

Passwordless Authentication in (Azure) Active Directory

Mgr. Michael Grafnetter

@MGrafnetter
dsinternals.com

26. 3. 2020

Agenda

- Passwordless Authentication Overview
- Microsoft Authenticator
- FIDO2
- Windows Hello for Business
- Choosing The Right Technology



Passwords
Are
Dead



Passwords Are Difficult to Remember



Rob Price 
@robaeprice

Follow



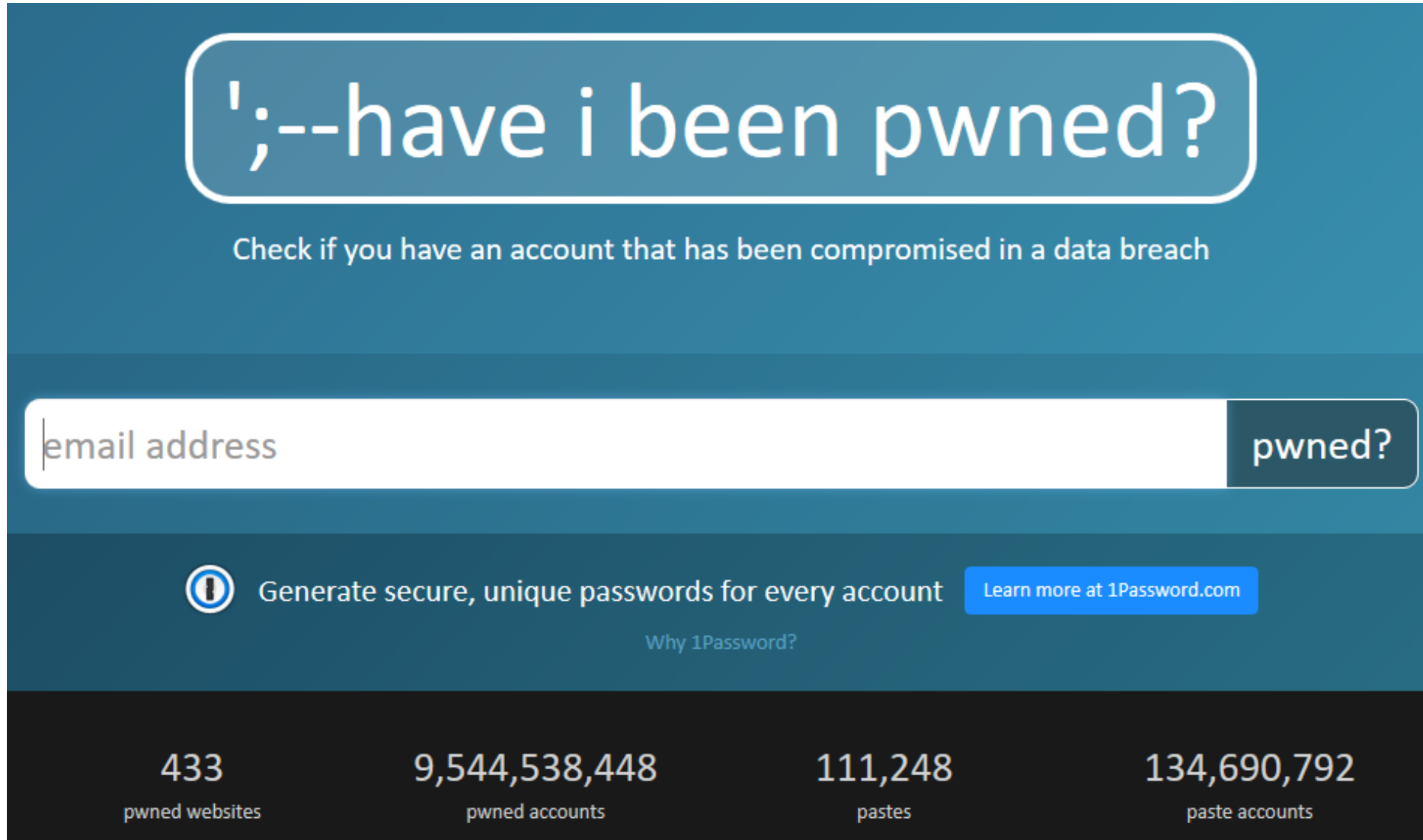
A password for the Hawaii emergency agency was inadvertently published in an **@AP** photo in July 2017 after being written on a post-it note.

uk.businessinsider.com/hawaii-emergen ...



8:27 PM - 16 Jan 2018

Passwords Are Exposed in Data Breaches




The image shows the homepage of the 'have i been pwned?' website. At the top, the title 'have i been pwned?' is displayed in a large, white, rounded box. Below it, a subtitle reads 'Check if you have an account that has been compromised in a data breach'. A search bar with the placeholder text 'email address' is positioned below the subtitle, followed by a 'pwned?' button. Further down, there is a section for 1Password, featuring an information icon, the text 'Generate secure, unique passwords for every account', and a blue button labeled 'Learn more at 1Password.com'. Below this is a link 'Why 1Password?'. The bottom of the page features a dark blue footer with four statistics: '433 pwned websites', '9,544,538,448 pwned accounts', '111,248 pastes', and '134,690,792 paste accounts'.

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

email address pwned?

 Generate secure, unique passwords for every account [Learn more at 1Password.com](#)

[Why 1Password?](#)

433	9,544,538,448	111,248	134,690,792
pwned websites	pwned accounts	pastes	paste accounts

Passwords Are Reused



Passwords of these accounts have been found in the dictionary:

```
ADATUM\larry_admin  
CONTOSO\harry
```

...


These groups of accounts have the same passwords:

Group 1:

```
ADATUM\smith  
ADATUM\srv_sql01
```

Group 2:

```
ADATUM\Administrator  
ADATUM\joe_admin  
CONTOSO\Administrator  
CONTOSO\joe_admin
```

**Thomas Eklund**
@limp15000

Follow

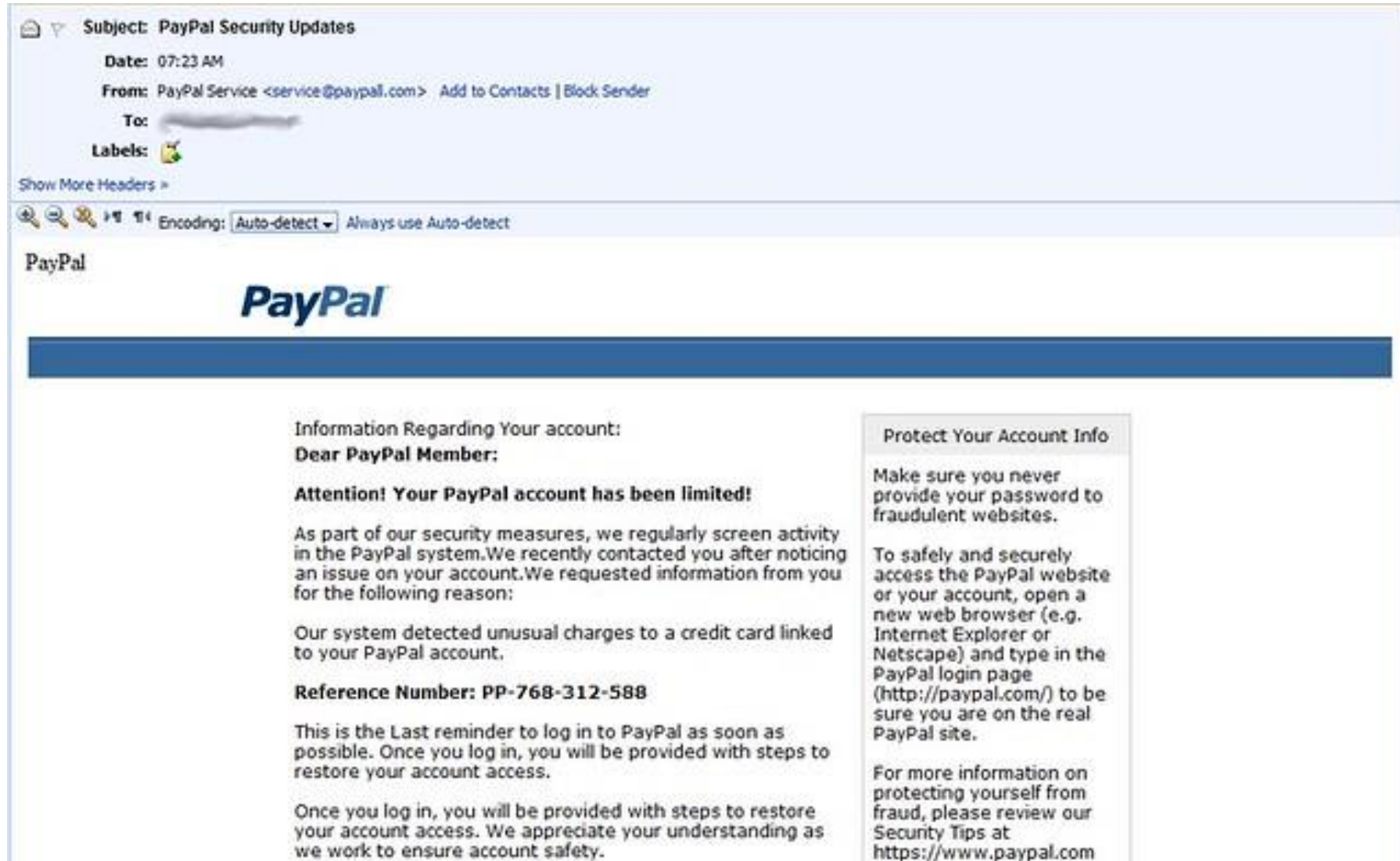
Replied to @MGrafnetter @SwiftOnSecurity @haveibeenpwned

Thanks for the great script [#DSInternals](#) Just convinced a customer for a quick check... Results are appalling, can't get too specific but more than 50% are in [@haveibeenpwned](#) and don't get me started on admins who have the same password for their normal account and domain admin..

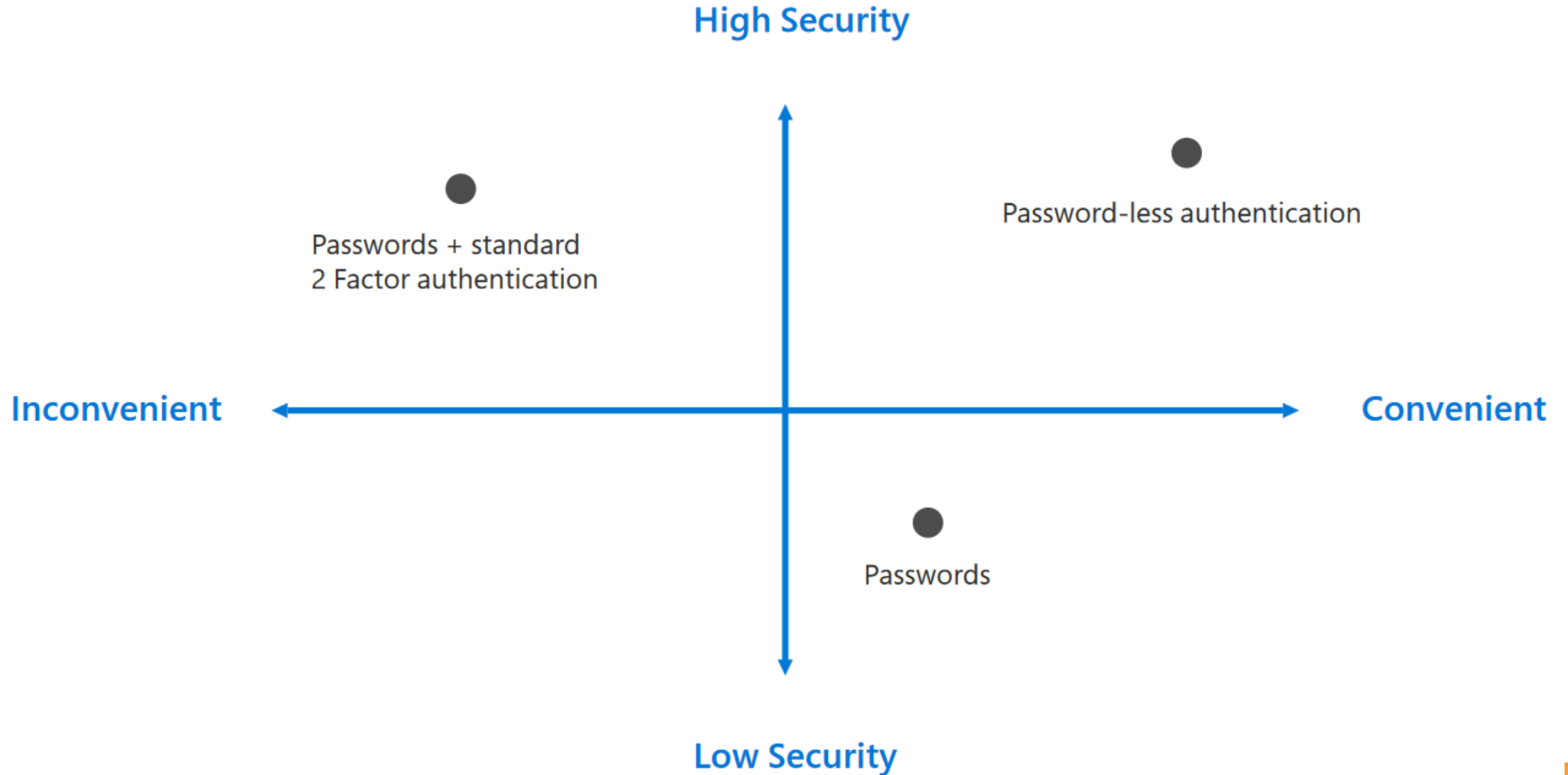
4:08 PM - 1 Oct 2018



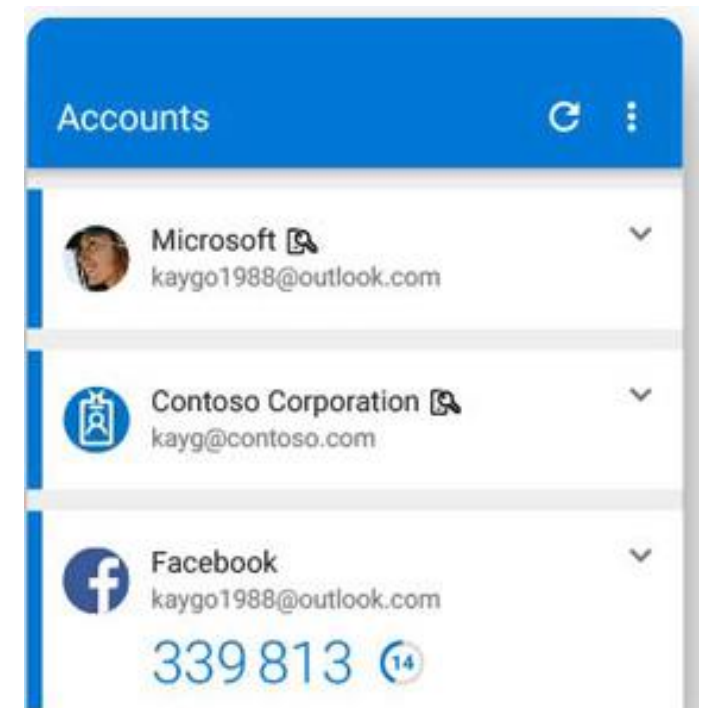
Passwords Are Subject to Phishing Attacks



Microsoft's Strategy is Passwordless



Passwordless Authentication Options

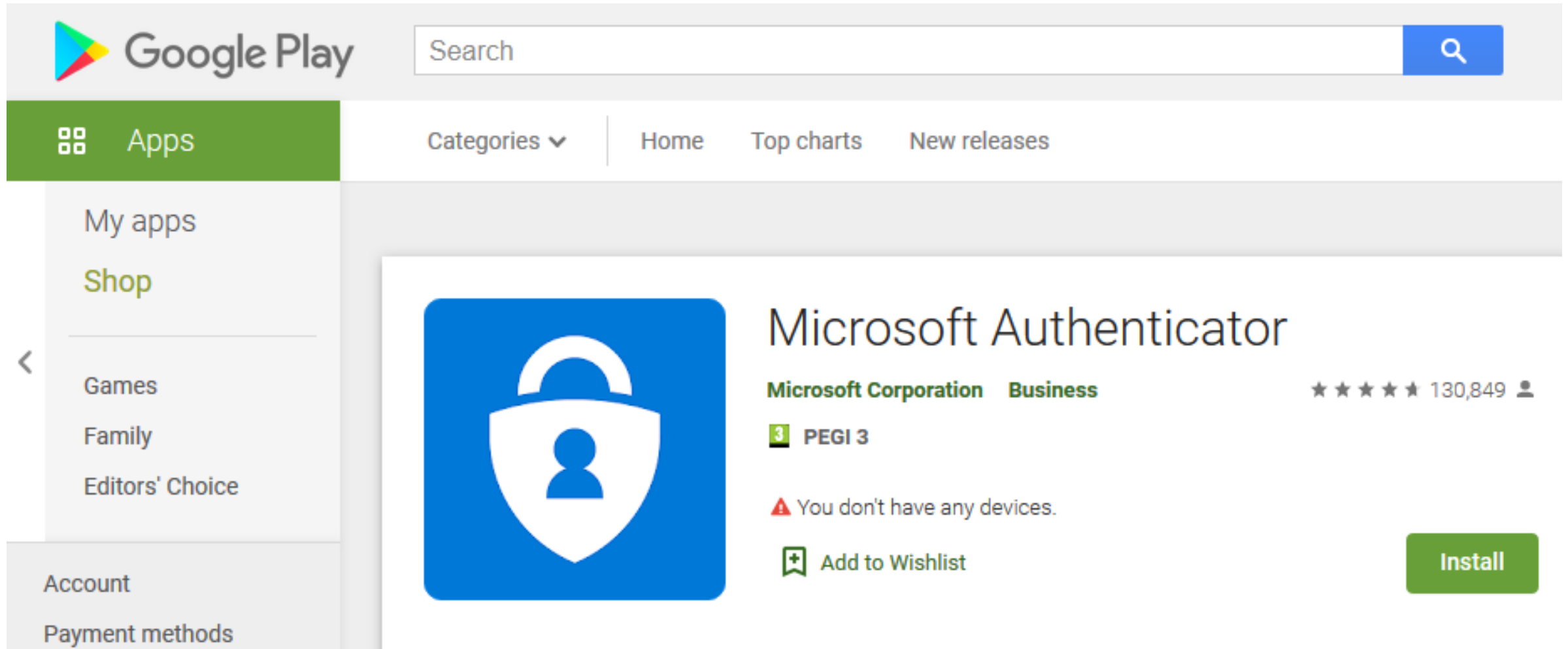


What About Smart Cards?



Microsoft Authenticator App

Android



The screenshot displays the Google Play Store interface. At the top, the Google Play logo is on the left, and a search bar with a magnifying glass icon is on the right. Below the search bar, a green bar highlights the 'Apps' category, with a grid icon to its left. To the right of 'Apps', there are links for 'Categories', 'Home', 'Top charts', and 'New releases'. A left sidebar menu contains 'My apps', 'Shop' (highlighted in green), 'Games', 'Family', 'Editors' Choice', 'Account', and 'Payment methods'. The main content area shows the 'Microsoft Authenticator' app by 'Microsoft Corporation', categorized as 'Business'. The app icon is a blue square with a white shield and a person silhouette. It has a 5-star rating from 130,849 reviews and a PEGI 3 rating. A warning message states 'You don't have any devices.' Below this is an 'Add to Wishlist' button with a plus icon. A large green 'Install' button is positioned on the right side of the app card.

Google Play

Search

Apps

Categories Home Top charts New releases

My apps

Shop

Games

Family

Editors' Choice

Account

Payment methods

Microsoft Authenticator

Microsoft Corporation Business

★★★★★ 130,849

3 PEGI 3

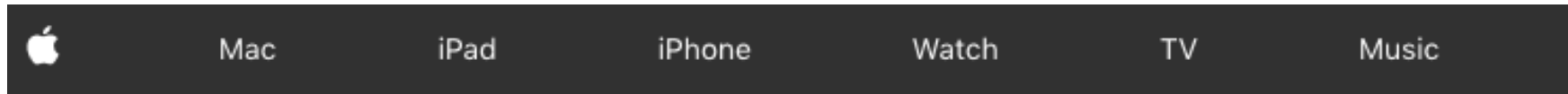
⚠ You don't have any devices.

+ Add to Wishlist

Install



iOS + watchOS



App Store Preview

This app is available only on the App Store for iPhone, iPad, and Apple Watch.



Microsoft Authenticator 4+

Microsoft Corporation

#14 in Productivity

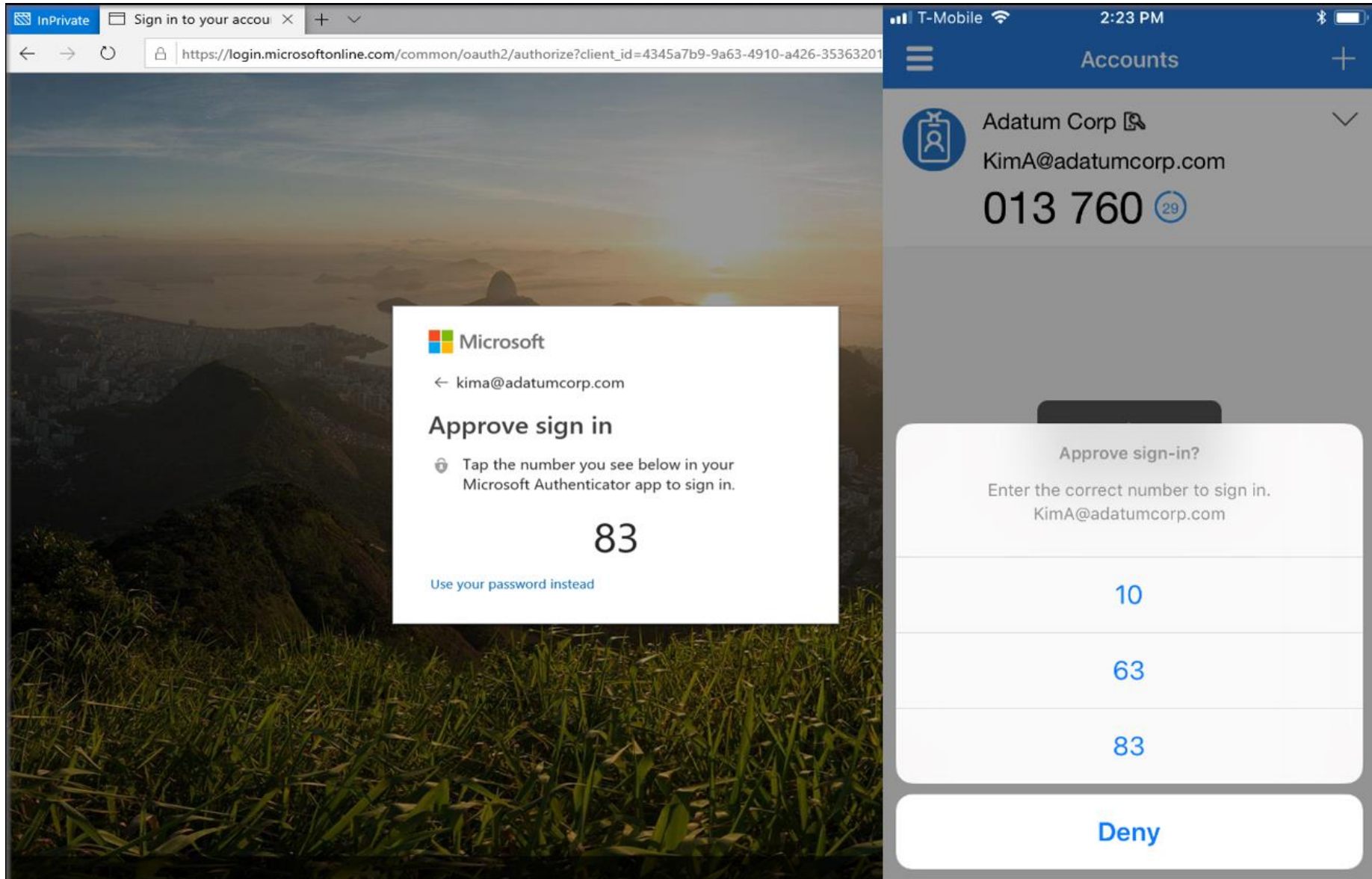
★★★★★ 4.7, 23.4K Ratings

Free

Screenshots [iPhone](#) iPad Apple Watch

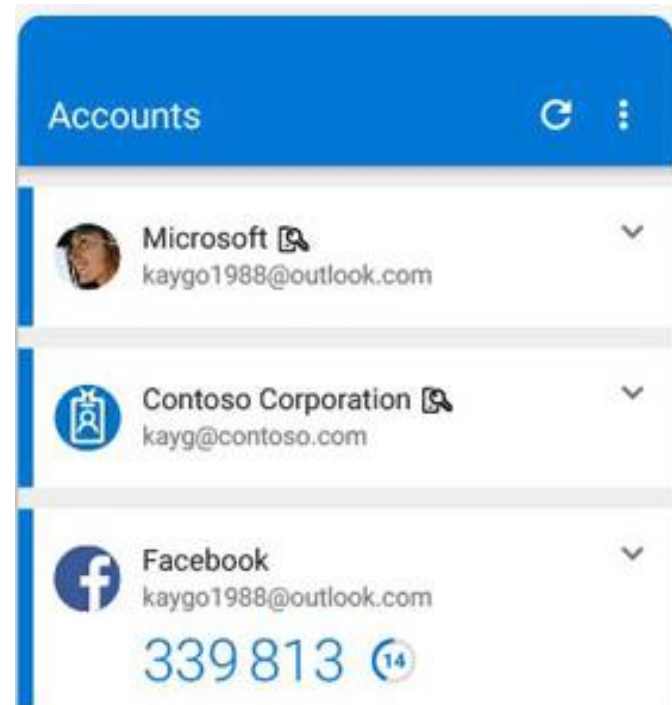


Passwordless Phone Sign-In



Demo

Passwordless Phone Sign-In



Enabling Phone Sign-in

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

Home > DSInternals > Security > Authentication methods - Authentication method policy (Preview)

Authentication methods - Authentication method policy (Preview)

DSInternals - Azure AD Security

» Reset

Click here to enable users for the enhanced registration preview. →

Authentication method	Target	Registration
FIDO2 Security Key	All users	Yes
Microsoft Authenticator passwordless sign-in	All users	Yes

Microsoft Authenticator passwordless sign-in settings

Save Discard

Your tenant must be enabled for MFA with push notifications through the Microsoft Authenticator app in order to use this method.

ENABLE

☒ Yes ☐ No

TARGET

☒ All users ☐ Select users

USE FOR:

- Sign in
- Strong authentication

Name	Type	Registration
All users	Group	Optional



Self-Service Registration

https://aka.ms/mysecurityinfo





Security info

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

Default sign-in method: Microsoft Authenticator - notification [Change](#)

+

Add method

	Phone	+ [REDACTED] 0	Change	Delete
	Microsoft Authenticator	Michael's iPhone		Delete
	Security key	YubiKey 5		Delete
	Email	michael.grafnetter@outlook.com	Change	Delete



Pairing the App

Configure mobile app

Complete the following steps to configure your mobile app.

1. Install the Microsoft authenticator app for [Windows Phone](#), [Android](#) or [iOS](#).
2. In the app, add an account and choose "Work or school account".
3. Scan the image below.



[Configure app without notifications](#)

If you are unable to scan the image, enter the following information in your app.

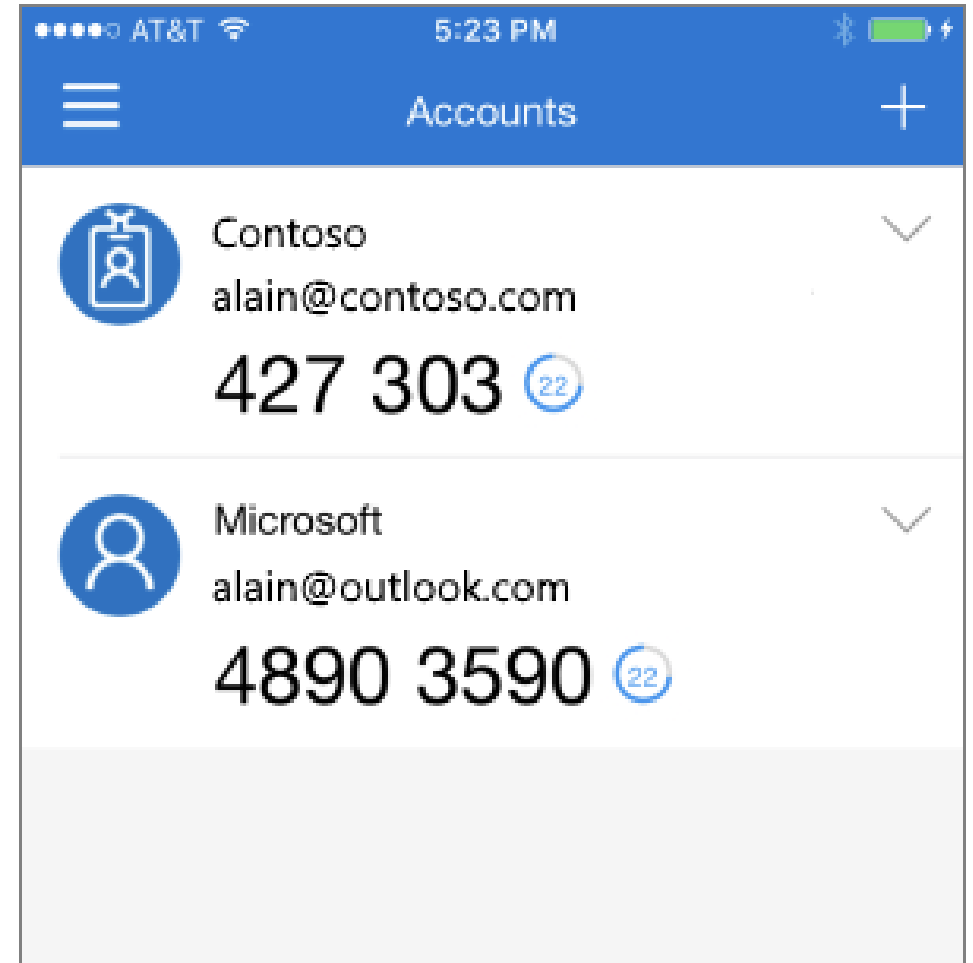
Code: 857 634 999

Url: <https://co1pfpad16.phonefactor.net/pad/648069390>

If the app displays a six-digit code, you are done!

Done

cancel



Supported Scenarios

- Azure Active Directory Accounts
- Microsoft Accounts
- No Windows Sign-in
- Self-Service Enrollment Only

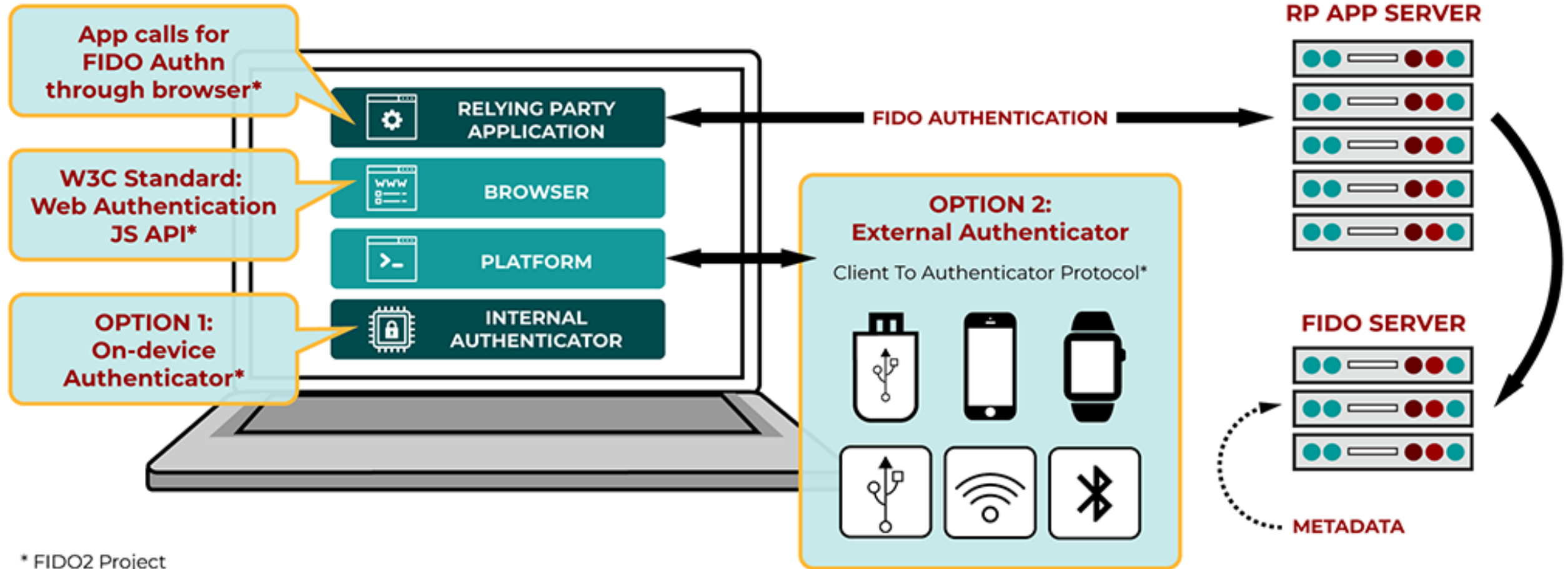


FIDO2

Fast
IDentity
Online



FIDO2 Overview



* FIDO2 Project

FIDO Alliance Board Level Members

FIDO Alliance Government Level Members

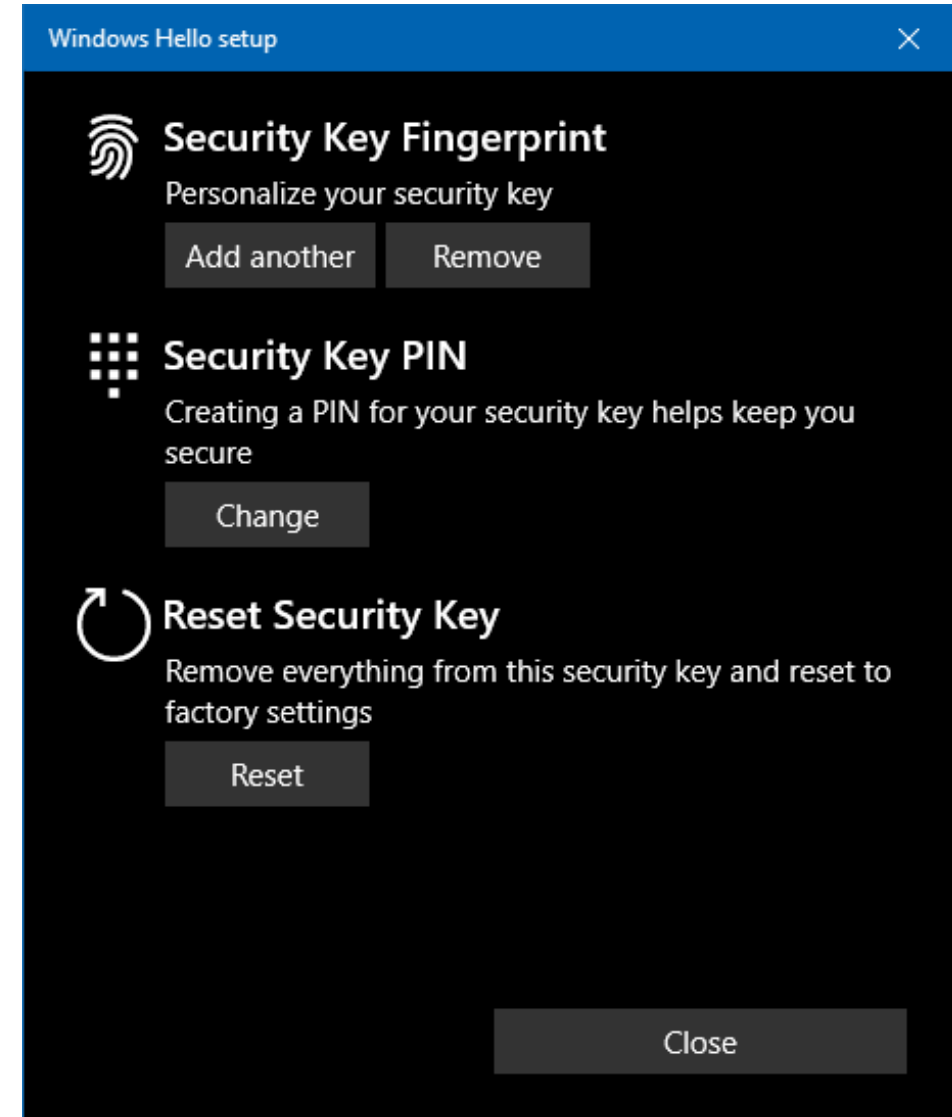
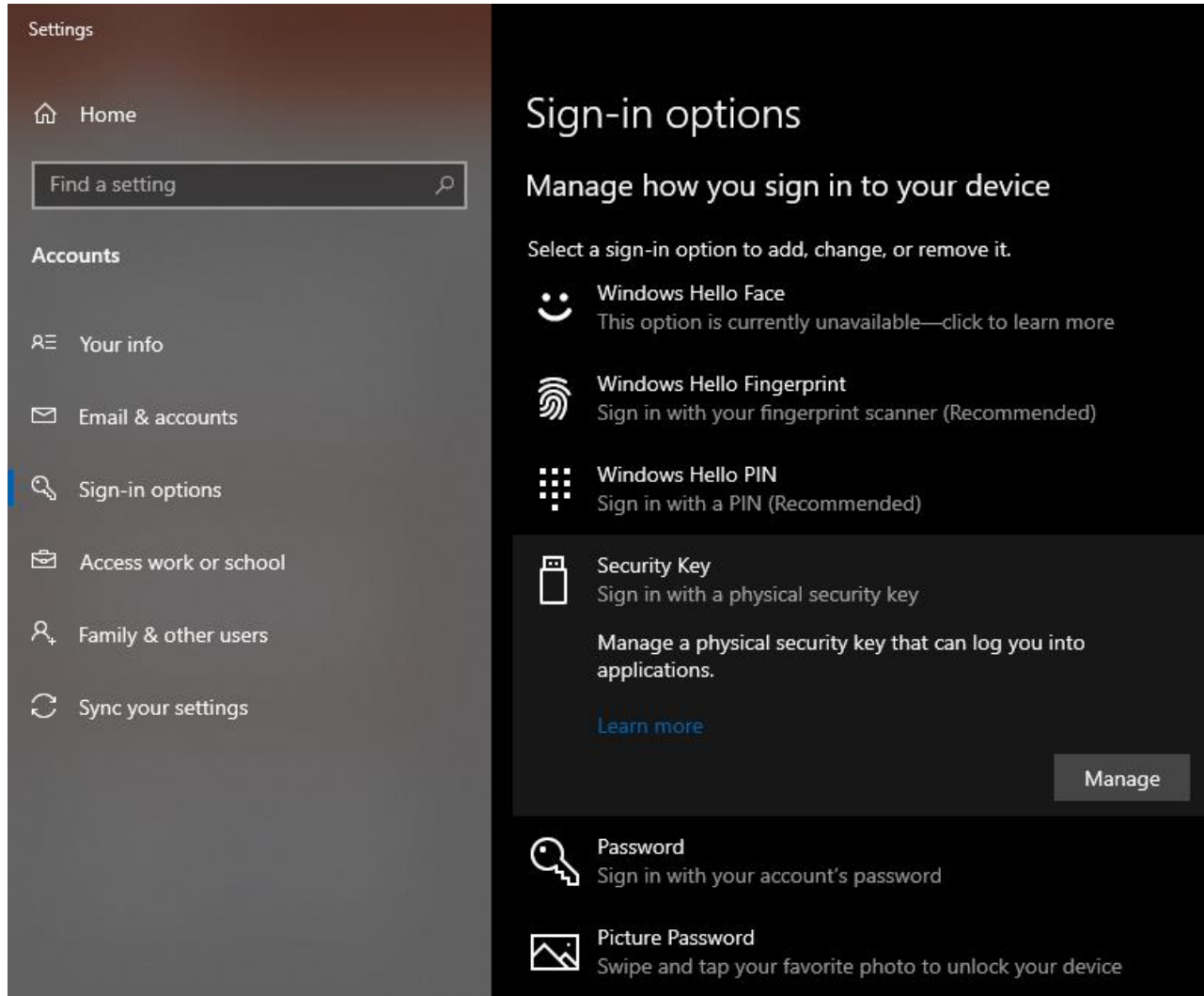
 <p>Australian Government Digital Transformation Office</p>	 <p>Cabinet Office</p>	 <p>CAICT 中国信息通信研究院 China Academy of Information and Communications Technology</p>	 <p>ETDA ETDA www.eta.or.th</p>	 <p>Federal Office for Information Security</p>
 <p>NIST National Institute of Standards and Technology U.S. Department of Commerce</p>	 <p>TTA 한국정보통신기술협회 Telecommunications Technology Association</p>			



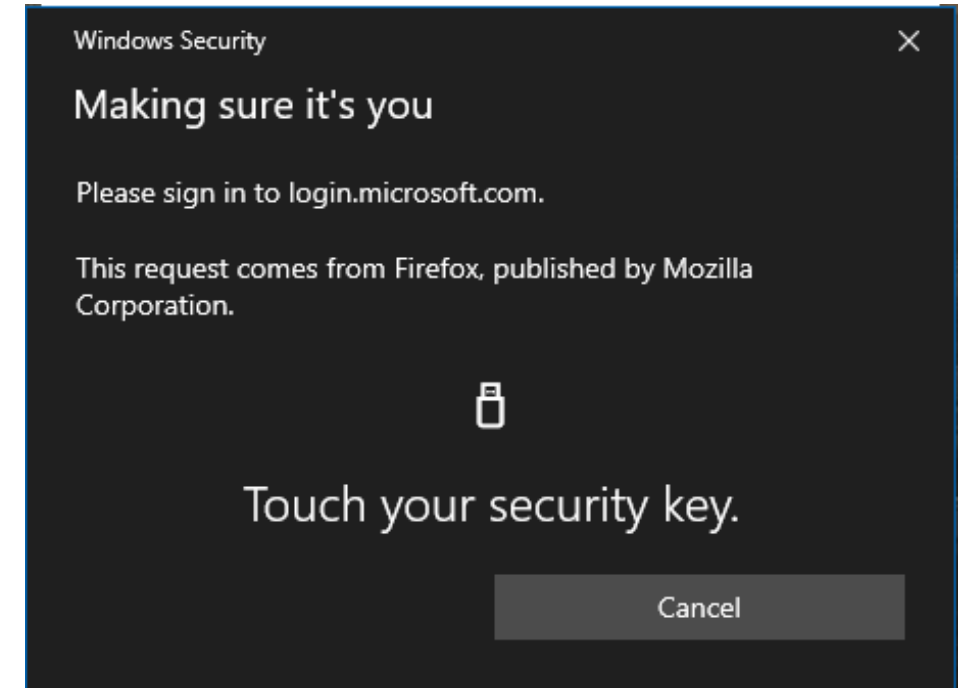
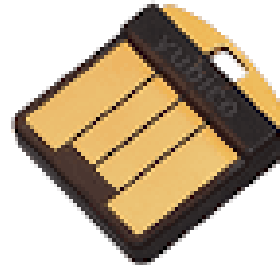
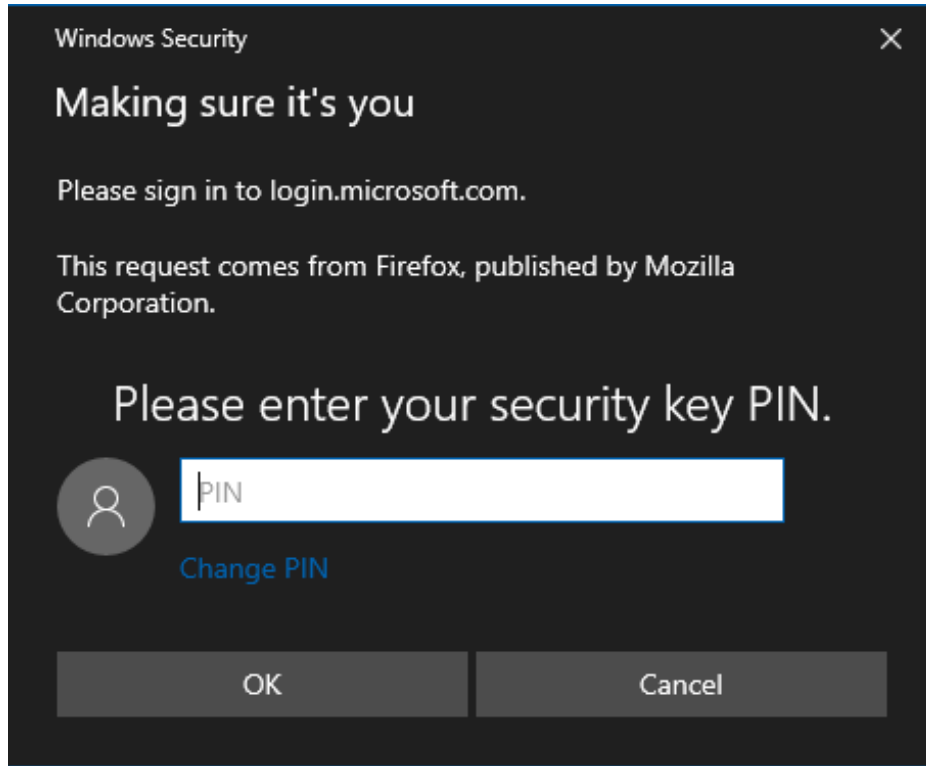
FIDO U2F vs. FIDO2



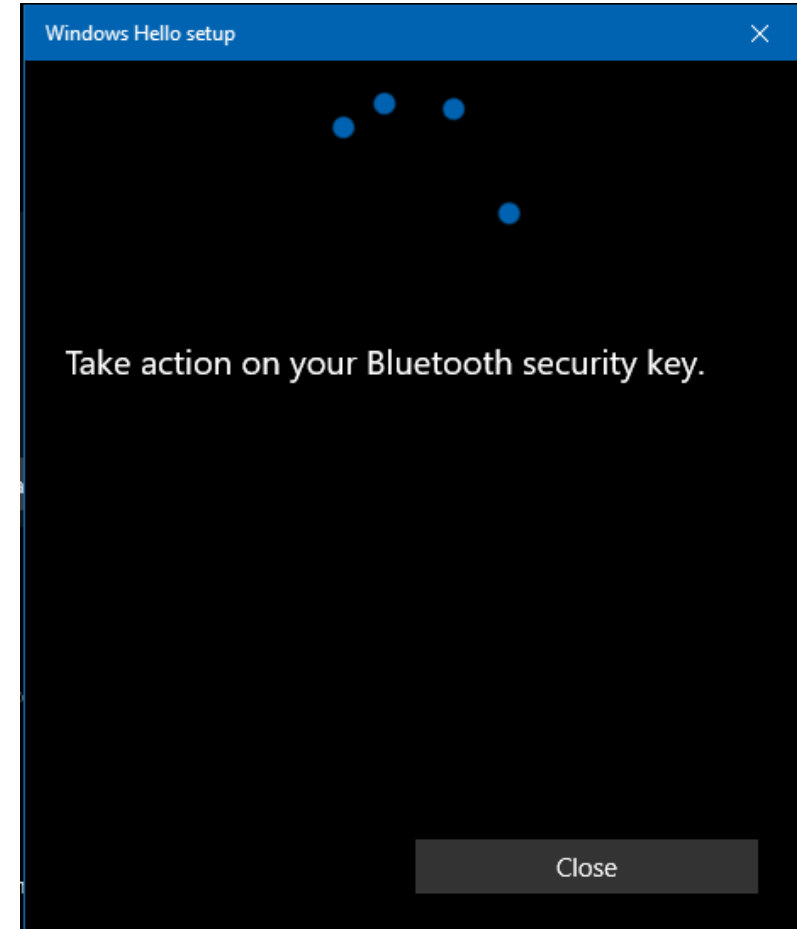
FIDO2 Device Management in Windows



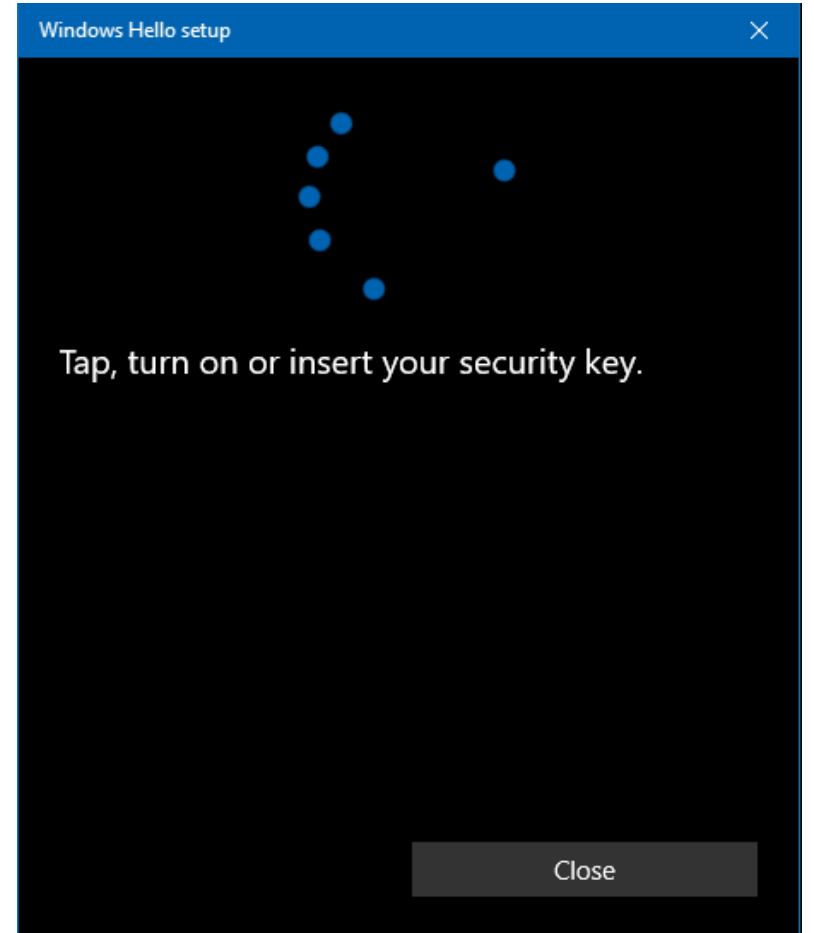
Device Authentication: PIN + Touch




Device Authentication: Biometrics




FIDO2 Device Interface: USB, Bluetooth, NFC




FIDO2 Usernameless Login




Sign-in options




Sign in with Windows Hello or a security key
Choose this only if you have enabled Windows Hello or a security key for your account.



Sign in with GitHub



Sign in with Google



Forgot my username


Back

Windows Security

Making sure it's you

Please sign in to login.microsoft.com.

This request comes from Firefox, published by Mozilla Corporation.




Michael Grafnetter


michael@dsinternals.com

login.microsoft.com

More choices



michael@dsinternals.com



michael.grafnetter@outlook.com

OKCancel



JmLEadmzHpm5K3i5gVFO-MJz43GukTKYkcRR8qO6...

Stay signed in?

Stay signed in so you don't have to sign in again next time.

☐ Don't show this again

NoYes

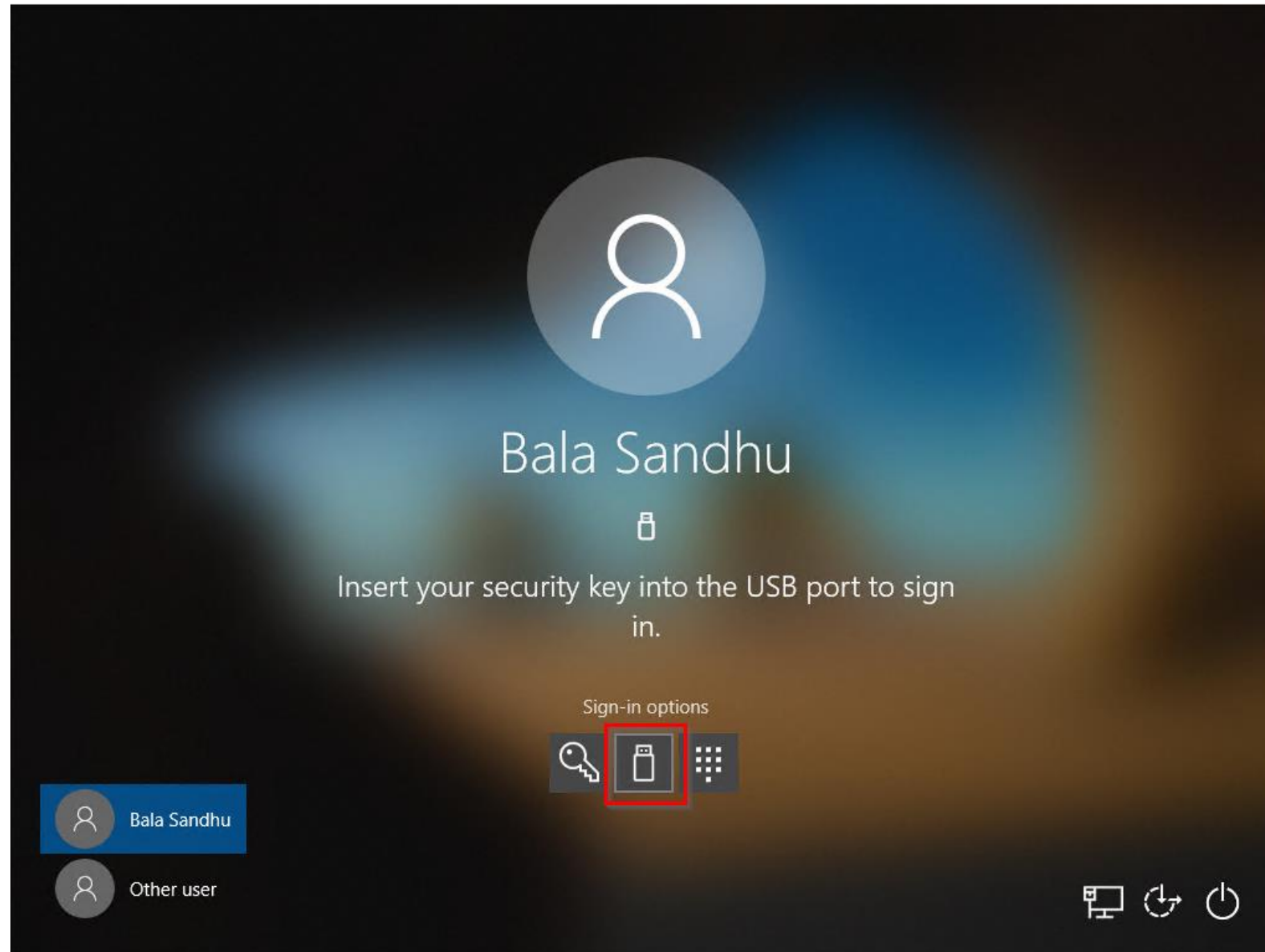


Demo

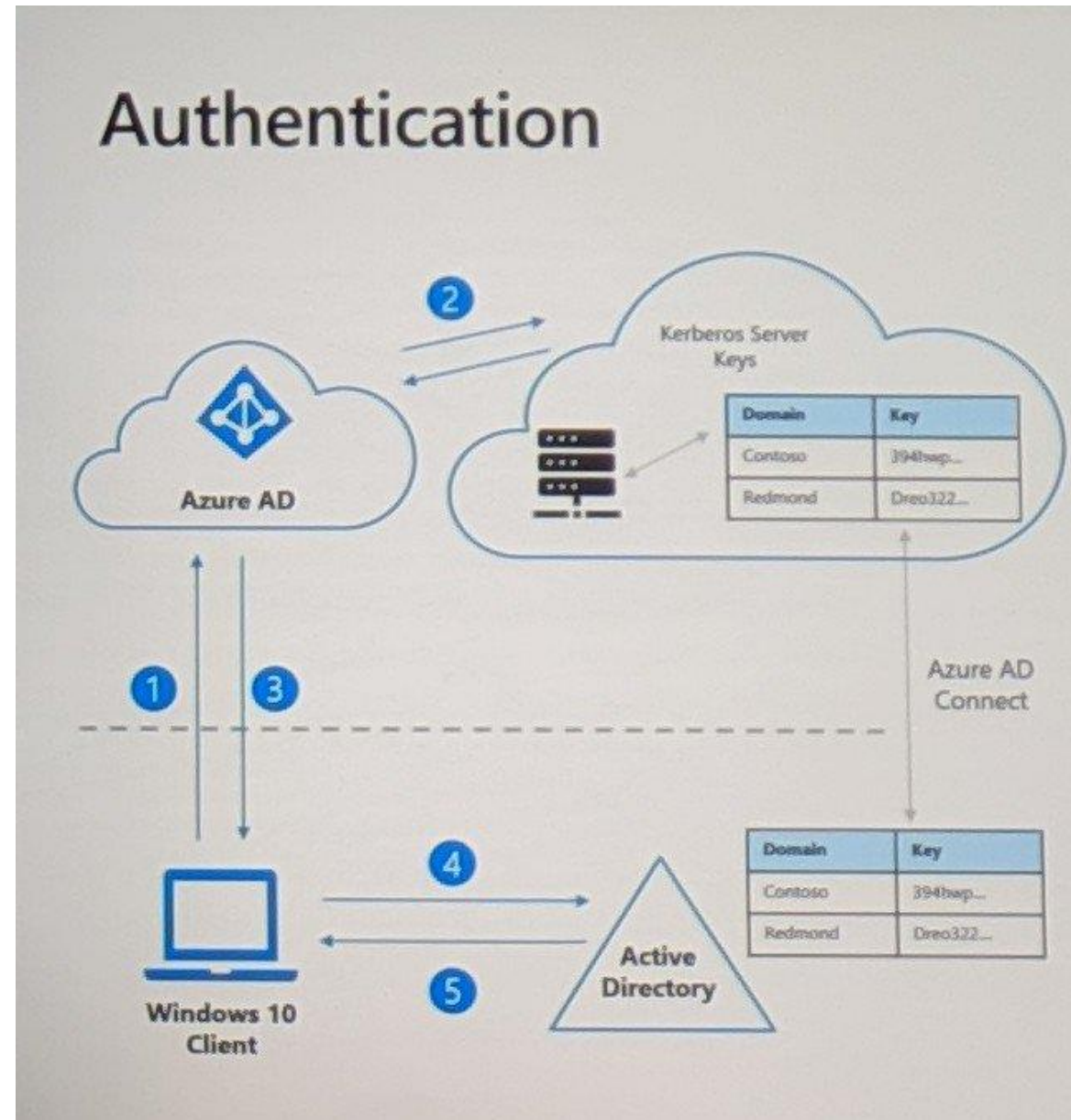
FIDO2 Sign-In



Windows Logon – Azure AD Joined



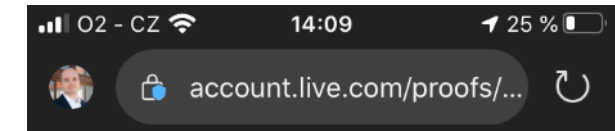
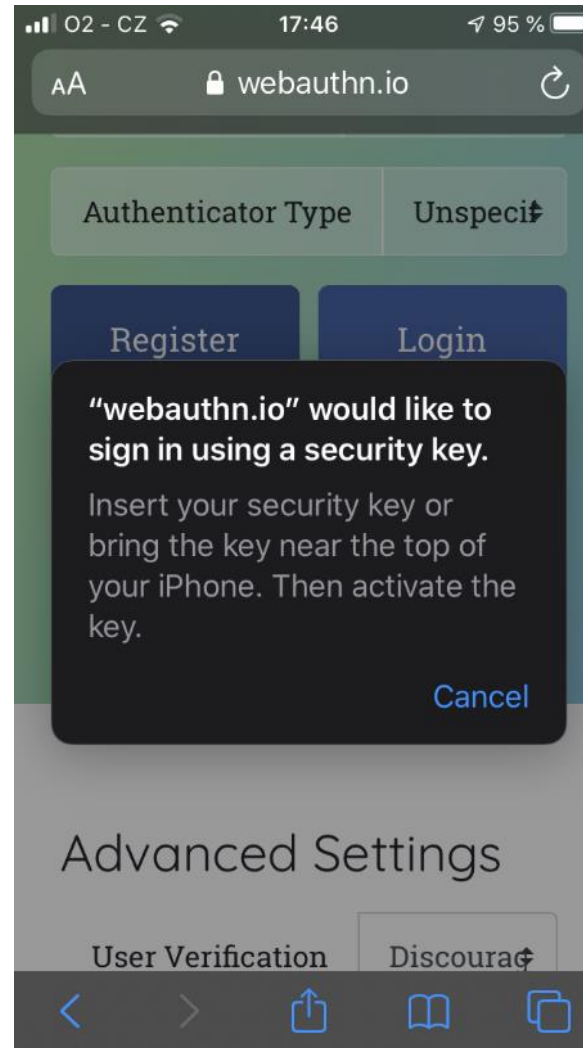
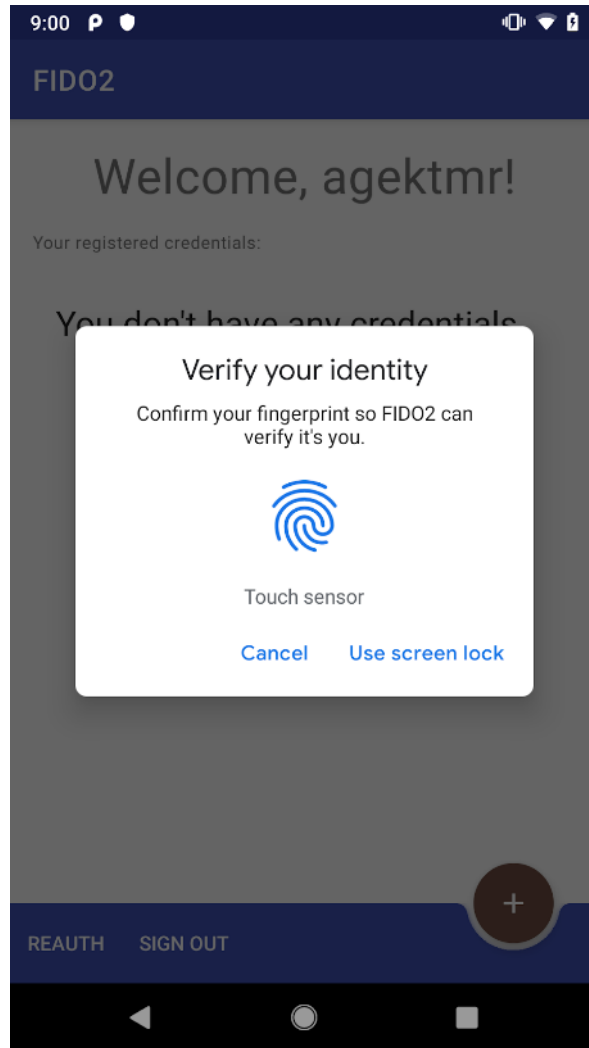
TBA: Authentication in Hybrid Environments



FIDO2 Browser Support



FIDO2 Mobile Browser Support



Windows Hello and security keys

Now you can sign in without a password using Windows Hello or security keys. A security key is a physical device (like a USB security key) that you can use to sign in to your account instead of a password. [Learn more about signing in with Windows Hello or a security key.](#)

Your browser or operating system does not support this

[Manage your sign-in methods](#)

Recovery code

You can use your recovery code if you lose access to your security info. You need to print out your recovery code and keep it in



Enabling FIDO2 Support In Azure AD

ENABLE

☒ Yes ☐ No

USE FOR:

- Sign in
- Strong authentication

TARGET

☒ All users ☐ Select users

Name	Type	Registration
All users	Group	Optional ▼ ...

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 added.

FIDO2 Authenticator Management

Manage your sign-in methods

NAME	SIGN-IN METHODS		ADDED ON	LAST USED	
Feitian BioPass		Security key	3/16/2020 2:16 PM	3/21/2020 2:28 PM	Remove
YubiKey Nano		Security key	9/6/2019 6:00 PM	3/21/2020 2:18 PM	Remove
Feitian AllinPass USB		Security key	3/16/2020 2:38 PM	3/21/2020 2:16 PM	Remove

- + [Add another security key](#)
- + [Set up Windows Hello](#)



Auditing FIDO2 Keys In (Azure) AD



```
Get-ADObject -LDAPFilter '(msDS-KeyCredentialLink=*)' -Properties 'msDS-KeyCredentialLink' |  
  Select-Object -ExpandProperty 'msDS-KeyCredentialLink' |  
  Get-ADKeyCredential |  
  Where-Object Usage -eq FIDO |  
  Format-Table -View FIDO
```

DisplayName	Flags	FidoFlags	Created	HolderDN
eWMB Goldengate G320	Attestation	UserPresent, UserVerified, AttestationData, ExtensionData	2019-08-29	CN=John Doe,CN=...
eWBM Goldengate G310	Attestation	UserPresent, UserVerified, AttestationData, ExtensionData	2019-08-29	CN=John Doe,CN=...
YubiKey FIDO2	Attestation	UserPresent, UserVerified, AttestationData, ExtensionData	2019-07-11	CN=John Doe,CN=...
Yubikey 5	Attestation	UserPresent, UserVerified, AttestationData, ExtensionData	2019-06-21	CN=John Doe,CN=...
Feitian BioPass FIDO2	Attestation	UserPresent, UserVerified, AttestationData, ExtensionData	2019-08-26	CN=John Doe,CN=...



Free Feitian Sample Devices



<https://ftsafe.com/pathtopasswordless>

Windows Hello for Business



WHfB Provisioning UI

Your organization requires Windows Hello

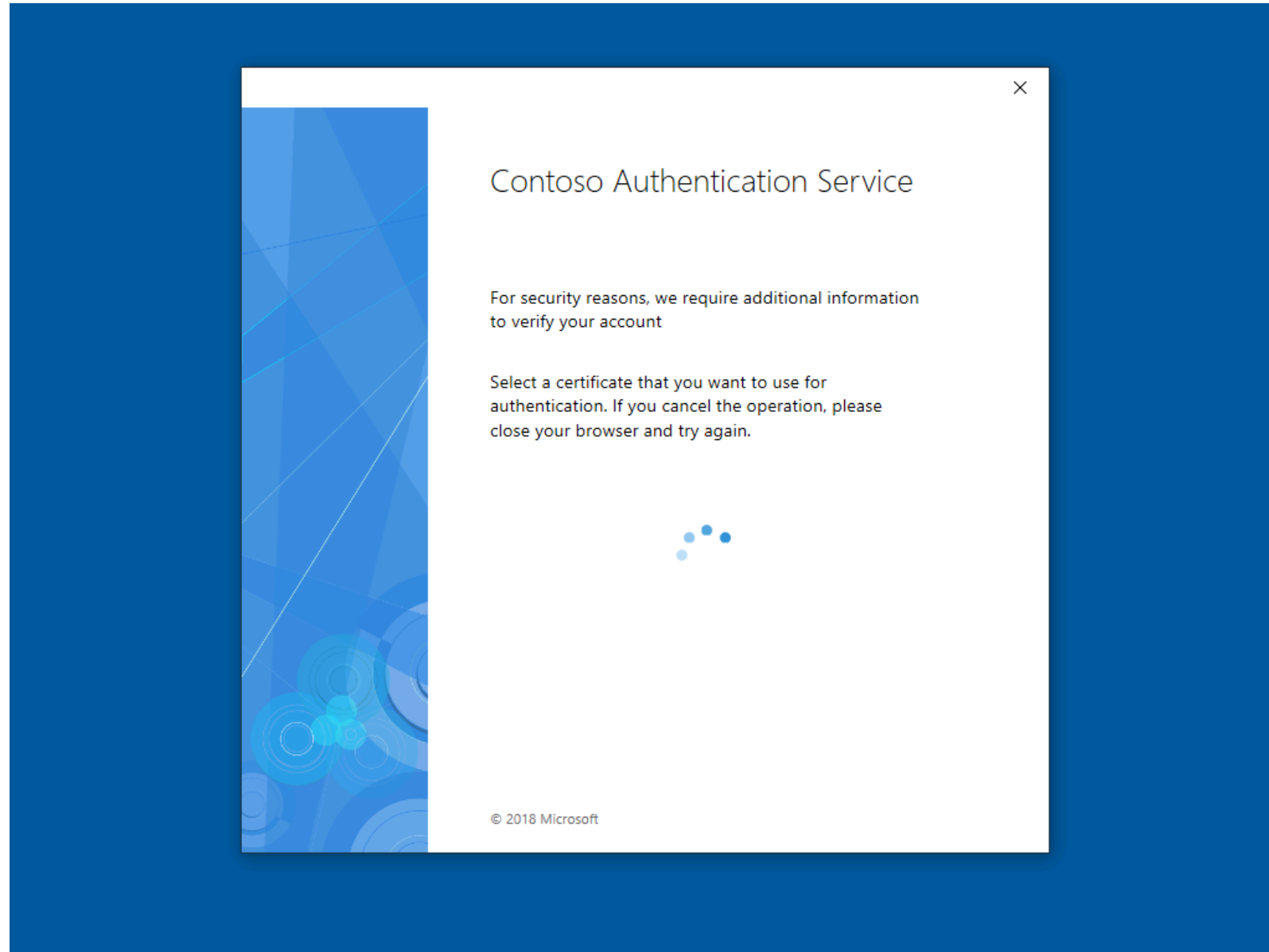
A password can be easily stolen. Windows Hello provides you with a combination of two factors-your device plus biometrics or a PIN-instead of a password to sign in to your device, apps, and services.
How can a PIN be safer than a long password?



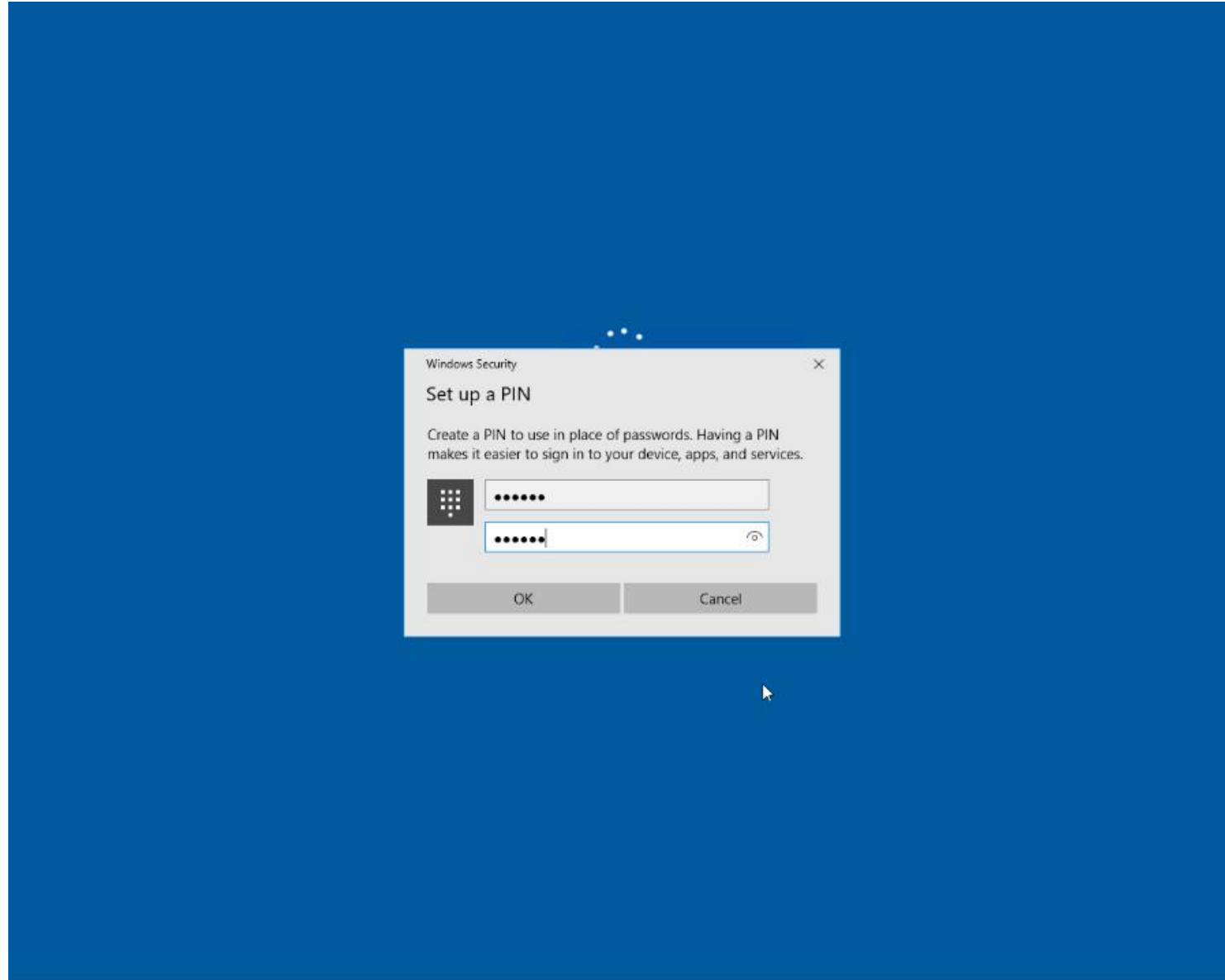
Set up PIN



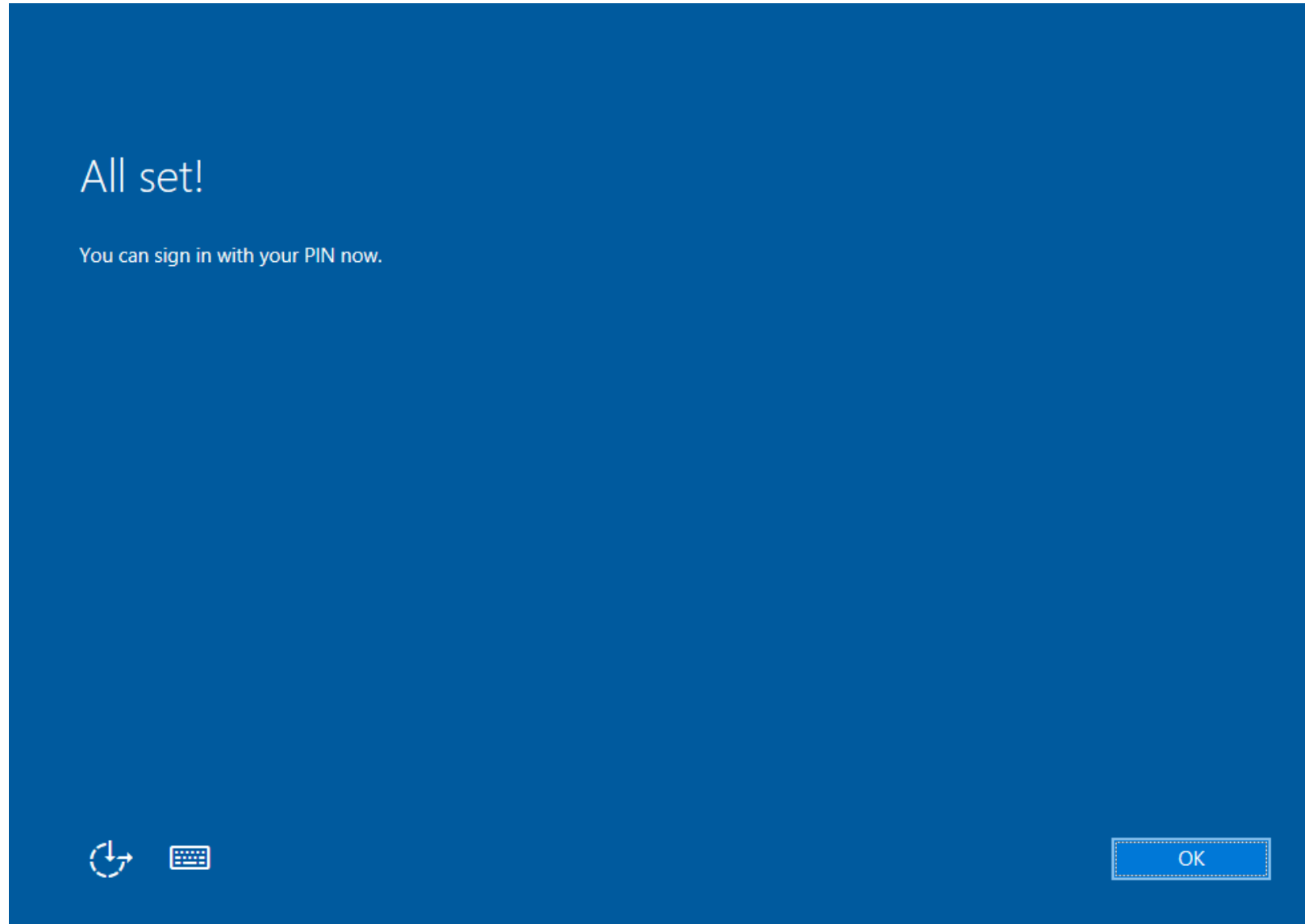
WHfB Provisioning UI



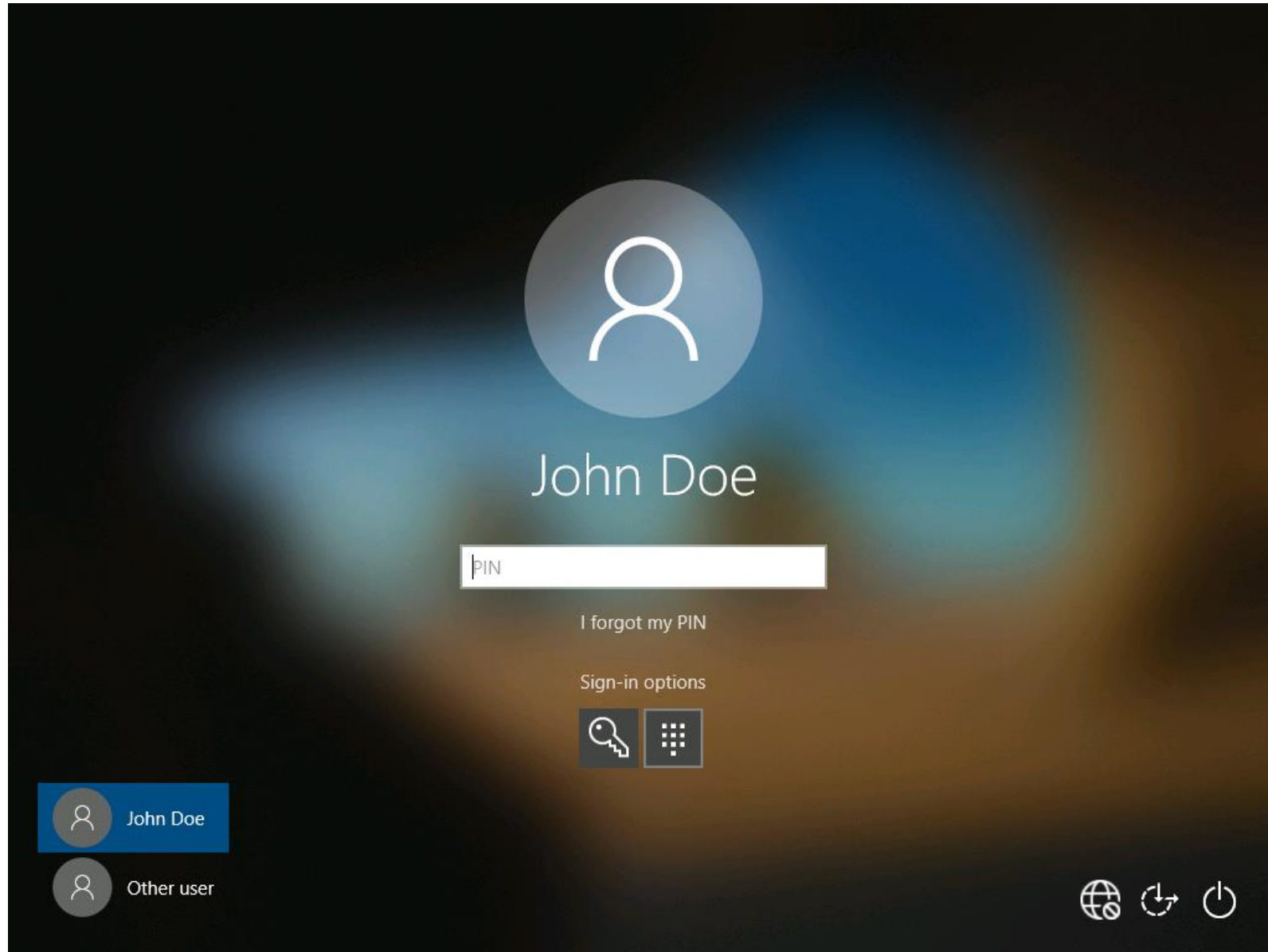
WHfB Provisioning UI



WHfB Provisioning UI



Windows 10 Logon Screen With PIN



Windows Hello UI

Sign-in options

*Some of these settings are hidden or managed by your organization.

Manage how you sign in to your device

Select a sign-in option to add, change, or remove it.



Windows Hello Face

This option is currently unavailable—click to learn more



Windows Hello Fingerprint

This option is currently unavailable—click to learn more



Windows Hello PIN

Sign in with a PIN (Recommended)

Your PIN is all set up to sign in to Windows, apps, and services.

[Learn more](#)

[I forgot my PIN](#)

Change

Remove



Security Key

Sign in with a physical security key



Password

Sign in with your account's password



Picture Password

Swipe and tap your favorite photo to unlock your device

Windows Security



Making sure it's you

Please sign in as michael.grafnetter@outlook.com to login.microsoft.com.

This request comes from Firefox, published by Mozilla Corporation.



Scan your finger on the fingerprint reader.

More choices



Fingerprint



PIN



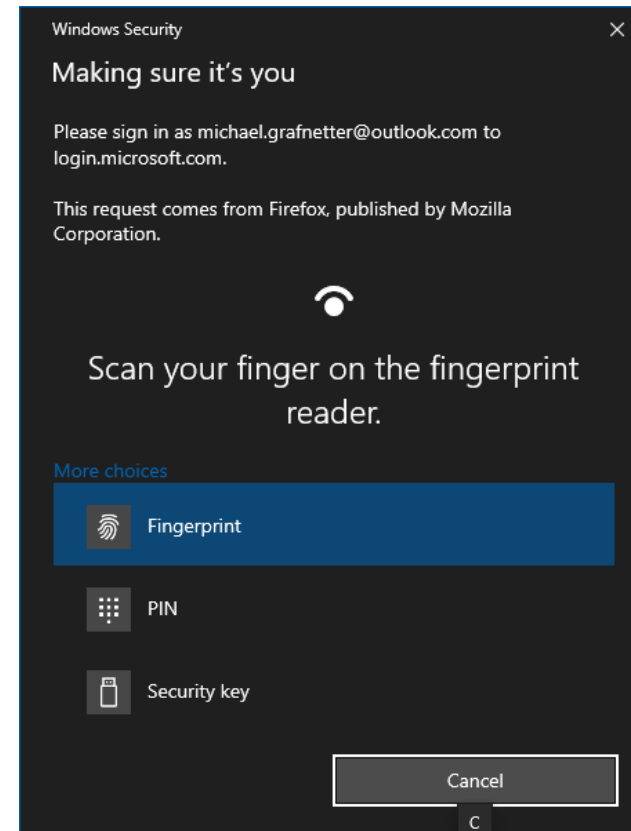
Security key

Cancel



Demo

Windows Hello Sign-In



Multifactor Device Unlock

Custom OMA-URI Settings

Windows 10 and later

OMA-URI Settings ⓘ

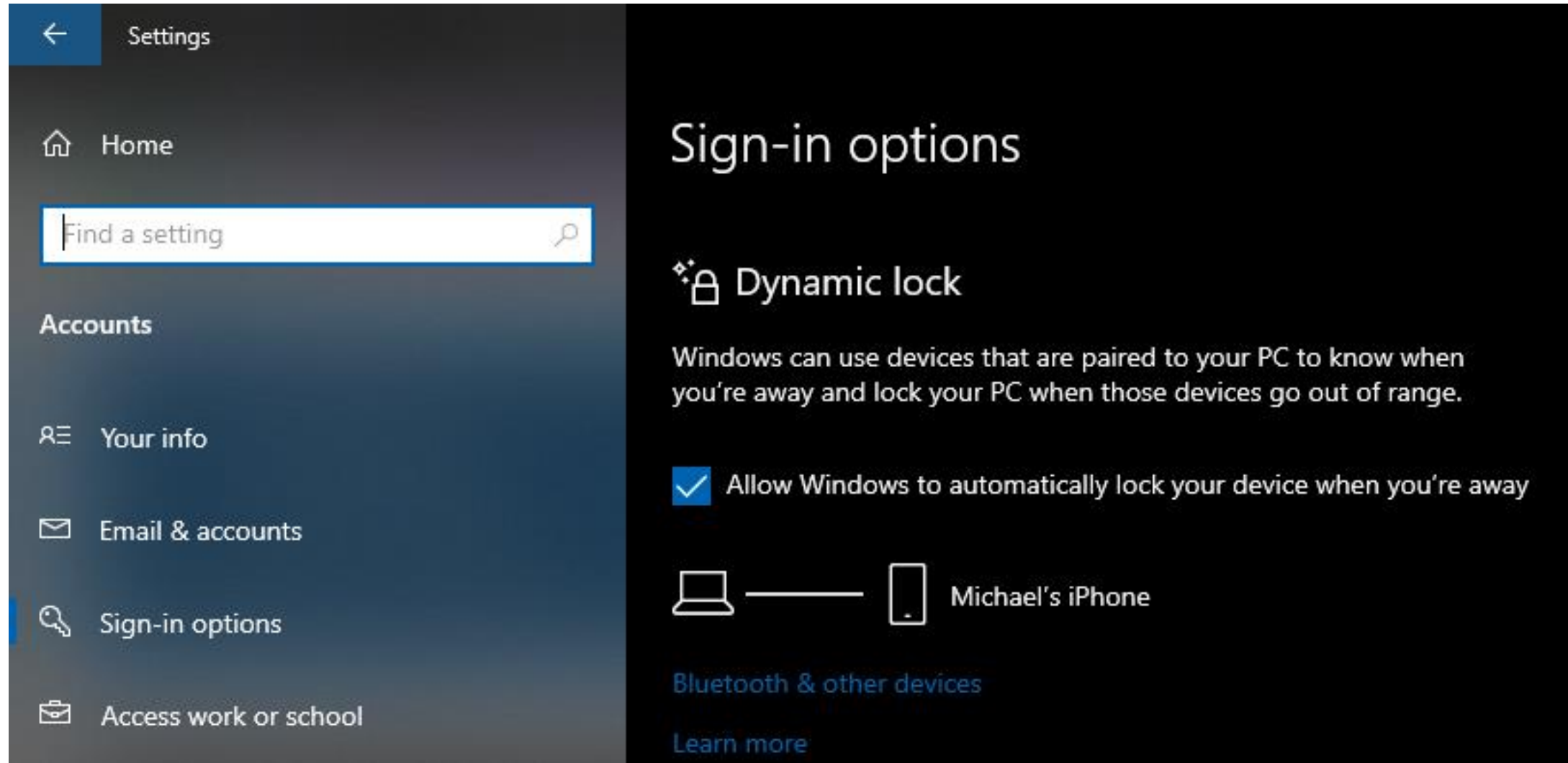
Add

Export

NAME	DESCRIPTION	OMA-URI	VALUE
Windows Hello Multifactor Unloc...	First unlock factor credential provider	./Device/Vendor/MSFT/PassportForWork/DeviceUn...	{D6886603-9D2F-4EB2-B667-1971041... ...
Windows Hello Multifactor Unloc...	Second unlock factor credential provider	./Device/Vendor/MSFT/PassportForWork/DeviceUn...	{27FBDB57-B613-4AF2-9D7E-4FA7A6... ...
Windows Hello Multifactor Unloc...	Configure unlock signals	./Device/Vendor/MSFT/PassportForWork/DeviceUn...	<rule schemaVersion="1.0"> <signal



Dynamic Lock



Deployment Options

- Hybrid Azure AD Joined Key Trust
- Hybrid Azure AD Joined Certificate Trust
- On Premises Key Trust
- On Premises Certificate Trust
- Azure AD Join Single Sign-on



WHfB Prerequisites (Varies)

- Windows 10 1703+
- Windows Server 2016
 - Active Directory Domain Services (AD DS)
 - Active Directory Federation Services (AD FS)
 - Active Directory Certificate Services (AD CS)
- Azure Active Directory
- Azure Multi-Factor Authentication (MFA)
- Microsoft Intune



Provisioning Methods

Save

Discard

Windows Hello for Business

Windows 10 and later

Name

WH4B

Description

Enter a description...

Platform

Windows 10 and later

Profile type

Identity Protection

Settings

7 configured

Scope (Tags)

0 scope(s) selected

Configure Windows Hello for Business: ⓘ

Enable

Minimum PIN length: ⓘ

6

Maximum PIN length: ⓘ

12

Lowercase letters in PIN: ⓘ

Allowed

Uppercase letters in PIN: ⓘ

Allowed

Special characters in PIN: ⓘ

Allowed

PIN expiration (days): ⓘ

365

Remember PIN history: ⓘ

3

Enable PIN recovery: ⓘ

Enable

Not configured

Use a Trusted Platform Module (TPM): ⓘ

Enable

Not configured

Allow biometric authentication: ⓘ

Enable

Not configured

Use enhanced anti-spoofing, when available: ⓘ

Enable

Not configured

Certificate for on-premise resources: ⓘ

Enable

Not configured

Use Windows Hello for Business

Previous Setting

Next Setting

Not Configured

Comment:

Enabled

Supported on:

At least Windows 10

Disabled

Options:

Help:

Do not start Windows Hello provisioning after sign-in

Windows Hello for Business is an alternative method for signing into Windows using your Active Directory or Azure Active Directory account that can replace passwords, Smart Cards, and Virtual Smart Cards.

If you enable this policy, the device provisions Windows Hello for Business using keys or certificates for all users.

If you disable this policy setting, the device does not provision Windows Hello for Business for any user.

If you do not configure this policy setting, users can provision Windows Hello for Business as a convenience credential that encrypts their domain password.

Select "Do not start Windows Hello provisioning after sign-in" when you use a third-party solution to provision Windows Hello for Business.

If you select "Do not start Windows Hello provisioning after sign-in", Windows Hello for Business does not automatically

OK

Cancel

Apply



Active Directory NGC Key Auditing



```
Get-ADUser -Identity john -Properties msDS-KeyCredentialLink |  
  Select-Object -ExpandProperty msDS-KeyCredentialLink |  
  Get-KeyCredential |  
  Out-GridView -OutputMode Multiple -Title 'Select credentials for removal...' |  
  foreach { Set-ADObject -Identity $PSItem.HolderDN -Remove @{ 'msDS-KeyCredentialLink' = $PSItem.ToDNWithBinary() } }
```

The screenshot shows a Windows dialog box titled "Select credentials for removal...". It contains a table with columns: Usage, Source, Flags, DeviceId, Created, and HolderDN. The table lists several credentials, with the third row (NGC, AzureAD, None, e9899e73-db27-4af9-b7eb-c4201d6577eb, 4/6/2017 9:45:07 AM, CN=John Doe,OU=Employees,DC=adatum,DC=com) highlighted in blue. The dialog also has a "Filter" search bar, an "Add criteria" button, and "OK" and "Cancel" buttons at the bottom right.

Usage	Source	Flags	DeviceId	Created	HolderDN
NGC	AD	None	ff4f6924-3e15-43c5-b48b-3263cdcb49be	7/1/2019 4:46:54 PM	CN=John Doe,OU=Employees,DC=adatum,DC=com
NGC	AD	None	dad4f214-e486-4bcf-8b83-928931d05fca	7/1/2019 4:52:57 PM	CN=John Doe,OU=Employees,DC=adatum,DC=com
NGC	AzureAD	None	e9899e73-db27-4af9-b7eb-c4201d6577eb	4/6/2017 9:45:07 AM	CN=John Doe,OU=Employees,DC=adatum,DC=com
NGC	AD	None	ff4f6924-3e15-43c5-b48b-3263cdcb49be	7/1/2019 5:49:51 PM	CN=John Doe,OU=Employees,DC=adatum,DC=com
NGC	AD	None	8b7d0d03-0563-4fed-a578-ed5289b3e8e8	7/8/2019 6:51:38 PM	CN=John Doe,OU=Employees,DC=adatum,DC=com
NGC	AD	None	62cf89cf-5f84-4ef4-8fe6-cf27db1e4986	7/1/2019 4:47:15 PM	CN=John Doe,OU=Employees,DC=adatum,DC=com
NGC	AD	MFANotUsed		8/23/2017 5:41:01 PM	CN=John Doe,OU=Employees,DC=adatum,DC=com
FIDO	AzureAD	Attestation	00000000-0000-0000-0000-000000000000	6/21/2019 4:04:56 PM	CN=John Doe,OU=Employees,DC=adatum,DC=com



Wrapping Things Up



Choosing The Right Technology

	Hello for Business	FIDO2	Authenticator App
Security	Platform	Hardware	Software
Removable Authenticator		Keyring	Phone
PIN	✓	✓	✓
Biometrics	Optional	Optional	Optional
Azure AD Sign-In	✓	✓	✓
Modern Auth App Sign-In	✓	✓	✓
Custom Web App Sign-In	✓	✓	Through Azure AD
Windows Sign-In	✓	Through Azure AD	
Phone App Sign-In		Partial Support	✓
Air Gap Scenarios	ADDS+ADFS	3 rd Party ADFS Providers	
Passwordless Provisioning	With a Smart Card	✓	With FIDO2 or a 2 nd Phone
Open Standards	Kerberos PKINIT, OAUTH	W3C WebAuthn, CTAP2	TOTP

Passwordless Authentication in (Azure) Active Directory

Mgr. Michael Grafnetter

@MGrafnetter
dsinternals.com

26. 3. 2020