

Ist MFA genug? Was ist Passwordless?

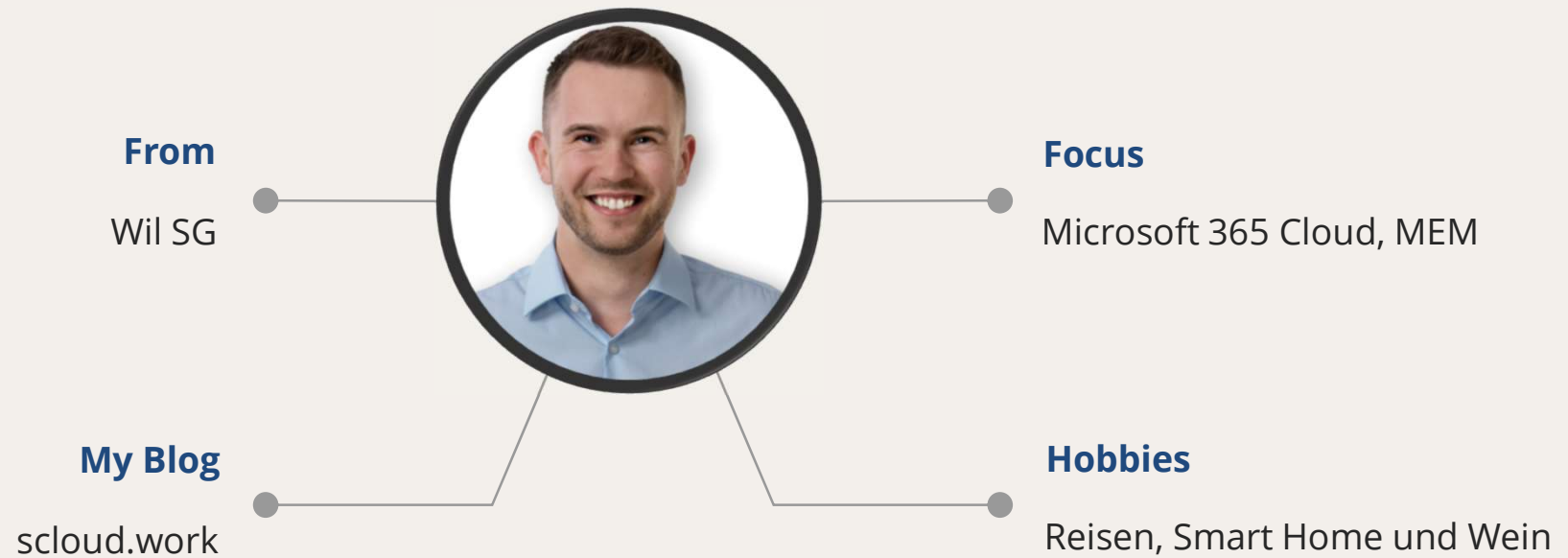
Florian Salzmann

26. Januar 2022

Themen









- Authentifizierungs Methoden
- MFA / Password-less / TAP
- Authentication Strength
- User Onboarding
- Demos

Florian



Ist MFA = MFA?

Authentifizierungs Methoden

Bad: Password	Good: Password and...	Better: Password and...	Best: Passwordless
123456	 SMS	 Authenticator (Push Notifications)	 Authenticator (Phone Sign-in)
qwerty			 Window Hello
password	 Voice	 Software Tokens OTP	 FIDO2 security key
iloveyou			 Certificates
Password1		 Hardware Tokens OTP (Preview)	

Quelle: <https://learn.microsoft.com/de-de/azure/active-directory/authentication/concept-authentication-methods>

MFA Methoden und Risiken

Risk of account takeovers



Source: <https://www.yubico.com/solutions/multi-factor-authentication/>

- SMS Phishing
- Abfangen von E-Mails
- MFA Fatigue
 - Benutzer drücken «einfach OK»

MFA Prompt schützen

Number matching

The image is a screenshot of a mobile device screen displaying a Microsoft Authenticator notification and a sign-in prompt. The notification, titled 'Note', is highlighted with a purple background and contains the following text: 'Number matching is a key security upgrade to traditional second factor notifications in Microsoft Authenticator. We will remove the admin controls and enforce the number match experience tenant-wide for all users starting February 27, 2023.' The date 'February 27, 2023' is enclosed in a red rectangular box. Below the notification, the sign-in screen is visible, showing a background image of a field. The sign-in screen has two main sections. The left section, titled 'Approve sign in', displays the number '83' and instructs the user to 'Tap the number you see below in your Microsoft Authenticator app to sign in.' with a link 'Use your password instead'. The right section, titled 'Are you trying to sign in?', shows the user's name 'Adatum Corporation' and email 'KimA@adatumcorp.com'. It prompts the user to 'Enter the number shown to sign in.' with a text input field labeled 'Enter number'. At the bottom of this section are two buttons: 'No, it's not me' in red and 'Yes' in grey.

Note

Number matching is a key security upgrade to traditional second factor notifications in Microsoft Authenticator. We will remove the admin controls and enforce the number match experience tenant-wide for all users starting February 27, 2023.

We highly recommend enabling number matching in the near term for improved sign-in security.

Approve sign in

Tap the number you see below in your Microsoft Authenticator app to sign in.

83

[Use your password instead](#)

Are you trying to sign in?

Adatum Corporation
KimA@adatumcorp.com

Enter the number shown to sign in.

Enter number

No, it's not me Yes

Password-less Optionen



Windows Hello for Business



Microsoft Authenticator App



FIDO2 Security Keys

Conditional Access

Authentication Strength

- Definieren, welcher zweite Faktor für einen Zugriff genutzt wird
- Schwache/Ungewünschte Methoden unterbinden
- Höheren Schutz für spezifische Applikationen anfordern

Verfügbare Abstufungen

- MFA (alle)
- Passwordless (FIDO2, WHfB, Zertifikat, MS Authenticator)
- Phishing-resistant (FIDO2, WHfB, Zertifikat)
- Benutzerdefinierte Definitionen möglich

User Onboarding

Temporary Access Pass + FIDO2 Key

- Passwort ist dem Benutzer nie bekannt
- TAP ist nur für eine begrenzte Zeit gültig
 - auch einmal Nutzung möglich (nicht empfohlen)

Home

Azure Active Directory

Overview

Users

All users

Deleted users

User settings

Groups

Devices

Applications

Protect & secure

Conditional Access

Identity Protection

Authentication methods

Password reset

Learn & support

Home > Users > Michael Scott [Test]

Michael Scott [Test] | Authentication methods

User

Search

+ Add authentication method

Want to switch back to the old authentication method?

Authentication methods are the way users prove their identity to applications and services.

Usable authentication methods

Authentication method

Temporary Access Pass

FIDO2 security key

Overview

Audit logs

Sign-in logs

Diagnose and solve problems

Manage

Custom security attributes (preview)

Assigned roles

Administrative units

Groups

Applications

Licenses

Devices

Azure role assignments

Authentication methods

Troubleshooting + Support

New support request

Add authentication method

Choose method

Temporary Access Pass

Create a Temporary Access Pass for Michael Scott [Test]. While the pass is valid, the user can use it to sign in and register strong credentials. [Learn more](#)

☒ Delayed start time

Start time

02/01/2023 8:00 PM

(UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

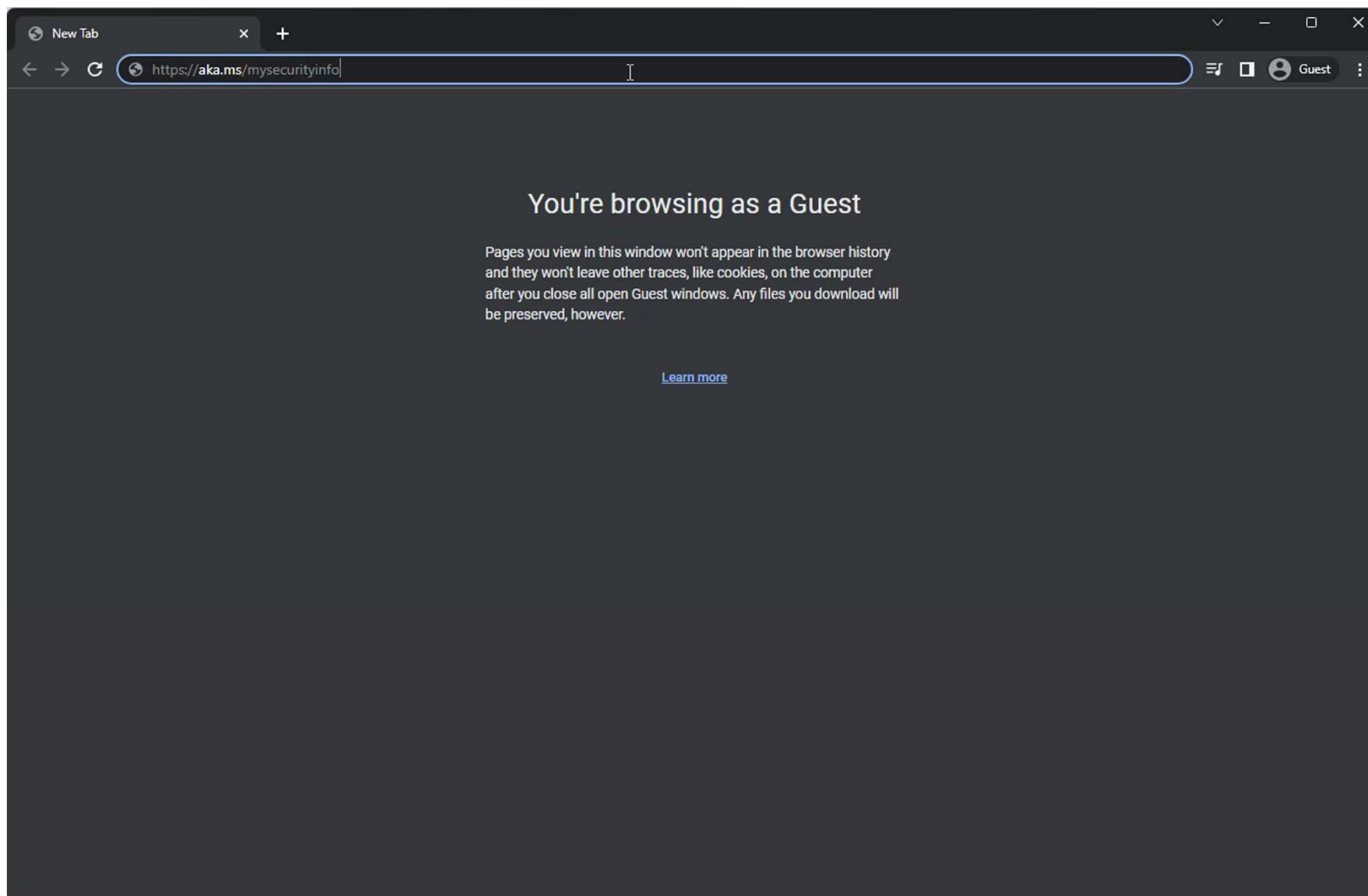
Activation duration

2 hours

One-time use

Yes No

Add



Konfiguration Windows Login

- Custom Profil für die Aktivierung
 - OMA-URI:
./Device/Vendor/MSFT/PassportForWork/SecurityKey/UseSecurityKeyForSignin
 - Data Type: Integer
 - Value: 1

Name *	Turn on FIDO Security Keys for Windows Sign-In
Description	Not configured
OMA-URI *	./Device/Vendor/MSFT/PassportForWork/Secu...
Data type	Integer ▼
Value *	1

DEMO



Benutzer Informationen

- Vorlagen von Microsoft (English):
<https://www.microsoft.com/en-us/download/details.aspx?id=57600>



Fragen?

Enabling your success.