What’s new in implement a Passwordless practice?

How hard can it be!

Workplace Ninja Virtual Edition 2021

V-Platin Sponsor

nwc services
one step ahead

RECAST SOFTWARE

Patch My PC
PATCH MANAGEMENT MADE EASY

glueckkanja gab

Lenovo

Microsoft

V-Gold Sponsor

scopewyse
we are what's next

sepago®

baseVISION
SECURE & MODERN WORKPLACE

Patron Sponsors

SD:>_
SwissDev Jobs

About "Ronny de Jong"

Focus

Microsoft Endpoint Manager

Azure Active Directory & Security

Certifications

Microsoft MVP

From

The Netherlands

Hobbies

Soccer, F1, Fishing, BBQ, CrossFit

My Blog

https://ronnydejong.com

Contact

https://www.linkedin.com/in/ronnydejong/
https://twitter.com/ronnydejong

About “Pim Jacobs”

Focus

Azure Active Directory

Microsoft Endpoint Manager

From

The Netherlands

My Blog

https://identity-man.eu

Certifications

Microsoft MVP

Hobbies

Blogging, Watching Soccer, (trying) to play soccer myself & spending time with my family

Contact

https://www.linkedin.com/in/pimjacobs89/

https://twitter.com/pimjacobs89

Agenda

Introduction of Passwordless

Because passwords are not enough…

Define a Passwordless strategy

Determine your deployment journey

Windows Hello for Business Cloud Trust

What is cloud trust & why should I plan to use it?

Temporary Access Pass

Bootstrap your identities without passwords

Next steps

Tips & tricks to kickstart your Passwordless deployment

Key takeaways:

- **Determine your passwordless state with activity monitoring**
- **Get used & deploy at least one passwordless method**
- **Nudge your end-users**

Introduction of Passwordless

Because passwords are not enough…

Introduction of Passwordless

What is Passwordless?

Promise to remove attack vector of standalone passwords

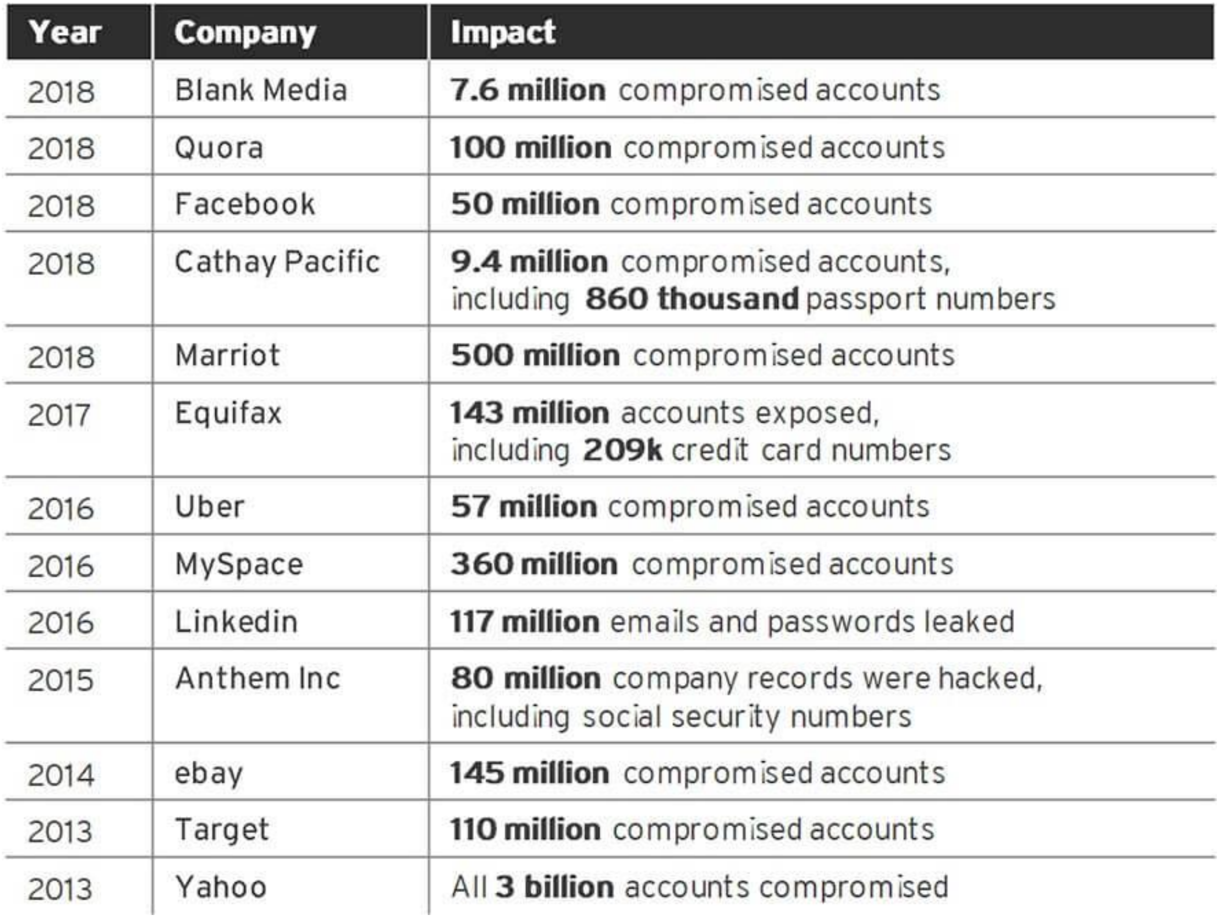
A better user experience than Passwords + Multi-Factor Authentication

Strong, device-based authentication methods

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

Introduction of Passwordless

Why Passwordless is important?



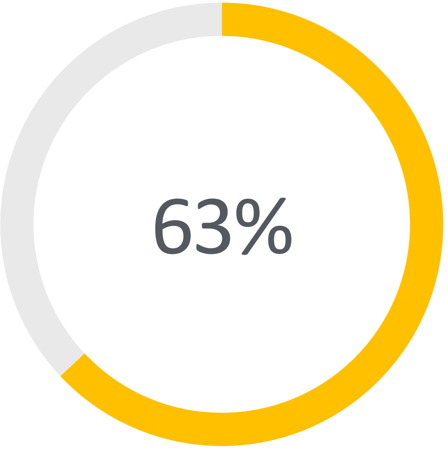
Year	Company	Impact
2018	Blank Media	**7.6 million** compromised accounts
2018	Quora	**100 million** compromised accounts
2018	Facebook	**50 million** compromised accounts
2018	Cathay Pacific	**9.4 million** compromised accounts, including **860 thousand** passport numbers
2018	Marriot	**500 million** compromised accounts
2017	Equifax	**143 million** accounts exposed, including **209k** credit card numbers
2016	Uber	**57 million** compromised accounts
2016	MySpace	**360 million** compromised accounts
2016	Linkedin	**117 million** emails and passwords leaked
2015	Anthem Inc	**80 million** company records were hacked, including social security numbers
2014	ebay	**145 million** compromised accounts
2013	Target	**110 million** compromised accounts
2013	Yahoo	All **3 billion** accounts compromised

Source: Visual Capitalist

Introduction of Passwordless

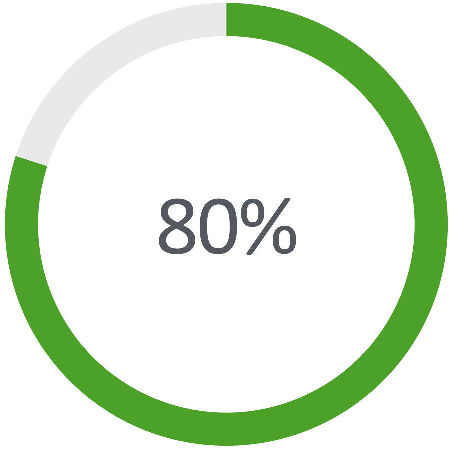
Passwords are expensive & vulnerable to breaches

Password reuse across multiple accounts



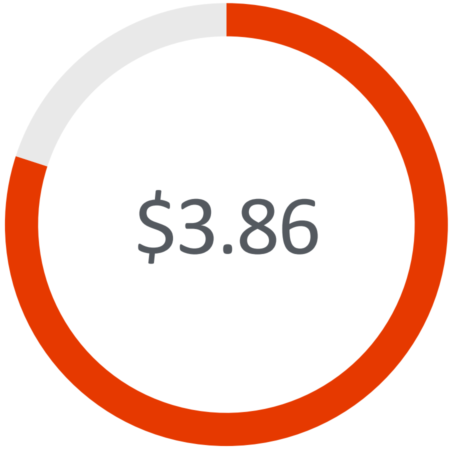
of workers admit to reuse of passwords

Passwords are the weak link



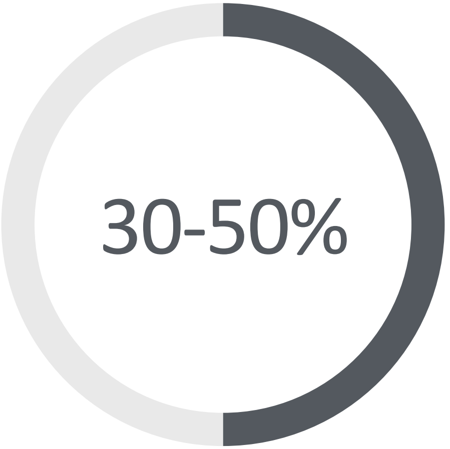
of breaches leveraged passwords

Data breaches are expensive



million, the average total cost of a data breach

Passwords generate tons of support calls



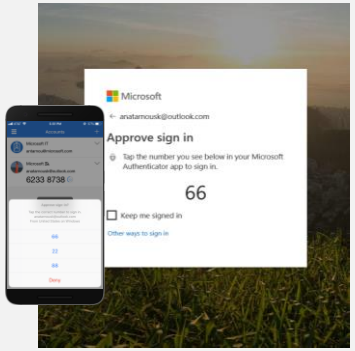
of help desk calls are related to password resets

Introduction of Passwordless

What Passwordless options we have?

- Make sign-in even more convenient and secure

Windows Hello



Microsoft

← anatamousk@outlook.com

Approve sign in

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

66

□ Keep me signed in

Other ways to sign in

Microsoft Authenticator

FIDO2 Security Keys

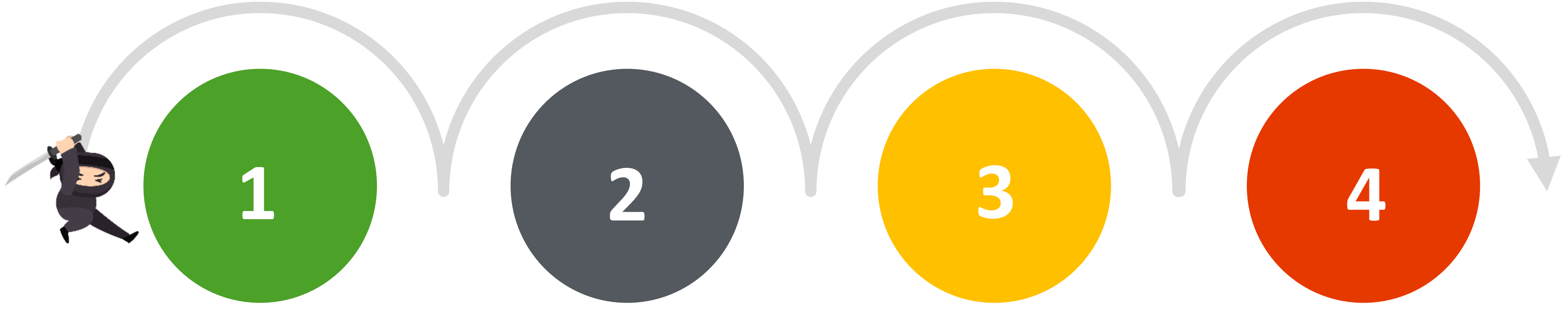
Define a Passwordless strategy

Prepare for the journey to a password freedom…

Define a Passwordless strategy

Achieve security promise

Achieve end-user promise



Deploy password-replacement offerings

Reduce user-visible password surface area

Transition to passwordless deployment

Eliminate passwords from identity directory

Define a Passwordless strategy

- Determine which Passwordless **method(s)** applies/fits my organization?
  - Requirements in place (TPM, corporate phone, shared devices)
  - Priority of Passwordless methods
  - Complexity of Passwordless methods
- Create a plan to introduce/implement in a phased approach.
  - Identity of your organization (departments, applications, work personas, IT structure)
  - Low hanging fruit/value add
- Be open for **innovation**. Passwordless is relatively new and develops continuous.
- User adoption is key!

Define a Passwordless strategy

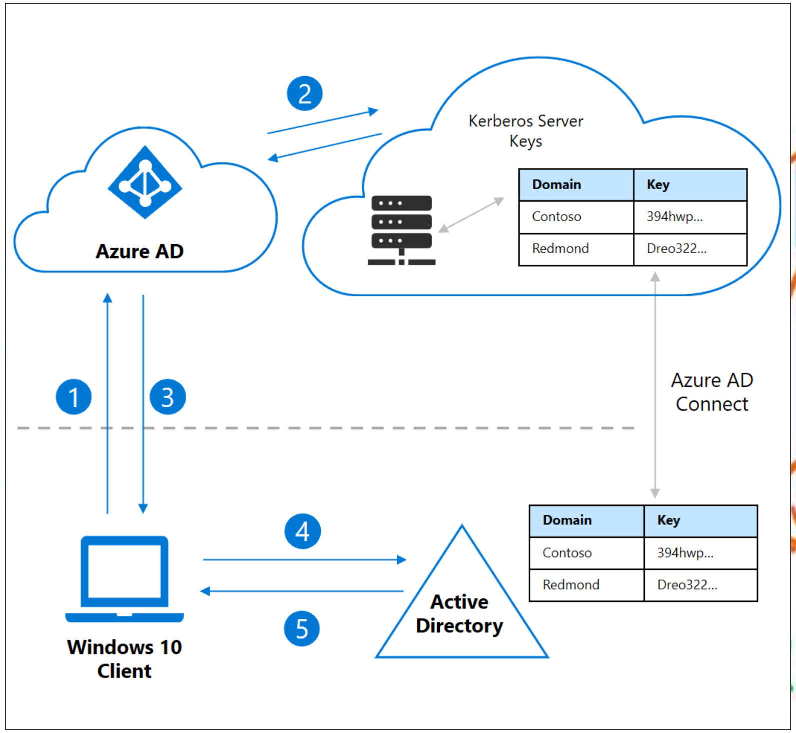
- Presence in Azure AD
- Modern Apps on Azure AD
- Device & Platform Ready
- Securely Bootstrap Creds
- Drive User Registration
- Track Rollout and Usage

Windows Hello for Business

Cloud Trust

Windows Hello for Business Cloud Trust

- What is Windows Hello for Business Cloud Trust?
  - Allows users to sign into their device with biometrics or a PIN
  - Breach, theft, and phish resistant credentials
  - Single sign-on experience



Domain	Key
Contoso	394hwp...
Redmond	Dreo322...

Domain	Key
Contoso	394hwp...
Redmond	Dreo322...

On Premises Certificate Trust

- Device is not AAD Registered
- No Certificate Deployed to Devices
- Requires 2016 ADFS

Not Modern!
st!

1. User signs into their Windows 10 device key and authenticates to Azure AD.
2. Azure AD checks the directory for a Kerberos server key matching the user's on-premises AD domain.
a. Azure AD generates a Kerberos TGT for the user's on-premises AD domain. The TGT only includes the user's SID. No authorization data is included in the TGT.
3. The TGT is returned to the client along with their Azure AD Primary Refresh Token (PRT).
4. The client machine contacts an on-premises AD domain controller and trades the partial TGT for a fully formed TGT.
5. The client machine now has an Azure AD PRT and a full Active Directory TGT and can access both cloud and on-premises resources.

Windows Hello for Business Cloud Trust

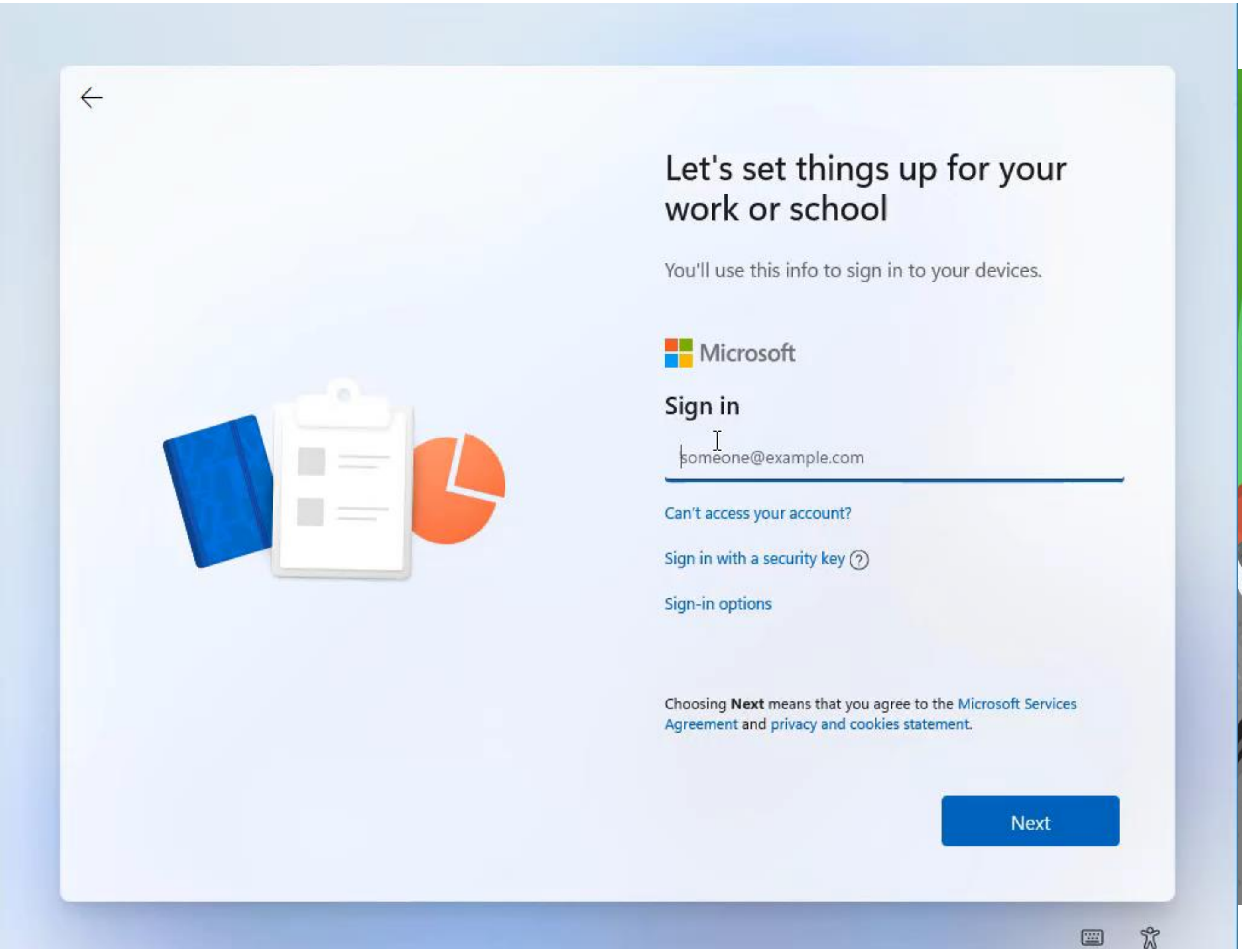
- Why using Cloud Trust?
  - Simplify Windows Hello for Business deployments

- What are we solving with Cloud Trust?
  - No PKI infrastructure required
  - No Azure AD Connect key sync dependency (write back/sync interval of max 30 minutes)
  - *No device write back (applies only for cert trust deployments)*
  - *No ADFS deployment required (applies only for cert trust deployments)*

- Requirements
  - Windows 10 Dev Channel or Windows 11 (21H2 - 10.0.21327 or higher)
  - Azure AD Connect 1.4.32 or higher
  - Windows Server 2008 R2 domain/forest functional level
  - Windows Server 2016/2019 domain controllers (with latest updates)

Demo

- **Validate Cloud Trust set up**
- **Cloud Trust user experience**
    - Enrollment
    - Instant access to resources



Let's set things up for your work or school

You'll use this info to sign in to your devices.

Microsoft

Sign in

someone@example.com

Can't access your account?

Sign in with a security key

Sign-in options

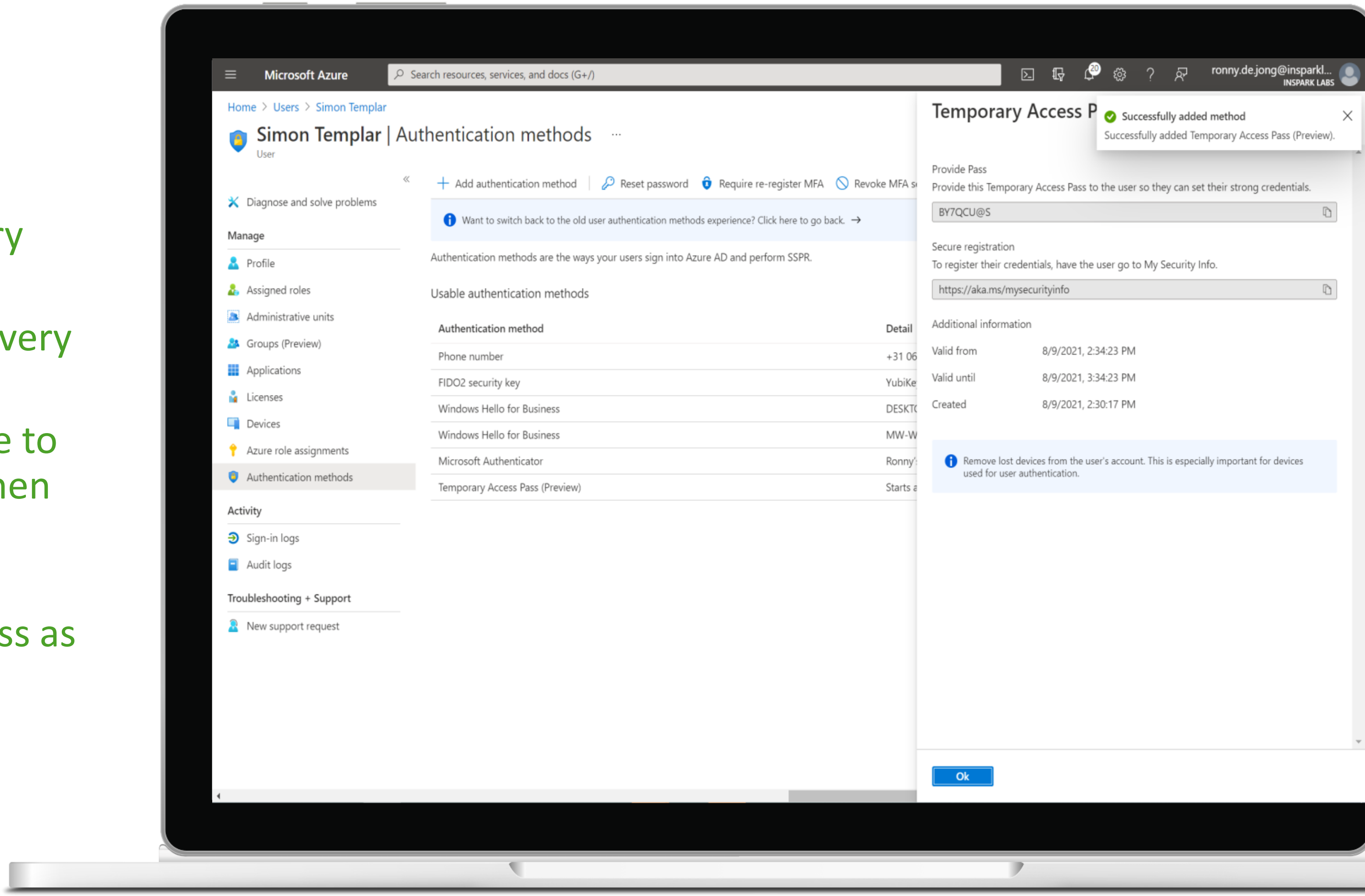
Choosing **Next** means that you agree to the Microsoft Services Agreement and privacy and cookies statement.

Temporary Access Pass

Bootstrapping your identities…and more

Temporary Access Pass

- Why using TAP?
  - Time-limited code for passwordless credentials set up and account recovery
  - Enables end-to-end passwordless user journeys and remote onboarding/recovery scenarios
  - User can receive a temporary passcode to login and register their account, and then register a passwordless credential
  - Streamline initial MFA registration via Authenticator App and set passwordless as primary authentication method


Microsoft Azure
Search resources, services, and docs (G+/)
20
ronny.de.jong@insparkl...
INSPARK LABS
Home > Users > Simon Templar

Simon Templar | Authentication methods

User

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

Authentication methods are the ways your users sign into Azure AD and perform SSPR.

Usable authentication methods

Authentication method	Detail
Phone number	+31 06
FIDO2 security key	YubiKe
Windows Hello for Business	DESKTO
Windows Hello for Business	MW-W
Microsoft Authenticator	Ronny'
Temporary Access Pass (Preview)	Starts a

Temporary Access P

Successfully added method

Successfully added Temporary Access Pass (Preview).

Provide Pass

Provide this Temporary Access Pass to the user so they can set their strong credentials.

BY7QCU@S

Secure registration

To register their credentials, have the user go to My Security Info.

https://aka.ms/mysecurityinfo

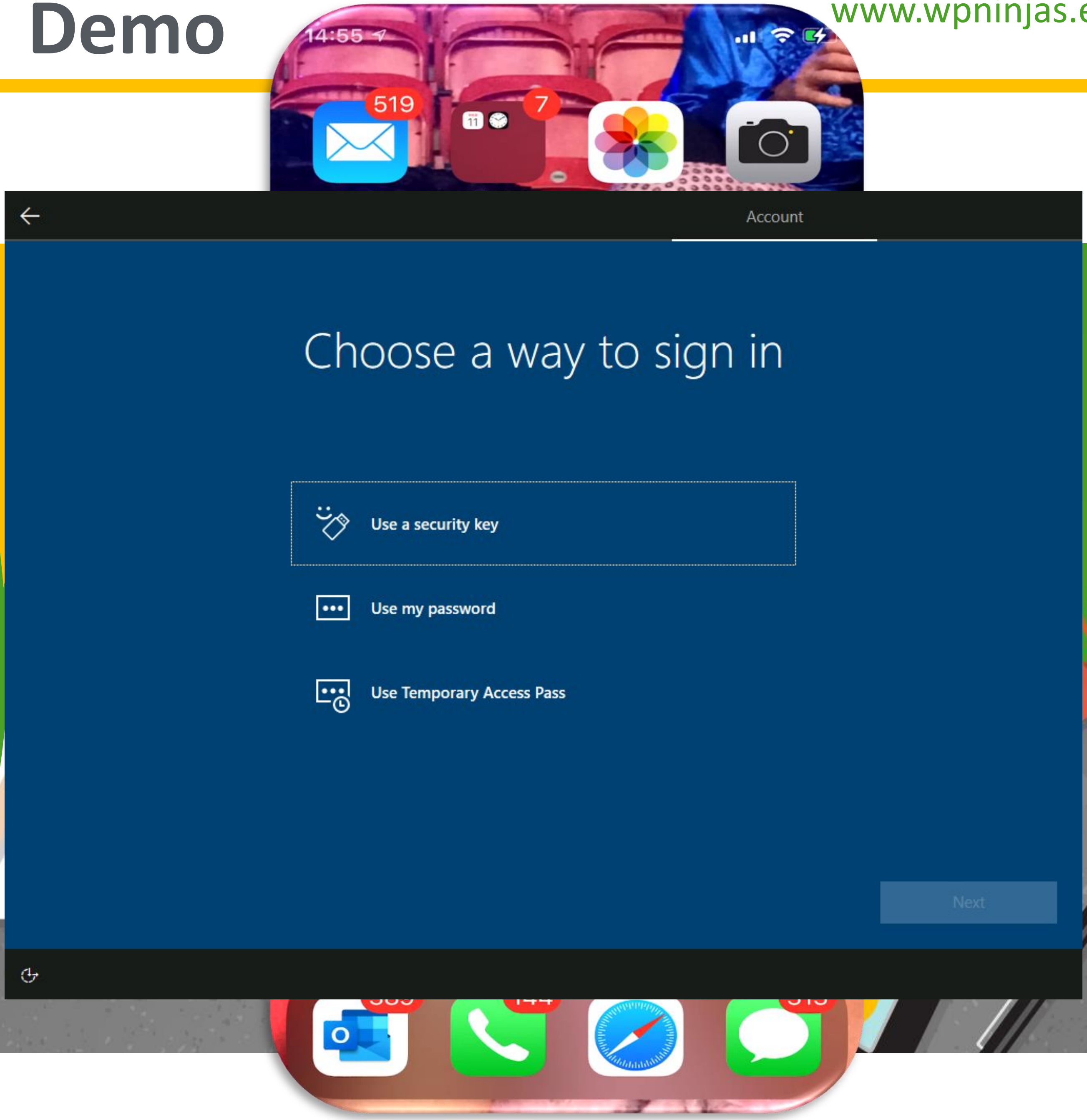
Additional information

Valid from	8/9/2021, 2:34:23 PM
Valid until	8/9/2021, 3:34:23 PM
Created	8/9/2021, 2:30:17 PM

Remove lost devices from the user's account. This is especially important for devices used for user authentication.

Demo

- **Setup Temporary Access Pass**
- **Temporary Access Pass user experience**
  - Joiner Authenticator App setup (one-time use)



Choose a way to sign in

- Use a security key
- Use my password
- Use Temporary Access Pass

Known challenges/limitations

- Passwords can still not be ‘**disabled**’. Password surface area (credential providers) is still required.
  - e.g. Remote Desktop, legacy apps, apps with own/local IdP
- Authenticator App
  - Passwordless Phone sign-in limited to a single tenant (Azure AD Registration)
- Nudge will not appear on mobile devices (Android & iOS)
- FIDO2
  - No lock on removal of FIDO-key.
- Windows Hello for Business
  - **No simple migration path** of Windows Hello for Business **Cert-trust** to **Cloud-trust** scenario.
- Temporary Access Pass
  - Cannot be restricted to a specific resource(s) (e.g. Exchange, SharePoint or Windows Autopilot enrollment)

Key takeaways

- Authenticator App
  - Improved registration (combines MFA & SSPR)
  - Nudge your end-users for using Authenticator App 😉

- Phone Sign-in
  - Use TAP for initial Authenticator App enrollment

- Windows Hello for Business Cloud-trust
  - Simplified deployment
  - Instantly active
  - Windows 10 Dev Channel & Windows 11 (Cloud-trust)

How & where to start tomorrow?

- Create a **Passwordless strategy.**
- Make sure the **correct AD Premium licenses** (P1 or P2) are in place.
- Make sure **Authentication Methods** are configured.
- Validate your **hardware-** & **software readiness**.
- **Start** deploying at least **one passwordless method**.
- Use **Conditional Access** to **ease** your Authenticator App **deployment**(s).
- **Bootstrap** your accounts with **Temporary Access Pass**.
- **Boost** your Authenticator App **deployment** by enabling ‘**Nudge**’ functionality.
- **Keep track** on **deployment** (registration & usage) with built-in **reports**.
- Make sure you have **mandate** from your **leadership** (buy-in).
- Explore* your Windows Hello for Business **migration** options to **Cloud-trust** deployment.

Q&A

Thank You