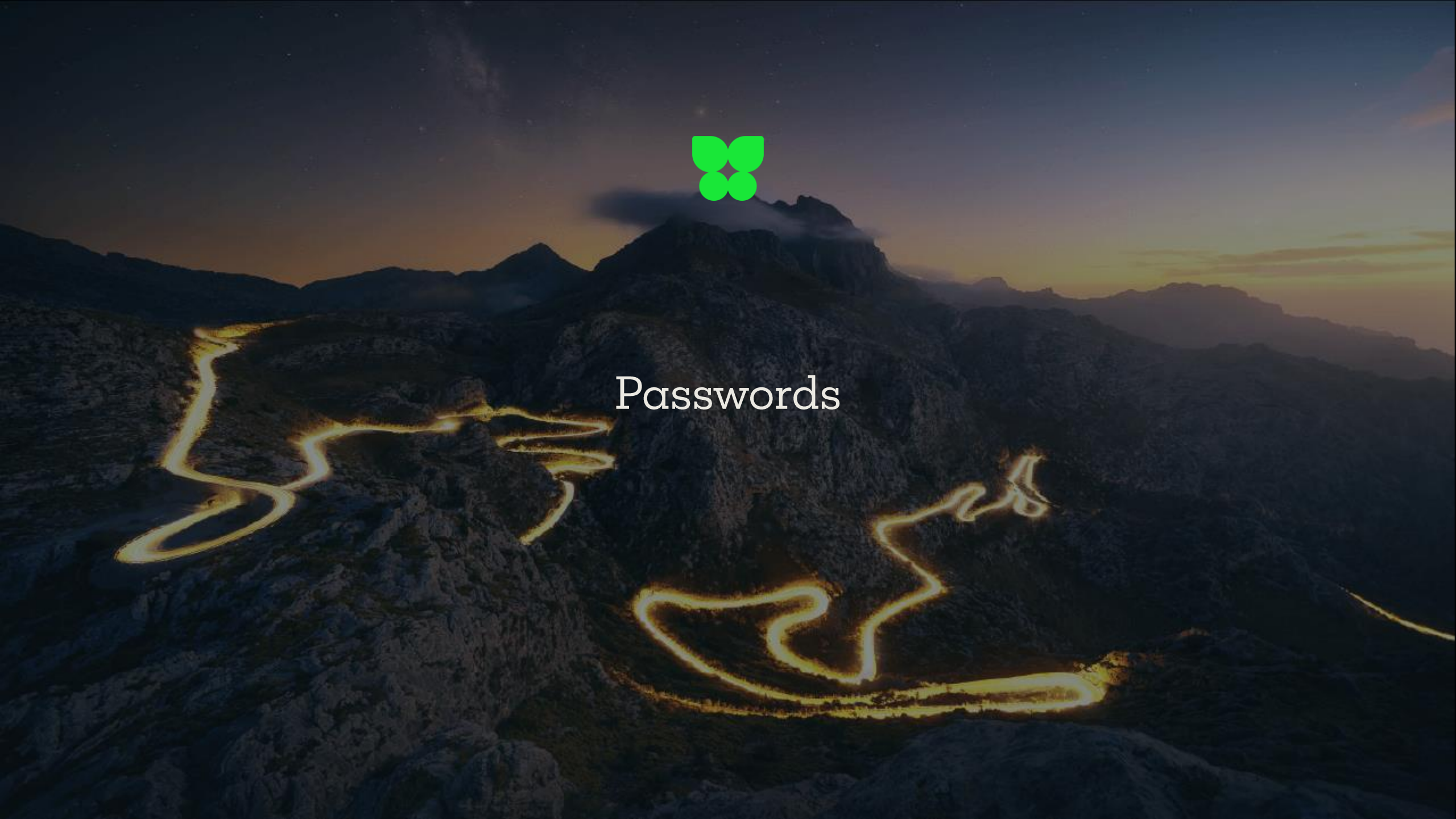
Turn your passwordless plans into a super secure reality

David Guest

Kocho

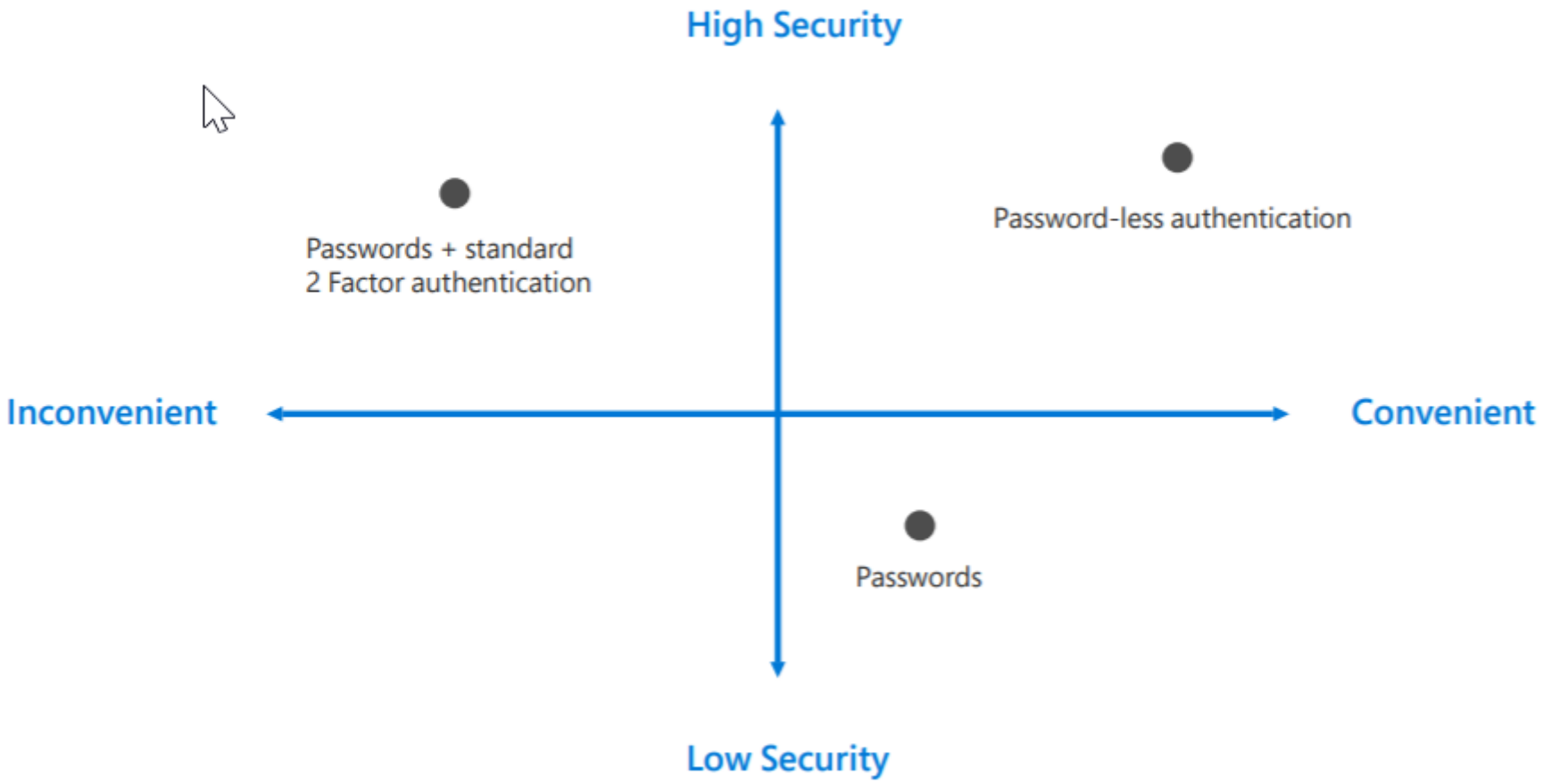
BECOME GREATER


Passwords

Passwords are expensive and insecure

Password reuse across multiple accounts	Passwords are the weak link	Data breaches are expensive	Passwords generate a lot of support calls
73% of passwords are duplicates	81% of breaches leveraged passwords	$3.92 million, the average total cost of a data breach	40% of help desk calls are related to password resets

There is a better way



Passwordless authentication solutions

Windows Hello for Business

Increase sign-in convenience with biometric authentication. Replace passwords with MFA on Windows 10 PCs.

Microsoft Authenticator

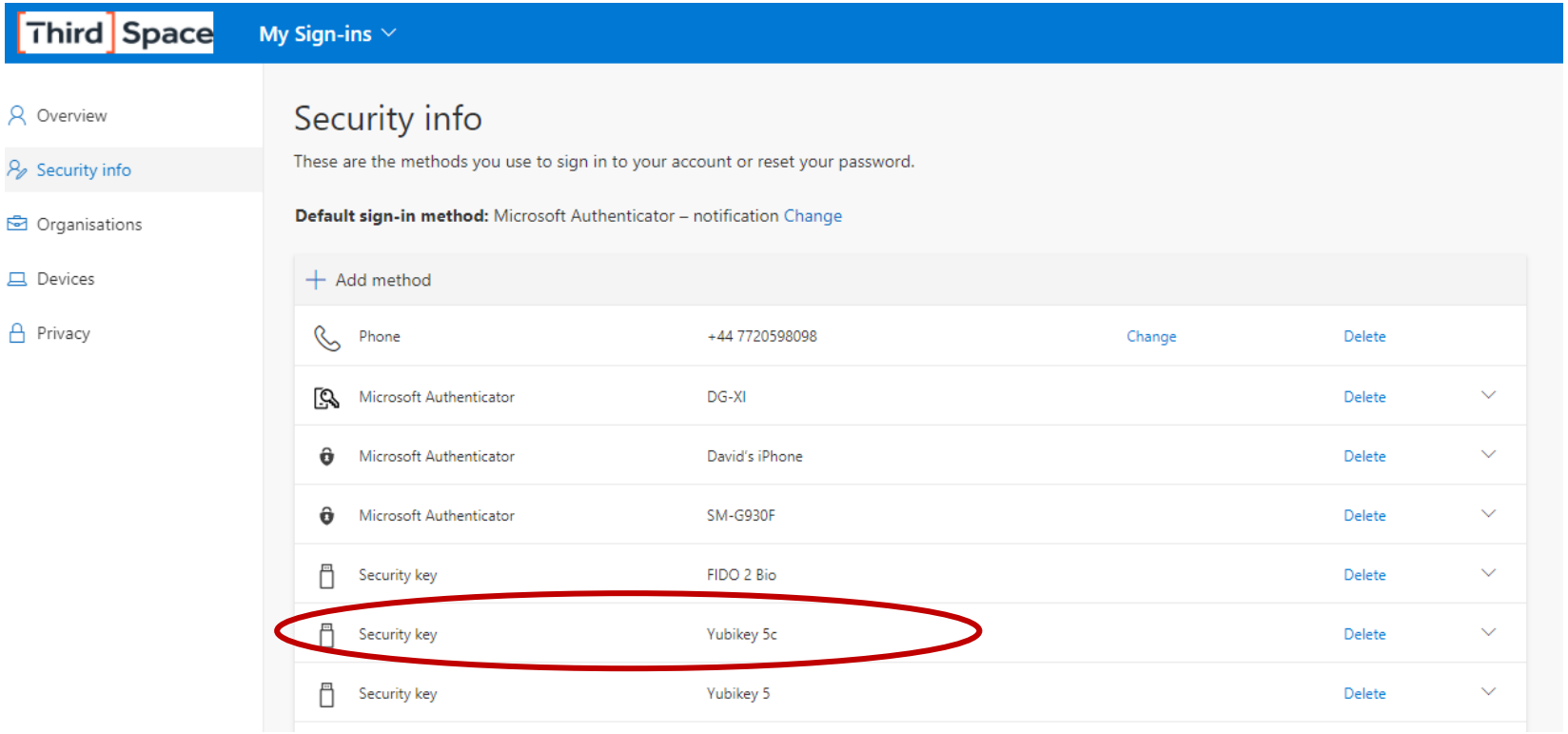
Authenticate with a mobile device. Get a push notification and verify identity with a biometric or PIN.

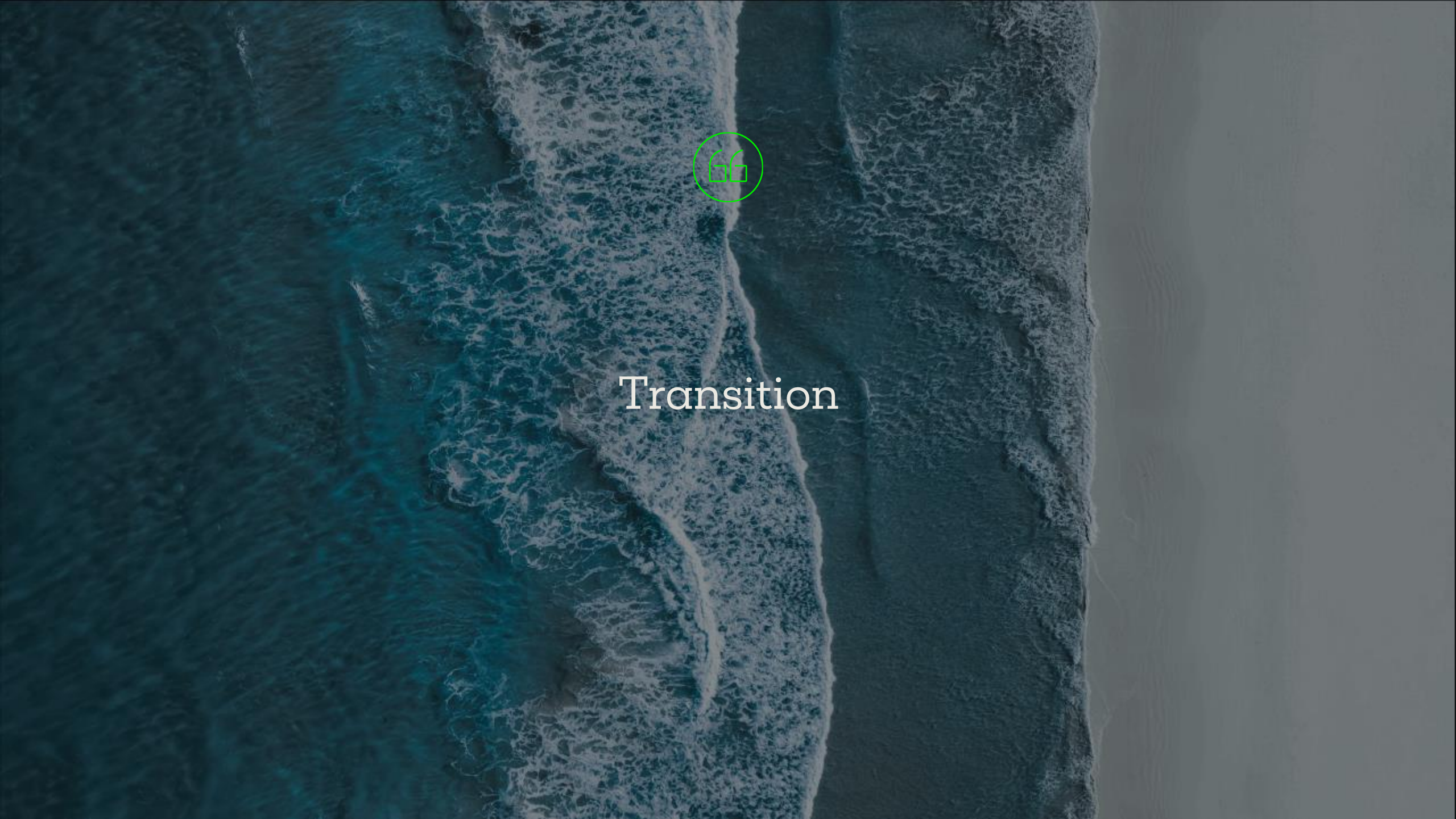
FIDO2 security keys

Replace passwords with a security key using MFA with the standards-based protocols on a mobile device.

User configuration

- From the My Sign-ins web pages
  - https://mysignins.microsoft.com/security-info




Transition

Eliminate passwords from identity directory

- User never types their password
- User never changes their password
- User doesn’t know their password
- User doesn’t even have a password
- More importantly…

Allows the achievement of the passwordless security promise

Deployment considerations

- Are you ready ?
  - → Hardware in place (TPM) ?
  - → Consider biometric/PIN capable devices
  - → Temporary Access Pass to enable MFA without MFA
- Windows Hello for Business deployment
  - Plan on moving to Hybrid and look at key trust deployments
- Active Directory/Server upgrades
  - Ensure you're upgrading to 2016+ and have latest patch to support passwordless

Enable passwordless

- Windows Hello for Business
  - Biometric / PIN
  - *Biometrics are only stored on the device*
- Phone sign-in with Authenticator app
- Security key

Secure traditional and modern systems

Enable passwordless via FIDO2/WebAuthn, smart card, partner platforms

YubiKey 5 Series

Multi-protocol

WebAuthn | FIDO2 | U2F | Smart card | Yubico OTP | OATH-HOTP | OATH-TOTP | OpenPGP | Static Passwords

New

YubiKey Bio

FIDO-only and Biometrics

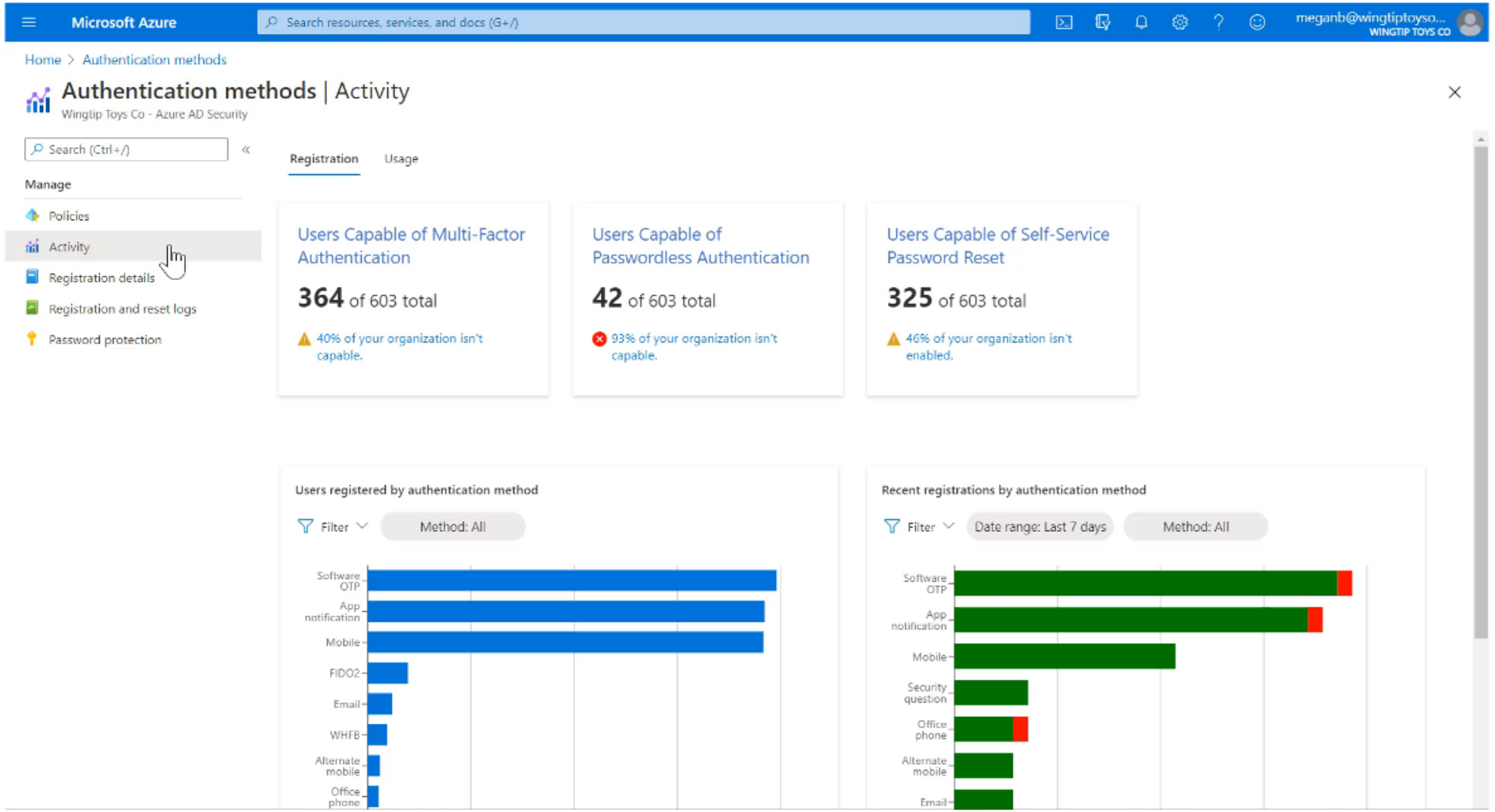
WebAuthn | FIDO2 | U2F

Security Key NFC

FIDO-only

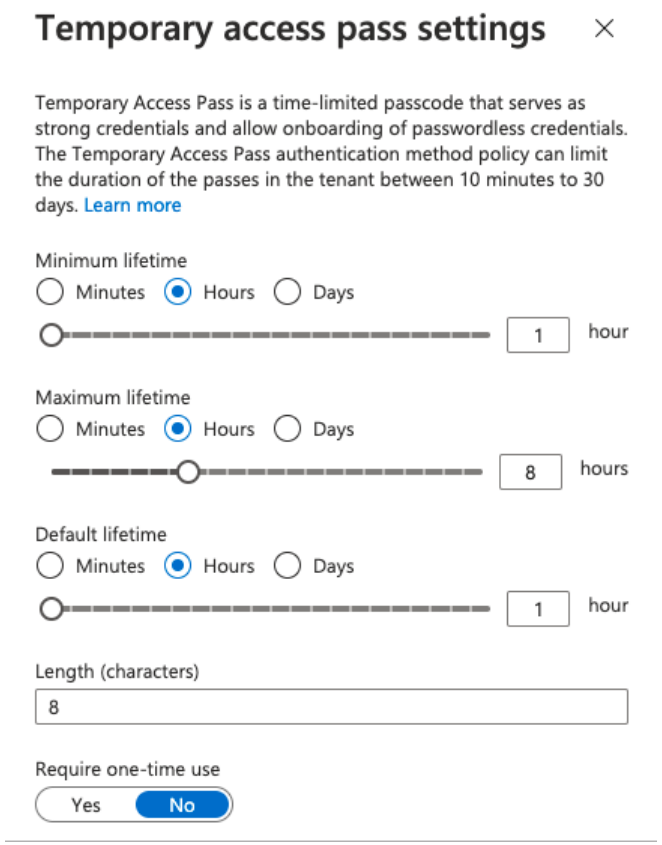
WebAuthn | FIDO2 | U2F

New Reporting & Insights for Auth Methods



Temporary Access Pass

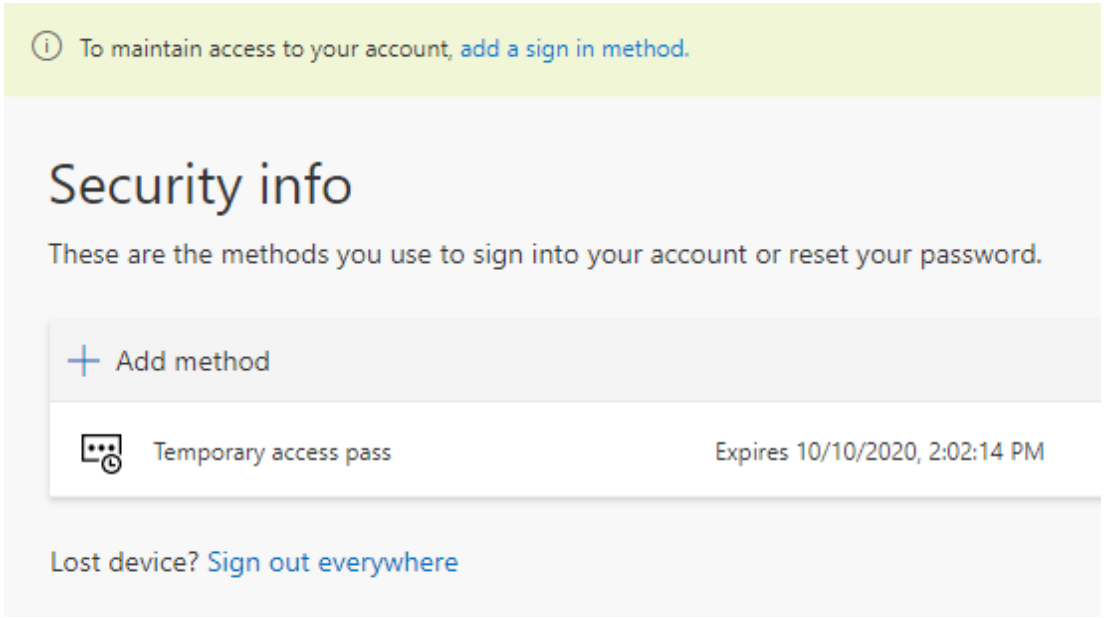
Enabling full passwordless flow



- Scoped to users and groups
- Set a duration and start time
- One-time use or multi-use
- Configurable in the Azure AD portal and in Microsoft Graph
- Satisfy MFA requirement

Temporary Access Pass uses

Register	A FIDO2 Security key
Register	Phone Sign-in
Bootstrap	WHfB/OOBE/Mobile/MacOS
Recover	Access to your account (Passwordless and MFA)



Enable Tenant

Set method specific settings for FIDO2 and TAPS

Configure your users in the authentication methods policy to enable passwordless authentication. Once configured, you will need to enable your users for the enhanced registration preview so they can register these authentication methods and use them to sign in.

Method	Target	Enabled
FIDO2 Security Key	All users	Yes
Microsoft Authenticator	All users	Yes
Text message (preview)		No
Temporary Access Pass (pr...	All users	Yes

Details

Method	Target	Enabled
FIDO2 Security Key	All users	Yes

Details

Save Discard

ENABLE

Yes No

USE FOR:

- Sign in
- Strong authentication

TARGET

All users Select users

Name	Type
All users	Group

GENERAL

Allow self-service set up

Yes No

Enforce attestation

Yes No

KEY RESTRICTION POLICY

Enforce key restrictions

Yes No

Restrict specific keys

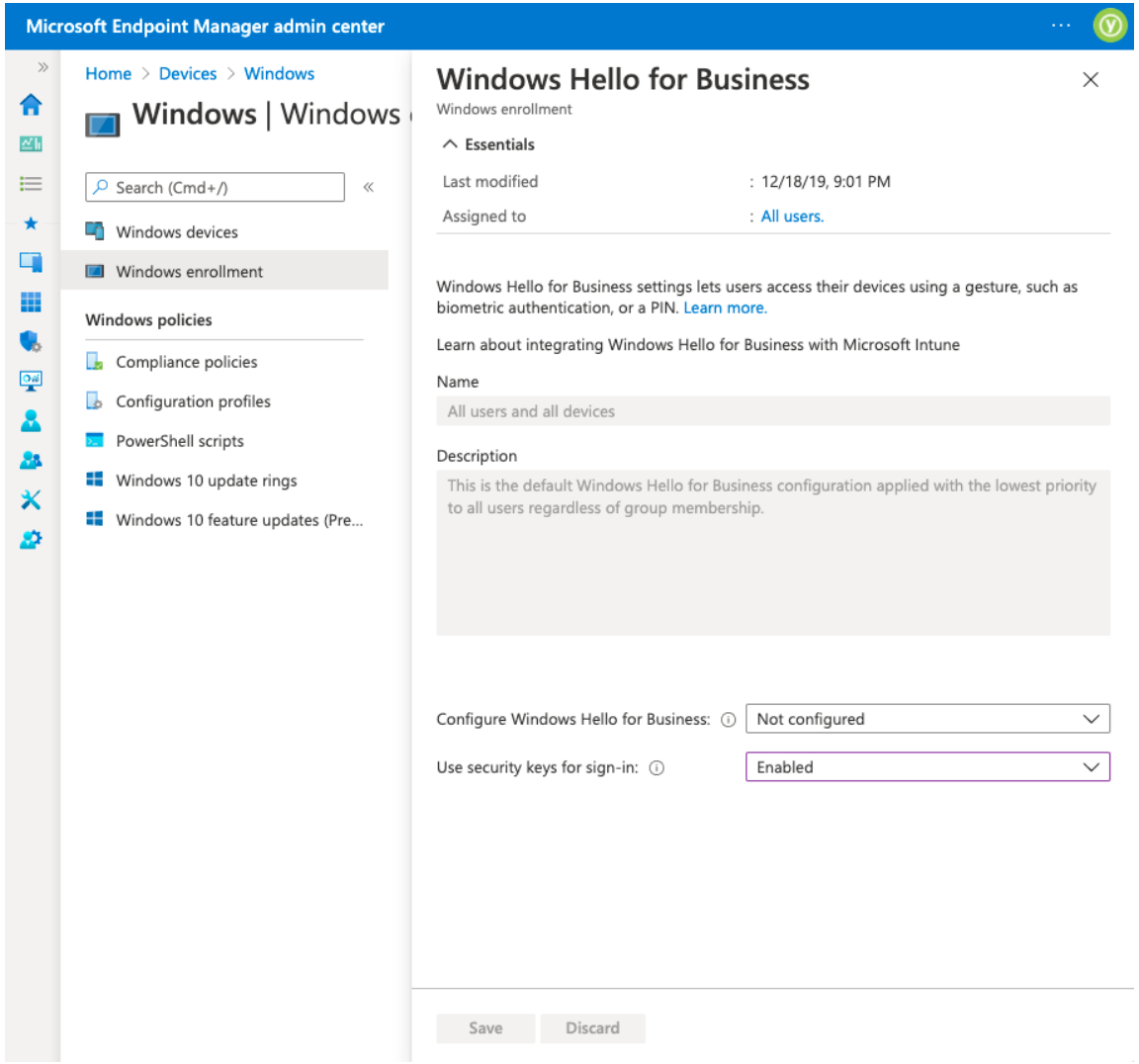
Allow Block

Add AAGUID

No AAGuids have been ad..

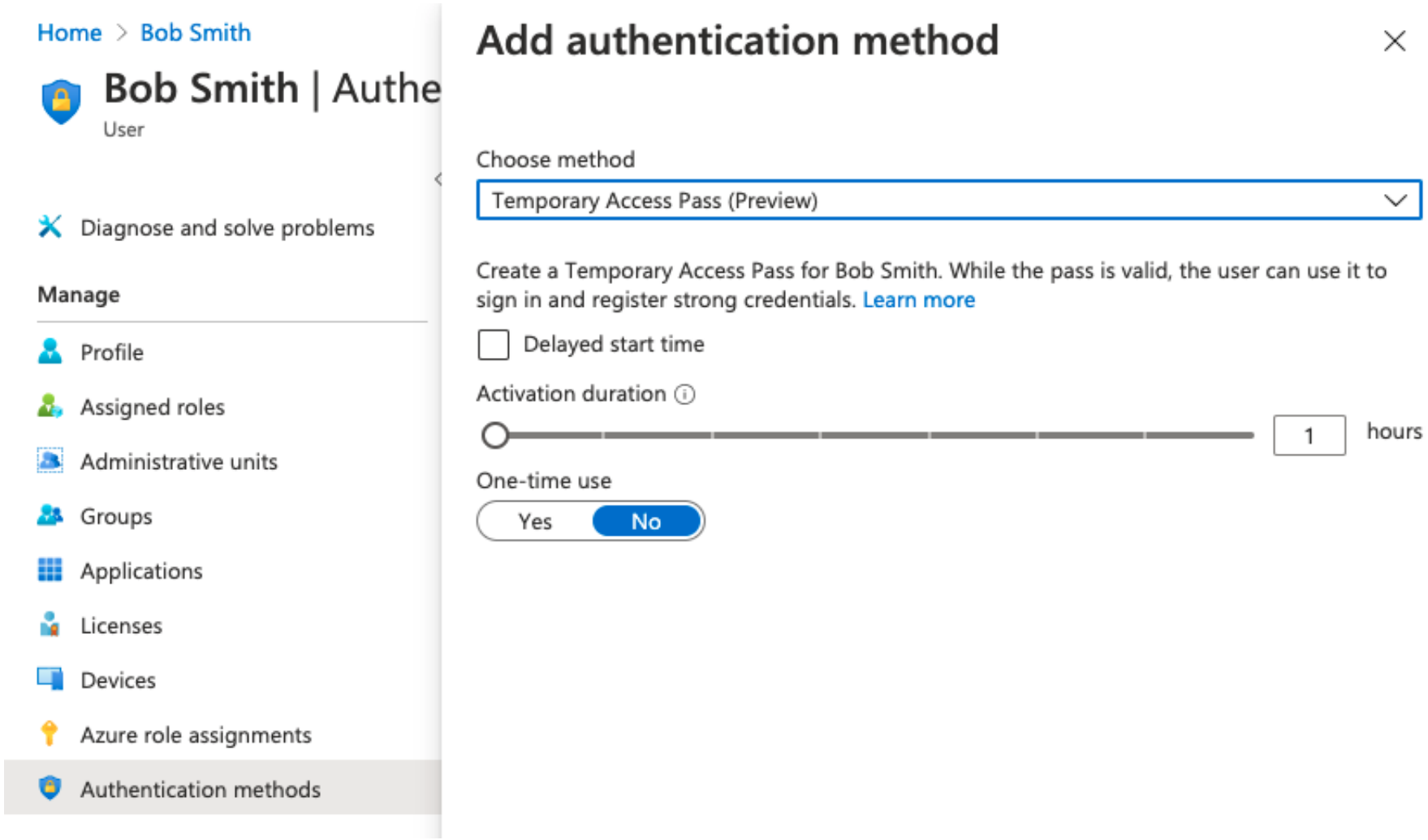
Enable device login

Endpoint Manager or Provisioning package for desktop login



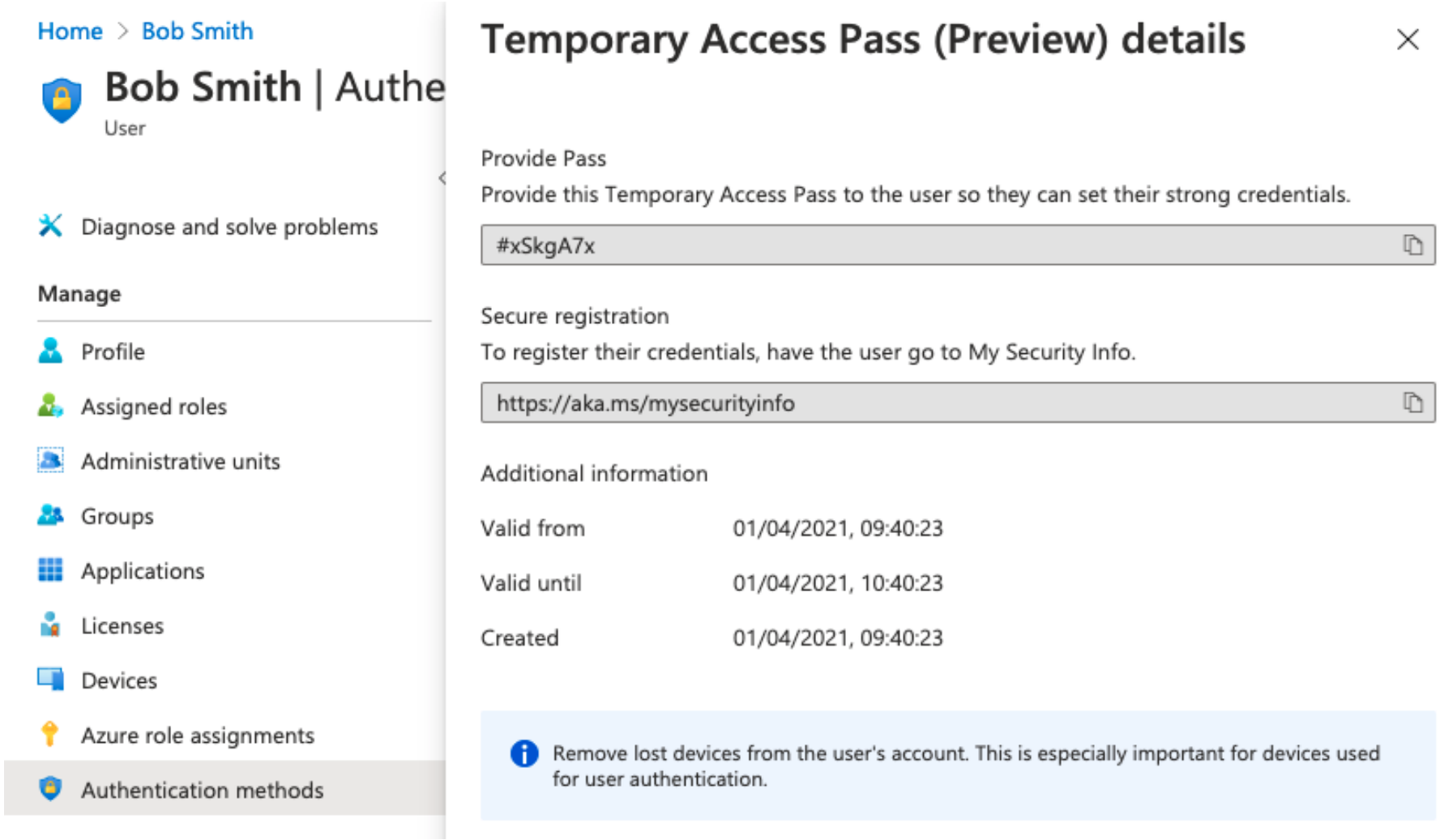
User enrolment

Create a Temporary Access Pass for the user



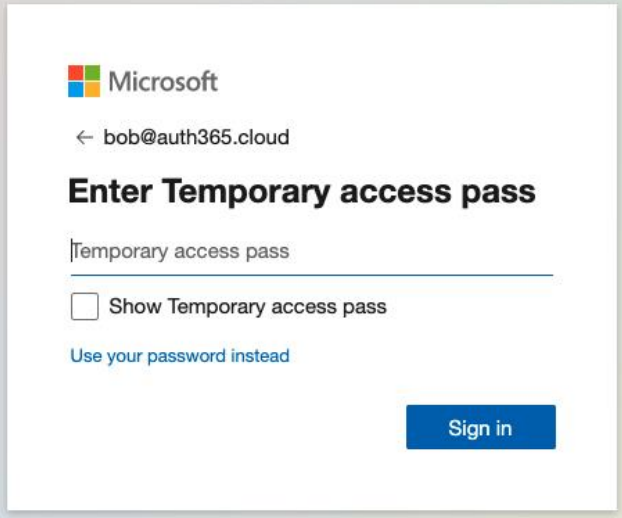
User enrolment

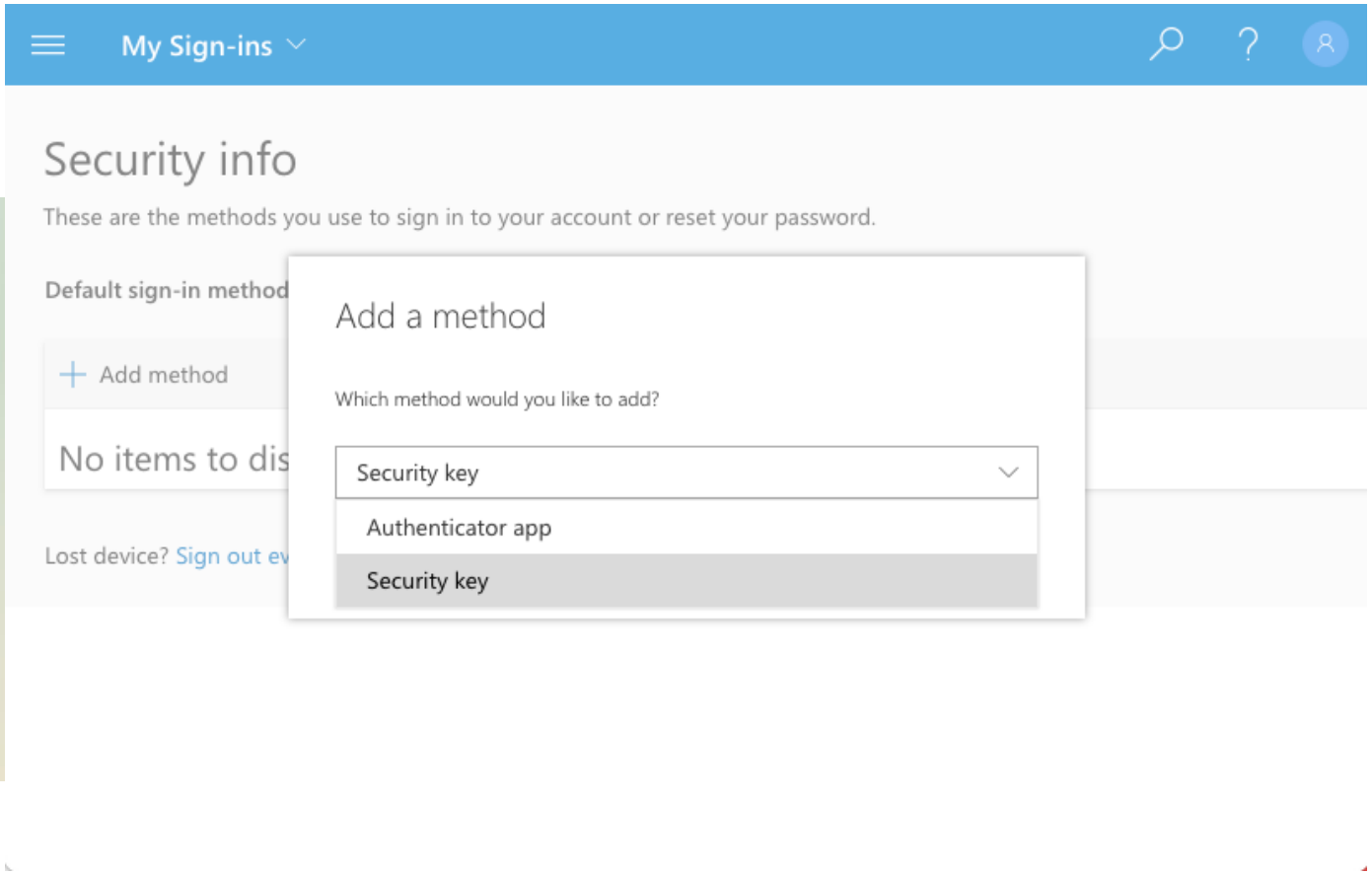
Create a Temporary Access Pass for the user



User enrolment

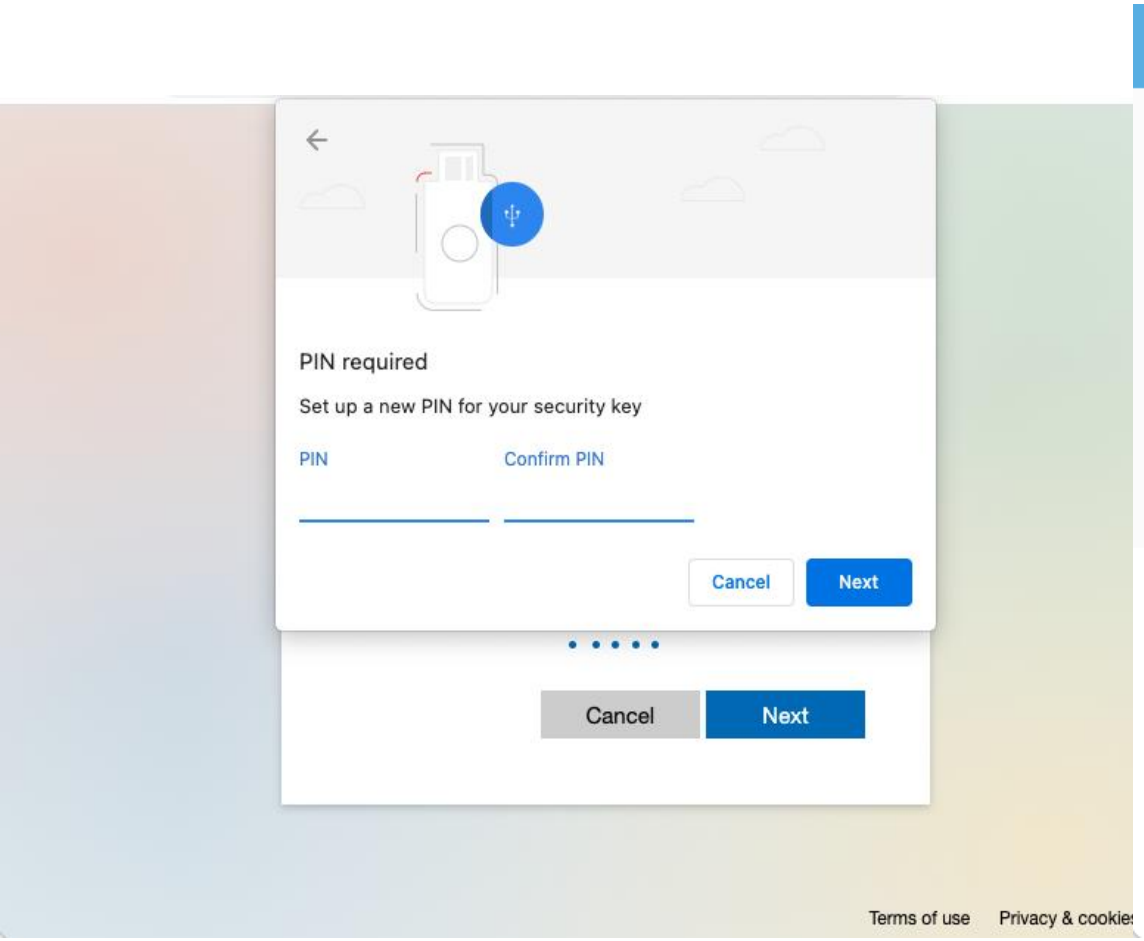
User enrols in self-service portal - https://mysignins.microsoft.com

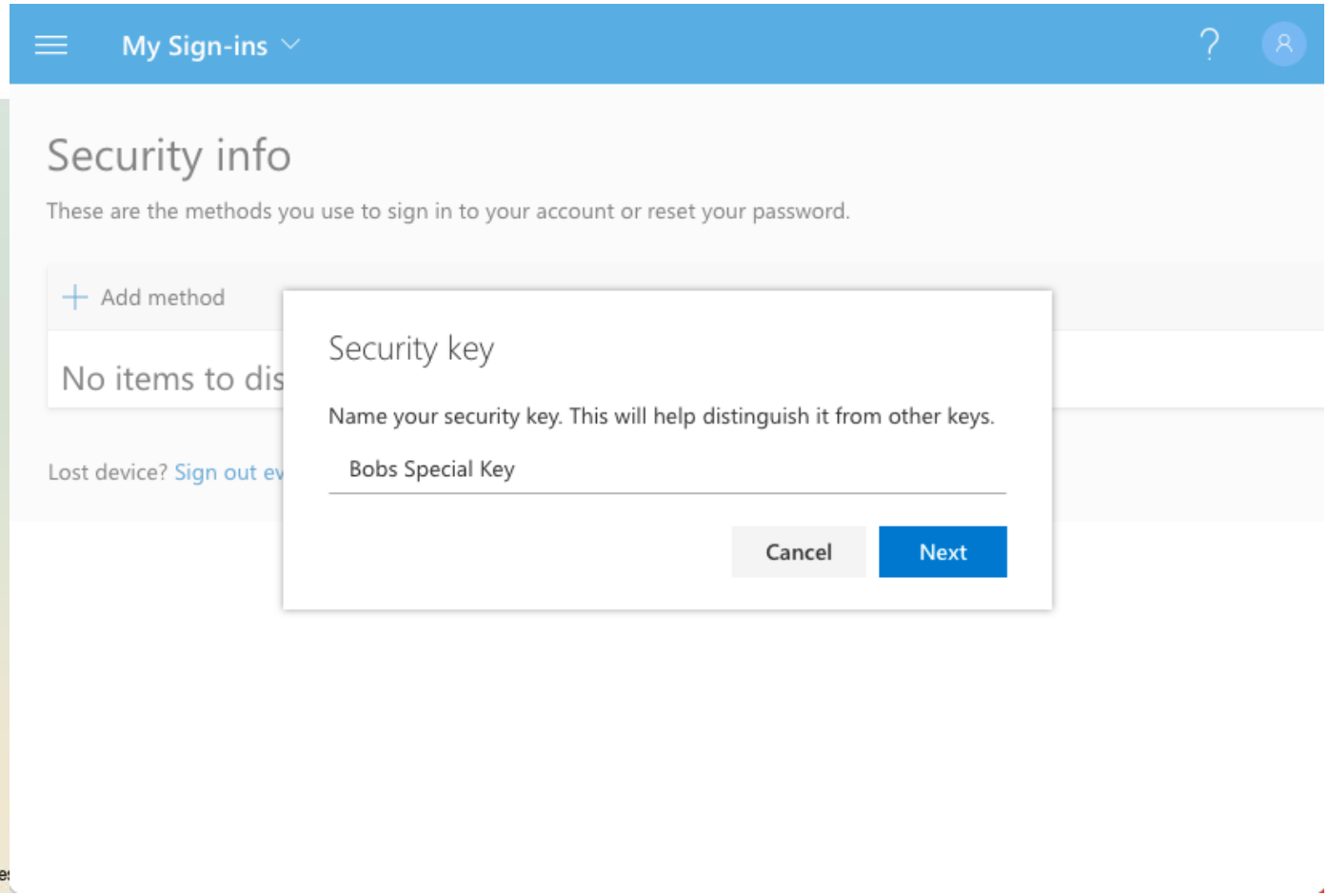




User enrolment

User enrols in self-service portal - https://mysignins.microsoft.com





Deployment Considerations

Platforms

Windows 10 login

- AADJ Only - 1903+
- Hybrid - 2004+
- Not for BYOD login scenarios (MSA)*

MacOS

- Browser support only at present

Mobile support

- No support for mobile apps
- Cannot login via mobile browsers*
- Can register YubiKey via mysignins on iOS

Experience

User Experience

- No tap and go (e.g. in retail)
- Need to enter PIN or Biometric
- PIN/Bio enforced by Windows/Azure

Enrolment

- Currently only self enroll as an option
- Currently no force PIN change*
- Deployment of TAPS

* coming?

Introduction to the YubiKey

Nic Sarginson - Principal Solutions Engineer

Useful Links

- **Product catalog**
  https://www.yubico.com/works-with-yubikey/catalog/
- **Support Home**
  https://support.yubico.com/support/home
- **Developer site - lots of info**
  https://developers.yubico.com/
- **Compare Keys**
  https://www.yubico.com/products/yubikey-hardware/compare-yubikeys/
- **HSM details and spec**
  https://www.yubico.com/product/yubihsm-2/
- **Azure setup overview**
  https://support.yubico.com/hc/en-us/articles/360016913619-YubiKeys-for-Microsoft-Azure-AD-Passwordless-Sign-In-Guide
- **AD Cert services overview**
  https://support.yubico.com/hc/en-us/articles/360013707820-YubiKey-Smart-Card-Deployment-Guide
- **OATH MFA overview**
  https://support.yubico.com/hc/en-us/articles/360015669179-Using-YubiKeys-with-Azure-MFA-OATH-TOTP

Yubico, Trusted Secure Authentication

Trusted choice for the largest companies in the world.

0
Account takeovers with YubiKeys

92%
Support reduction vs. mobile apps

4,500+
Business customers + a large # of consumers

19/20
US tech giants are customers

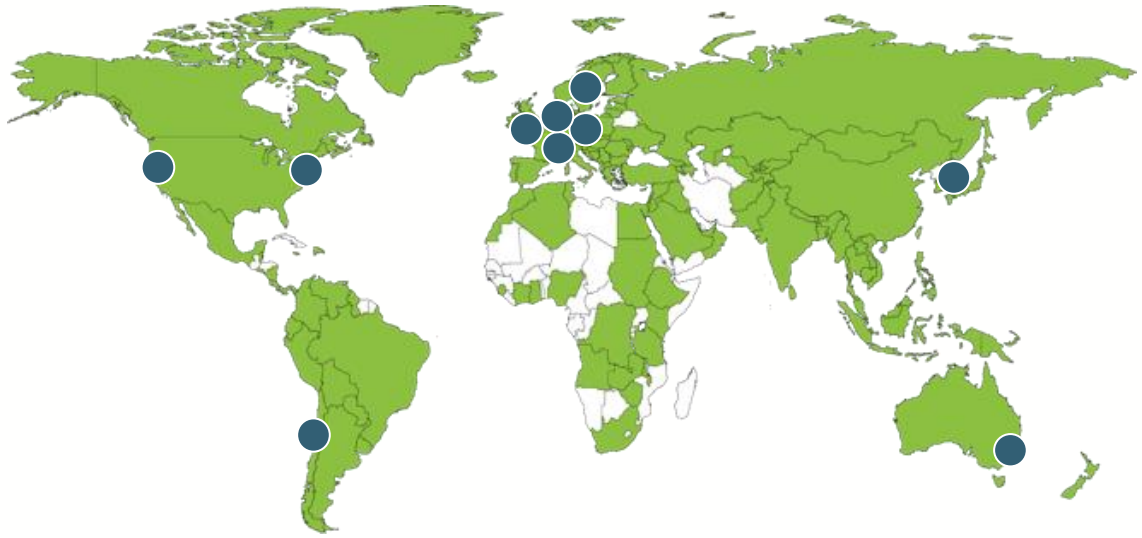
700+
Proven technology partner integrations

17m+
YubiKeys sold

330
Employees in 10 countries

Top tier
Investors

Customers in 160+ countries



fido ALLIANCE

yubico

#1 IT Security Problem: Stolen Credentials

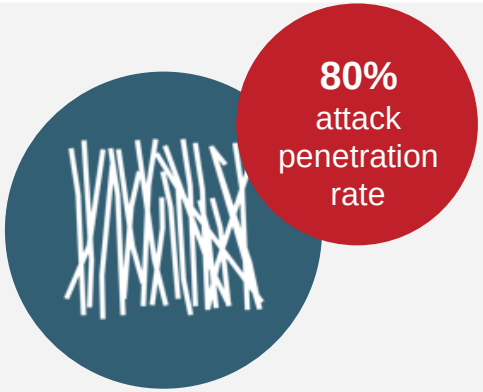
4.6+ Billion stolen credentials reported in 2019[1]

23.5 million breached accounts used 123456 as their password[2]

81% of data breaches from weak/stolen passwords[3]

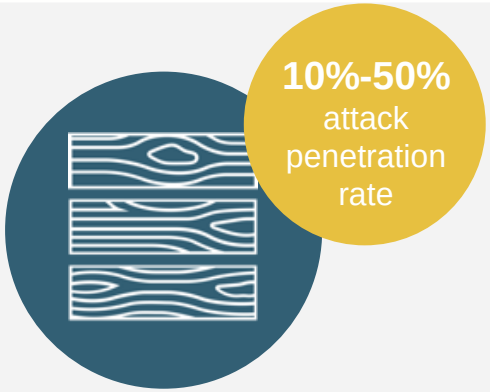
$3.9M average cost of a breach ($148/ record)[4]

Three Categories of Authentication



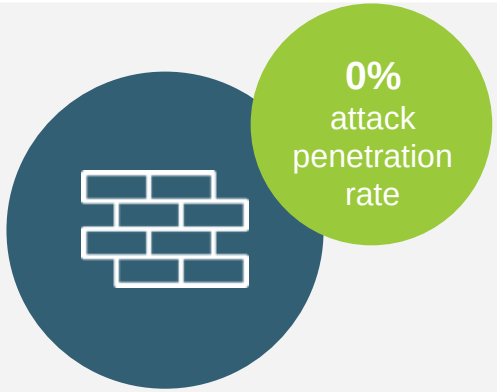
Username and Password

- Deployed everywhere
- Known usability gaps
- Costly and hard to sustain
- Common target for credential phishing



Basic 2FA: SMS, Email, Mobile

- Not purpose-built for security
- Uses existing technology stacks that are vulnerable to network and software attacks
- Common target for credential phishing

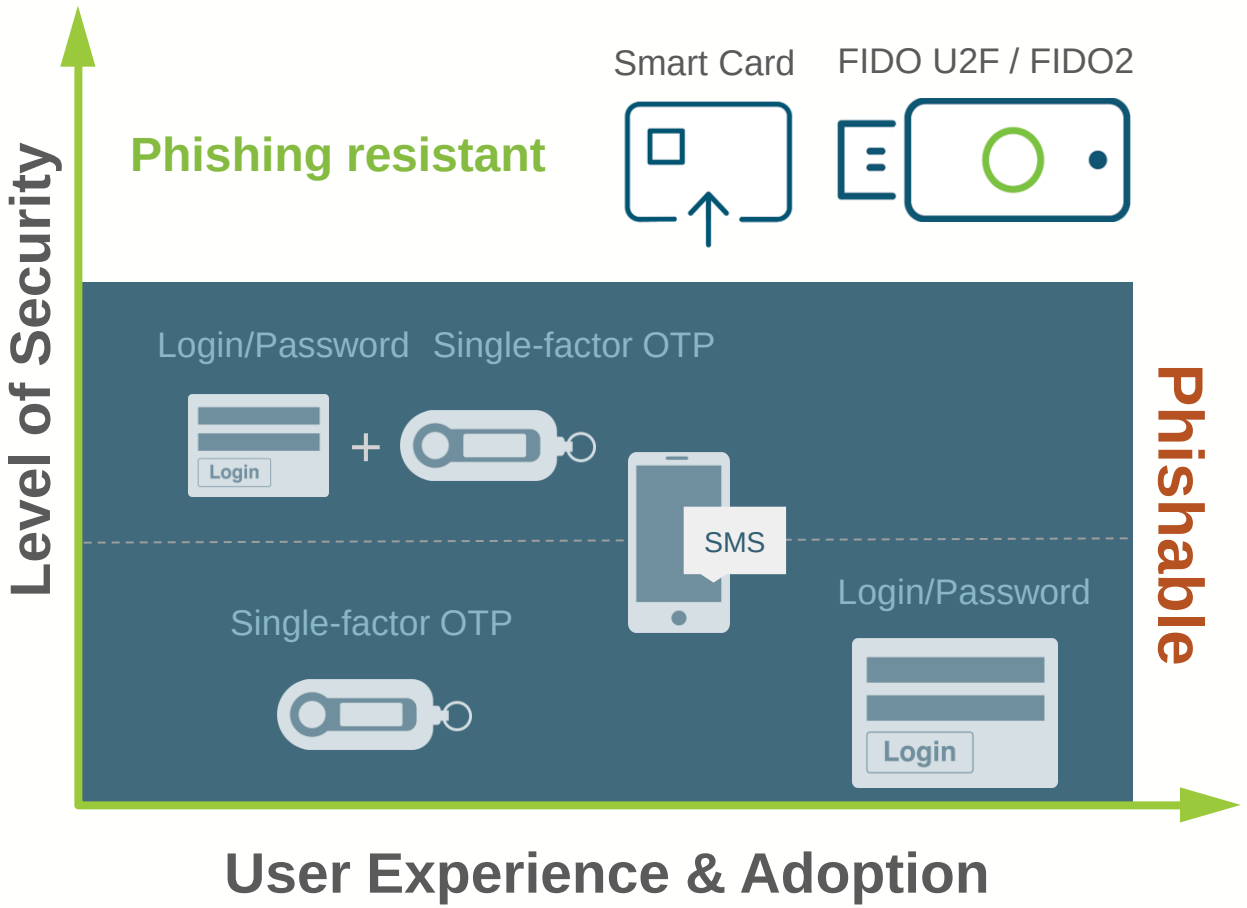


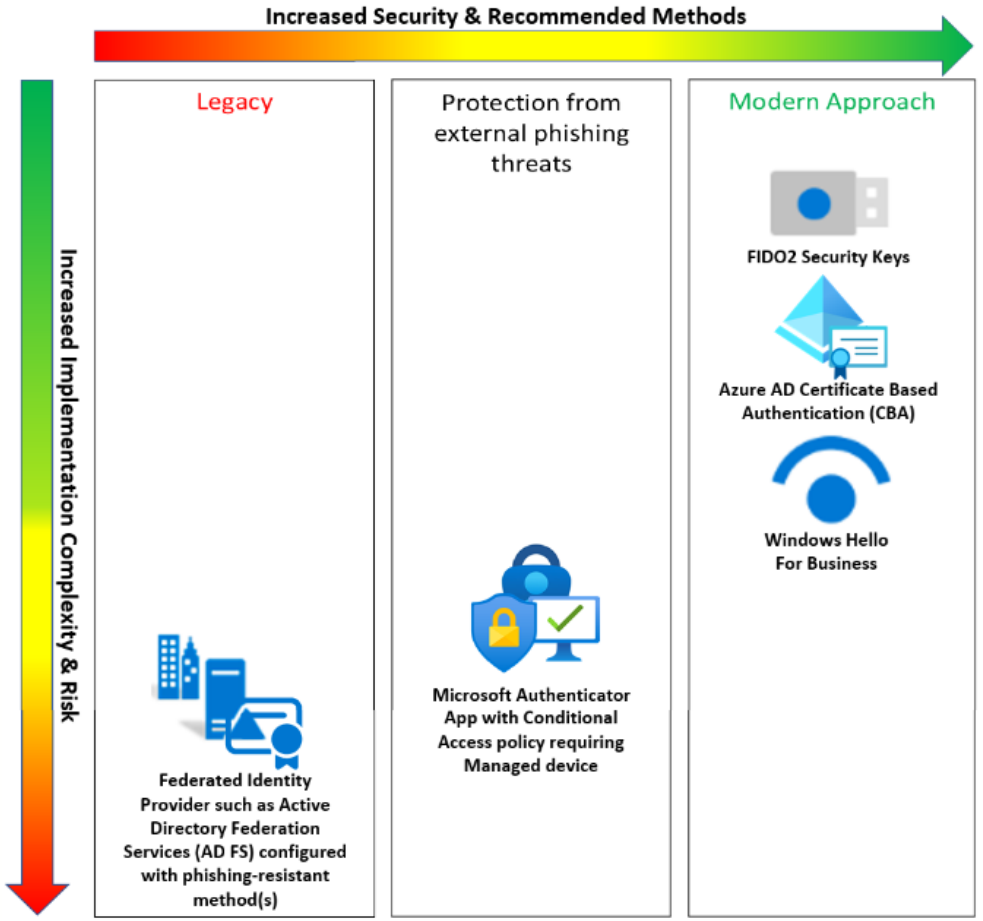
Strong Authentication

- Purpose-built for security
- No network connection, stored data, or client software required
- Highly phishing resistant

The Authentication Challenge

Most Methods are Phishable and Offer A Poor User Experience





yubico

Exec Order 14028

On May 12 2021, the Biden administration issued EO 14028 on “Improving the Nation’s Cybersecurity.”

This required adoption of zero trust frameworks within 60 days, and MFA within 180 days.

WHITE HOUSE

Administration Priorities COVID-19 Briefing Room

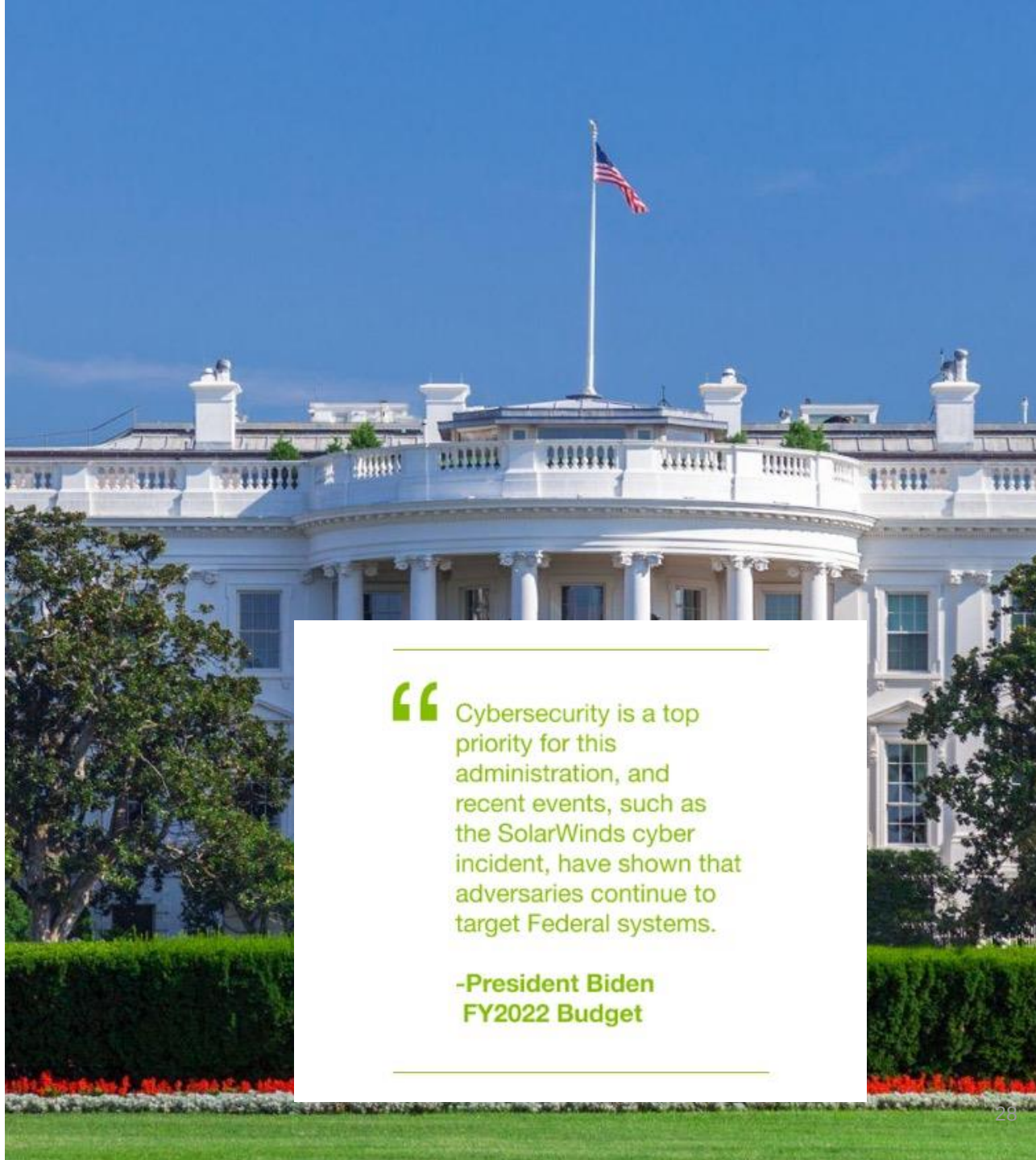
BRIEFING ROOM

Executive Order on Improving the Nation’s Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people’s security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The



> “Cybersecurity is a top priority for this administration, and recent events, such as the SolarWinds cyber incident, have shown that adversaries continue to target Federal systems.”
>
> **-President Biden FY2022 Budget**

OMB M-22-09

On Jan 26, 2022, the Office of Management and Budget (OMB) released a Zero Trust Strategy Memo

This sets a new baseline for access controls across the government that prioritizes defense against sophisticated phishing attacks.

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

January 26, 2022

M-22-09

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Acting Director

SUBJECT: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

This memorandum sets forth a Federal zero trust architecture (ZTA) strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024 in order to reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns. Those campaigns target Federal technology infrastructure, threatening public safety and privacy, damaging the American economy, and weakening trust in Government.

I. OVERVIEW

Every day, the Federal Government executes unique and deeply challenging missions: agencies[1] safeguard our nation's critical infrastructure, conduct scientific research, engage in diplomacy, and provide benefits and services for the American people, among many other public

> Agency staff, contractors, and partners, agency systems must discontinue support for authentication methods that fail to resist phishing, including protocols that register phone numbers for SMS or voice calls, supply one-time codes, or receive push notifications. That problem can be mitigated by providing those users with phishing-resistant tokens, including the PIV cards that agency staff and partners are generally issued.

The YubiKey

Modern authentication at scale

Easier to Use
One touch to authenticate

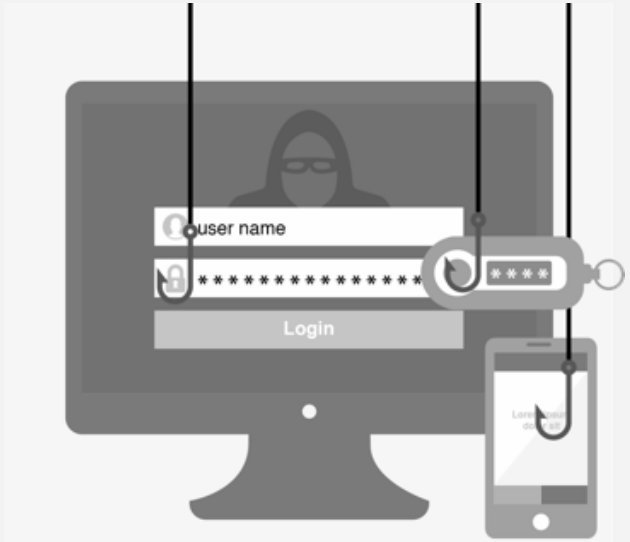
Stronger Security
Stops phishing and man-in-the-middle

Ubiquitous
One YubiKey to all systems

Quality & Standards
Industry best practice

Best TCO
Reduces IT support costs

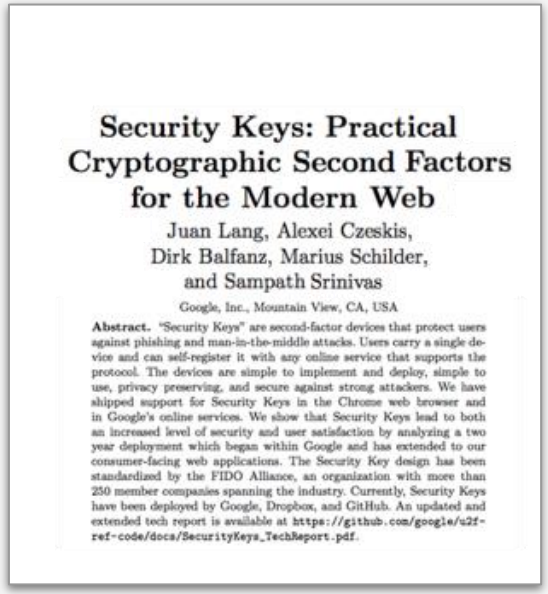
Best Total Cost of Ownership



Google

Problem:
One Time Password through Mobile Apps and SMS didn't stop phishing

Solution:
Google made YubiKeys mandatory for all employees, and optional for end-users



Security Keys: Practical Cryptographic Second Factors for the Modern Web

Juan Lang, Alexei Czeskis, Dirk Balfanz, Marius Schilder, and Sampath Srinivas

Google, Inc., Mountain View, CA, USA

Result:
Zero account takeovers
4X faster to login
92% support reduction
Zero failure rates

yubico

Best Total Cost of Ownership

https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html

Google

yubico

Top Business Scenarios

Privileged access

Secure privileged account users

Prevent account breaches

Mobile restricted

Secure call centers for mobile restricted users

Enable efficient log-in

Shared workstation

Protect shared workstation users

Enable efficient log-in, compared to mobile phone

Remote workforce

Enable remote workforce

Enable secure access from home

Office workers

Improve UX and security for office workers

Office 365

3rd party access

Protect corporate system access by 3rd parties

Protect IP, compliance

Customer base

Safeguard Yubico customers end customer

Secure their accounts

Quality and Standards

Secure production
Secrets controlled by customers.

Robust
Waterproof, crush safe, no batteries.

Compliance
FIPS, CSPN,DFARS, GDPR, PSD2, PIV, OATH, W3C, FIDO

The technology

The YubiKey - Easy, Fast, Reliable

YubiKey 5/FIPS Series

Multi-protocol

WebAuthn | FIDO2 | U2F | Smart card | Yubico OTP | OATH-HOTP | OATH-TOTP | OpenPGP | Static Passwords

YubiKey Bio

FIDO-only and Biometrics

WebAuthn | FIDO2 | U2F

Security Key NFC

FIDO-only

WebAuthn | FIDO2 | U2F

The YubiHSM2

Protecting secrets on servers

The Yubico Hardware Security Module is a small form factor networked HSM. If we are generating private keys on end user Yubikeys it makes sense to protect the private keys used to do this on hardware as well.

Offers a low cost, high security, small form factor, networked HSM for

- Root CA key protection
- Signing solutions
- Keys at rest protection
- Integration with MS-CA and EJBCA
- Easy to deploy
- Minimized design
- Affordable
- Secure chip and crypto processor
- FIPS 140-2 (level 3) Validated

The YubiHSM2 - features

Protecting secrets on servers

Extensive cryptographic capabilities
Modern algorithms and key lengths.

Role-based access controls for key management and key usage
Control which operations are done with keys, and by whom.

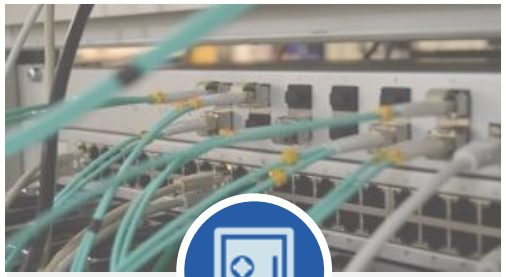
Network Shareable
Can be used by applications on other hosts.

Remote Management
Can be managed remotely.

The YubiHSM2

Protecting secrets on servers

Key protection



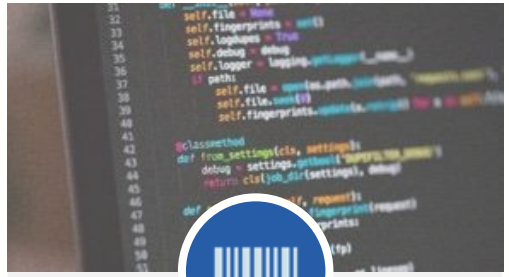
Safeguard your **smart card/PKI infrastructure**, CA- and database master keys from malicious attacks

Industry

a. Ensure supply chain integrity for your manufacturing plant

b. Enable secure IoT machine-to-machine communication

Software signing



Make sure to keep your software integrity solid and to enable tamper proof applications

Cryptocurrency

Enable a secure crypto ecosystem - protecting the exchange itself

YubiKey Multiple Protocol Support

FIDO2/U2F

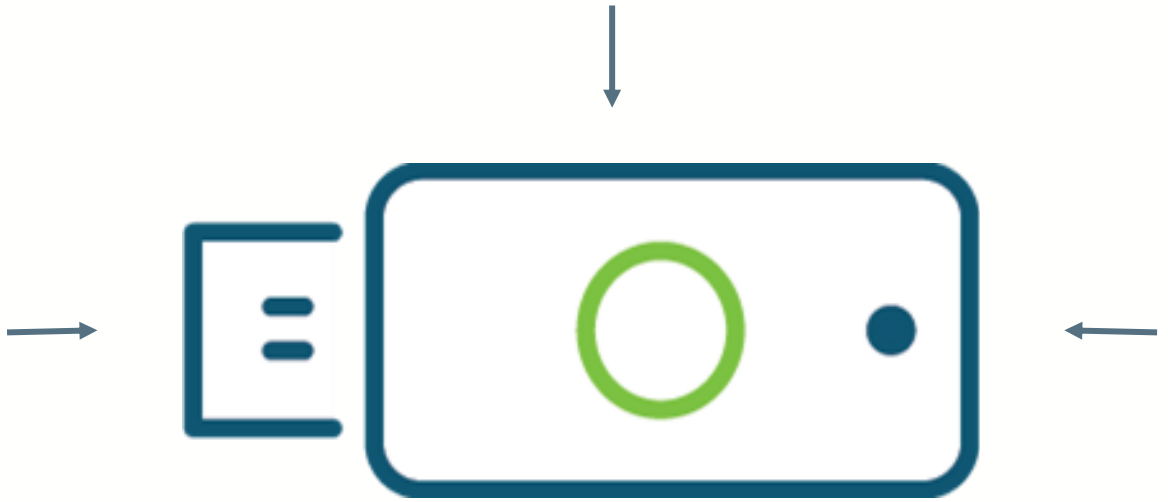
FIDO2 is an evolution of FIDO U2F and offers the same high level of security, with expanded authentication options such as Passwordless, 2FA and MFA.

Smart Card (PIV)

YubiKey provides baseline functionality to authenticate as a PIV-compliant smart card out-of-the-box on Microsoft Windows Server 2008 R2 and later servers, and Microsoft Windows 7 and later clients.

OpenPGP

OpenPGP is an open standard for signing and encrypting. It enables sign/encrypt operations using a private key stored on a smartcard (such as YubiKeys), through common interfaces.



OATH (TOTP/HOTP)

HOTP and TOTP are the two main standards for One-Time Password:
HOTP: Event-based One-Time Password
TOTP: Time-based One-Time Password

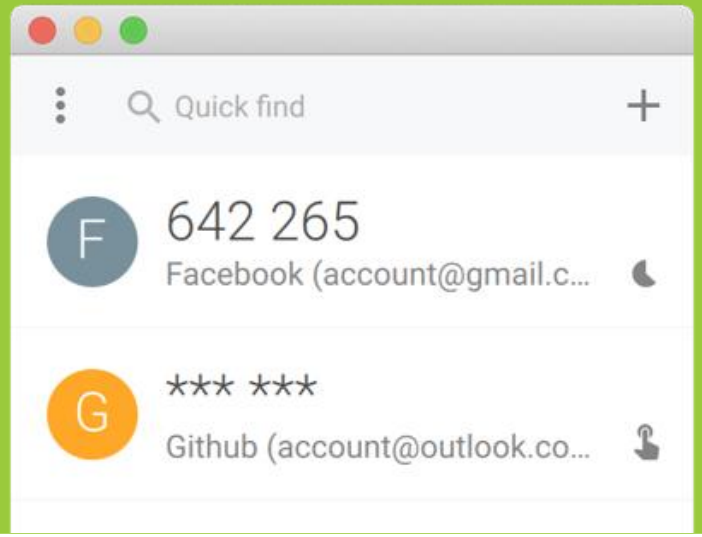
Slot 1 & 2

Yubico OTP
OATH-HOTP
Challenge-Response
Static Credential

Yubico Authenticator

The safest authenticator app experience across mobile and desktop

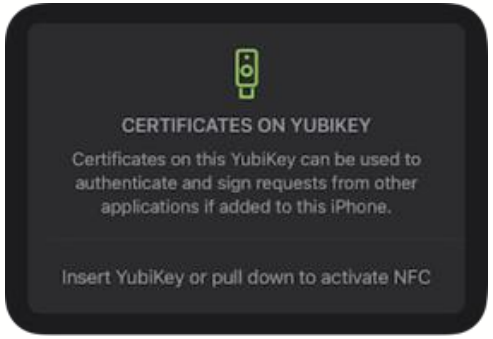
Windows Linux iOS Android mac OS



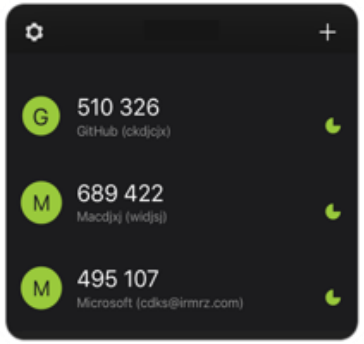
Hardware backed security

Portable credentials across devices

Easy and fast setup



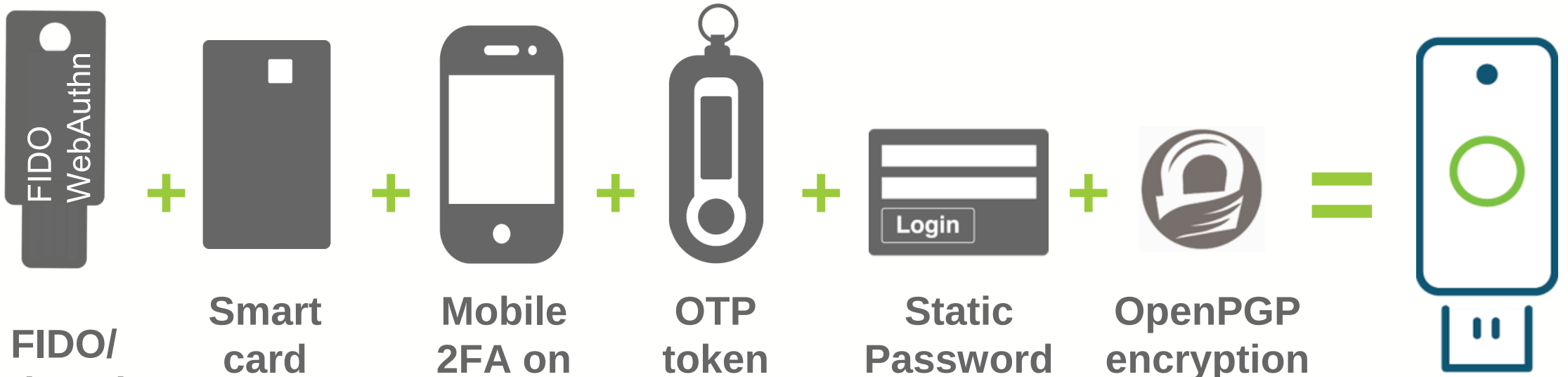
Smart card support On iOS



Secure multiple accounts

Six security features in one

- Use YubiKey as a stronger alternative or complement to other authentication solutions
- Seamless path from legacy to next generation authentication



FIDO/ WebAuthn device | **Smart card** | **Mobile 2FA on key** | **OTP token** | **Static Password** | **OpenPGP encryption**

Cryptography

OTP

Symmetric key crypto

Uses a single, shared secret between sender and receiver to both encrypt and decrypt the message.

Smart Card (PIV)

Public-key infrastructure (PKI)

Verifies and authenticates parties involved using a system of digital certificates, Certificate Authorities, and other registration authorities.

U2F / FIDO2

Public-key crypto (PKC) / Asymmetric crypto

Uses two keys, a public key to encrypt messages and a private key to decrypt them.

Common Use Cases

OTP

- VPN
- Client apps
- Web portals
- Password managers

Smart Card (PIV)

- Computer logon
- Admin access
- All employee access (current)
- VPN
- Encryption tools

U2F / FIDO2

- Cloud applications
- Web applications
- Computer login Windows 10+ (FIDO2)
- Password managers

Advantages

OTP

- YubiOTP / HOTP: No client software needed / Keyboard Interface
- OATH-TOTP: Need Yubico Authenticator
- Works with all OS/platforms
- Supports legacy systems
- Easy to implement

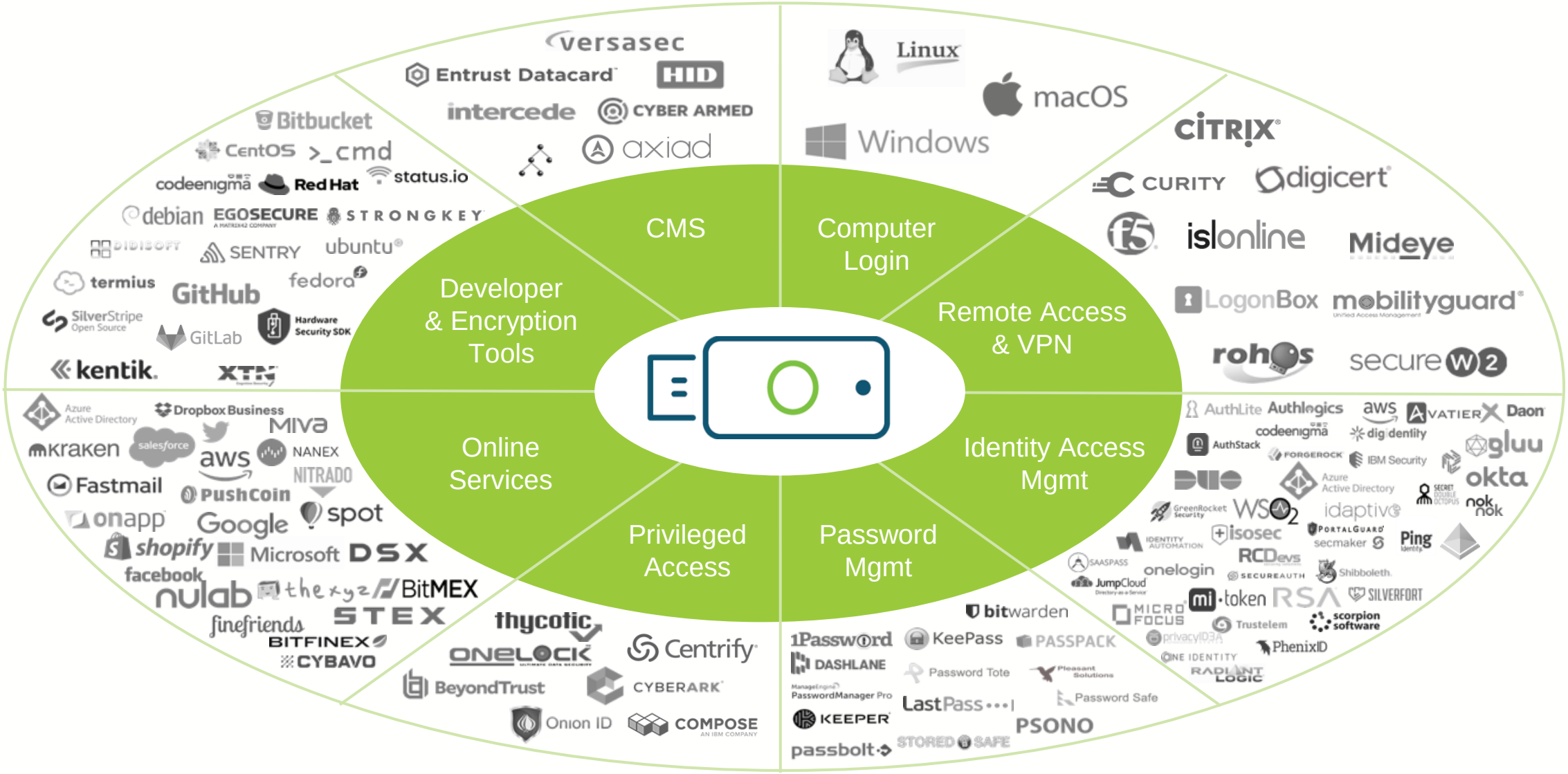
Smart Card (PIV)

- Improved form factor compared to traditional smart card
- No smart card reader needed
- Smart card touch - user presence needed to activate
- Touch-to-sign - user presence needed to digitally sign code

U2F / FIDO2

- High security
- High privacy
- Low overhead
- Frictionless user experience
- No drivers
- Self-register with various services
- Supports biometrics

Yubiquity: one key protecting 700+ apps



"View the complete list of verified services/apps that work with Yubico products on https://www.yubico.com/works-with-yubikey/catalog/"

FIDO2 & Phishing resistance

FIDO2 Overview

New open authentication standard offering new authentication choices

1960s
Usernames and passwords

2014
FIDO U2F
Phishing-resistant second factor

yubico Google

2019
FIDO2/WebAuthn
Phishing-resistant

Second factor

Multi-factor/ Passwordless

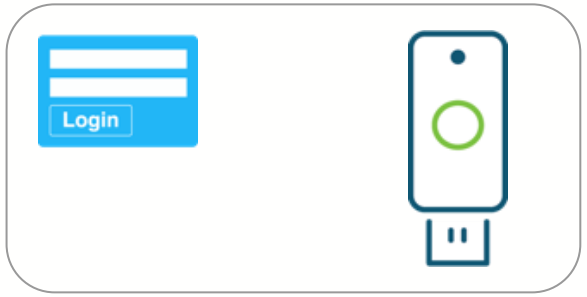
2022
PassKeys

Multi-factor/Passwordless (hardware bound/syncable)

Google Microsoft

FIDO2 Overview

New open authentication standard offering new authentication choices



Two Factor: Password + Authenticator

Second factor in a two factor authentication solution

Multi-Factor: Password + Authenticator or PIN or Biometric

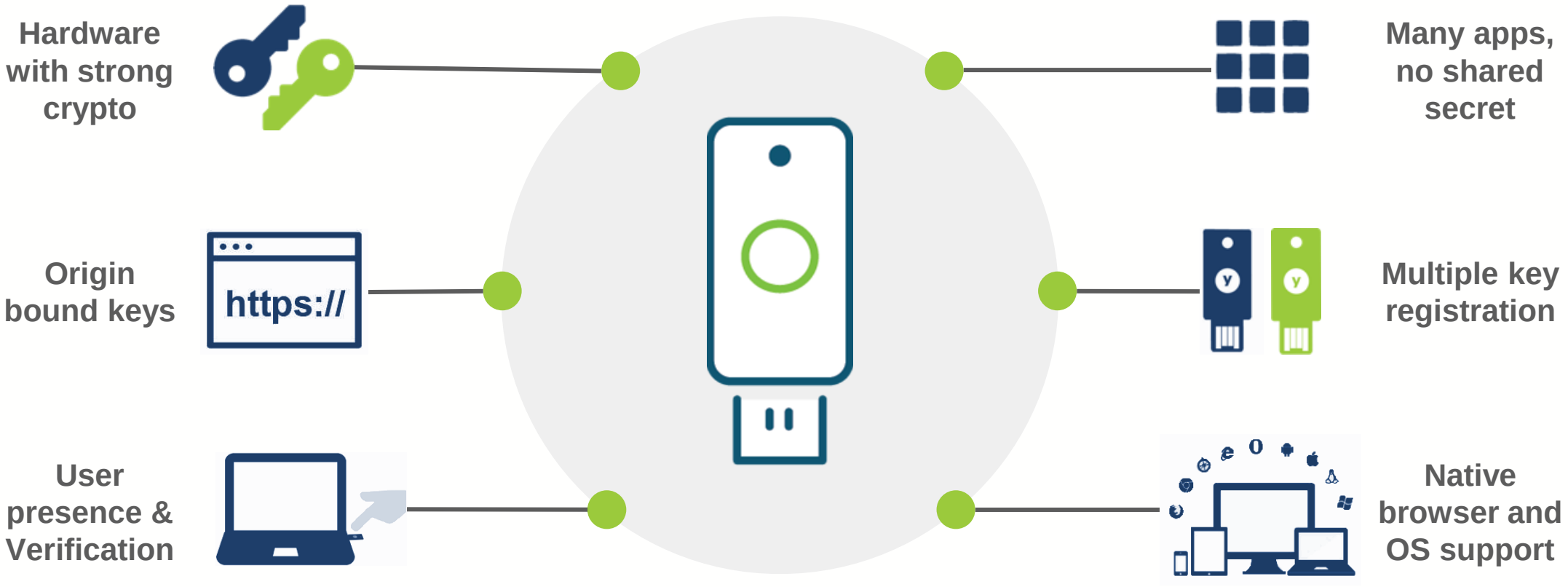
Multi-factor with combination of a hardware authenticator with touch, PIN, or biometric

Passwordless

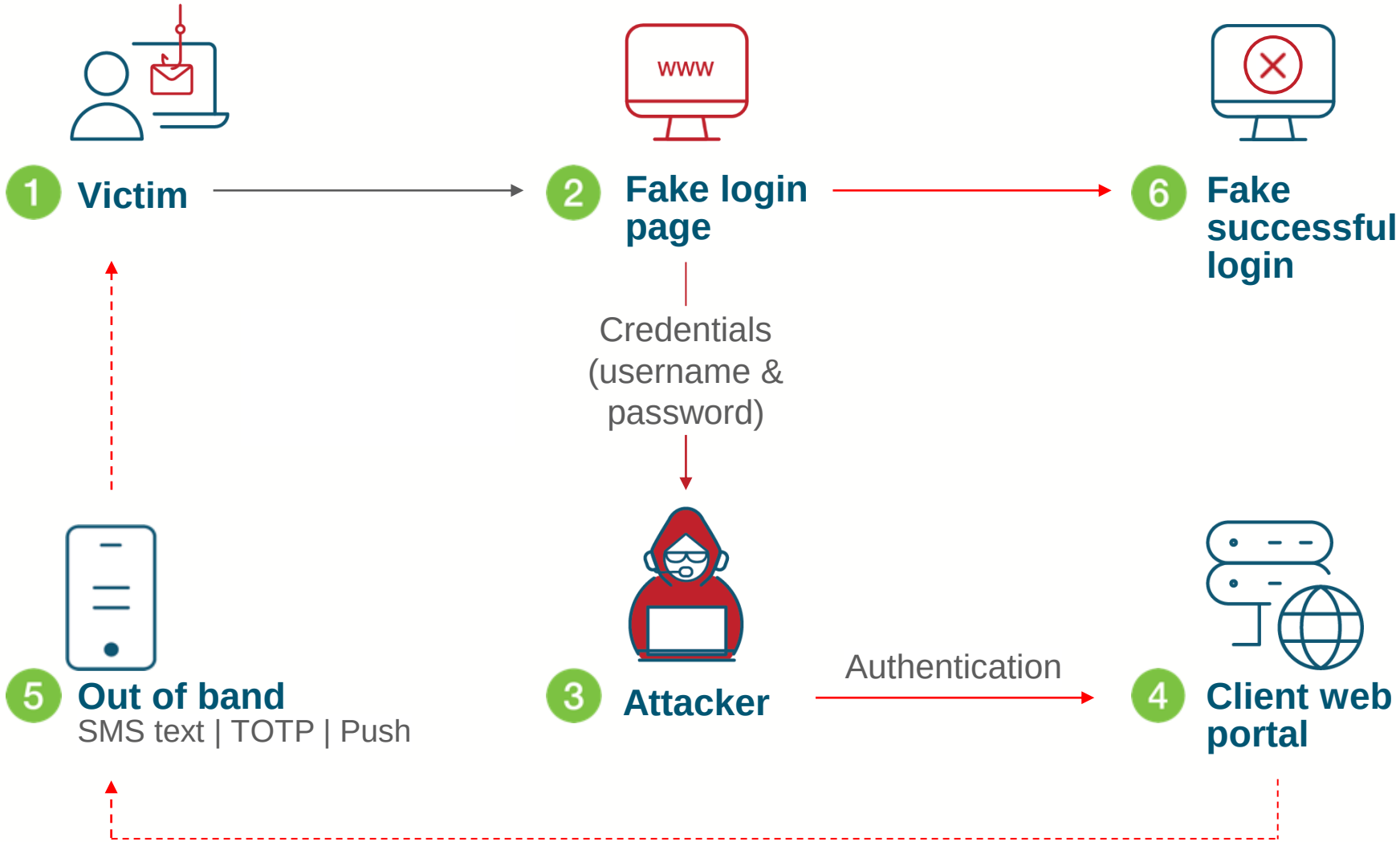
Replaces passwords completely with strong authentication for a secure authentication experience that is also very easy to use

FIDO2 and Passwordless

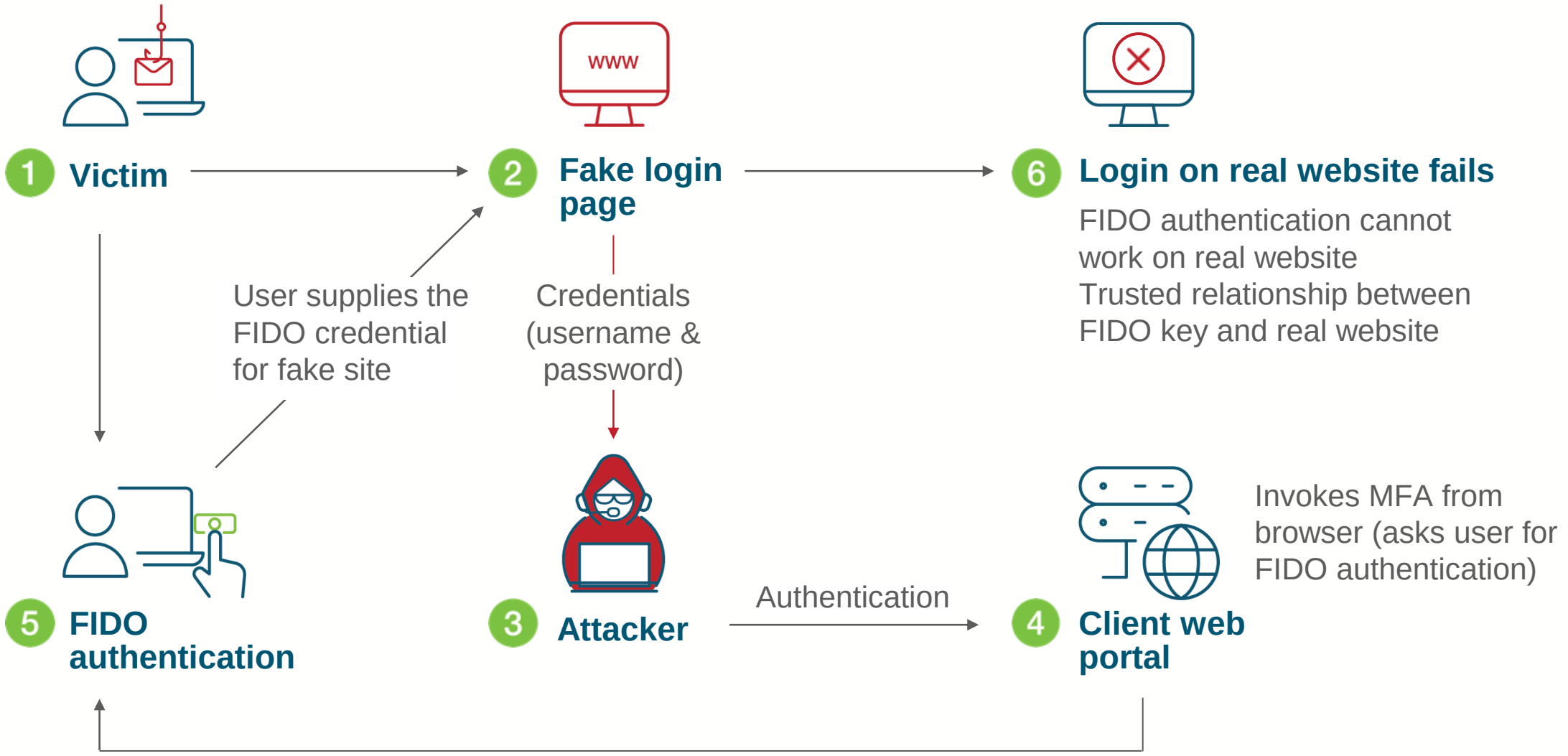
New open authentication standard offering new authentication choices



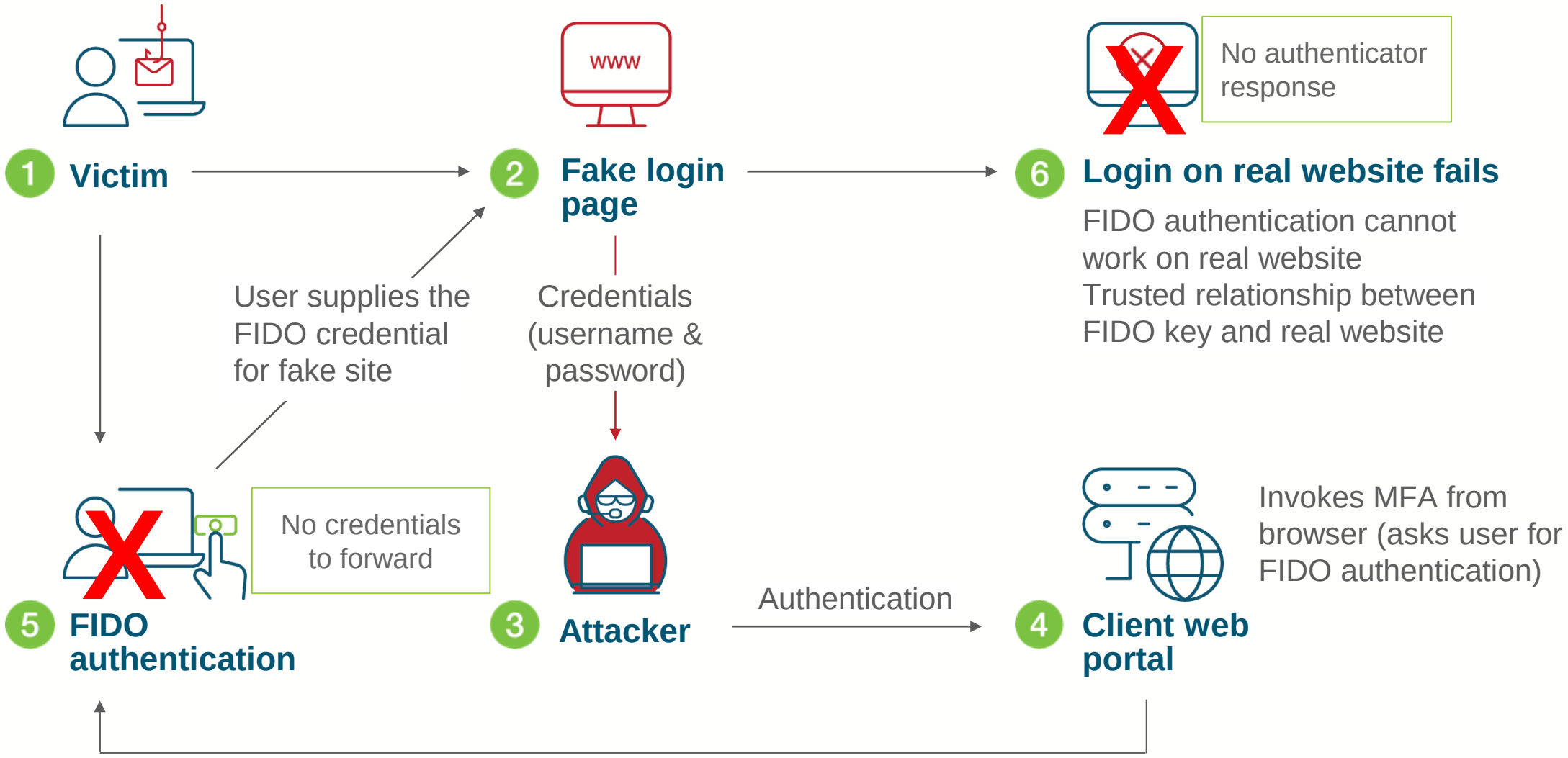
FIDO2/PIV provide phishing resistance



FIDO2/PIV provide phishing resistance



FIDO2/PIV provide phishing resistance



FIDO2 example deployment

Hyatt - MS Azure AD, EndPoint Manager, Autopilot + FIDO Security Keys

1 IT configures:
Autopilot profile
Temporary Access
Pass (TAP)

Intune

2 IT communicates
Azure AD information to
Hardware distributor
for PC setup

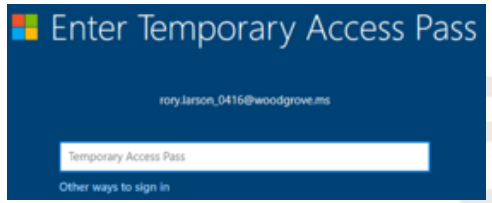
Hardware distributor
uploads device IDs

3 Devices are shipped
directly to user
together with the
FIDO security key

Colleague unboxes
PC, turns it on
and connects it
to the internet

4 Devices
automatically
join Azure AD,
enroll in Intune

User logs
in via TAP



5 User registers
the FIDO security key
… and off they go!

Product Summary

YubiKey Summary - Product Portfolio

	YubiKey 5 Series Multi-protocol series for organizations	**Bio & Security Key Series** FIDO series for individuals and organizations	**YubiKey 5 FIPS Series** Built for government and highly-regulated organizations	**YubiHSM 2** World's smallest HSM for highly-security conscious orgs
Passwordless	●		●	
Multi-protocol (OTP, U2F/FIDO2, Smart Card)	●	FIDO2, U2F only	●	●
Server Protection			●	

YubiKey Summary - The Yubico Platform

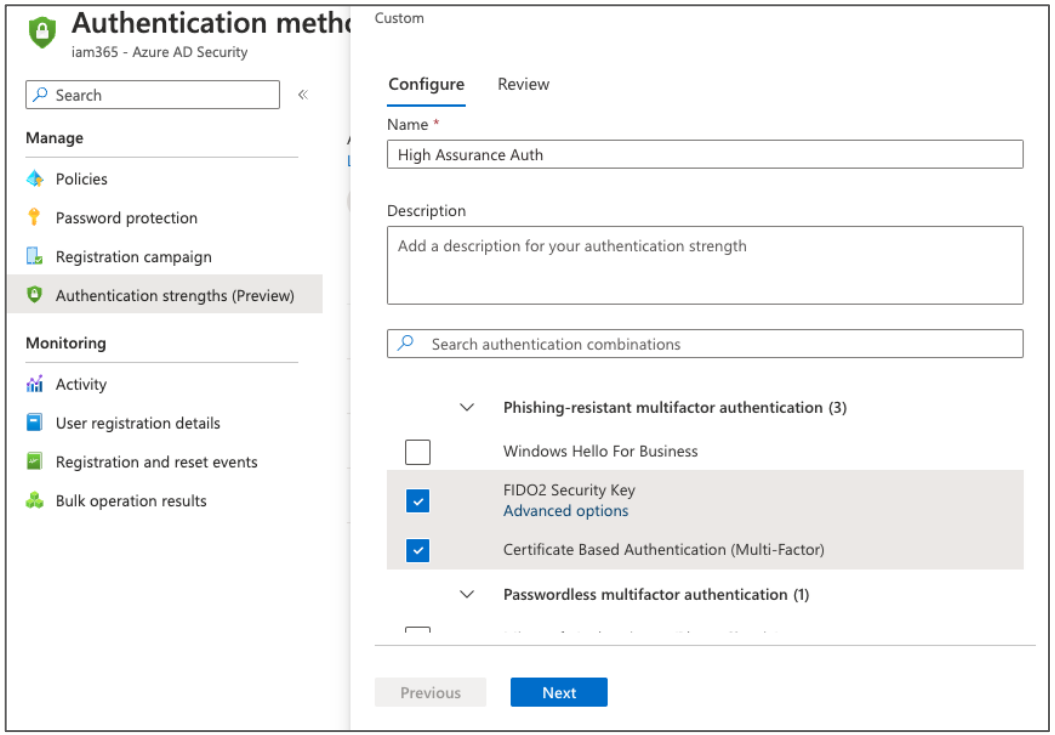
Services	Support	Customization	Subscription	
Integrations	Open source servers	SDKs, libraries, APIs	3rd party	YubiCloud validation
Certifications	FIPS, CSPN (BSI cross certification coming)			
Software features	**Driverless OTP** Yubico OTP, OATH	**Public Key** PIV smart card, OpenPGP, FIDO, WebAuthn	**Yubico Authenticator** for desktop and mobile	**HSM SDK**
Hardware form factors	 Authenticators	 Bio	 HSM	

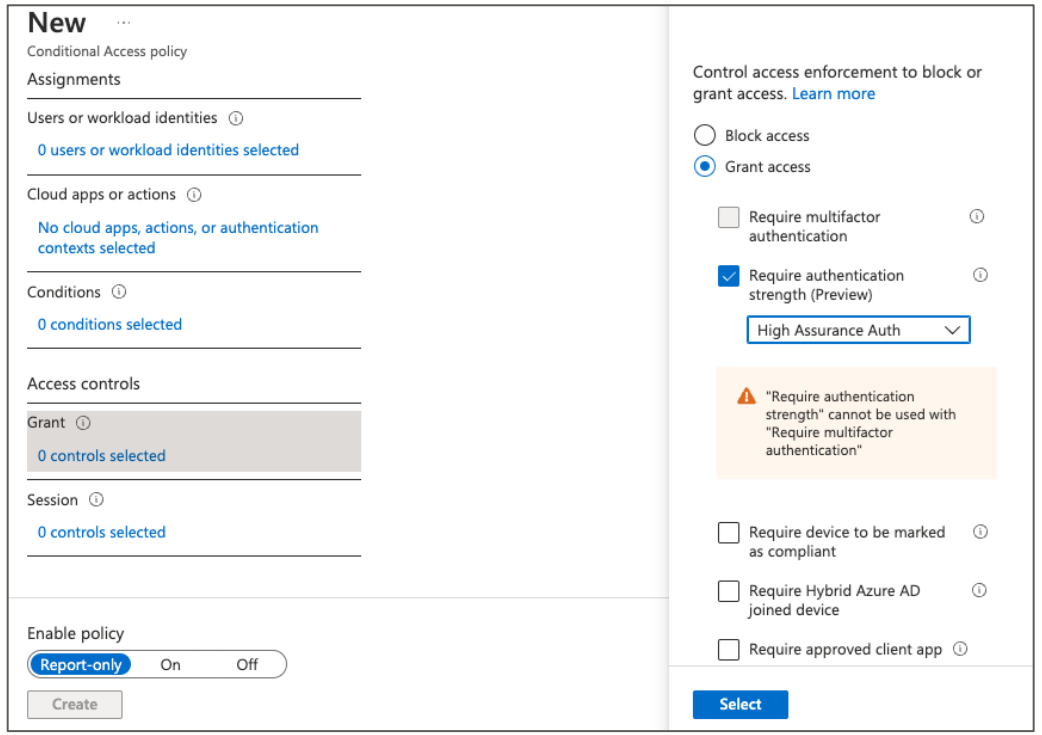
Deeper look at MS Passwordless

New Shiny Things

Latest updates and improvements

- **CA Authentication Strengths, ie enforce FIDO/CBA only**
  - Definable authentication strength requirements





New Shiny Things

Latest updates and improvements

- **Certificate Based Authentication**
  - Direct certificate authentication to Azure, no need to federate
  - Supports desktop login for AAD joined Win 10 and 11 devices
  - Meets MFA requirements in Conditional Access
  - Supported on iOS in native apps and with MS Auth app for MS apps
- **WebauthN support for RDP**
  - Win 10 and 11 clients support WebauthN passthrough
  - Server side is 2022 currently
  - Web based support, not supported for login or in apps currently
- **AVD support for FIDO**
  - Supported for sign-on and redirect to session

YubiKey 5 features and use cases

Multi-protocol suite addresses large range of requirements

WebAuthn, FIDO2, U2F

Use Cases:
- Authentication
- Single sign-On
- Enterprise & Consumer

Smart Card Credential

Use Cases:
- AD/ADFS/RDP CBA
- Digital Signatures
- Encryption

TOTP

Use Cases:
- MFA
- RADIUS
- VPN

One-Time Password

Use Cases:
- IAM services
- 3rd party
- Legacy

SSH

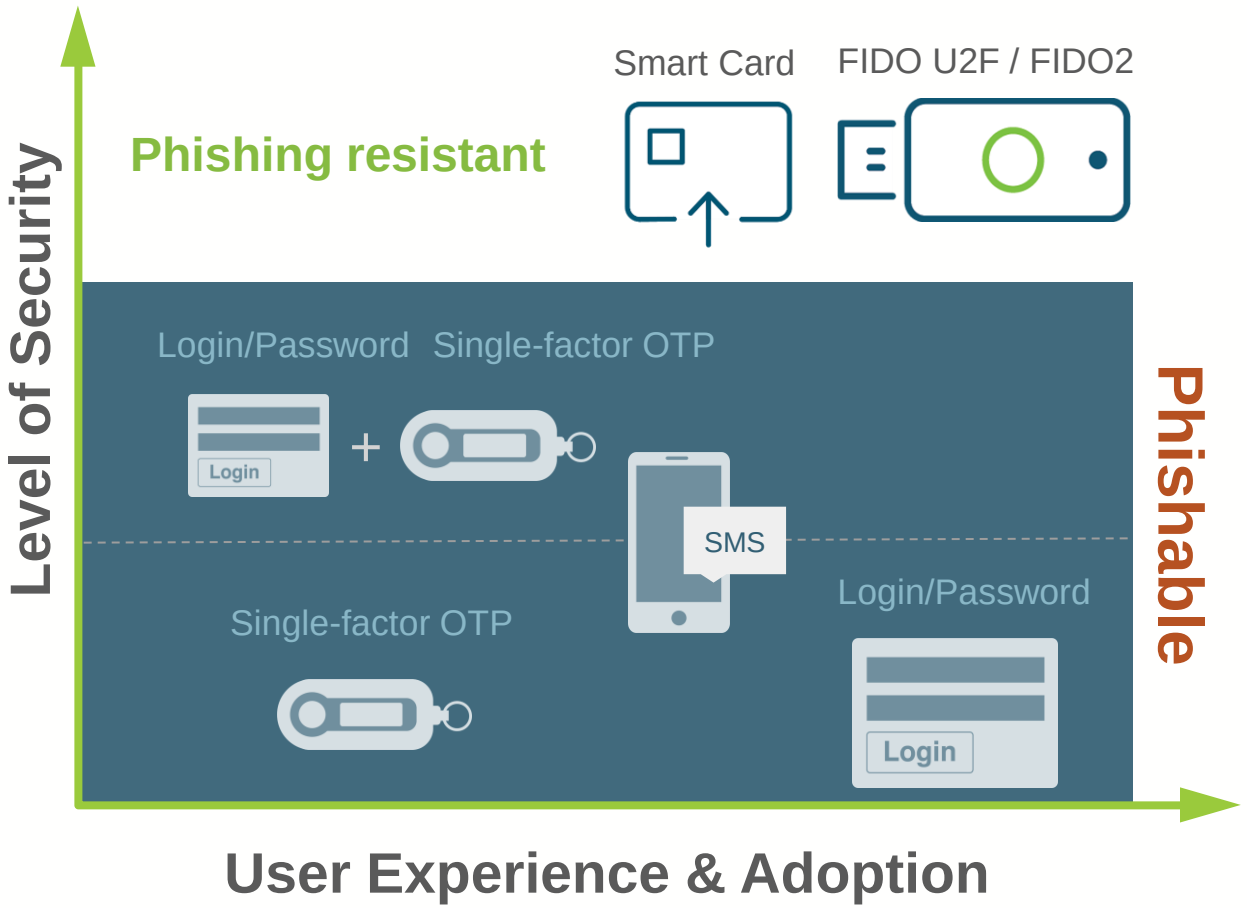
Login

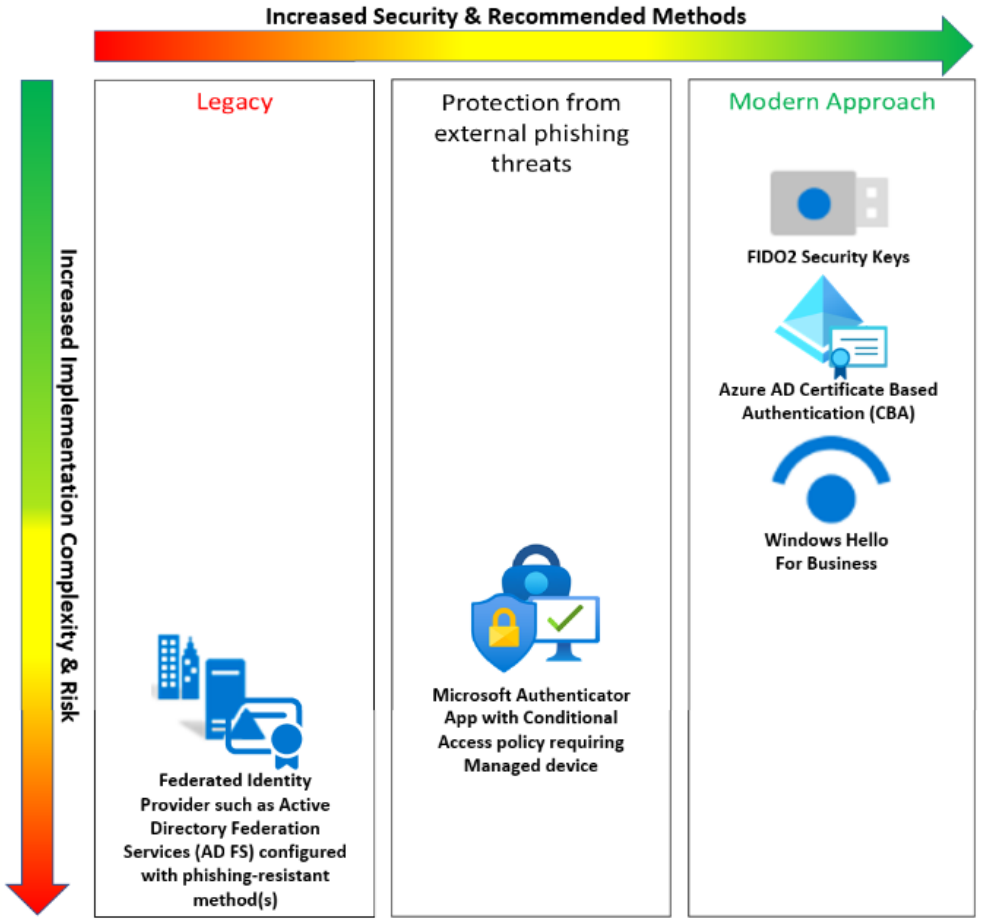
...

Other use cases include PGP, HMAC C/R, threshold signatures, key escrow, disk encryption.

The Authentication Challenge

Most Methods are Phishable and Offer A Poor User Experience





YubiKey and Microsoft

Helping customers migrate, enhance, evolve

1. OTP Authentication
2. Certificate Authentication
3. Passwordless Authentication With FIDO2
4. Hybrid Authentication With FIDO2

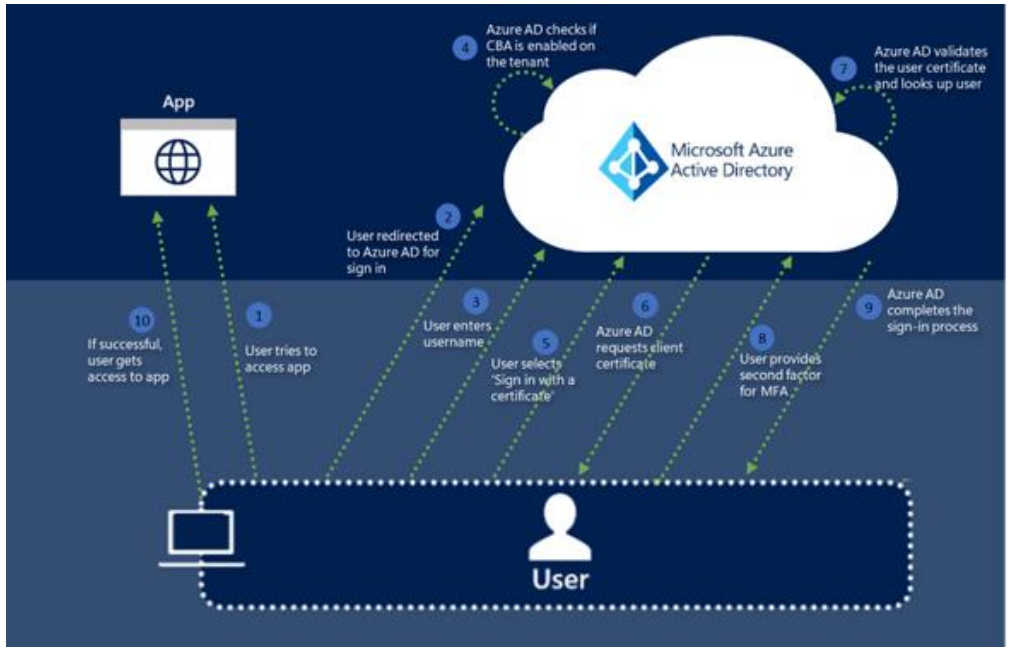
Four Authentication Options Covering:

MFA, Smart card, Federation, Passwordless

YubiKey and Microsoft

Helping customers migrate, enhance, evolve

- Direct certificate auth to Azure now in preview
- Previously needed to federate
- Allows smoother migration from on-prem auth to cloud
- Latest Win10/11 release supports direct desktop login and SSO
- https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-certificate-based-authentication



YubiKey and Microsoft

Office 365

Cloud native and wants to achieve:

- Web authentication

Azure AD is bundled with Office 365, thus Office 365 customers can enable Passwordless.

M365 backend is Azure AD and includes Office 365.

Azure AD

Wants to use Azure AD as IDP:

- Desktop authentication (Windows 10/11 only)
- Web authentication to federated apps and services

Supported platforms include Azure AD joined:

- Windows 10 v1903 or higher for Webauthn
- **PREVIEW - Certificate Based Authentication**

Hybrid Azure AD

(AD + AAD)

Wants to extend Azure AD passwordless to allow SSO to on-prem resources such as applications and file shares:

- Desktop authentication (FIDO2 or Smart Card)
- Web authentication to federated apps and services

Supported platforms include Azure AD joined:

- Windows 10 v1903 or higher for Webauthn

Hybrid Azure AD

- Windows 10 v2004 or higher

On-prem AD only

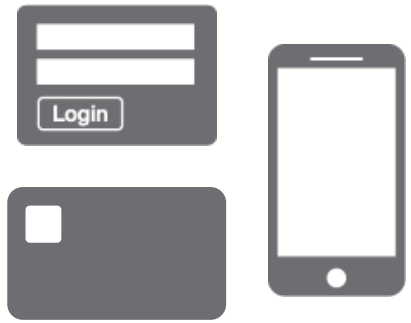
Has older Windows machines or Macs and wants to deliver the same passwordless experience (with PIN)

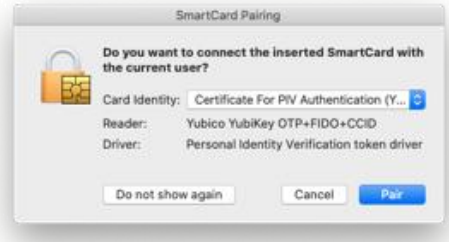
*Not a candidate for FIDO2 Passwordless, but...

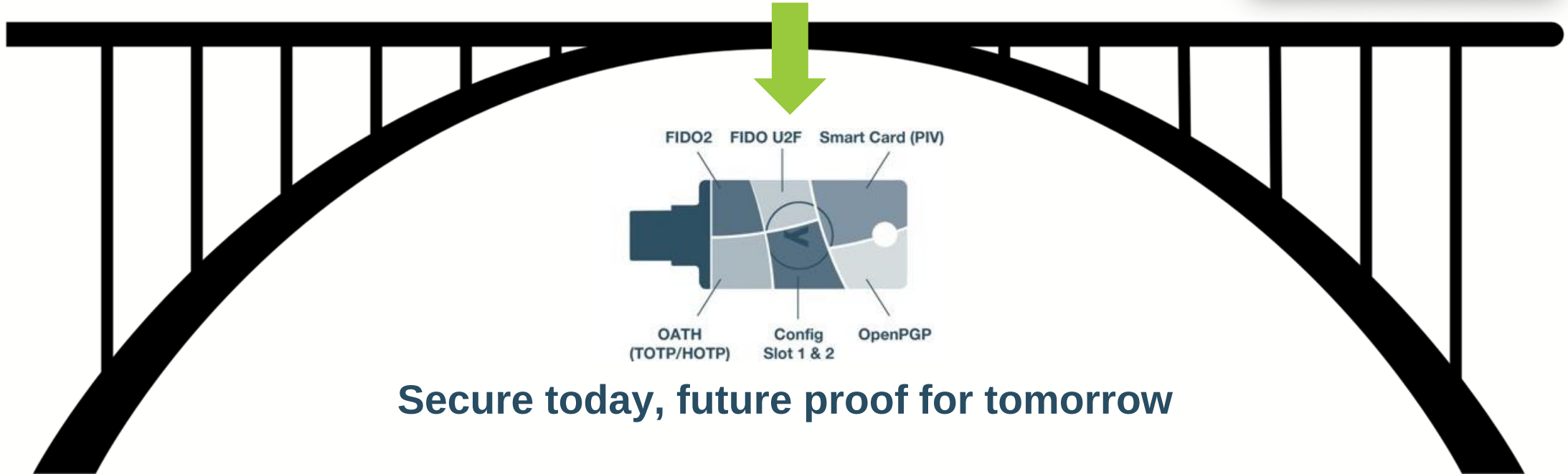
Great candidate for passwordless with AD + smart card. Also ideal for legacy apps, Macs, etc.

YubiKey as the ‘Passwordless Bridge’

Helping customers migrate, enhance, evolve







Secure today, future proof for tomorrow

yubico

Microsoft and Yubico passwordless

	Windows Hello Platform	Microsoft/Yubico Authenticator Software	PIV + FIDO2 Security Keys Hardware
			
Use case	• Office workers with dedicated PC • Leverage the security of the TPM • FIDO2 certified	• Good Solution for mobile/non-PC users • Can be used to bootstrap Windows Hello for Business	• Shared workstations, first line workers and mobile restricted • Backup/break-glass strong method for Admins - bootstrap Windows Hello
User experience	• Microsoft's 1st passwordless experience • Sign in using a PIN or biometric recognition with Windows devices	• Sign in using a mobile phone with biometric scanner, or PIN • YubiKey as MFA 2nd factor	• Sign in using FIDO2/PIV security device - access device based on organization controls and authenticate based on PIN or biometrics

Microsoft and Yubico passwordless

Windows Hello
Platform

- Information workers with dedicated PC
- Leverage the security of the TPM
- FIDO2 certified

Authenticate with Windows Hello for Business

- Simplify login process (no username / password)
- Multi factor by nature (ownership of computer + PIN/biometrics)
- Based on asymmetric secrets

Add YubiKey

- **Bootstrap new (OOBE) device with YubiKey & AutoPilot**
- User credential becomes portable (not tied to one computer)
- Enrolling of Windows Hello on a device becomes easier, no need for complex enrollment process
- In case of PC failure, user can rapidly provision another device with near zero downtime
- Presence of a TPM in the device becomes irrelevant
- Ideal zero-trust scenario, since the credential container is now portable and does not rely on the physical computer as the perimeter

Microsoft and Yubico passwordless

Microsoft Authenticator
Software

- Good Solution for mobile/non-PC users
- Can be used to bootstrap Windows Hello for Business

Authenticate with Microsoft Authenticator App

- Simplify login process (no password)
- Multi factor by nature (ownership of phone + PIN/biometrics)
- Based on asymmetric secrets

Complement with YubiKey Authenticator

- Use the YubiKey as the Root of Trust to quickly and securely provision users on a new device
- Adds extra level of security to standard MFA for auth or bootstrapping registrations of FIDO2
- Can be bulk enrolled and activated (Powershell)
- Eliminates reliance on phone battery and coverage

Microsoft and Yubico passwordless

PIV + FIDO2 Security Keys
Hardware

- Shared workstations, first line workers and mobile restricted
- Backup/break-glass strong method for Admins - bootstrap Windows Hello

Win10 shared device MFA options

FIDO2/PIV Hardware key	Windows Hello	Microsoft authenticator
Unrestricted	Compliments	

- Gives authentication mobility
- Not tied to device or browser
- Cross platform
- Up to 10 YubiKeys can be registered per user for FIDO2
- Compliments WHfB but does not require WHfB to be deployed
- Bridges other authentication protocols

Passwordless - Enablement and delivery

Deployment Considerations

Platforms

Windows 10/11 login

- AADJ Only - Win 10 1903+
- Hybrid - Win 10 2004+
- Not for BYOD login scenarios (MSA)*
- No Mac login support for FIDO2 just PIV

Web authentication (cross platform)

- Edge, Safari, Chrome etc

Mobile support

- MS mobile apps + MS App + CBA
- iOS Mail etc support smart card
- Can’t login via mobile browsers via FIDO2*
- Can register YubiKey via mysignins on iOS

Experience

User Experience

- Need to enter PIN or Biometric
- PIN/Bio enforced by Windows/Azure
- No tap and go (e.g. in retail)

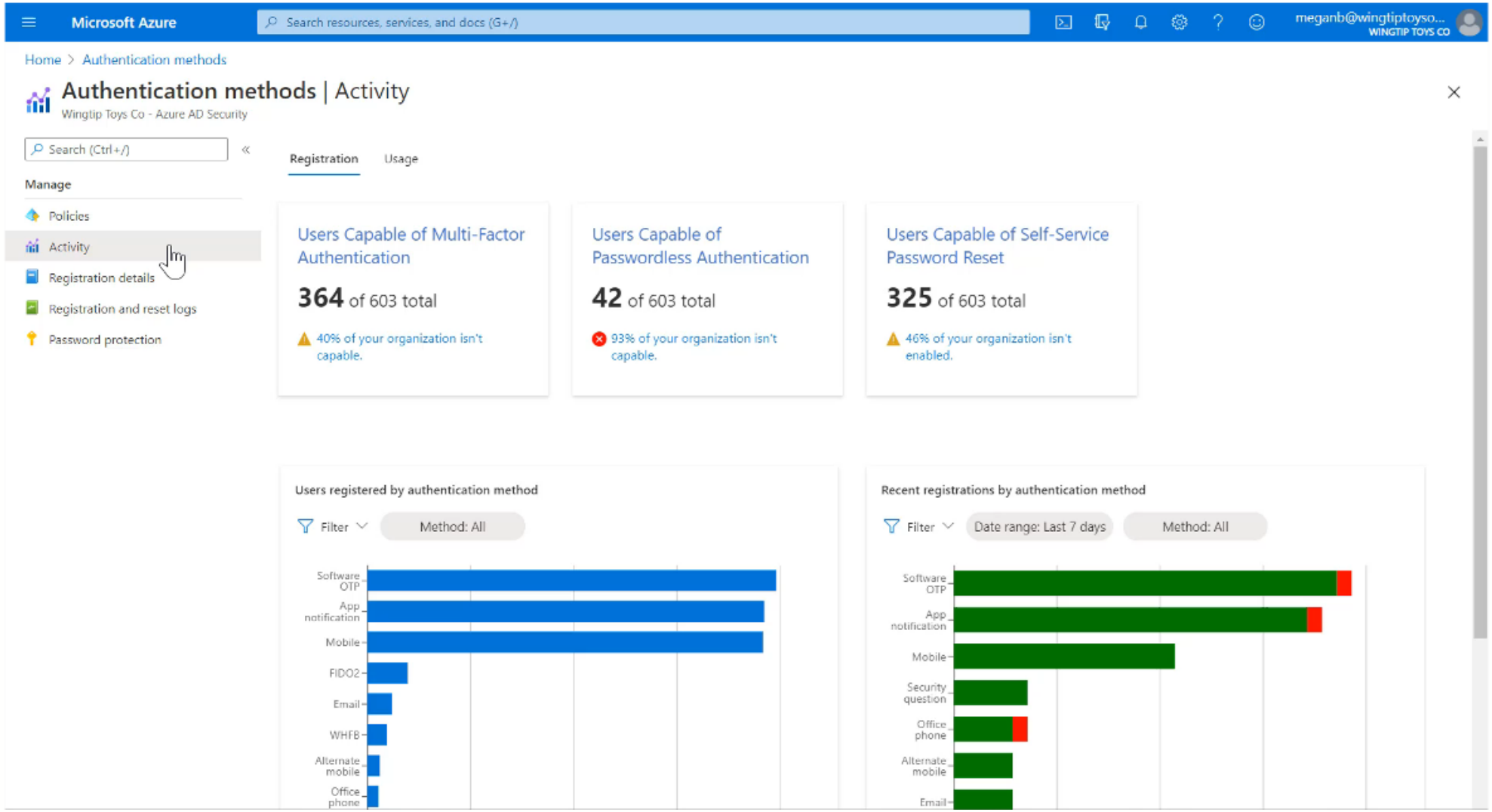
Enrollment

- Currently only self enrol as an option
- Currently no force PIN change*
- Deployment of TAPS eases user flow
- CBA meets MFA requirements

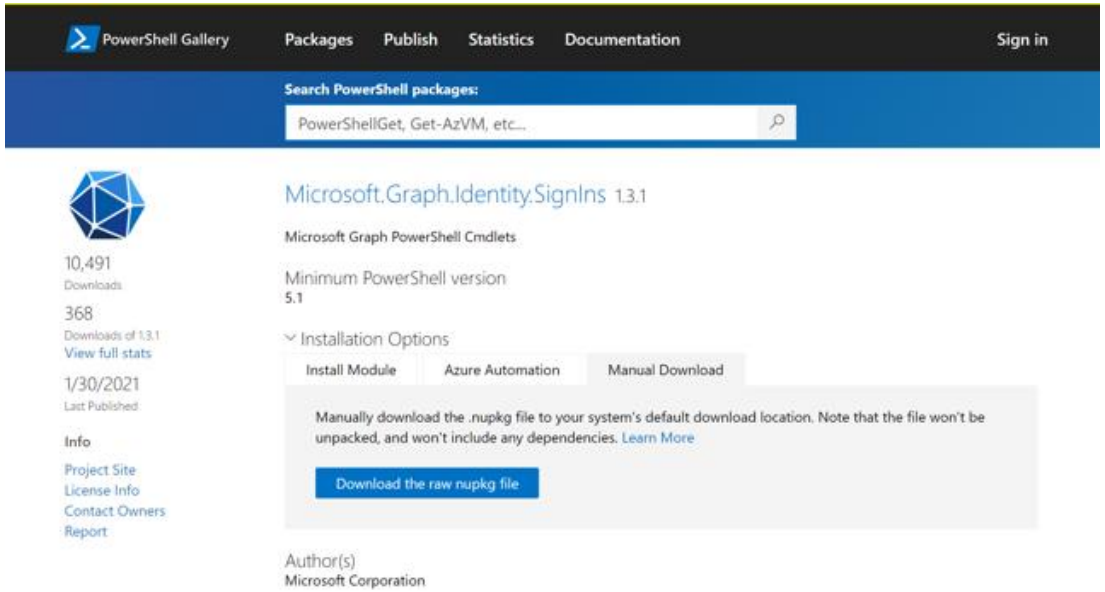
* coming?

72

Reporting & Insights for Auth Methods



API resources



- **Authentication Methods Policies**

Azure AD auth policy API

- **Authentication Methods**

Azure AD auth methods API

- **Temporary Access Pass**

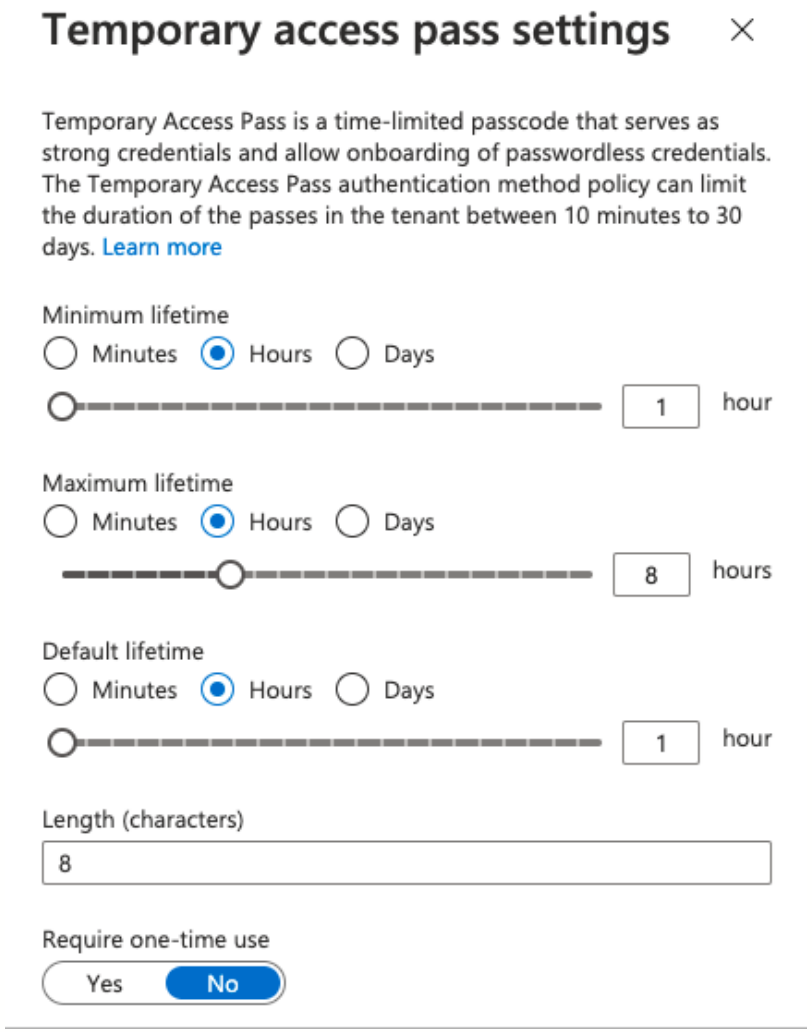
Azure AD TAPS methods API

- **PowerShell**

PowerShell Gallery | Microsoft.Graph.Identity.SignIns

Temporary Access Pass

Enabling full passwordless flow

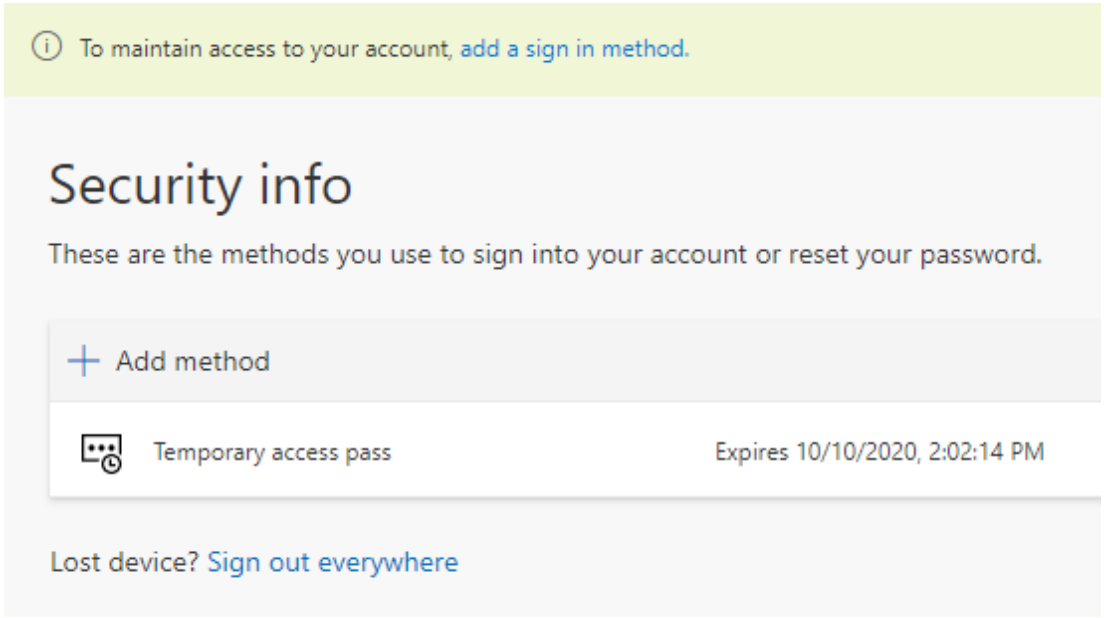


- Scoped to users and groups
- Set a duration and start time
- One-time use or multi-use
- Configurable in the Azure AD portal and in Microsoft Graph
- Satisfy MFA requirement

Temporary Access Pass uses

Enabling full passwordless flow

Register	**A FIDO2 Security key**
Register	**Phone Sign-in**
Bootstrap	**WHfB/OOBE/Mobile/MacOS**
Recover	**Access to your account (Passwordless and MFA)**



Enablement Areas

- FIDO2/CBA enabled in tenant
- Device login enabled
- User self enrollment
- Full passwordless flow (TAPS and CBA)

Enable Tenant

Set method specific settings for FIDO2, CBA and TAPS

Configure your users in the authentication methods policy to enable passwordless authentication. Once configured, you will need to enable your users for the enhanced registration preview so they can register these authentication methods and use them to sign in.

Method	Target	Enabled
FIDO2 Security Key	All users	Yes
Microsoft Authenticator		No
Text message (preview)		No
Temporary Access Pass	All users	Yes
Certificate-based authenti...	All users	Yes

Method	Target	Enabled
FIDO2 Security Key	All users	Yes

Details

Save Discard

ENABLE

Yes / No

USE FOR:

- Sign in
- Strong authentication

TARGET

All users / Select users

Name	Type
All users	Group

GENERAL

Allow self-service set up

Yes / No

Enforce attestation

Yes / No

KEY RESTRICTION POLICY

Enforce key restrictions

Yes / No

Restrict specific keys

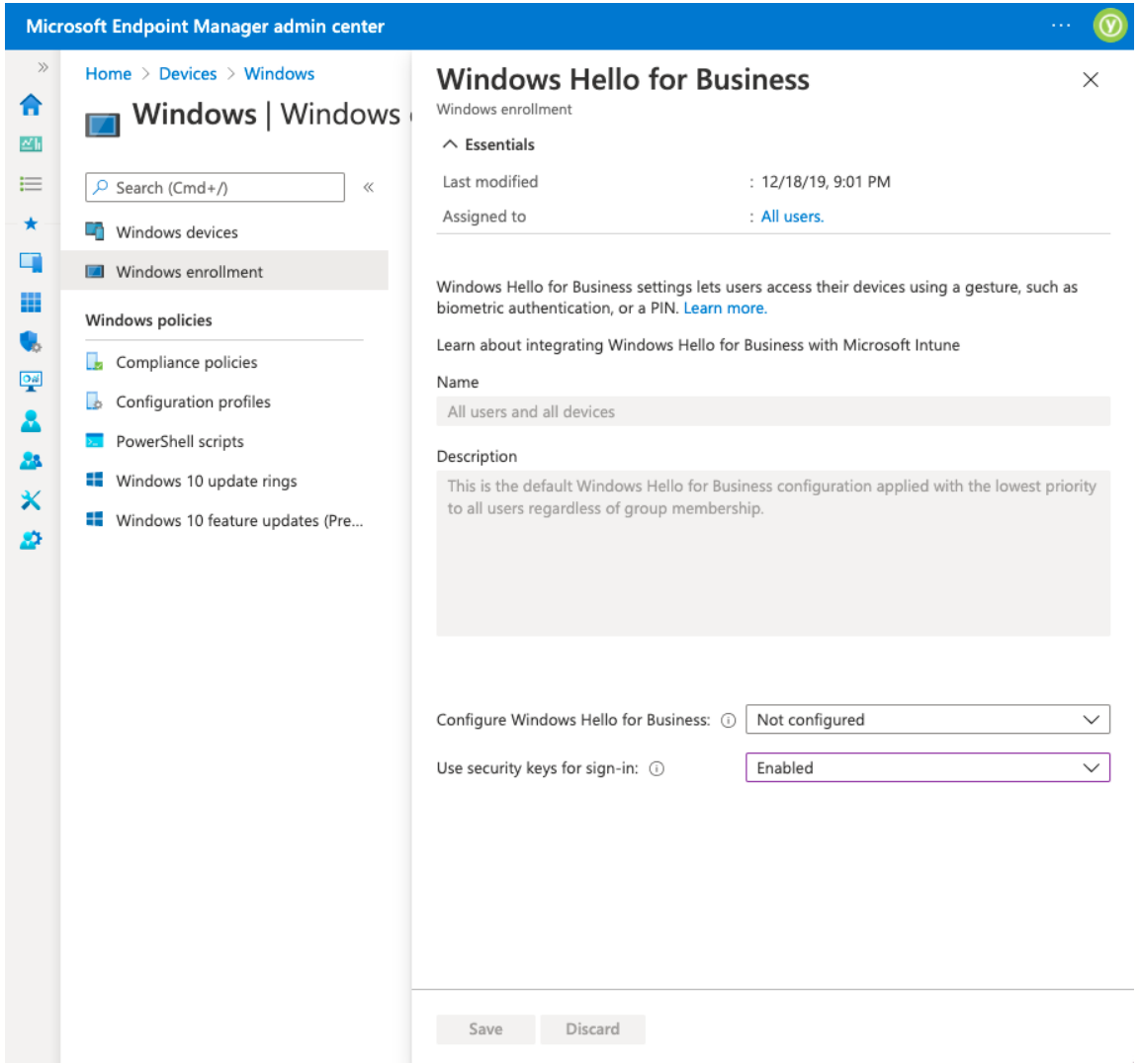
Allow / Block

Add AAGUID

No AAGuids have been ad..

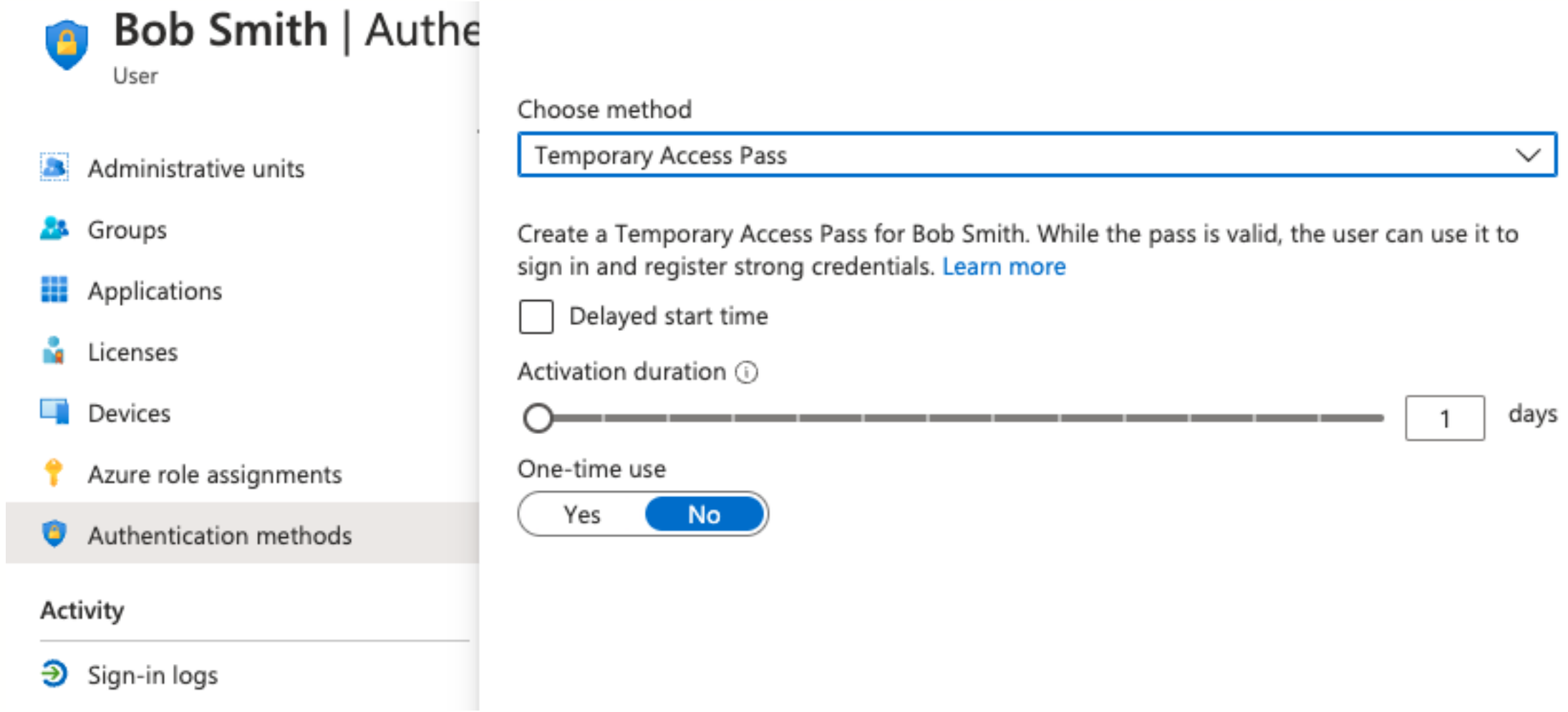
Enable device login

Endpoint Manager or Provisioning package for desktop login



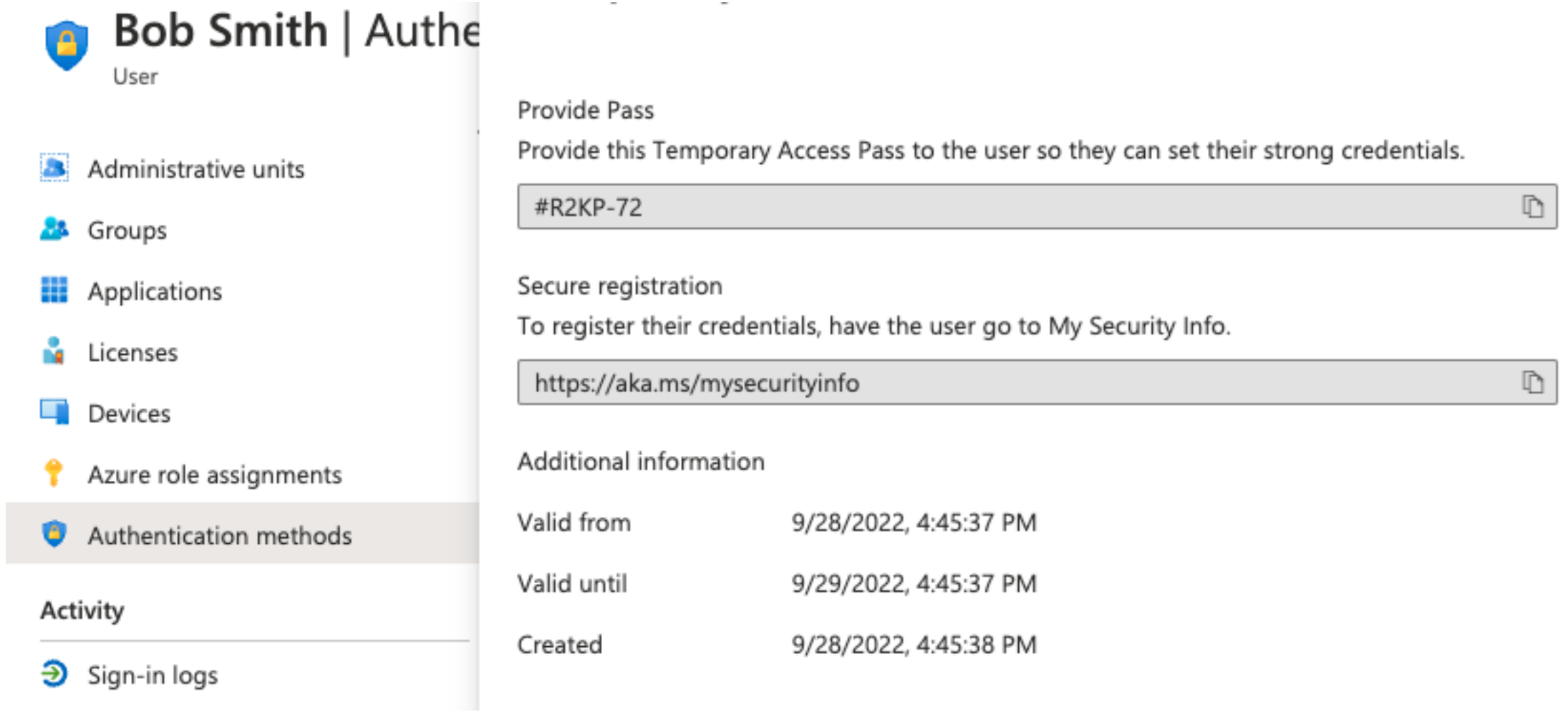
User enrollment

Create a Temporary Access Pass for the user



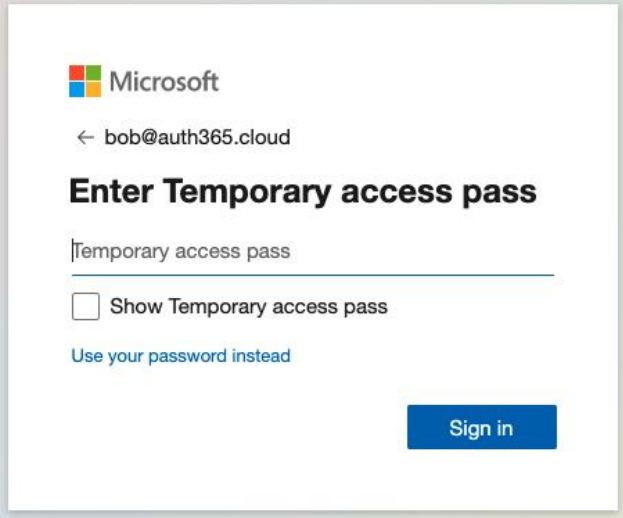
User enrollment

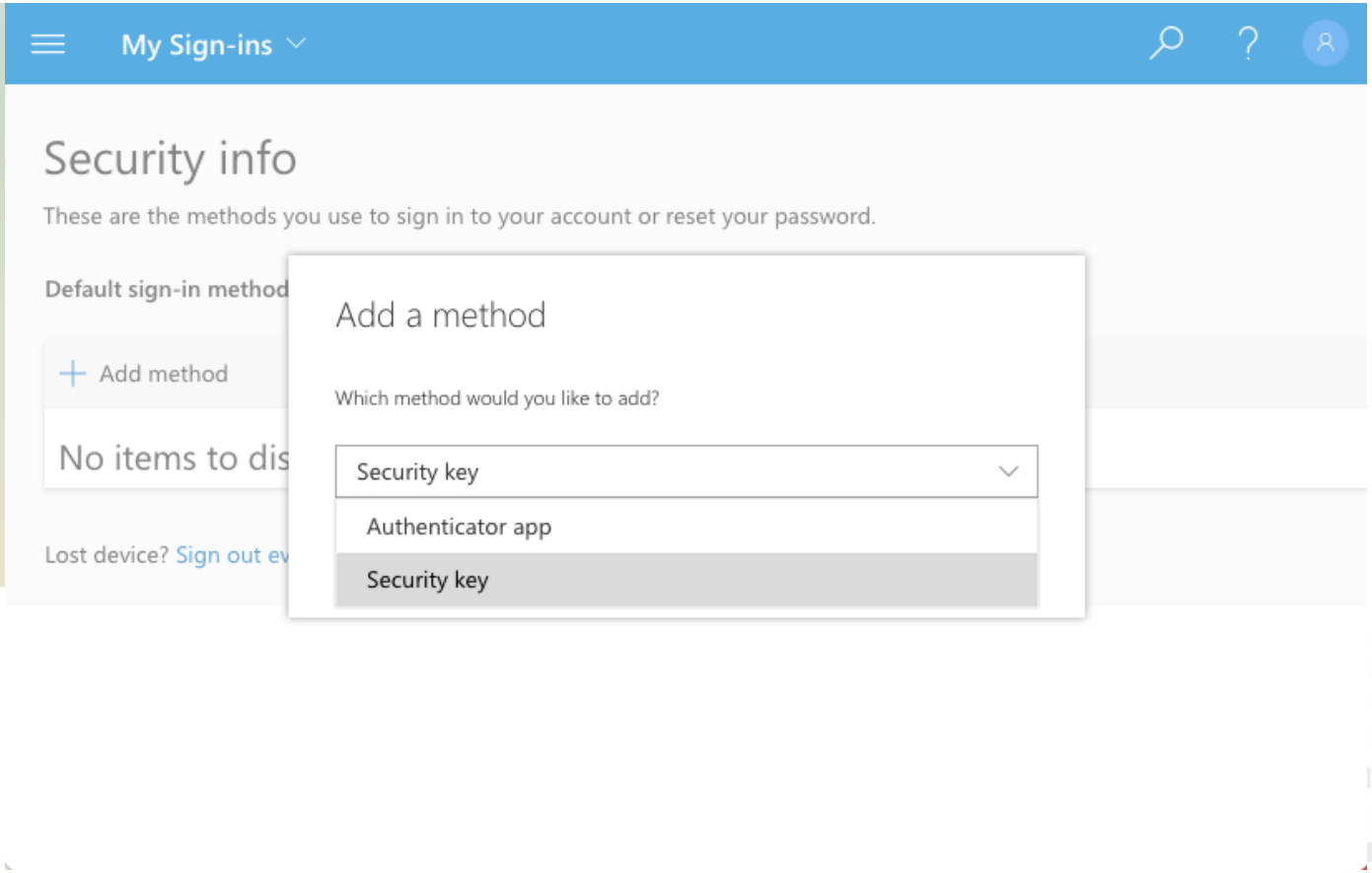
Create a Temporary Access Pass for the user



User enrollment

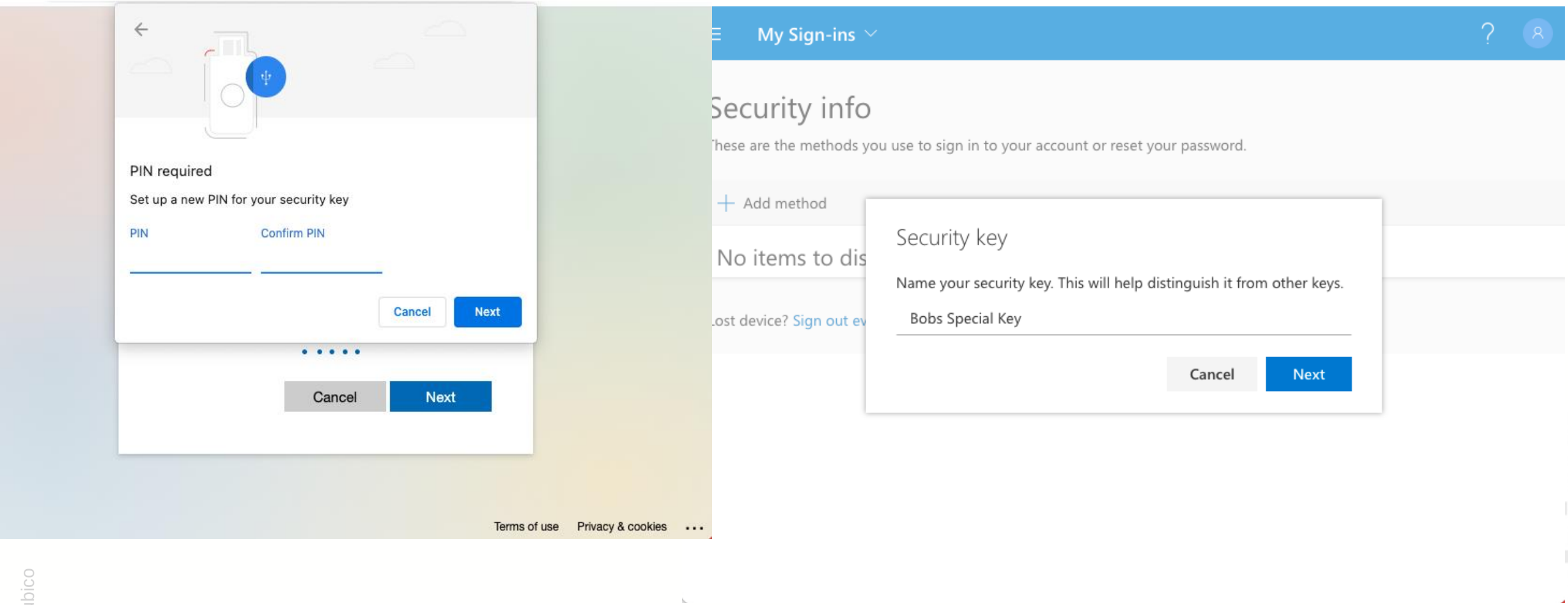
User enrolls in self-service portal - https://mysignins.microsoft.com





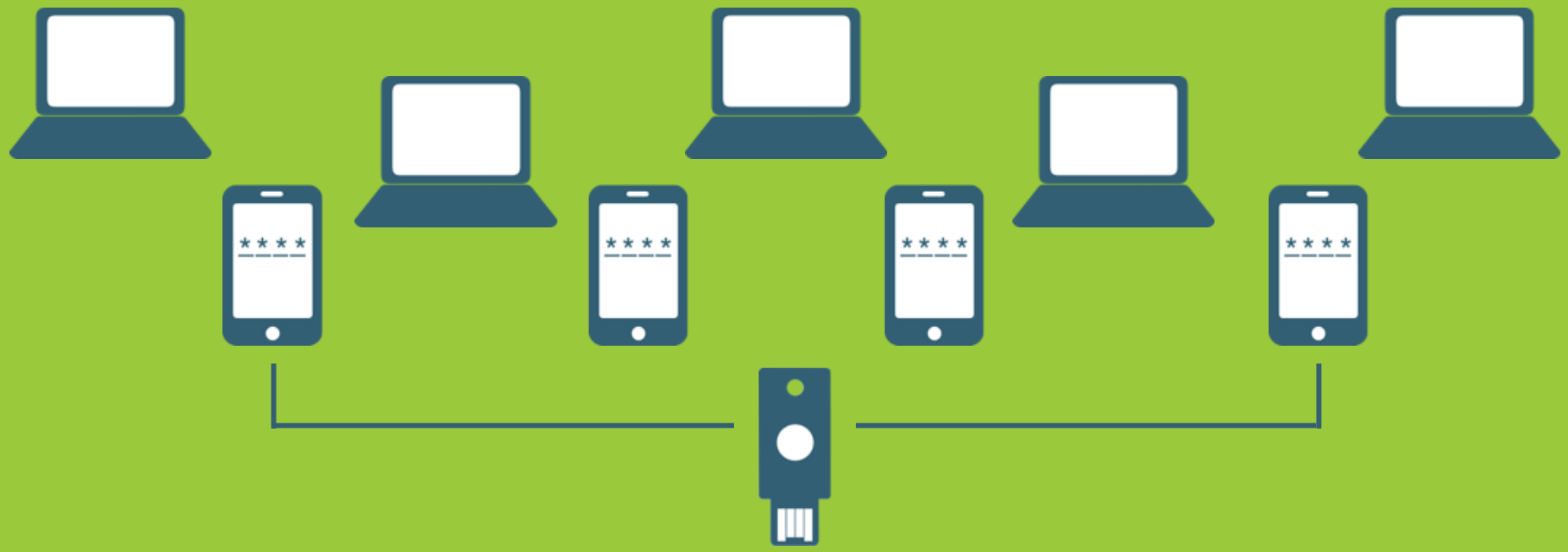
User enrollment

User enrolls in self-service portal - https://mysignins.microsoft.com



The YubiKey - Simplified Authentication

Multi-device Access



Portable Root of Trust for Multiple Devices
Securing Desktops, Websites and Services

yubico