

Strengthening Enterprise Security

Lessons Learned from Deploying Phishing-Resistant Authentication at Scale



About me



Olivier Debonne

Technology Expert @ Savaco

Over 25 years of IT experience

All the way back to the Windows NT 4.0 era

Today my focus is Entra, Microsoft 365 and Azure

Has a passion for retro computing



[@olivierdebonne](https://twitter.com/olivierdebonne)



<https://www.linkedin.com/in/olivierdebonne>

So, what's the problem we are facing?

Explaining an Adversary-in-The-Middle (AiTM) or Transparent Proxy attack

Red flags

- URL in the mail is fraudulent
- Number matching map is not accurate



Laptop of an innocent user

Sign-in + MFA

Evilginx(-as-a-service)
proxy



Microsoft Entra

Mailbox

Teams

AVD

VPN



Bad actor



The solution?

Perhaps further educating coworkers?

Trust me bro, it doesn't work (100%)



The solution? Technology can help!

Strengthen your authentication methods

Configure a phishing-resistant authentication method:

- FIDO2 security key
- Passkey in Microsoft Authenticator
- Windows Hello for Business
- Certificate-Based Authentication

And make it the required authentication method!



Authentication methods

According to Microsoft (outdated)

Bad: Password

Good: Password
and...

Better: Password
and...

A bit better:
~~**Best:** Passwordless~~ **Best:** Phishing-resistant

123456

qwerty

password

iloveyou

Password1



SMS



Voice



Authenticator
(Push Notifications)



Software
Tokens OTP



Hardware Tokens OTP
(Preview)



Authenticator
(Phone Sign-in)



Windows
Hello



FIDO2 security key



Certificates



Windows
Hello



FIDO2 security key



Passkeys in
Microsoft
Authenticator

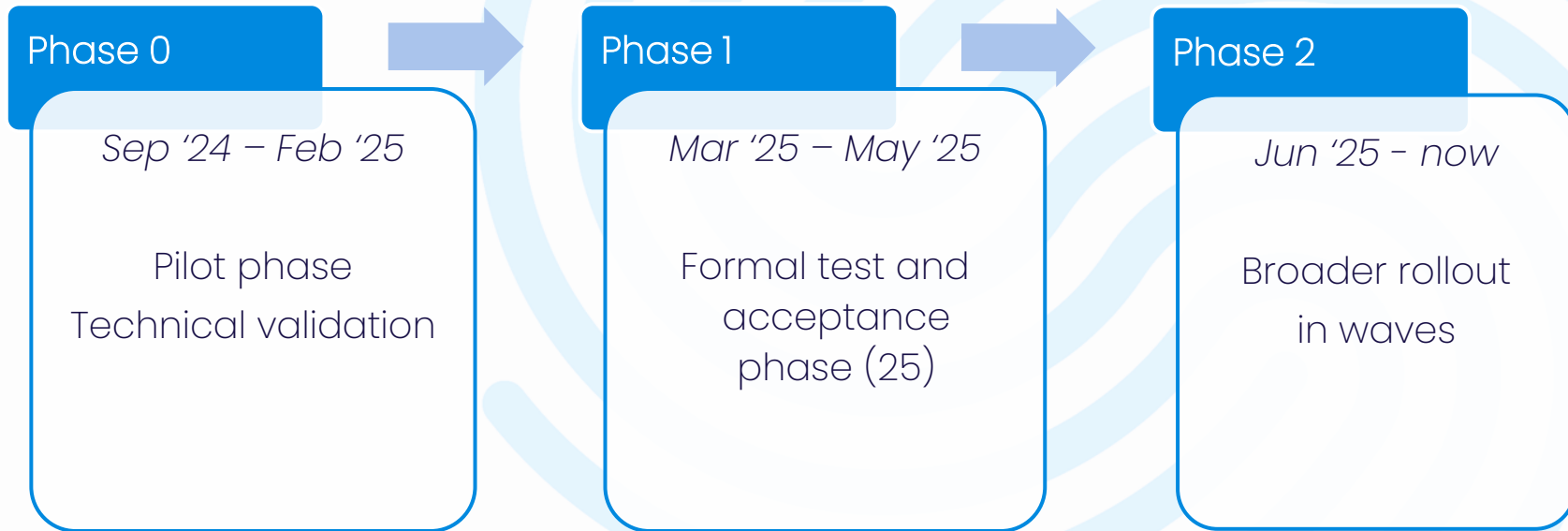


Certificates



Rollout in multiple phases

The project started all the way back in September 2024



Before phase 0: Protect cloud administrator accounts with FIDO2 security keys



Phase 0: technical validation and pilot

Preparations

Are we going to give everyone a FIDO2 security key?

- USB-A or USB-C, with or without NFC, nano form-factor, with biometrics?
- + : very durable, no battery, can be used to sign-in in Windows
- : price, the logistical nightmare to take care of

Or use passkeys in Microsoft Authenticator?

- BYOD policy for mobile devices (MAM)
 - Let's compile a list of all mobile devices (Intune)
 - Which versions of iOS and Android do we have?
 - More than 70% of all mobile devices are compatible (end of 2024)
- + : same functionality/security as a FIDO2 security key, biometrics, free!
- : Personal device, requires Internet connectivity, doesn't work in China



Phase 0: technical validation and pilot

Which route did we choose?



Let's go for passkeys in Microsoft Authenticator

Give everyone without compatible phone a FIDO2 security key (USB-C)



Passkeys in Microsoft Authenticator

Requirements

You need a mobile phone with, at least:

- Android 14
- iOS 17 (in practice iOS 18, for extra **AutoFill** options)

Other requirements (cross-device auth):

- Bluetooth (no pairing needed) on both devices
- Internet connectivity on both devices

Easy to create the passkey from within Microsoft Authenticator

- Go to your account > Create a passkey (at least nowadays)



Enforce the use of passkeys

Require the use of passkeys and Windows Hello for Business

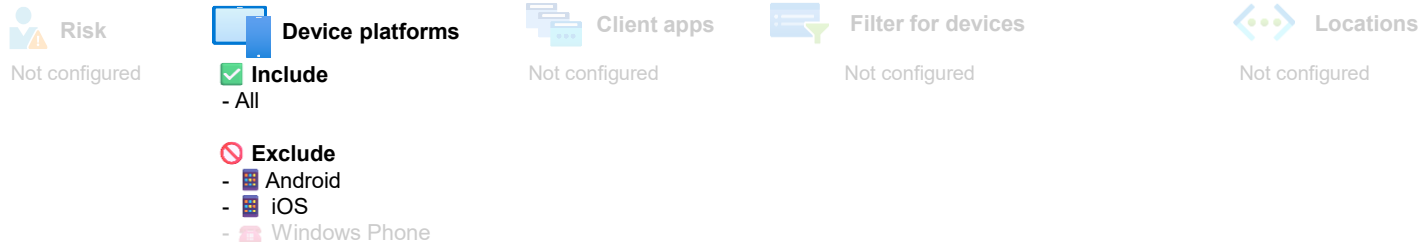
Add an Entra conditional access policy that leverages authentication strengths that requires a phishing-resistant authentication method

View Authentication Strength

Name	MFA with Passkeys and WH4B
Type	Custom
Description	
Creation Date	10/2/2025, 9:56 PM
Modified Date	10/2/2025, 9:56 PM
Authentication Flows	Windows Hello For Business / Platform Credential
	OR
	Passkeys (FIDO2)



CAU051-All: Require phishing-resistant authentication for all users - Desktop



Users

Grant access



All cloud apps

- ✓ **Include:**
Groups
 - M365 - CA - Require phishing-resistant authentication
- ✗ **Exclude:**
Groups
 - M365 - CA - Break-glass admin accounts
 - M365 - CA - Do not enforce phishing-resistant authentication
 - M365 - CA - No Azure MFA required

Grant Controls

- ✓ Multifactor authentication
- ✓ Auth strength: MFA with Passkeys and WH4B
- ✓ Compliant device
- ✓ Hybrid Azure AD joined device
- ✓ Approved client app
- ✓ App protection policy
- ✓ Change password
- ✓ Custom authentication factor
- ✓ Terms of use

- ✓ **Include:**
 - All
- ✗ **Exclude:**
 - Microsoft Rights Management Services

Session Controls

- ✗ App enforced restrictions
- ✗ Conditional Access App Control
App Control Policy
- ✗ Sign-in frequency
Periodic reauthentication
- ✗ Persistent browser session
Always persistent
- ✗ Continuous access evaluation
Strictly enforce location policies
- ✗ Disable resilience defaults
- ✓ Token protection for session



CAU052-All: Require phishing-resistant authentication for all users - Mobile



Risk

Not configured



Device platforms



Include

- Android
- iOS
- Windows Phone



Client apps

Not configured



Filter for devices

Not configured



Locations

Not configured



Users

Grant access



All cloud apps

✓ **Include:**
Groups

- M365 - CA - Require phishing-resistant authentication

✗ **Exclude:**
Groups

- M365 - CA - Break-glass admin accounts
- M365 - CA - Do not enforce phishing-resistant authentication
- M365 - CA - No Azure MFA required

Grant Controls



Multifactor authentication



Auth strength:MFA with Passkeys and TAP



Compliant device



Hybrid Azure AD joined device



Approved client app



App protection policy



Change password



Custom authentication factor



Terms of use

✓ **Include:**
- All

✗ **Exclude:**

- Azure Credential Configuration Endpoint Service
- Windows Azure Active Directory
- Microsoft Rights Management Services

Session Controls



App enforced restrictions



Conditional Access App Control
App Control Policy



Sign-in frequency
Periodic reauthentication



Persistent browser session
Always persistent



Continuous access evaluation
Strictly enforce location policies



Disable resilience defaults



Token protection for session



CAU053-Azure: Allow registration of Passkeys in Microsoft Authenticator



Users

Grant access



Selected cloud apps

- ✓ **Include:**
- Groups**
- M365 - CA - Require phishing-resistant authentication

Grant Controls

- ✓ **Include:**
- Multifactor authentication
- Auth strength: Multifactor authentication
- Compliant device
- Hybrid Azure AD joined device
- Approved client app
- App protection policy
- Change password
- Custom authentication factor
- Terms of use

- ✓ **Include:**
- Azure Credential Configuration Endpoint Service
- Windows Azure Active Directory

Session Controls

- ✓ **Include:**
- App enforced restrictions
- Conditional Access App Control
- App Control Policy
- Sign-in frequency
- Periodic reauthentication
- Persistent browser session
- Always persistent
- Continuous access evaluation
- Strictly enforce location policies
- Disable resilience defaults
- Token protection for session

Phase 1: test and acceptance phase (25-ish)

March 2025 – May 2025

We have a formal test group:

- Selection of 25 personas throughout the organization
- They are familiar with the concept of testing

To validate what we've learned during the pilot (★)

Do all the apps work with phishing-resistant authentication?

During this phase, things can and may break (as long as)

To finetune the policies (if needed)

To finetune the documentation, procedures, instructions



Results of the test and acceptance phase

Did we push through or abandoned the project?

Actually, very positive, 99% of the things work

For the 1%, there are (temporary) workarounds



What if something doesn't work?

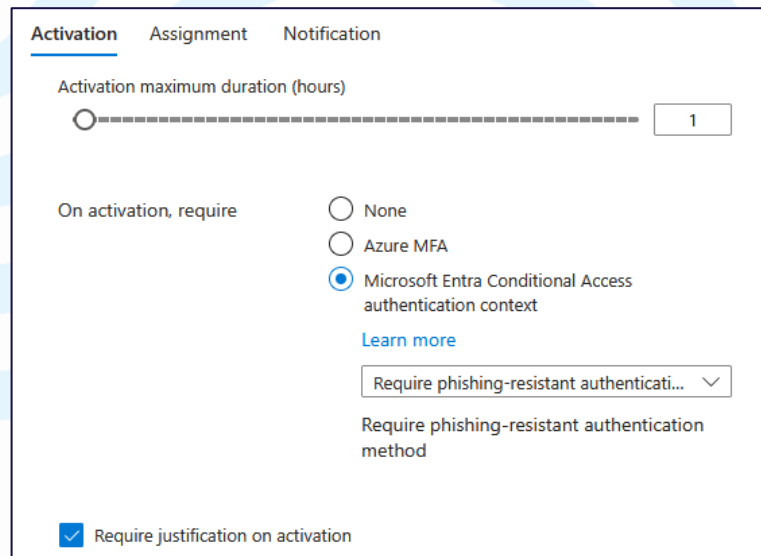
Leverage Entra PIM to temporary bypass phishing-resistant authentication

Users can add themselves to a group to temporarily (max. 1 hour) bypass phishing-resistant authentication

Fallback to regular MFA

Combined use of technologies:

- Entra PIM (Groups)
- Entra Conditional Access
- Authentication Contexts
- Authentication Strength



The screenshot shows the 'Activation' tab of a configuration page. It includes a slider for 'Activation maximum duration (hours)' set to 1. Under 'On activation, require', the 'Microsoft Entra Conditional Access authentication context' option is selected. A dropdown menu shows 'Require phishing-resistant authentication...'. At the bottom, the 'Require justification on activation' checkbox is checked.

Activation Assignment Notification

Activation maximum duration (hours)

1

On activation, require

☐ None

☐ Azure MFA

☒ Microsoft Entra Conditional Access authentication context

[Learn more](#)

Require phishing-resistant authentication... ▾

Require phishing-resistant authentication method

☒ Require justification on activation



Phase 2: broad roll-out

June 2025 - ...

Wave 1 – 100 technical colleagues

T -60 days

Create
additional
awareness

Training

T -30 days

Email with
onboarding
procedure

FAQ

T -14 days

Technical
consultation
days

T -7 days

Friendly
reminder

T -0 days

Enforce
policy

Fix the lazy
folks...



Problems/issues encountered

While onboarding a passkey in Microsoft Authenticator

Issues with certain (Android) phones (next slide)

What? An iPhone 14 still running iOS 16, in 2025?

- Owner ignored the error messages

Sometimes we **had** to use the *alternate registration flow* (scan QR code) for registration

- Buried away under the **Having Trouble?** option
- Then choosing **create your passkey a different way**
- Unfortunately, only possible when attestation is disabled :(

Issues with Bluetooth on some laptops (driver-related)



Problems/issues encountered

Android-specific

Hard to predict behavior on Android

Add Microsoft Authenticator as preferred service

Some Samsung phones are stubborn and want to save the passkey in a Samsung app

Same with some Google Pixel phones

Some phones (Nokia G42, OnePlus 8T) require Android 15

Some phones (Xiaomi POCO X4 Pro 5G) are stuck on Android 13

On some phones it appeared to be fine, but failed to work



And now... onboarding++

This is where the fun begins...

Migration

Give everyone
time to onboard

Enforce with
policies

New users

Lost/stolen device

Generate TAP

Leverage Entra ID Governance to request and
deliver the TAP to the end user

Not SSPR capable (if you still use passwords)

Refer to Jan Bakker's excellent blogposts on these topics



Other problems/issues encountered

Incompatibilities, unexpected behavior, things to keep in mind

Careful with enforcement of attestation

Not compatible with all PowerShell modules to connect to M365

Fat applications running on Windows Server 2019 is no go

Pass-through in a Citrix session

- But not to a subsequent RDP session
- RDP in RDP is no issue

Reauthentication on mobile phone is seamless (at least on iOS)

Some (mobile) apps don't support passkeys (Xurrent)

Credential refresh in Power BI (mobile app)



Various other tidbits to share

What else did we learn over the past 12 months?

You can have multiple FIDO2 security keys connected

FIDO2 security keys with NFC are complex to use

- Where is the NFC reader?
- Connecting a FIDO2 security key using USB-C is fine

So, are we there yet?

- No, there is also something as **Infostealers**
- Robust malware protection remains essential!

What do we do with Windows Hello for Business?



Conclusion

The threat is real

Regular MFA does not suffice anymore

Phishing-resistant authentication is the answer

- Plan for user education
- When using a corporate device, hardly any impact
- Besides all the onboarding issues, it just works (fine)!
- Temporary bypass

The end user experience (mobile/browser) is way better now

Key takeaway
start your journey now with your (cloud) admin accounts



Questions?

