



Modernising Authentication Methods

...like a Boss

NORDIC

– VIRTUAL SUMMIT –

Presented by

- Michael Mardahl
- Cloud architect
- APENTO (Denmark)
- Twitter @michael_mardahl
- MVP Security
- MVP Enterprise Mobility



NORDIC

– VIRTUAL SUMMIT –

(Also) Presented by

- Jan Ketil Skanke
- Principal Cloud architect
- CloudWay (Norway)
- Twitter @JankeSkanke
- MVP Security
- MVP Enterprise Mobility



NORDIC

— VIRTUAL SUMMIT —

Why are we here?

(Literally)

Because...

- We wanna go Passwordless
 - Trust us.
- The new management experience is being enforced January 2024!
 - Get a head start
- We want more control
 - More granularity
 - Single pane of glass

What is this new experience?

Old way

- Policies for SSPR authentication
 - In it's own blade
 - No granularity
 - Very basic
- Policies for MFA authentication
 - In it's own portal
 - No granularity
 - Very basic

New way

- Authentication Method Policies
 - Unified under Azure AD Security
 - All methods in one place
 - Granular controls
 - Group assignments
 - Role based access
 - Manage as code (Graph API)
 - New features added only here
 - Simple migration experience
 - MODERN!

What is this new experience?

Microsoft Azure

Search resources, services, and docs (G+)

Home > iPhase | Security > Security | Authentication methods >

Authentication methods | Policies

Search

Got feedback?

Manage

Policies

Password protection

Registration campaign

Authentication strengths (Preview)

Monitoring

Activity

User registration details

Registration and reset events

Bulk operation results

Use this policy 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](#)

If your tenant doesn't yet use [combined security info registration](#), turn it on now – it's required to use this policy.

Manage migration

In January 2024, the legacy multifactor authentication and self-service password reset policies will be deprecated and you'll manage all authentication methods here in the authentication methods policy. Use this control to manage your migration from the legacy policies to the new unified policy. [Learn more](#)

[Manage migration \(Preview\)](#)

Method	Target	Enabled
FIDO2 security key	All users	Yes
Microsoft Authenticator	All users	Yes
SMS (preview)	All users	Yes
Temporary Access Pass	All users	Yes
Third-party software OATH tokens (preview)		No
Voice call (preview)		No
Email OTP (preview)	All users	Yes
Certificate-based authentication	All users	Yes

☐ Pre-migration:

Use policy for authentication only, respect legacy policies.

☐ Migration In Progress:

Use policy for authentication and SSPR, respect legacy policies.

☒ Migration Complete:

Use policy for authentication and SSPR, ignore legacy policies.

DEMO – How to migrate

(Let's all pray to the demo gods)

NO!



**I CAN STILL USE
PER USER MFA RIGHT?**

Migration strategy (What did we do?)

- Replicate existing policies
 - All SSPR methods except »security questions«
 - All MFA Legacy methods
- KISS (Keep It Super Simple).
 - Go for status quo
 - Don't bother with »better«
 - Optimize after migration
- Switch to «Migration in progress»
 - Then turn off the old policy controls
- Switch to «Migration complete»
 - Now your passwordless journey begins!

Methods available to users

- ☐ Mobile app notification
- ☐ Mobile app code
- ☒ Email
- ☒ Mobile phone
- ☒ Office phone
- ☐ Security questions

verification options [\(learn more\)](#)

Methods available to users:

- ☐ Call to phone
- ☐ Text message to phone
- ☒ Notification through mobile app
- ☒ Verification code from mobile app or hardware token

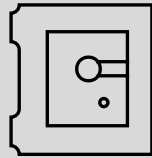
Moving to passwordless

(Now we're getting somewhere!)

PASSWORDS ARE GREAT!!



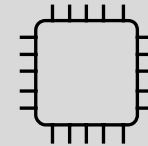
Passwordless is great!



Promise to remove attack
vector of standalone
passwords



A better user experience
than Passwords + MFA
(Multi-Factor
Authentication)

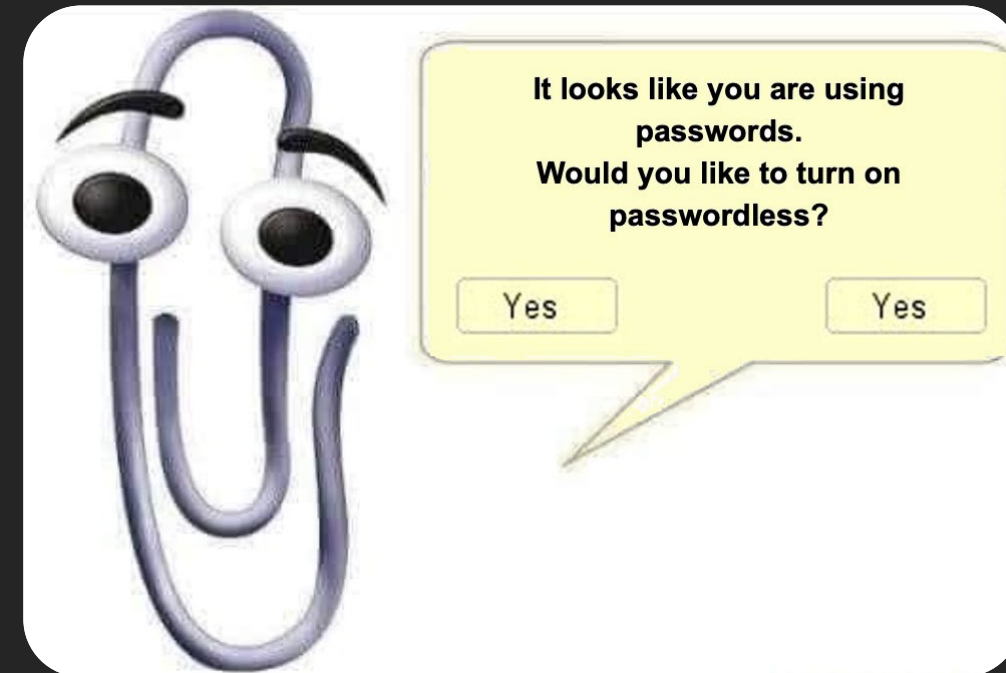


Strong, device-based
authentication methods

- Windows Hello for Business
- Microsoft Authenticator – Passwordless phone sign-in
- FIDO2 security keys (platform and external)

Passwordless #FTW

- Conditional Access is still king
- Windows Hello for Business is a quick win for Windows devices
- Authenticator is really awesome
 - Number matching
 - Get users used to typing in a number from the screen into the app
- FIDO2
- Authentication Strengths
 - Start ramping up requirements
 - Start with highly privileged systems
 - Azure portal, HR, Payroll etc.
- Awareness
 - Tell the users about passwordless. Get them hooked!



A LITTLE BIRDY TOLD ME THAT
NUMBER MATCHING WILL BE ON
FOR EVERYONE LIKE **NOW !!!!!**



DEMO – Authentication Strengths and stuff

(Behold the glory!)

Miscellaranironious!

- Combined registration experience should be turned on.
If for some odd reason you have not been forced into this experience
- Always exclude the «Break the glass» account when testing these new things.
Else you can get locked out!



THANK YOU

For listening and going passwordless!

Feedback form (not phishing we promise ^_^) >

Nordic Virtual Summit 2023 - 4th
edition

