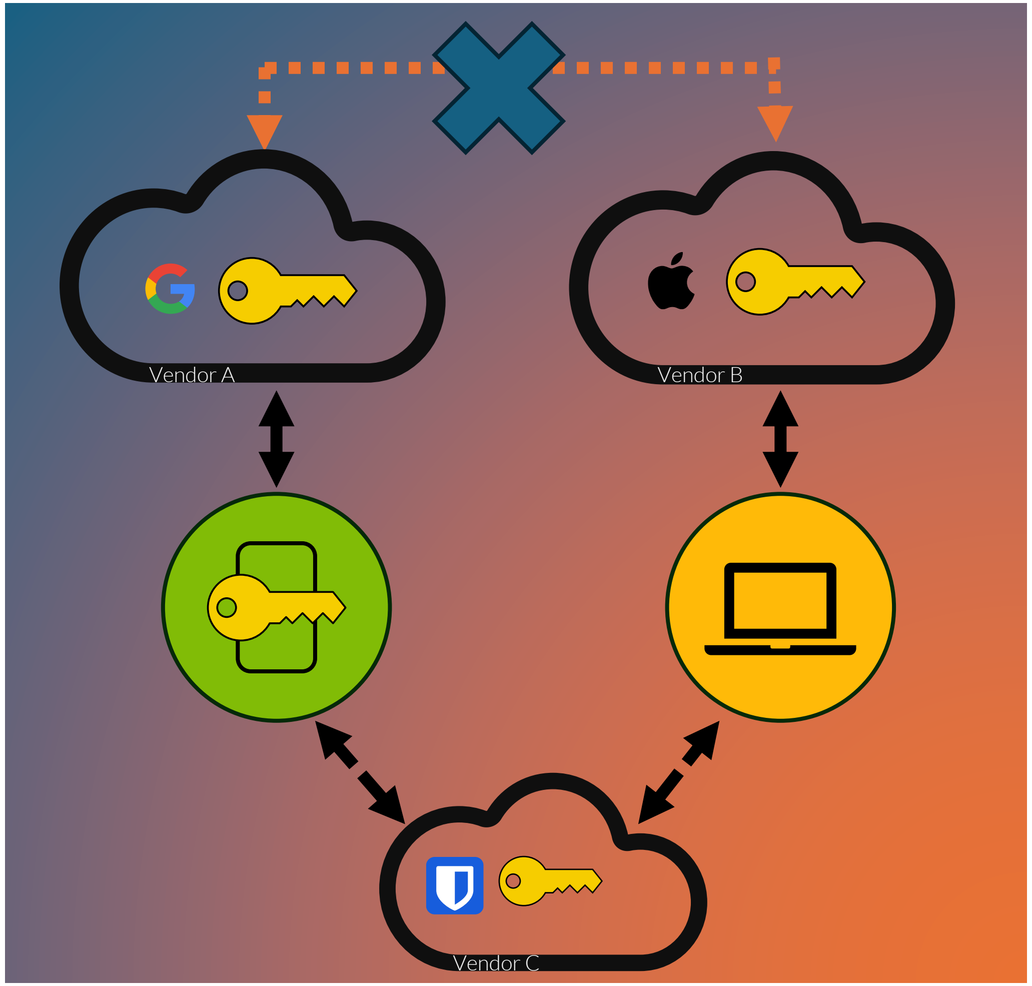
Controlled usage

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

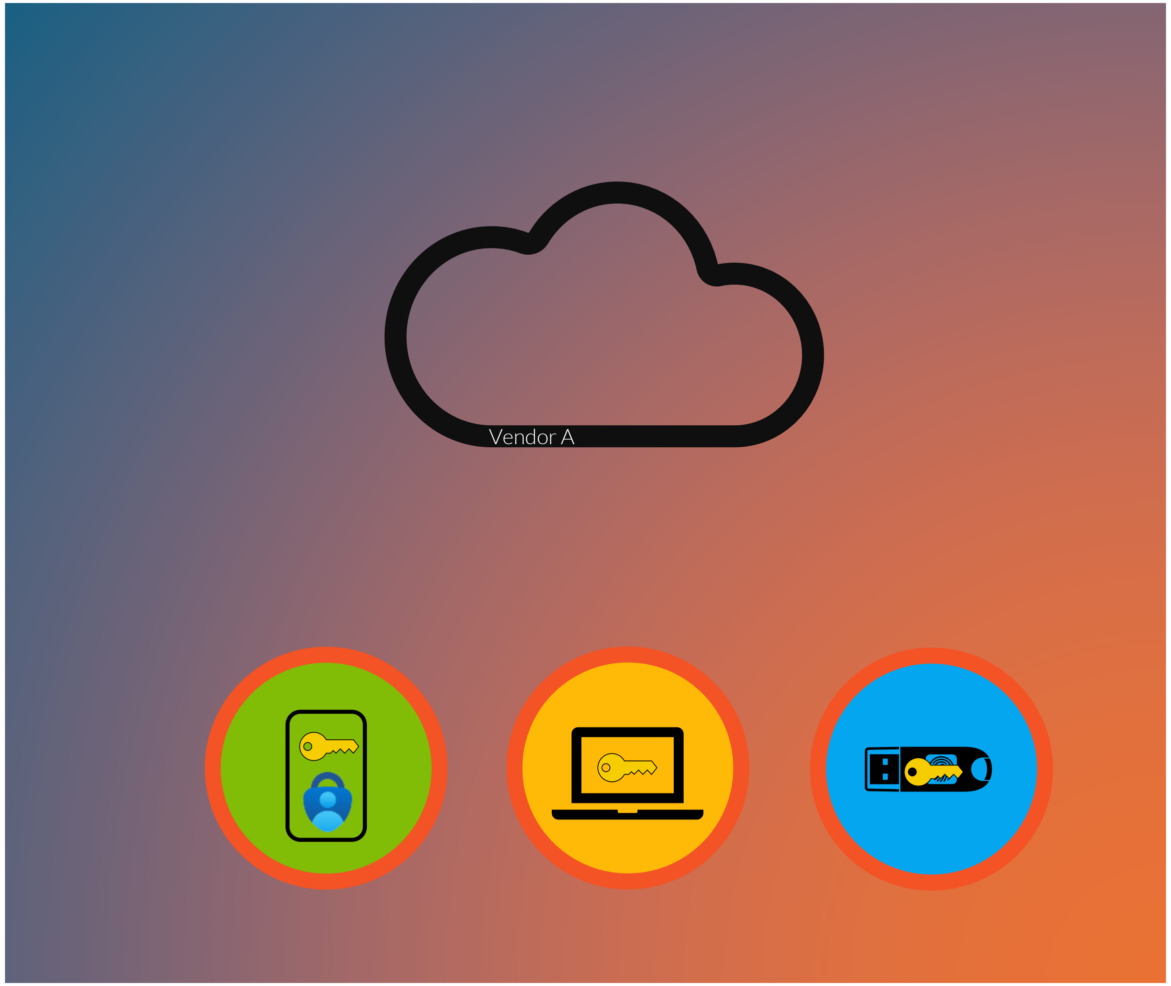
Synced vs. Device-bound passkeys



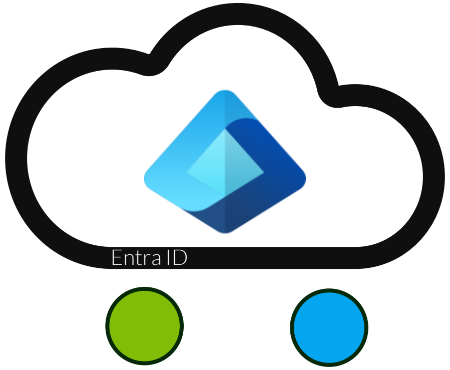
- Native cross vendor sync is not possible
- Workarounds
  - Cross-Device Authentication
  - Third-party passkey provider

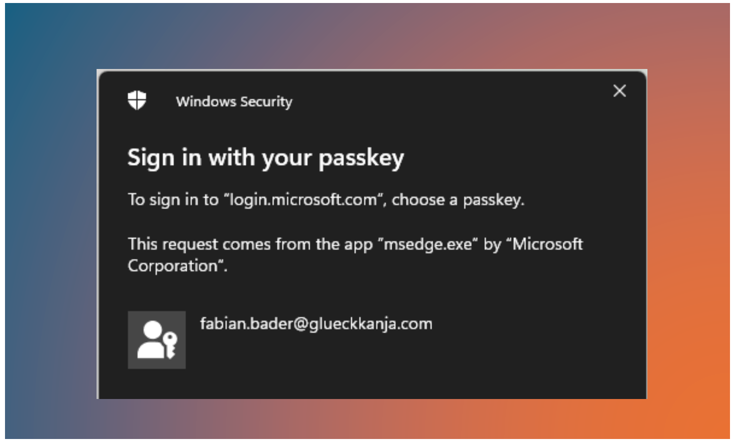
Synced vs. Device-bound passkeys

- 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



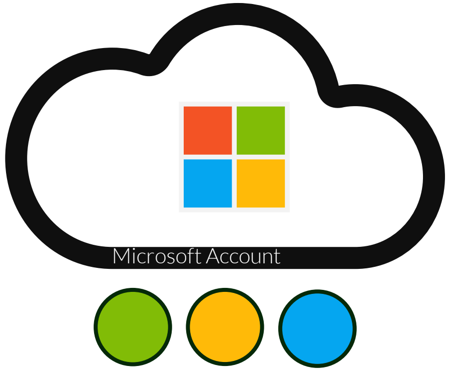

Windows Security

Sign in with your passkey

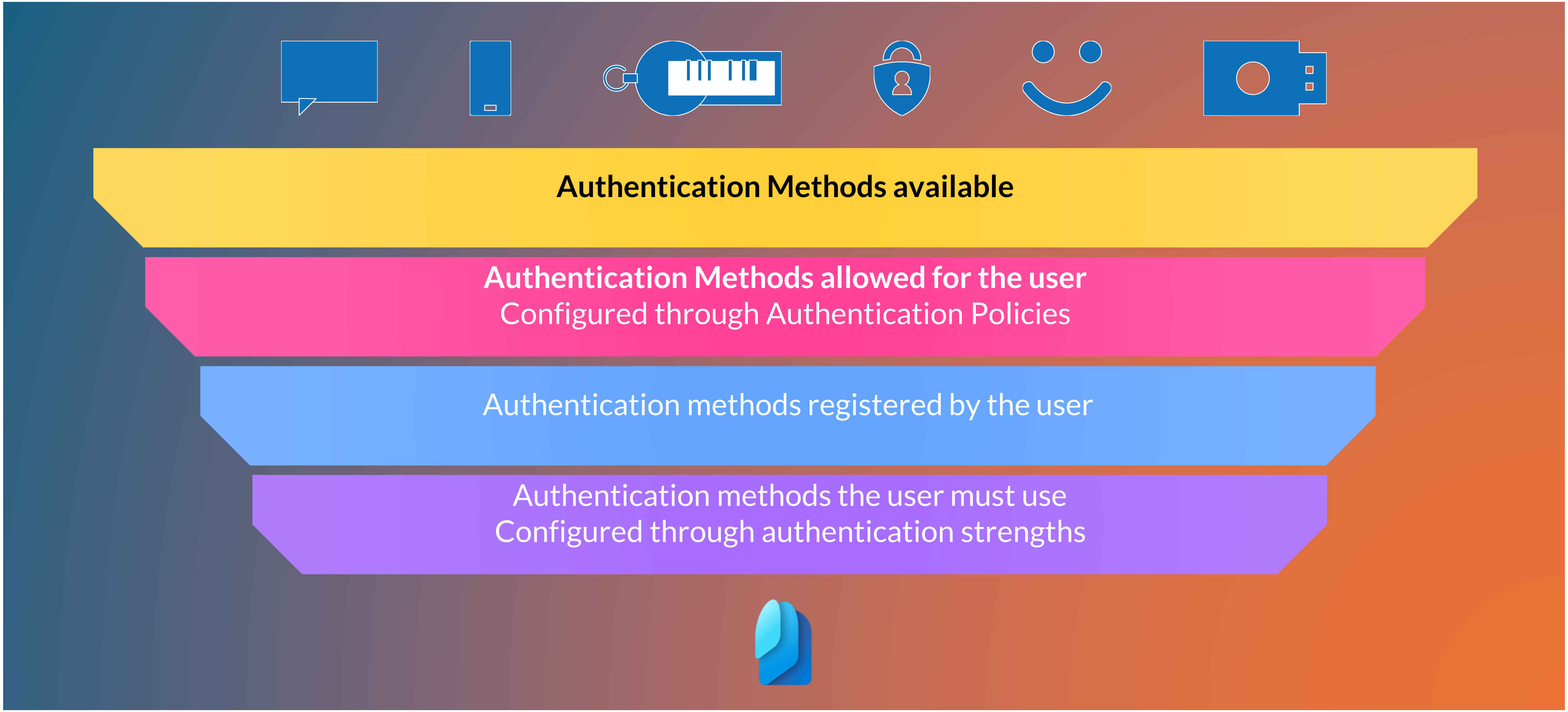
To sign in to "login.microsoft.com", choose a passkey.

This request comes from the app "msedge.exe" by "Microsoft Corporation".

fabian.bader@glueckkanja.com



Auth Funnel - Thanks @merill

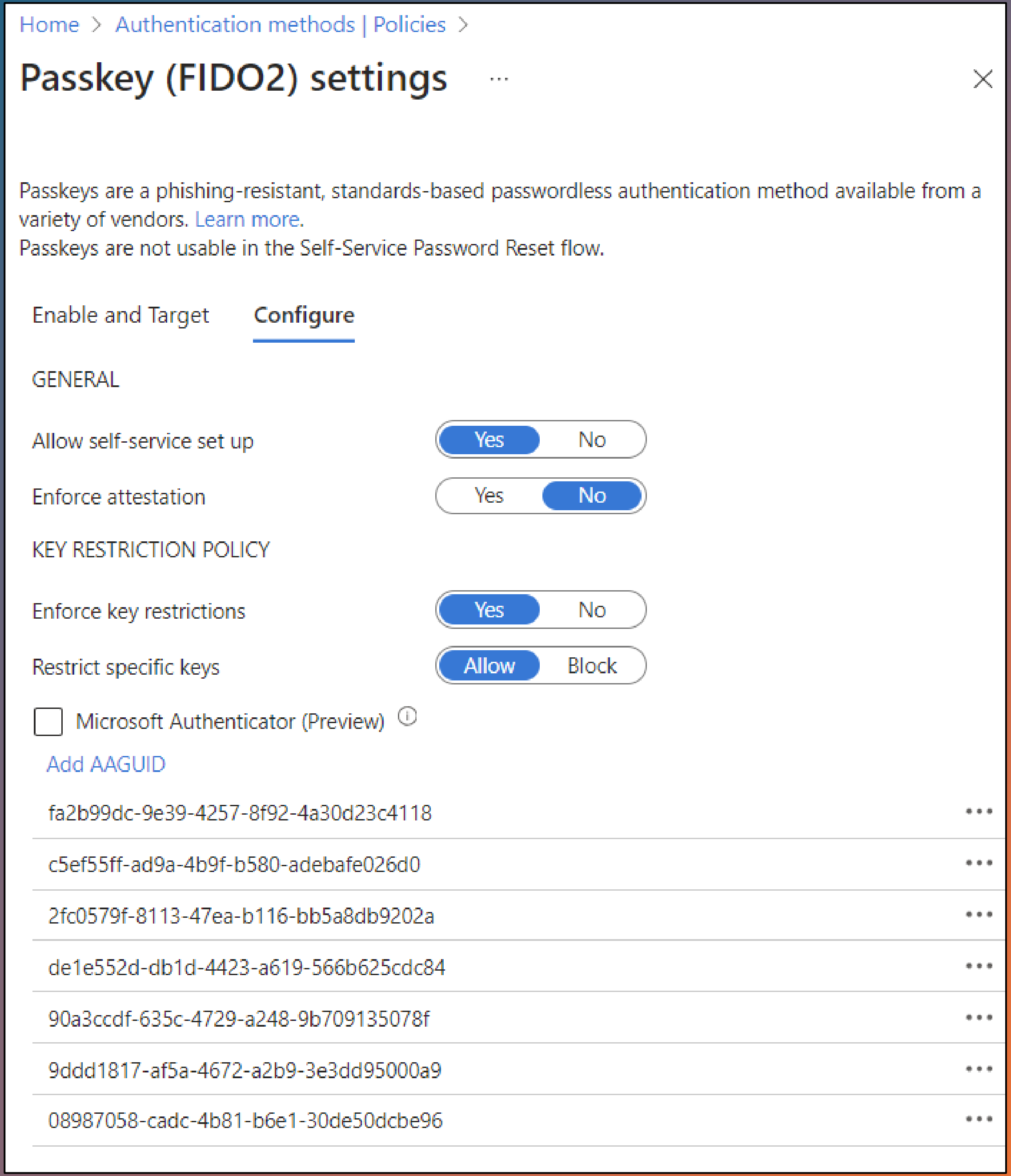


Authentication Methods available

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



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 (Preview)

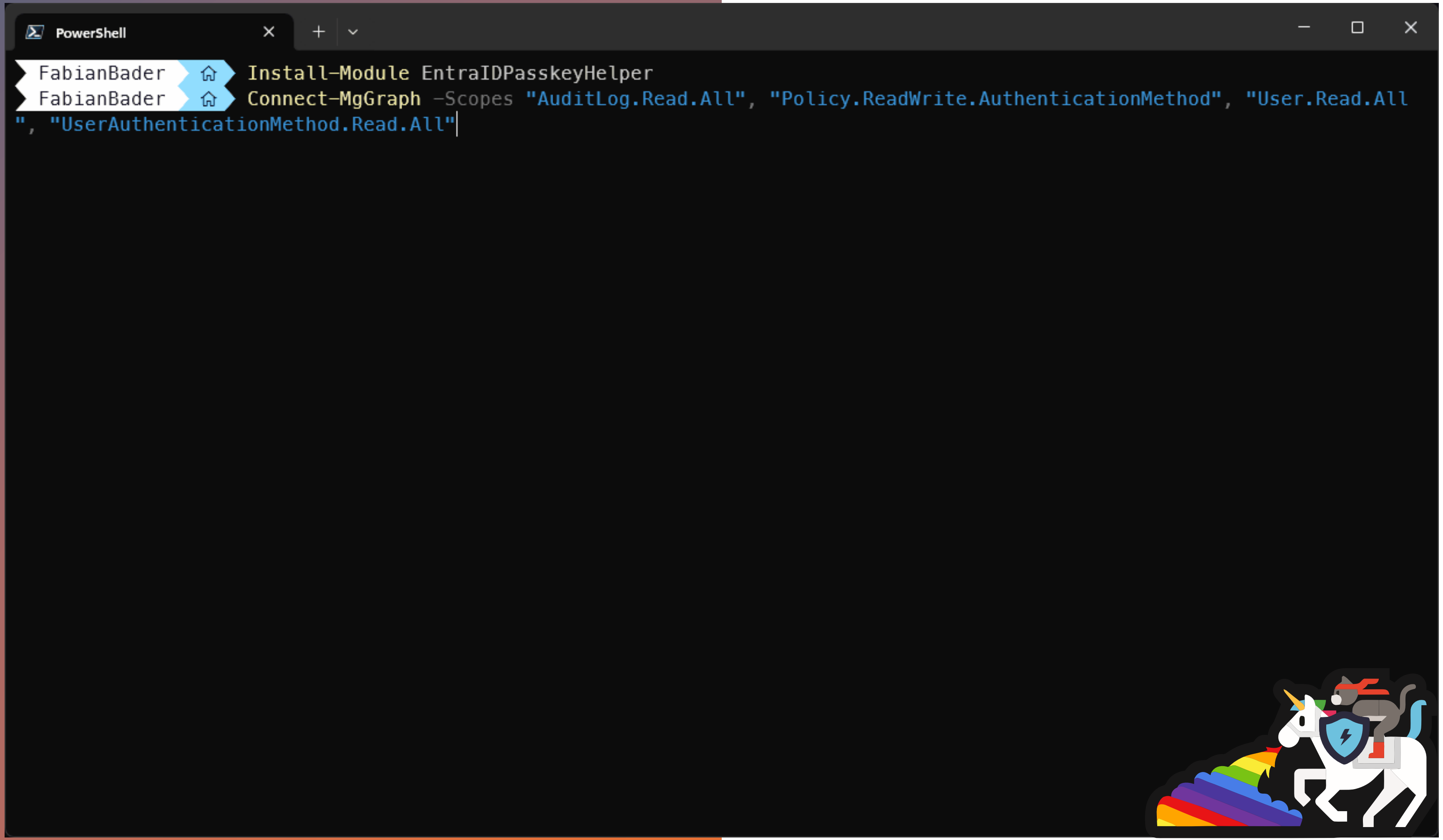
Add AAGUID

fa2b99dc-9e39-4257-8f92-4a30d23c4118
c5ef55ff-ad9a-4b9f-b580-adebafe026d0
2fc0579f-8113-47ea-b116-bb5a8db9202a
de1e552d-db1d-4423-a619-566b625cdc84
90a3ccdf-635c-4729-a248-9b709135078f
9ddd1817-af5a-4672-a2b9-3e3dd95000a9
08987058-cadc-4b81-b6e1-30de50dcbe96

Authentication Methods allowed for the user
Configured through Authentication Policies

Define which Passkeys can be registered by your users

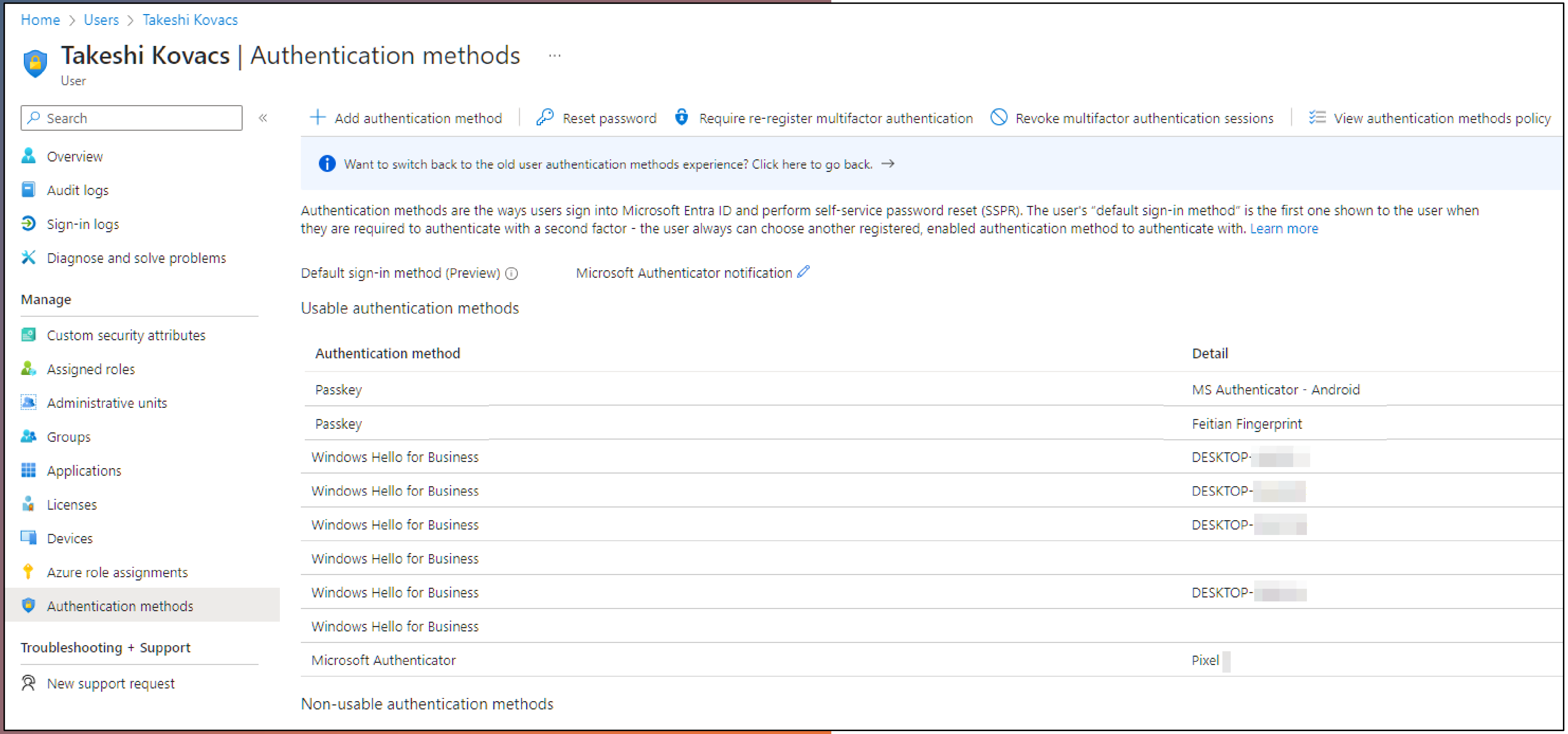
👌 Quick Tipp



```
FabianBader ⌂ Install-Module EntraIDPasskeyHelper
FabianBader ⌂ Connect-MgGraph -Scopes "AuditLog.Read.All", "Policy.ReadWrite.AuthenticationMethod", "User.Read.All
", "UserAuthenticationMethod.Read.All"
```

PSGallery Version v1.0.3 PSGallery Downloads 3.1k

Authentication methods registered by the user



Home > Users > Takeshi Kovacs

Takeshi Kovacs | Authentication methods ···

User

Search
«
Overview
Audit logs
Sign-in logs
Diagnose and solve problems
Manage
Custom security attributes
Assigned roles
Administrative units
Groups
Applications
Licenses
Devices
Azure role assignments
Authentication methods
Troubleshooting + Support
New support request
+ Add authentication method
Reset password
Require re-register multifactor authentication
Revoke multifactor authentication sessions
View authentication methods policy

Want to switch back to the old user authentication methods experience? Click here to go back. →

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

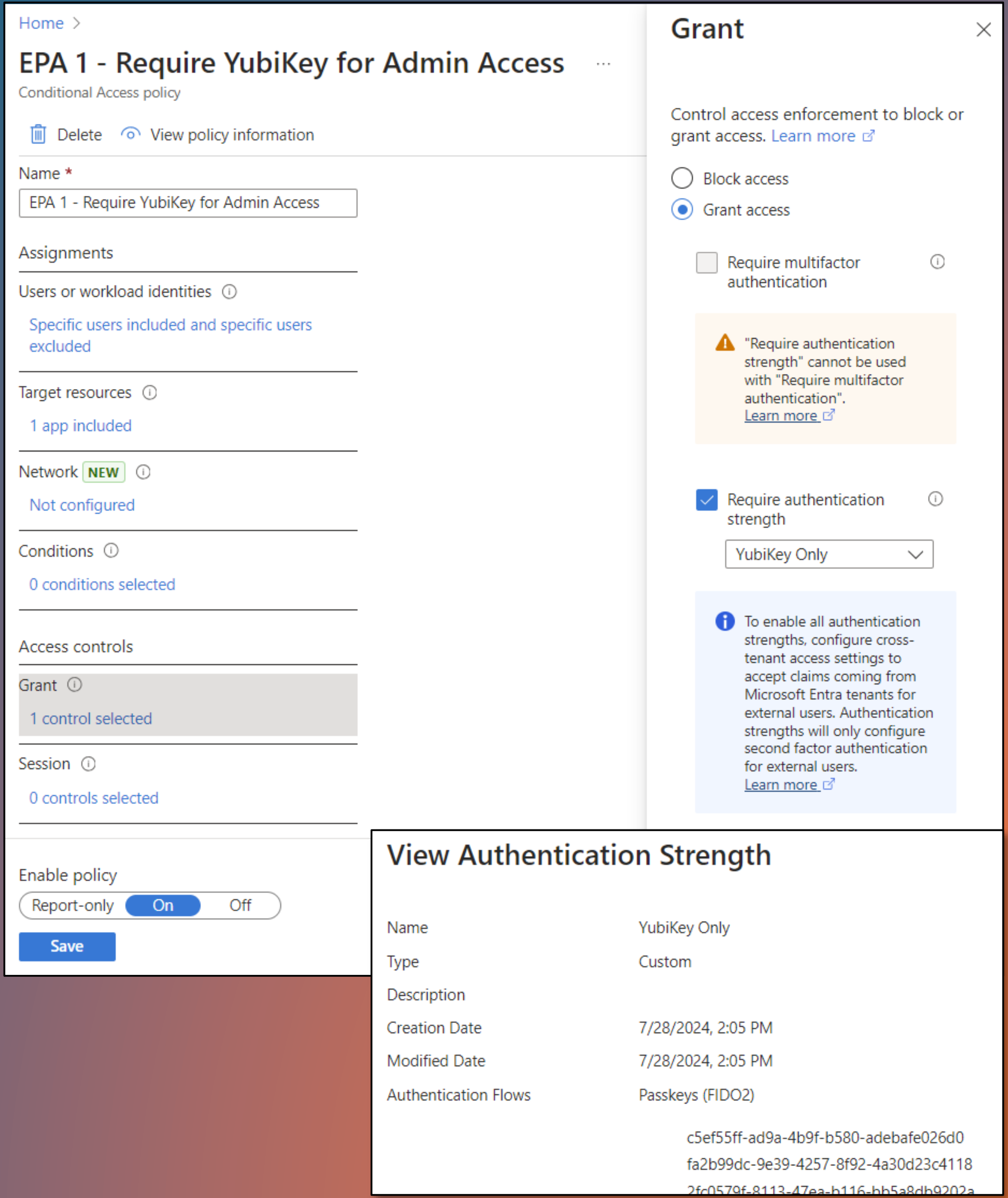
Authentication method	Detail
Passkey	MS Authenticator - Android
Passkey	Feitian Fingerprint
Windows Hello for Business	DESKTOP-[redacted]
Windows Hello for Business	DESKTOP-[redacted]
Windows Hello for Business	DESKTOP-[redacted]
Windows Hello for Business	
Windows Hello for Business	DESKTOP-[redacted]
Windows Hello for Business	
Microsoft Authenticator	Pixel [redacted]

Non-usable authentication methods

Define which Passkeys can be used in specific situations

Authentication methods the user must use

Configured through authentication strengths



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 ⓘ

Specific users included and specific users excluded

Target resources ⓘ

1 app included

Network NEW ⓘ

Not configured

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ

1 control selected

Session ⓘ

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 ⓘ

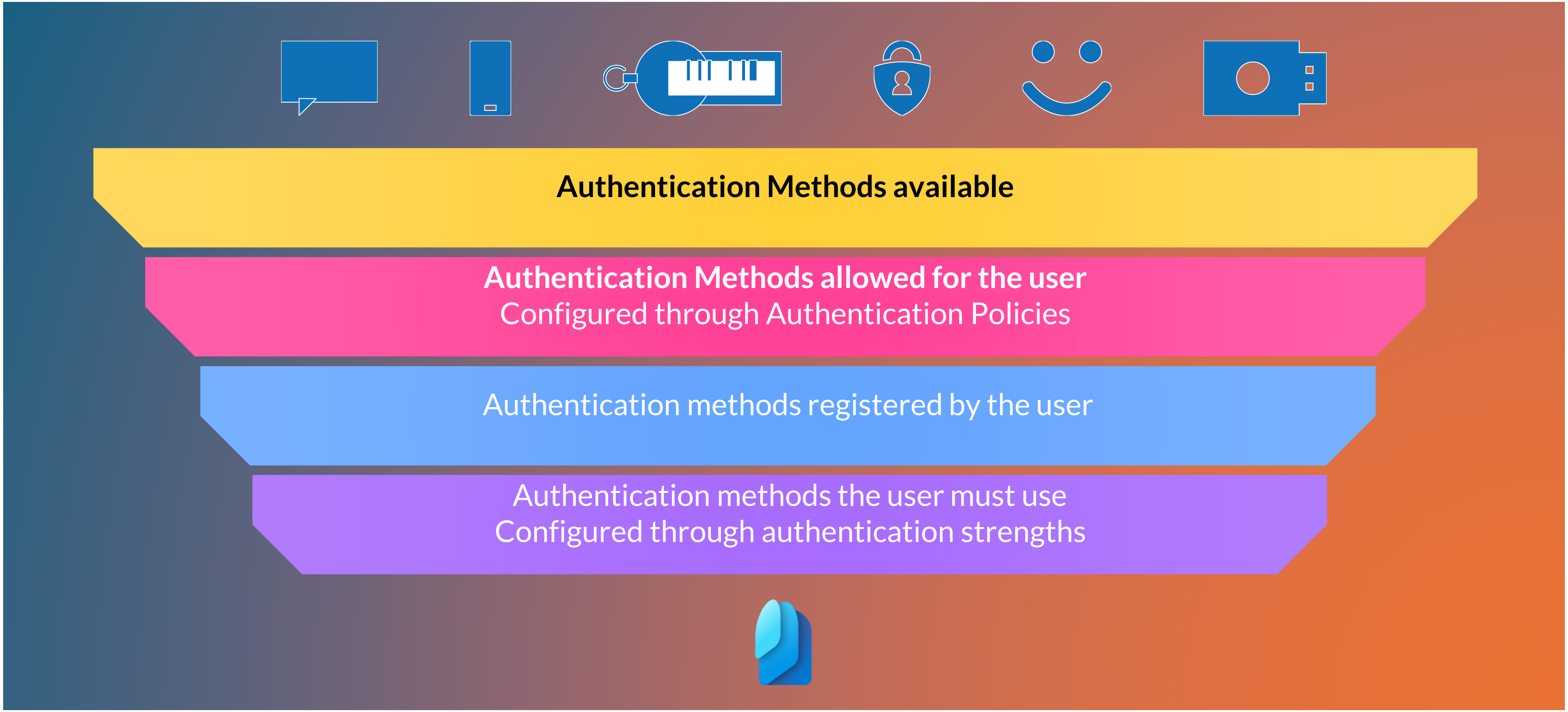
YubiKey Only

To enable all authentication strengths, configure cross-tenant access settings to accept claims coming from Microsoft Entra tenants for external users. Authentication strengths will only configure second factor authentication for external users. Learn more

View Authentication Strength

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)
	c5ef55ff-ad9a-4b9f-b580-adebafe026d0 fa2b99dc-9e39-4257-8f92-4a30d23c4118 2fc0579f-8113-47ea-b116-bb5a8db9202a

Auth Funnel - Thanks @merill



Authentication Methods available

Authentication Methods allowed for the user
Configured through Authentication Policies

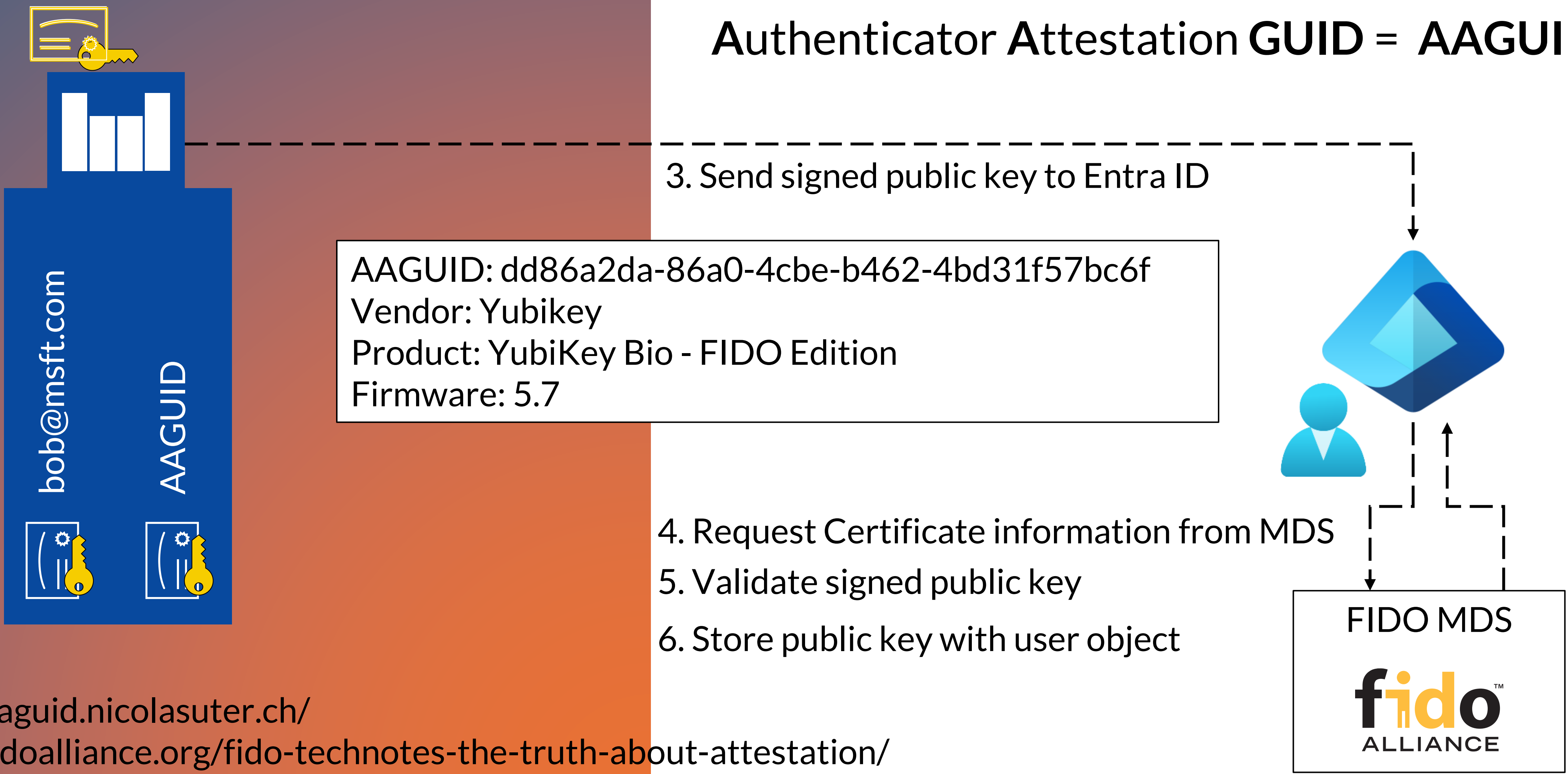
Authentication methods registered by the user

Authentication methods the user must use
Configured through authentication strengths

Attestion? 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/

What can we do with Passkeys?

Registration

Same Device

Cross Device

Authentication

Same Device

Cross Device

CLOUD IDENTITY SUMMIT '24

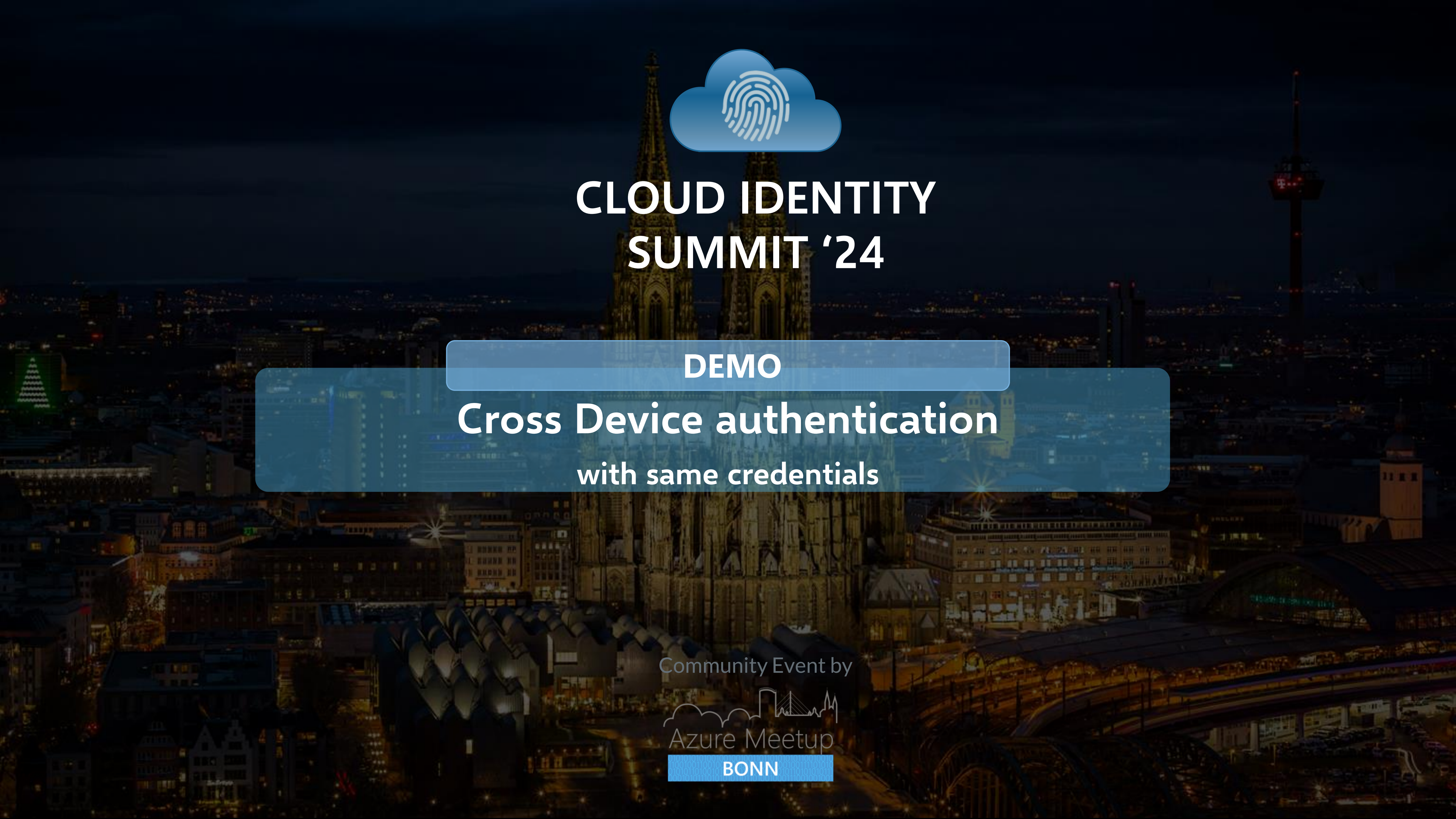
DEMO

Same device registration

Community Event by

Azure Meetup

BONN



CLOUD IDENTITY SUMMIT ‘24

DEMO

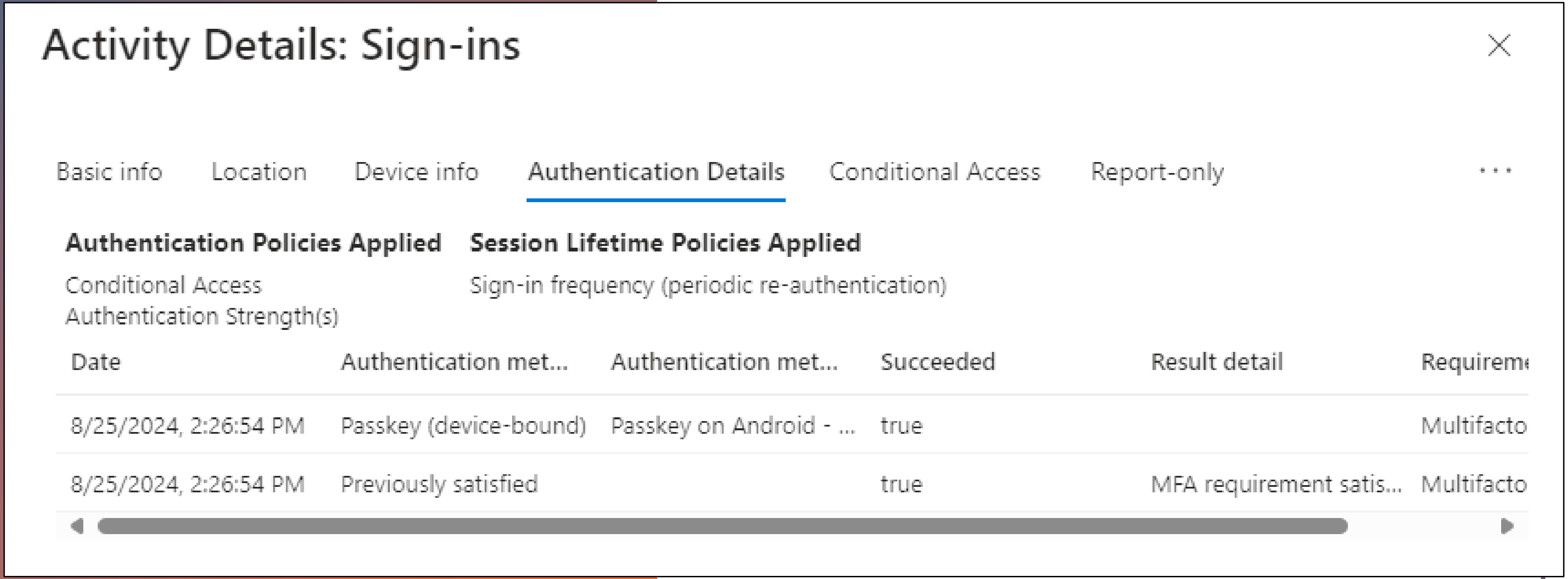
Cross Device authentication

with same credentials

Community Event by

Azure Meetup
BONN

Sign-in logs



Activity Details: Sign-ins

Authentication Policies Applied

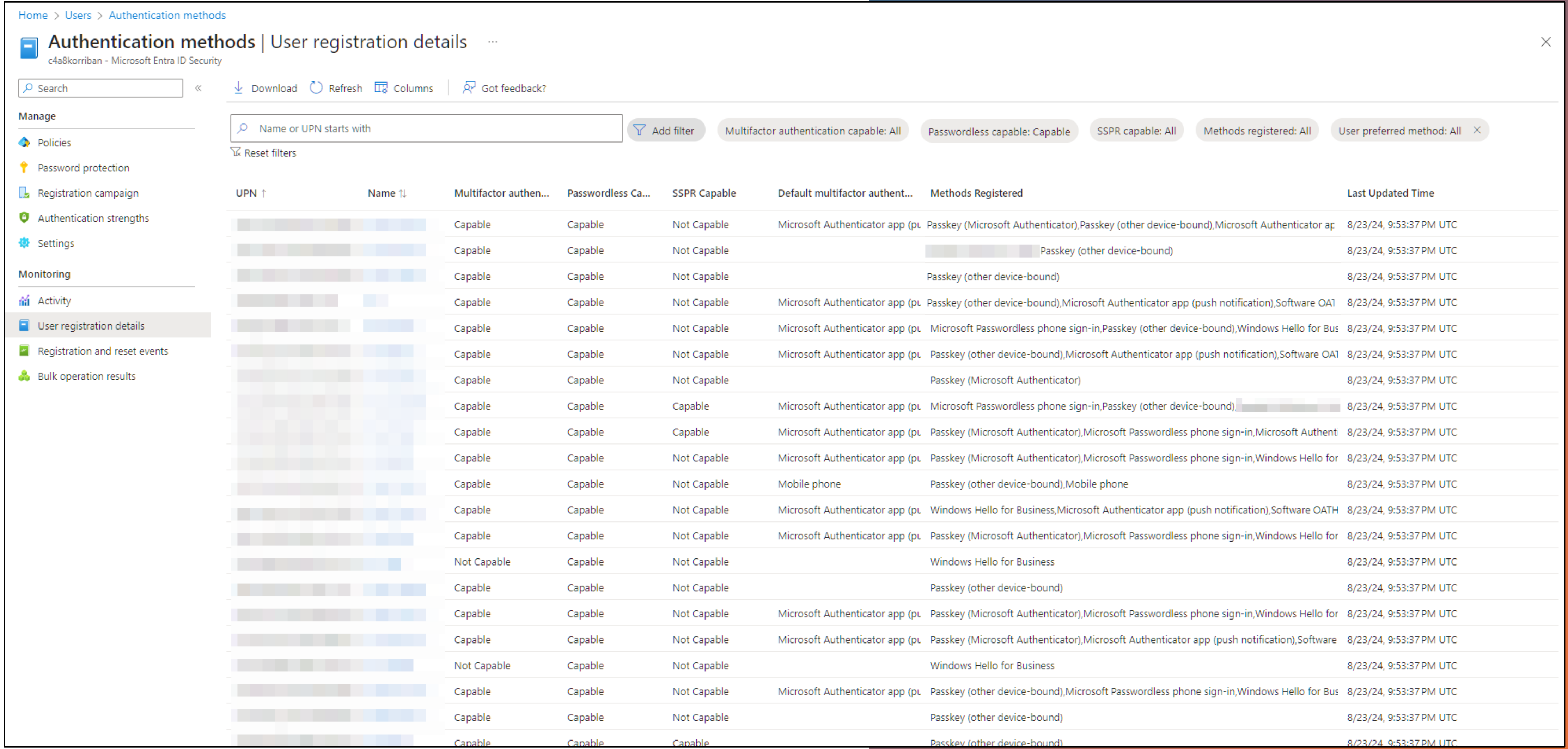
Conditional Access
Authentication Strength(s)

Session Lifetime Policies Applied

Sign-in frequency (periodic re-authentication)

Date	Authentication met...	Authentication met...	Succeeded	Result detail	Requireme
8/25/2024, 2:26:54 PM	Passkey (device-bound)	Passkey on Android - ...	true		Multifacto
8/25/2024, 2:26:54 PM	Previously satisfied		true	MFA requirement satis...	Multifacto

User registration details



Authentication methods | User registration details

c4a8korriban - Microsoft Entra ID Security

Multifactor authentication capable: All

Passwordless capable: Capable

SSPR capable: All

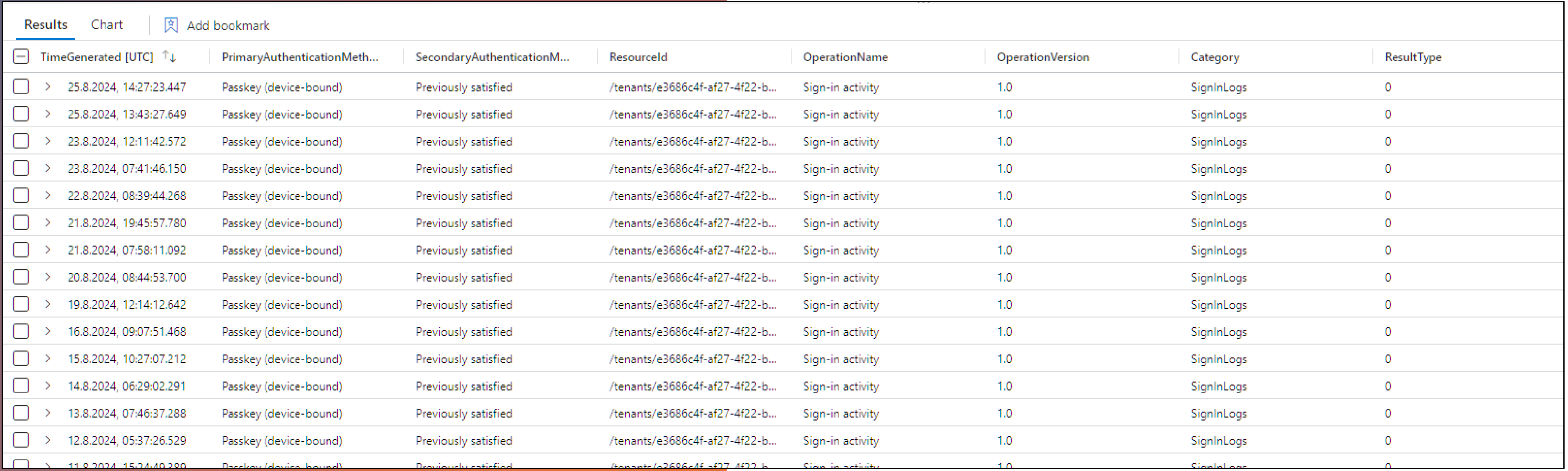
Methods registered: All

User preferred method: All

UPN ↑	Name ↑↓	Multifactor authen...	Passwordless Ca...	SSPR Capable	Default multifactor authent...	Methods Registered	Last Updated Time
[redacted]	[redacted]	Capable	Capable	Not Capable	Microsoft Authenticator app (pu	Passkey (Microsoft Authenticator),Passkey (other device-bound),Microsoft Authenticator ap	8/23/24, 9:53:37 PM UTC
[redacted]	[redacted]	Capable	Capable	Not Capable		[redacted] Passkey (other device-bound)	8/23/24, 9:53:37 PM UTC
[redacted]	[redacted]	Capable	Capable	Not Capable		Passkey (other device-bound)	8/23/24, 9:53:37 PM UTC
[redacted]	[redacted]	Capable	Capable	Not Capable	Microsoft Authenticator app (pu	Passkey (other device-bound),Microsoft Authenticator app (push notification),Software OAT	8/23/24, 9:53:37 PM UTC
[redacted]	[redacted]	Capable	Capable	Not Capable	Microsoft Authenticator app (pu	Microsoft Passwordless phone sign-in,Passkey (other device-bound),Windows Hello for Bus	8/23/24, 9:53:37 PM UTC
[redacted]	[redacted]	Capable	Capable	Not Capable	Microsoft Authenticator app (pu	Passkey (other device-bound),Microsoft Authenticator app (push notification),Software OAT	8/23/24, 9:53:37 PM UTC
[redacted]	[redacted]	Capable	Capable	Not Capable		Passkey (Microsoft Authenticator)	8/23/24, 9:53:37 PM UTC
[redacted]	[redacted]	Capable	Capable	Capable	Microsoft Authenticator app (pu	Microsoft Passwordless phone sign-in,Passkey (other device-bound), [redacted]	8/23/24, 9:53:37 PM UTC
[redacted]	[redacted]	Capable	Capable	Capable	Microsoft Authenticator app (pu	Passkey (Microsoft Authenticator),Microsoft Passwordless phone sign-in,Microsoft Authent	8/23/24, 9:53:37 PM UTC
[redacted]	[redacted]	Capable	Capable	Not Capable	Microsoft Authenticator app (pu	Passkey (Microsoft Authenticator),Microsoft Passwordless phone sign-in,Windows Hello for	8/23/24, 9:53:37 PM UTC
[redacted]	[redacted]	Capable	Capable	Not Capable	Mobile phone	Passkey (other device-bound),Mobile phone	8/23/24, 9:53:37 PM UTC
[redacted]	[redacted]	Capable	Capable	Not Capable	Microsoft Authenticator app (pu	Windows Hello for Business,Microsoft Authenticator app (push notification),Software OATH	8/23/24, 9:53:37 PM UTC
[redacted]	[redacted]	Capable	Capable	Not Capable	Microsoft Authenticator app (pu	Passkey (Microsoft Authenticator),Microsoft Passwordless phone sign-in,Windows Hello for	8/23/24, 9:53:37 PM UTC
[redacted]	[redacted]	Not Capable	Capable	Not Capable		Windows Hello for Business	8/23/24, 9:53:37 PM UTC
[redacted]	[redacted]	Capable	Capable	Not Capable		Passkey (other device-bound)	8/23/24, 9:53:37 PM UTC
[redacted]	[redacted]	Capable	Capable	Not Capable	Microsoft Authenticator app (pu	Passkey (Microsoft Authenticator),Microsoft Passwordless phone sign-in,Windows Hello for	8/23/24, 9:53:37 PM UTC
[redacted]	[redacted]	Capable	Capable	Not Capable	Microsoft Authenticator app (pu	Passkey (Microsoft Authenticator),Microsoft Authenticator app (push notification),Software	8/23/24, 9:53:37 PM UTC
[redacted]	[redacted]	Not Capable	Capable	Not Capable		Windows Hello for Business	8/23/24, 9:53:37 PM UTC
[redacted]	[redacted]	Capable	Capable	Not Capable	Microsoft Authenticator app (pu	Passkey (other device-bound),Microsoft Passwordless phone sign-in,Windows Hello for Bus	8/23/24, 9:53:37 PM UTC
[redacted]	[redacted]	Capable	Capable	Not Capable		Passkey (other device-bound)	8/23/24, 9:53:37 PM UTC
[redacted]	[redacted]	Capable	Capable	Capable		Passkey (other device-bound)	8/23/24, 9:53:37 PM UTC

Log Analytics (KQL)

```
SigninLogs
| where TimeGenerated > ago(90d)
| extend PrimaryAuthenticationMethod = tostring(parse_json(AuthenticationDetails)[0].authenticationMethod)
| extend SecondaryAuthenticationMethod = tostring(parse_json(AuthenticationDetails)[1].authenticationMethod)
| where PrimaryAuthenticationMethod has "Passkey" or  SecondaryAuthenticationMethod has "Passkey"
```



	TimeGenerated [UTC] ↑↓	PrimaryAuthenticationMeth...	SecondaryAuthenticationM...	ResourceId	OperationName	OperationVersion	Category	ResultType
□ ›	25.8.2024, 14:27:23.447	Passkey (device-bound)	Previously satisfied	/tenants/e3686c4f-af27-4f22-b...	Sign-in activity	1.0	SignInLogs	0
□ ›	25.8.2024, 13:43:27.649	Passkey (device-bound)	Previously satisfied	/tenants/e3686c4f-af27-4f22-b...	Sign-in activity	1.0	SignInLogs	0
□ ›	23.8.2024, 12:11:42.572	Passkey (device-bound)	Previously satisfied	/tenants/e3686c4f-af27-4f22-b...	Sign-in activity	1.0	SignInLogs	0
□ ›	23.8.2024, 07:41:46.150	Passkey (device-bound)	Previously satisfied	/tenants/e3686c4f-af27-4f22-b...	Sign-in activity	1.0	SignInLogs	0
□ ›	22.8.2024, 08:39:44.268	Passkey (device-bound)	Previously satisfied	/tenants/e3686c4f-af27-4f22-b...	Sign-in activity	1.0	SignInLogs	0
□ ›	21.8.2024, 19:45:57.780	Passkey (device-bound)	Previously satisfied	/tenants/e3686c4f-af27-4f22-b...	Sign-in activity	1.0	SignInLogs	0
□ ›	21.8.2024, 07:58:11.092	Passkey (device-bound)	Previously satisfied	/tenants/e3686c4f-af27-4f22-b...	Sign-in activity	1.0	SignInLogs	0
□ ›	20.8.2024, 08:44:53.700	Passkey (device-bound)	Previously satisfied	/tenants/e3686c4f-af27-4f22-b...	Sign-in activity	1.0	SignInLogs	0
□ ›	19.8.2024, 12:14:12.642	Passkey (device-bound)	Previously satisfied	/tenants/e3686c4f-af27-4f22-b...	Sign-in activity	1.0	SignInLogs	0
□ ›	16.8.2024, 09:07:51.468	Passkey (device-bound)	Previously satisfied	/tenants/e3686c4f-af27-4f22-b...	Sign-in activity	1.0	SignInLogs	0
□ ›	15.8.2024, 10:27:07.212	Passkey (device-bound)	Previously satisfied	/tenants/e3686c4f-af27-4f22-b...	Sign-in activity	1.0	SignInLogs	0
□ ›	14.8.2024, 06:29:02.291	Passkey (device-bound)	Previously satisfied	/tenants/e3686c4f-af27-4f22-b...	Sign-in activity	1.0	SignInLogs	0
□ ›	13.8.2024, 07:46:37.288	Passkey (device-bound)	Previously satisfied	/tenants/e3686c4f-af27-4f22-b...	Sign-in activity	1.0	SignInLogs	0
□ ›	12.8.2024, 05:37:26.529	Passkey (device-bound)	Previously satisfied	/tenants/e3686c4f-af27-4f22-b...	Sign-in activity	1.0	SignInLogs	0
□ ›	11.8.2024, 15:24:49.380	Passkey (device-bound)	Previously satisfied	/tenants/e3686c4f-af27-4f22-b...	Sign-in activity	1.0	SignInLogs	0

Our best practices and tips

- ☑ Use TAP and same device registration for initial onboarding
- ☑ On Windows devices use WHfB & Cloud Kerberos Trust
- ☑ Enable attestation (after GA)
- ☑ Allow phone sign-in on Android until passkey support for apps is supported
- ☑ Restrict Security Info Registration via Conditional Access
- ☑ Enforce phishing resistant using Authentication Strength to prevent downgrade AiTM attacks
- ☑ No synced passkeys for privileged users
- ☑ Every passkey is better than a password even with MFA

CLOUD IDENTITY SUMMIT ‘24

Thanks to our sponsors

Gold Sponsors

adesso

e·on

glueck kanja

Microsoft

TEAL
ALWAYS CHALLENGING IT

Bronze Sponsors

MSC
Cyber Guard GmbH

T2KEN
swiss made software

CLOUD IDENTITY SUMMIT '24

Ask Me Anything (AMA)

Roundtable discussion and Q&A
on experiences from the field and current trends!

Meet the speakers and exchange
with members of the community!

4:40 PM @5th Floor

Community Event by

Azure Meetup
BONN

Bronze
Sponsors

CLOUD IDENTITY SUMMIT ‘24

Your Feedback is Important!

https://www.identitysummit.cloud/feedback/

Community Event by

Azure Meetup
BONN