What is Windows Virtual Desktop

Microsoft service on Azure for VDI/RDSH management

- Enables a multi-user Windows 10 experience, optimized for Office 365 ProPlus
- Most scalable service to deploy and manage
- Most flexible service allowing you to virtualize both desktops and apps
- Windows 7 virtual desktop with free Extended Security Updates
- Integrated with the security and management of Microsoft 365

High level architecture

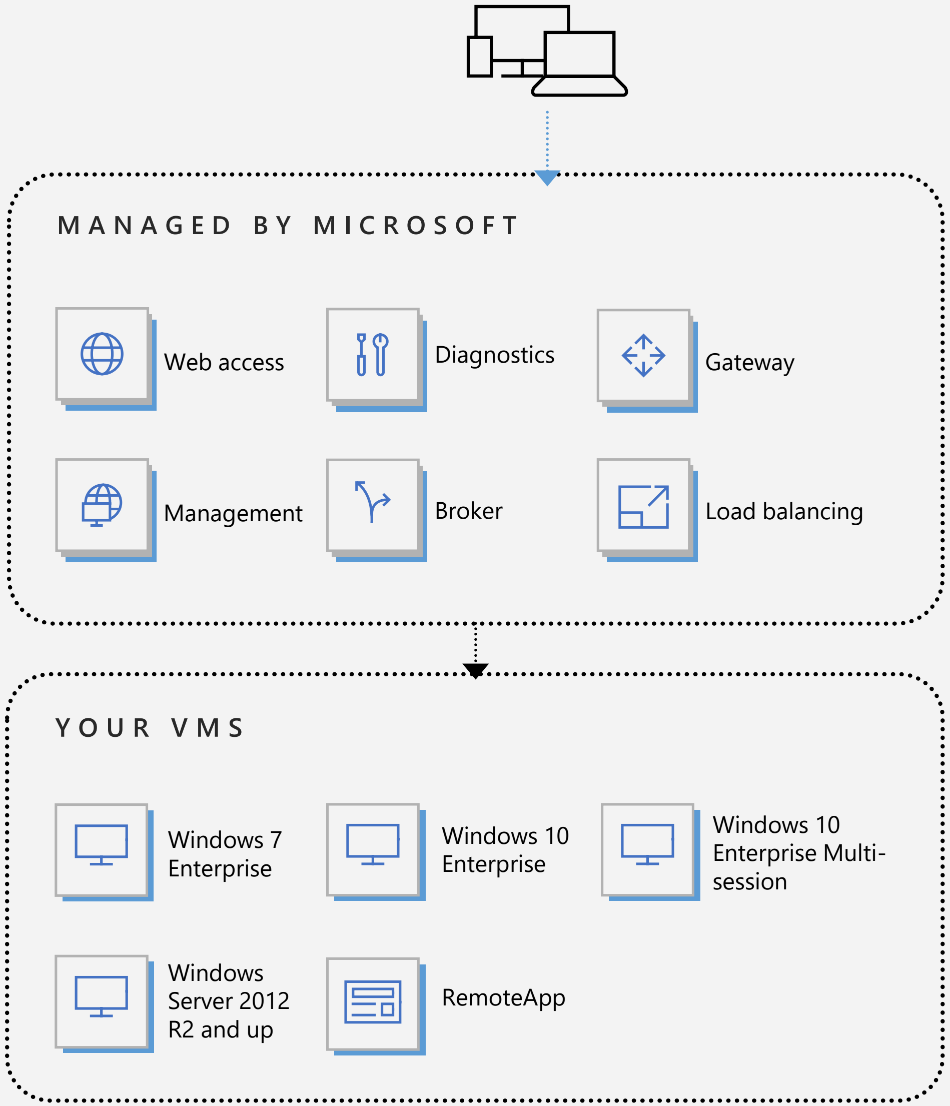
Provides virtualization infrastructure as a managed service

Tools for easy diagnostics and load balancing

Utilizes Azure Active Directory identity management service

Deploy and manage VMs in Azure subscription

Simply connect to on-premise resources



MANAGED BY MICROSOFT

Web access

Diagnostics

Gateway

Management

Broker

Load balancing

YOUR VMS

Windows 7 Enterprise

Windows 10 Enterprise

Windows 10 Enterprise Multi-session

Windows Server 2012 R2 and up

RemoteApp

Multi-user Windows 10 experience

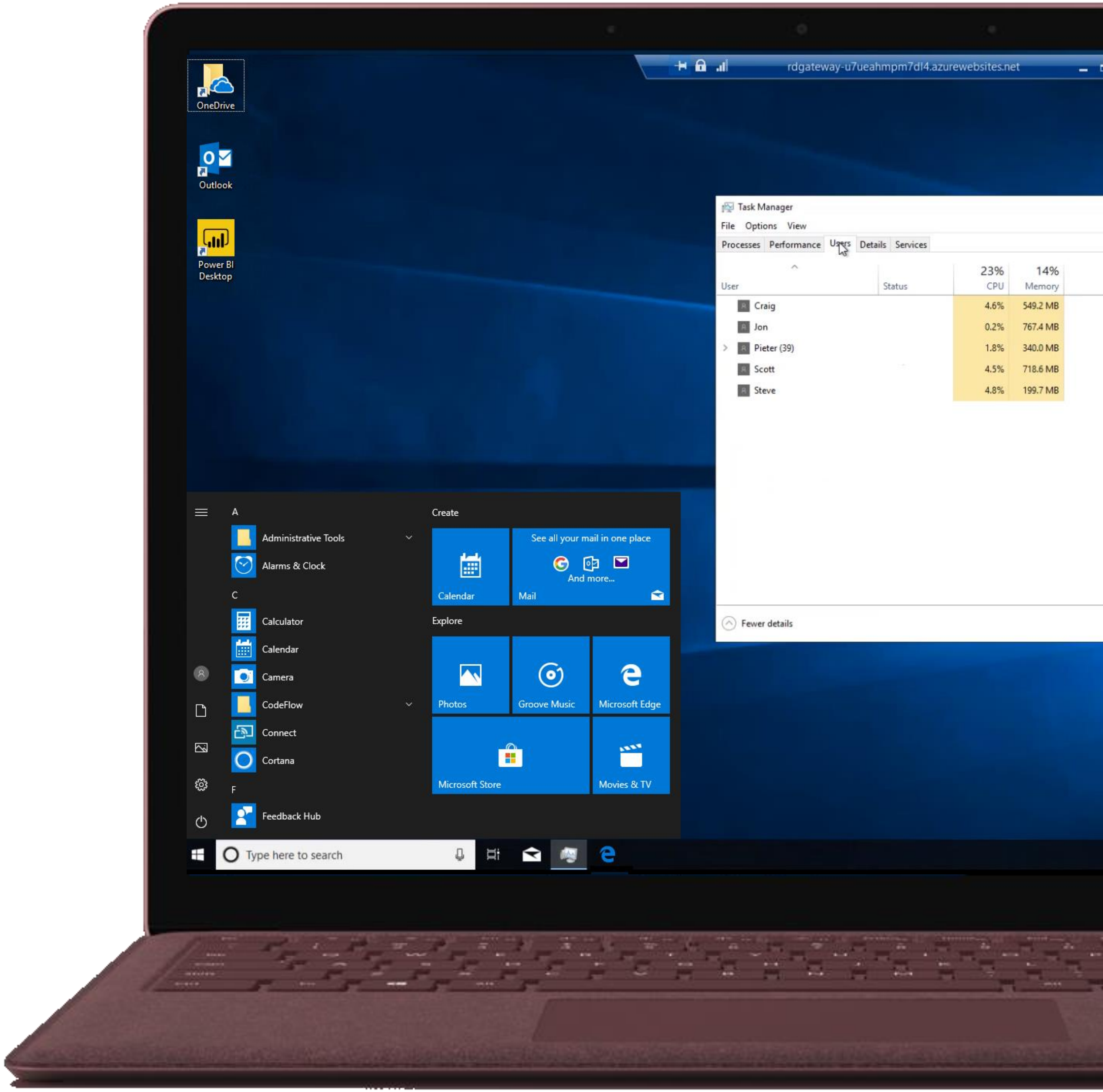
Windows 10 Enterprise with multi-session capability

Semi-annual channel cadence

Great application compatibility

Support for Modern Apps like Edge, Cortana and Microsoft Store

Optimized for Office 365 ProPlus



User	Status	23% CPU	14% Memory
Craig		4.6%	549.2 MB
Jon		0.2%	767.4 MB
Pieter (39)		1.8%	340.0 MB
Scott		4.5%	718.6 MB
Steve		4.8%	199.7 MB

Eliminate passwords

"One of the biggest security issues is passwords." ~ Satya Nadella

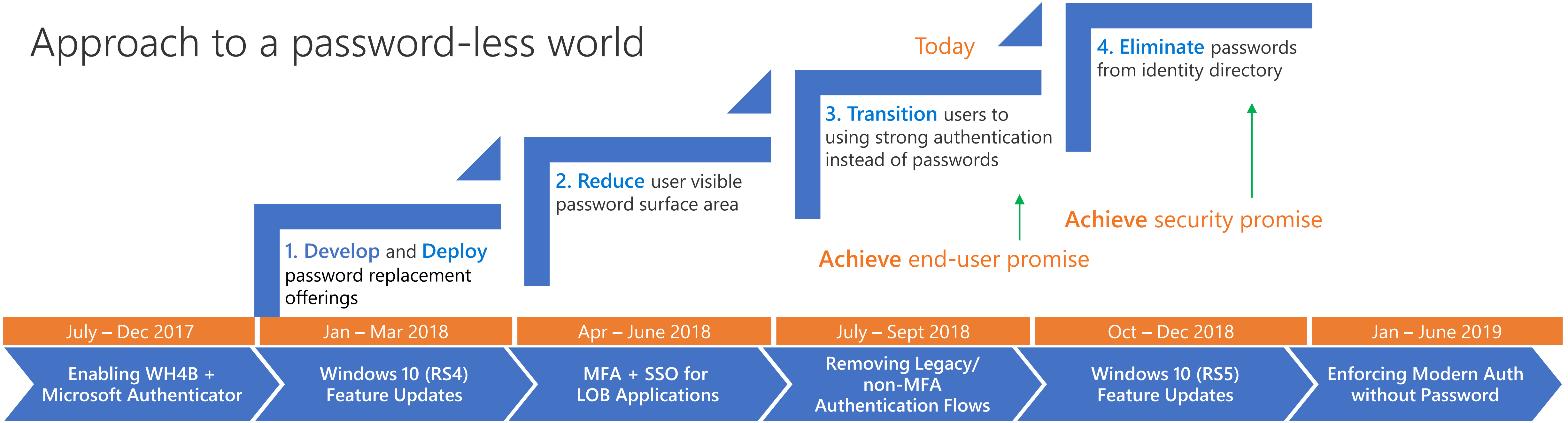
Through strong and Multi-factor Authentication (MFA)

Biometric on Device — Windows Hello for Business – Available on all Windows 10 Machines **TODAY** with improvements coming in RS4 and RS5

Microsoft Authenticator — Microsoft Authenticator – Available **TODAY** across all mobile platforms, integral in corporate bootstrapping of MFA

Device + Biometric — FIDO 2.0 Devices – Enabling ultimate flexibility for users and increase security across all forms of Identity and Auth *(Coming soon)*

Approach to a password-less world



Today

1. **Develop** and **Deploy** password replacement offerings

2. **Reduce** user visible password surface area

3. **Transition** users to using strong authentication instead of passwords

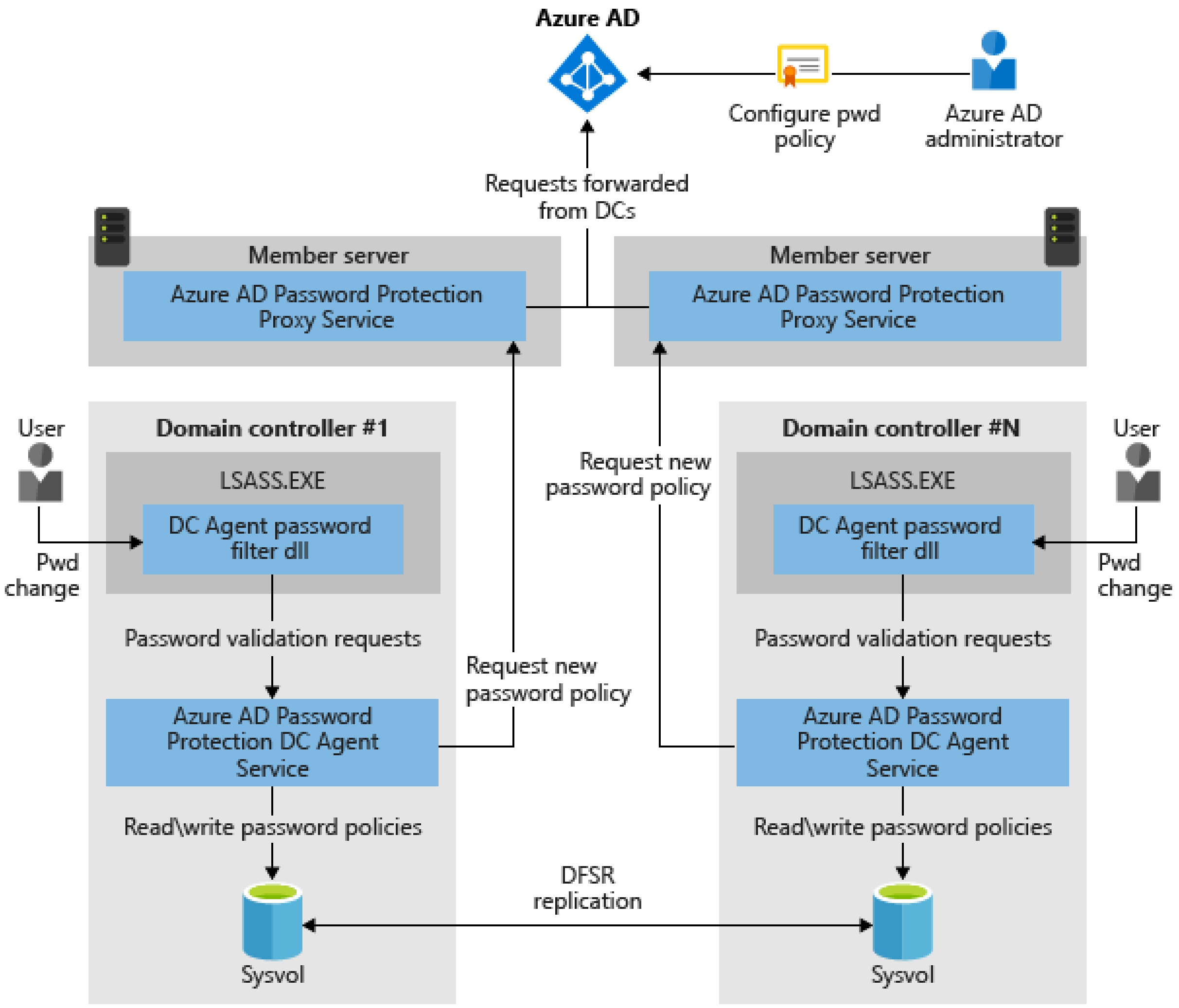
4. **Eliminate** passwords from identity directory

Achieve end-user promise

Achieve security promise

July – Dec 2017	Jan – Mar 2018	Apr – June 2018	July – Sept 2018	Oct – Dec 2018	Jan – June 2019
Enabling WH4B + Microsoft Authenticator	Windows 10 (RS4) Feature Updates	MFA + SSO for LOB Applications	Removing Legacy/ non-MFA Authentication Flows	Windows 10 (RS5) Feature Updates	Enforcing Modern Auth without Password

Leveraging Azure Password Protection


Azure AD
Configure pwd policy
Azure AD administrator
Requests forwarded from DCs
Member server
Azure AD Password Protection Proxy Service
Member server
Azure AD Password Protection Proxy Service
User
Domain controller #1
LSASS.EXE
DC Agent password filter dll
Pwd change
Password validation requests
Azure AD Password Protection DC Agent Service
Read\write password policies
Sysvol
Request new password policy
Request new password policy
DFSR replication
Domain controller #N
LSASS.EXE
DC Agent password filter dll
User
Pwd change
Password validation requests
Azure AD Password Protection DC Agent Service
Read\write password policies
Sysvol

- Leverage the power of the Azure cloud by enforcing a “banned password list” on premises

- As users are trying to change their passwords, they get blocked from using easily guessable passwords, (like Password1)

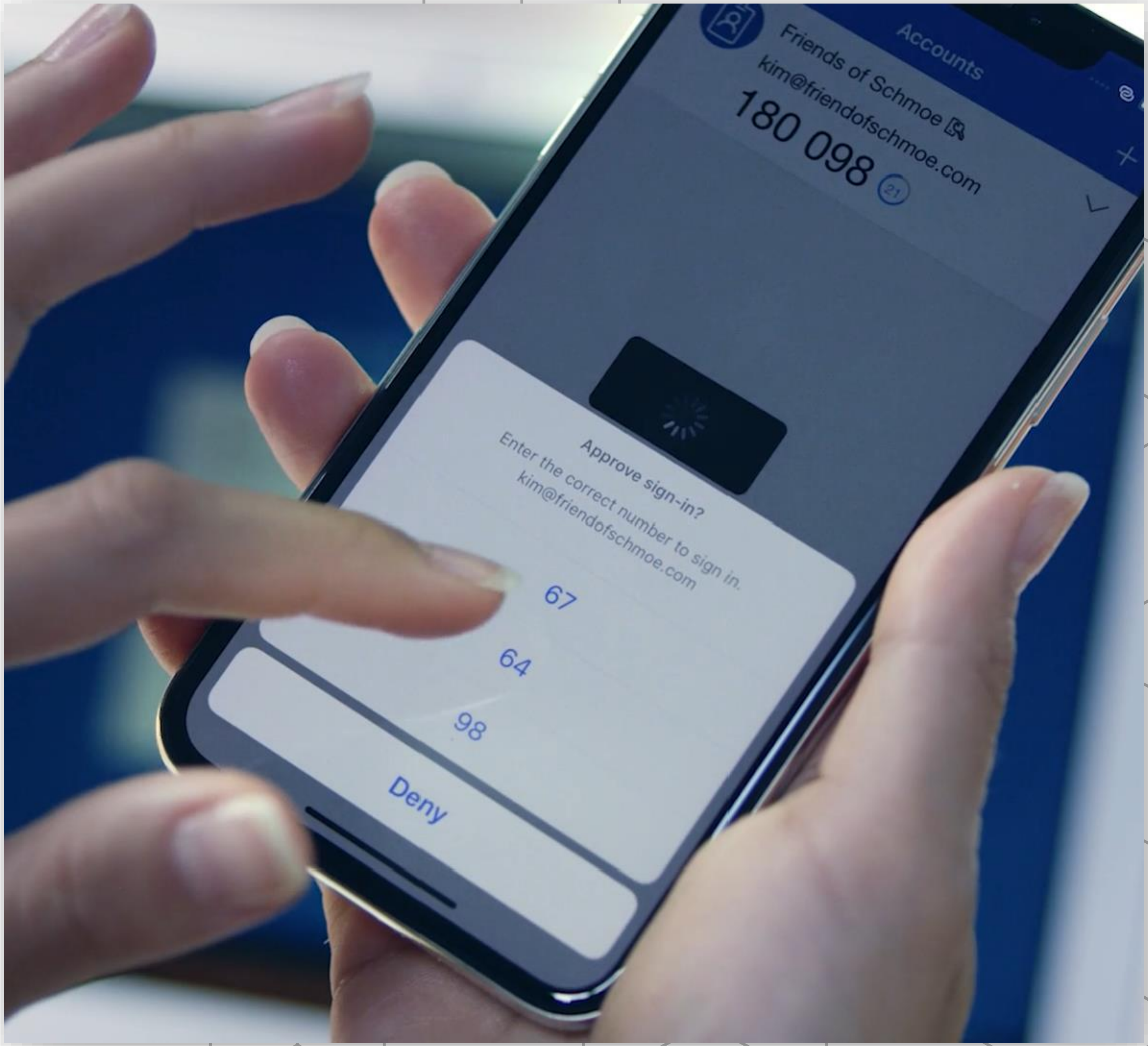
- This increases security for the IT Admin, and decreases cost for security incident responders

10:36

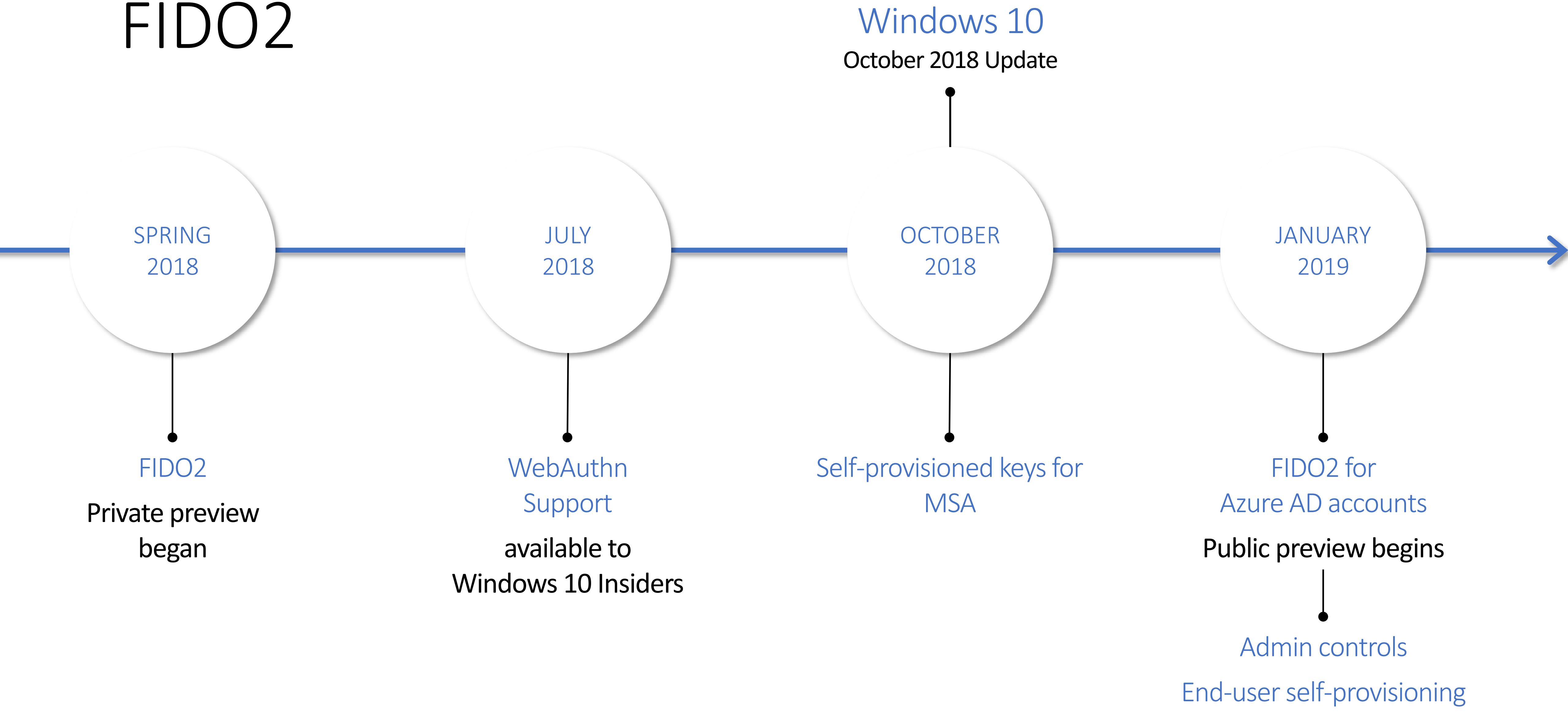
Friday, September 14

Microsoft Authenticator

Microsoft's password-less anywhere solution



FIDO2



Windows 10

October 2018 Update

SPRING 2018

FIDO2

Private preview began

JULY 2018

WebAuthn Support

available to Windows 10 Insiders

OCTOBER 2018

Self-provisioned keys for MSA

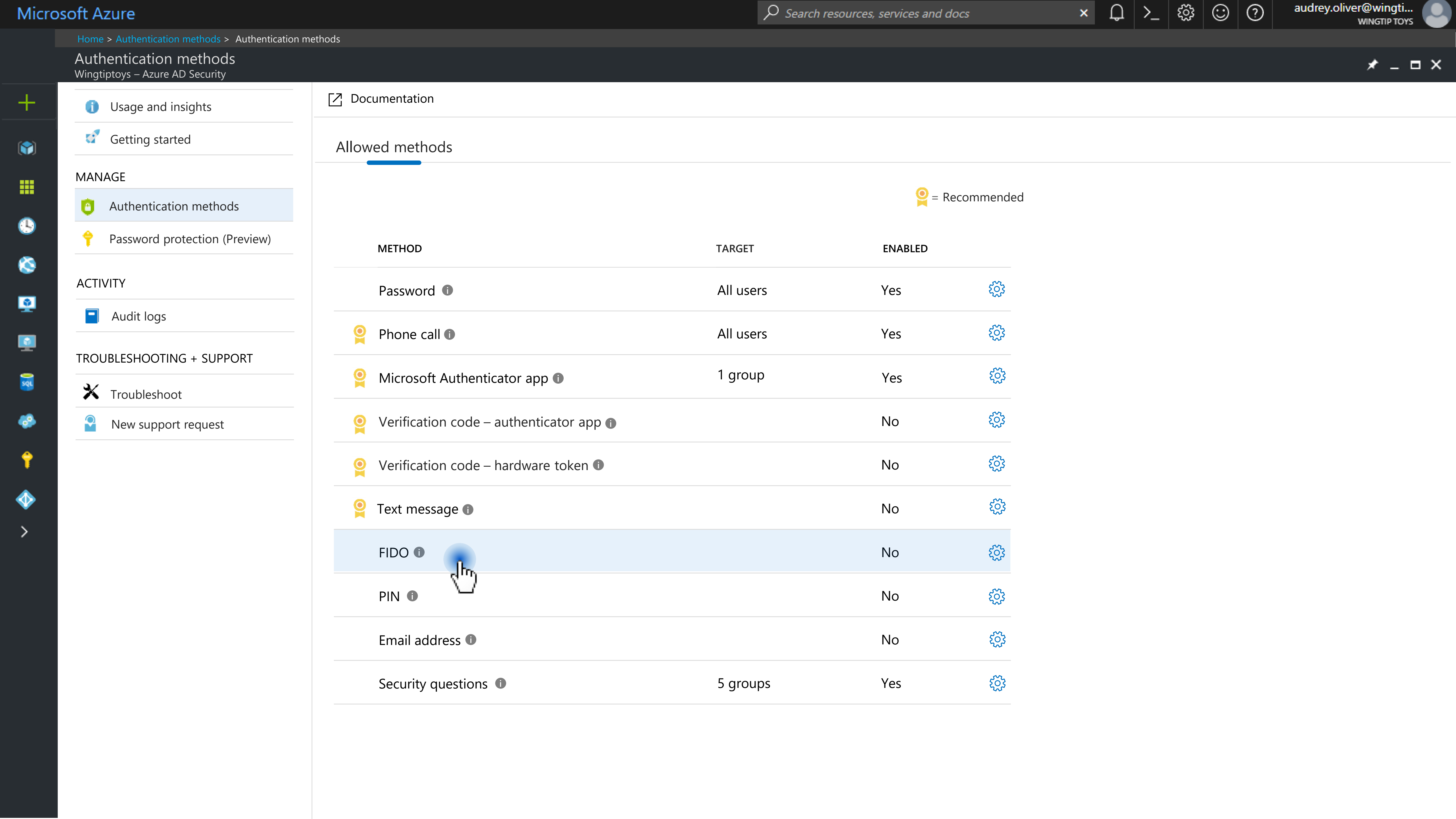
JANUARY 2019

FIDO2 for Azure AD accounts

Public preview begins

Admin controls

End-user self-provisioning



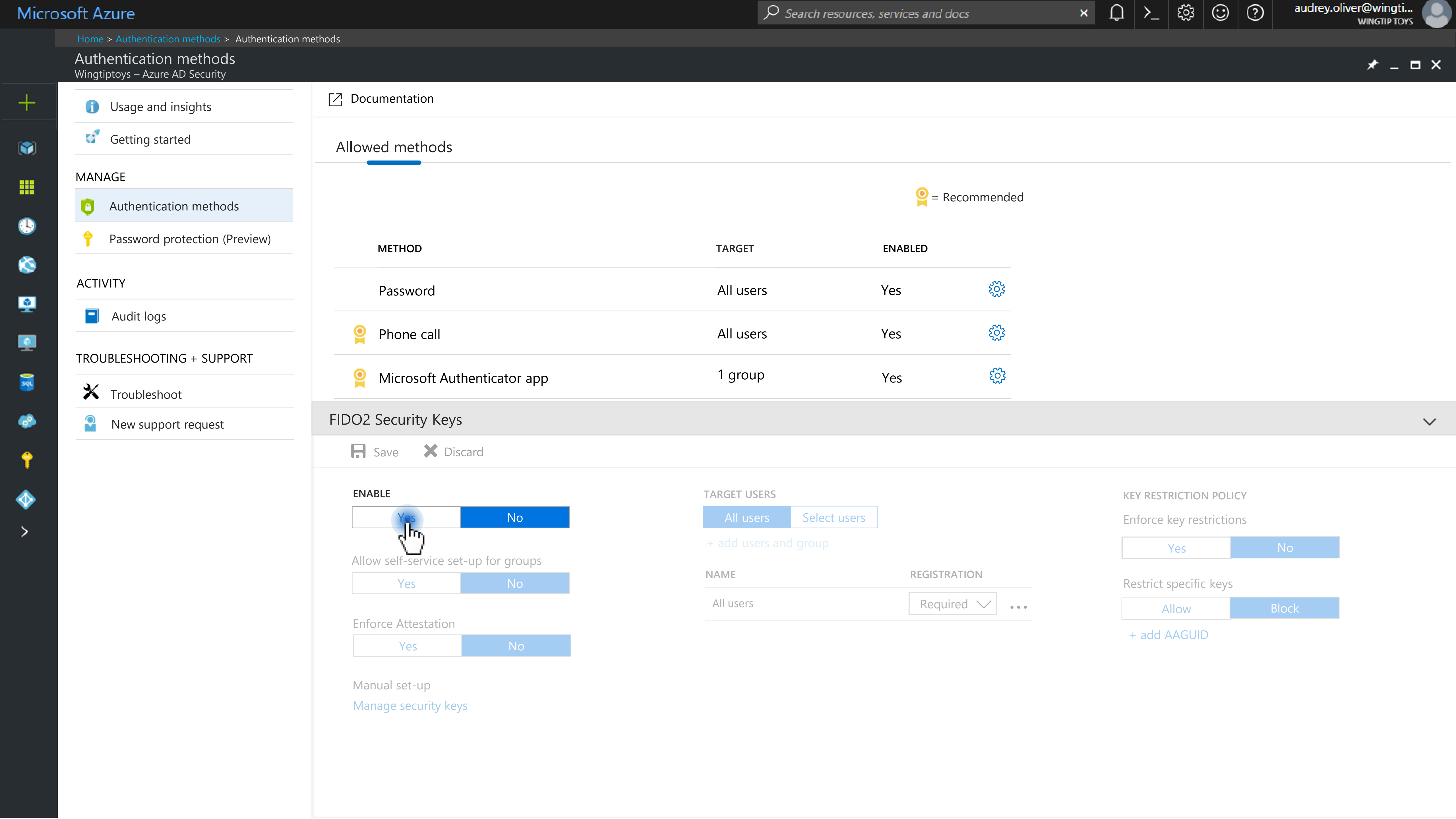
Authentication methods

Wingtiptoys – Azure AD Security

Allowed methods

🏅 = Recommended

	METHOD	TARGET	ENABLED
	Password	All users	Yes
🏅	Phone call	All users	Yes
🏅	Microsoft Authenticator app	1 group	Yes
🏅	Verification code – authenticator app		No
🏅	Verification code – hardware token		No
🏅	Text message		No
	FIDO		No
	PIN		No
	Email address		No
	Security questions	5 groups	Yes



Authentication methods

Wingtiptoys – Azure AD Security

Allowed methods

🏅 = Recommended

METHOD	TARGET	ENABLED
Password	All users	Yes
🏅 Phone call	All users	Yes
🏅 Microsoft Authenticator app	1 group	Yes

FIDO2 Security Keys

ENABLE

Yes [✓ No]

Allow self-service set-up for groups

Yes [✓ No]

Enforce Attestation

Yes [✓ No]

Manual set-up

Manage security keys

TARGET USERS

[✓ All users] Select users

+ add users and group

NAME	REGISTRATION
All users	Required

KEY RESTRICTION POLICY

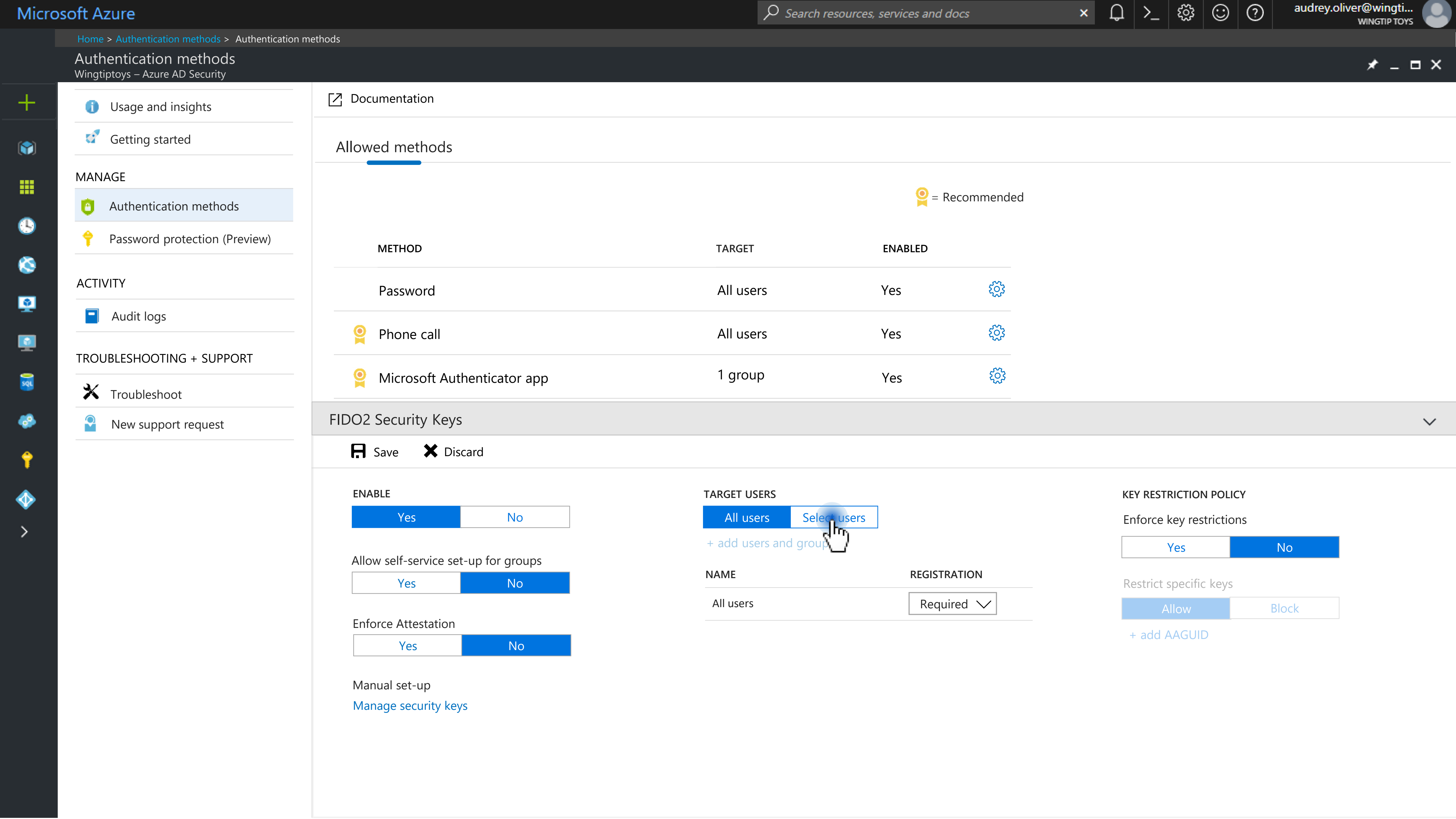
Enforce key restrictions

Yes [✓ No]

Restrict specific keys

Allow [✓ Block]

+ add AAGUID



METHOD	TARGET	ENABLED
Password	All users	Yes
Phone call	All users	Yes
Microsoft Authenticator app	1 group	Yes

FIDO2 Security Keys

ENABLE: [✓ Yes] No

Allow self-service set-up for groups: Yes [✓ No]

Enforce Attestation: Yes [✓ No]

Manual set-up

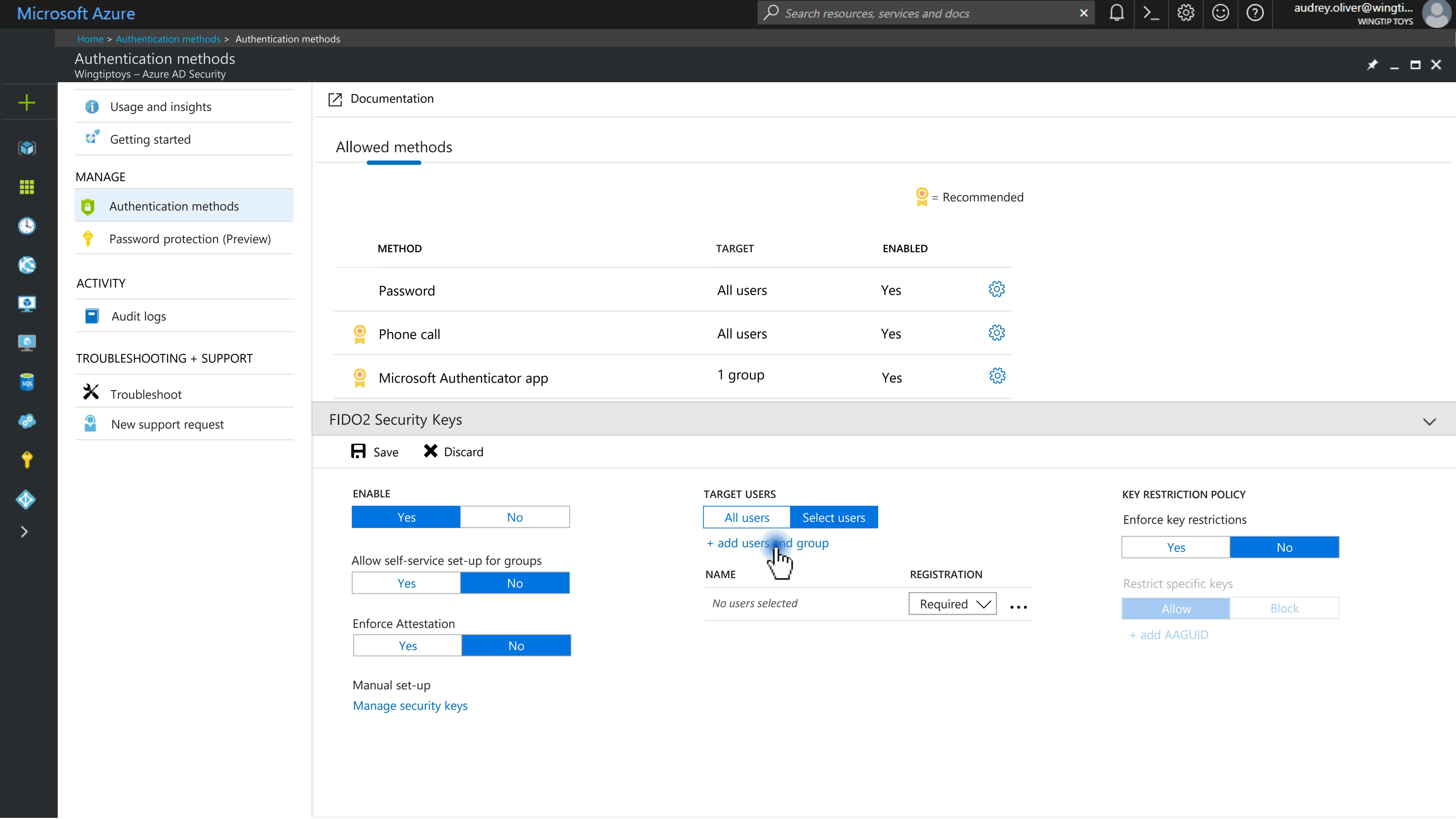
TARGET USERS: [✓ All users] Select users

NAME	REGISTRATION
All users	Required

KEY RESTRICTION POLICY

Enforce key restrictions: Yes [✓ No]

Restrict specific keys: [✓ Allow] Block



Authentication methods

Wingtiptoys – Azure AD Security

Allowed methods

🏅 = Recommended

	METHOD	TARGET	ENABLED
	Password	All users	Yes
🏅	Phone call	All users	Yes
🏅	Microsoft Authenticator app	1 group	Yes

FIDO2 Security Keys

ENABLE

[✓ Yes] No

Allow self-service set-up for groups

Yes [✓ No]

Enforce Attestation

Yes [✓ No]

Manual set-up

Manage security keys

TARGET USERS

All users [✓ Select users]

+ add users and group

NAME	REGISTRATION
No users selected	Required

KEY RESTRICTION POLICY

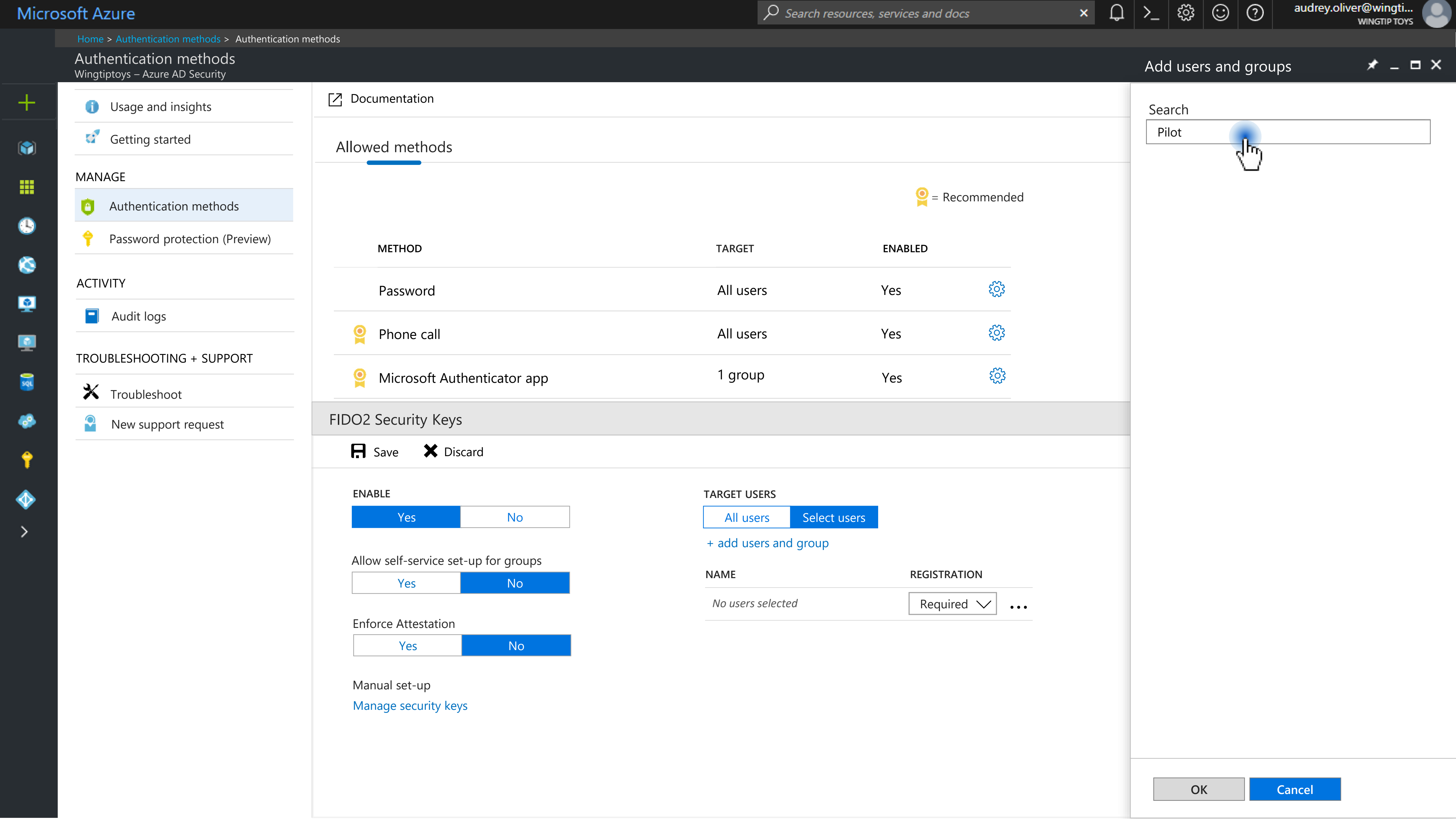
Enforce key restrictions

Yes [✓ No]

Restrict specific keys

[✓ Allow] Block

+ add AAGUID



Microsoft Azure
Search resources, services and docs
audrey.oliver@wingti...
WINGTIP TOYS
Home > Authentication methods > Authentication methods

Authentication methods

Wingtiptoys – Azure AD Security

Allowed methods

🎖 = Recommended

METHOD	TARGET	ENABLED
Password	All users	Yes
🎖 Phone call	All users	Yes
🎖 Microsoft Authenticator app	1 group	Yes

FIDO2 Security Keys

ENABLE

[✓ Yes] No

Allow self-service set-up for groups

Yes [✓ No]

Enforce Attestation

Yes [✓ No]

Manual set-up

Manage security keys

TARGET USERS

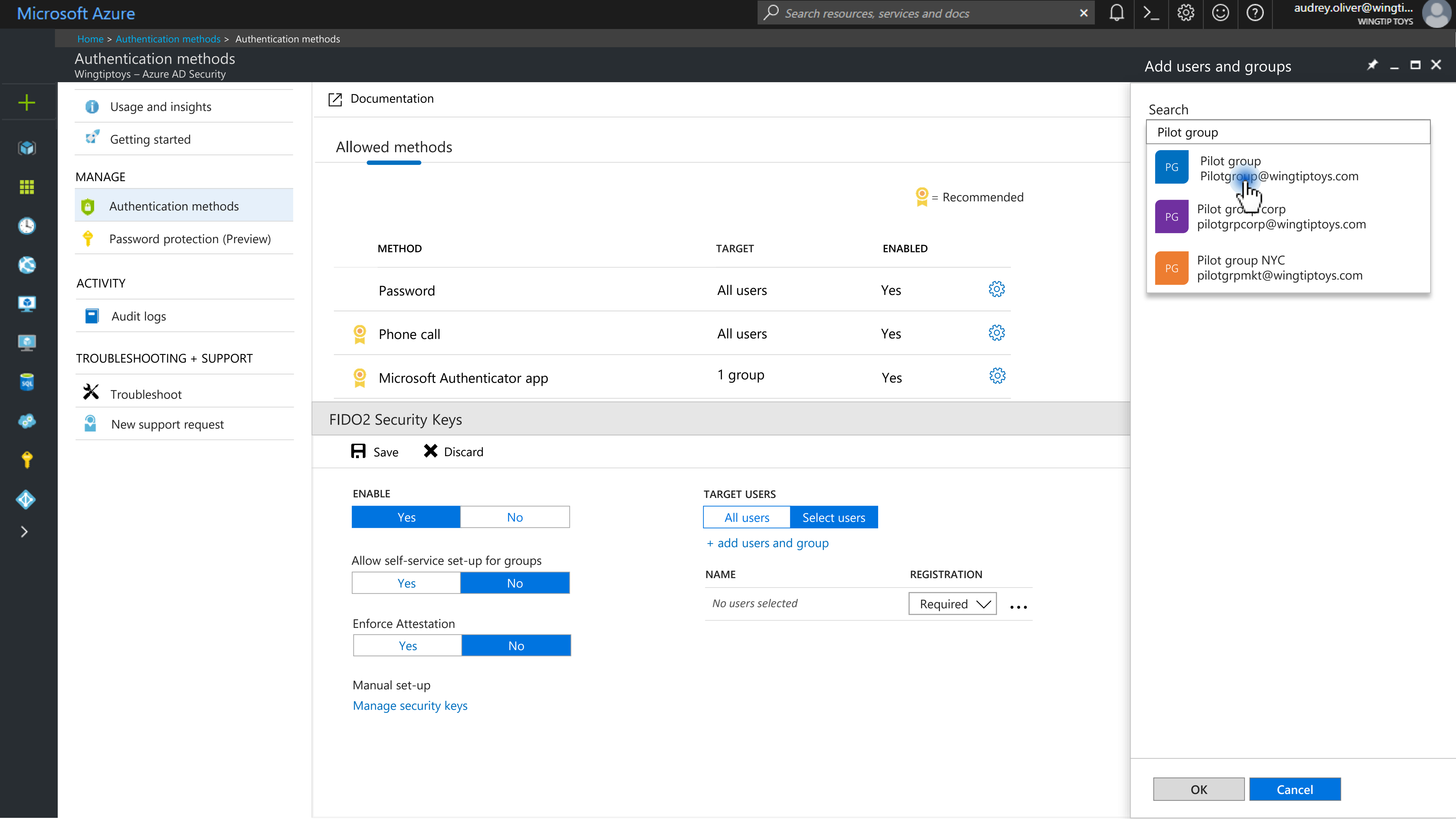
All users [✓ Select users]

+ add users and group

NAME	REGISTRATION
No users selected	Required

Add users and groups

Search: Pilot



Microsoft Azure

Search resources, services and docs

audrey.oliver@wingti...
WINGTIP TOYS

Home > Authentication methods > Authentication methods

Authentication methods

Wingtiptoys – Azure AD Security

- Usage and insights
- Getting started

MANAGE

- Authentication methods
- Password protection (Preview)

ACTIVITY

- Audit logs

TROUBLESHOOTING + SUPPORT

- Troubleshoot
- New support request

Documentation

Allowed methods

= Recommended

METHOD	TARGET	ENABLED
Password	All users	Yes
Phone call	All users	Yes
Microsoft Authenticator app	1 group	Yes

FIDO2 Security Keys

Save   Discard

ENABLE

Yes [✓] | No

Allow self-service set-up for groups

Yes | No [✓]

Enforce Attestation

Yes | No [✓]

Manual set-up

Manage security keys

TARGET USERS

All users | Select users [✓]

+ add users and group

NAME	REGISTRATION
No users selected	Required

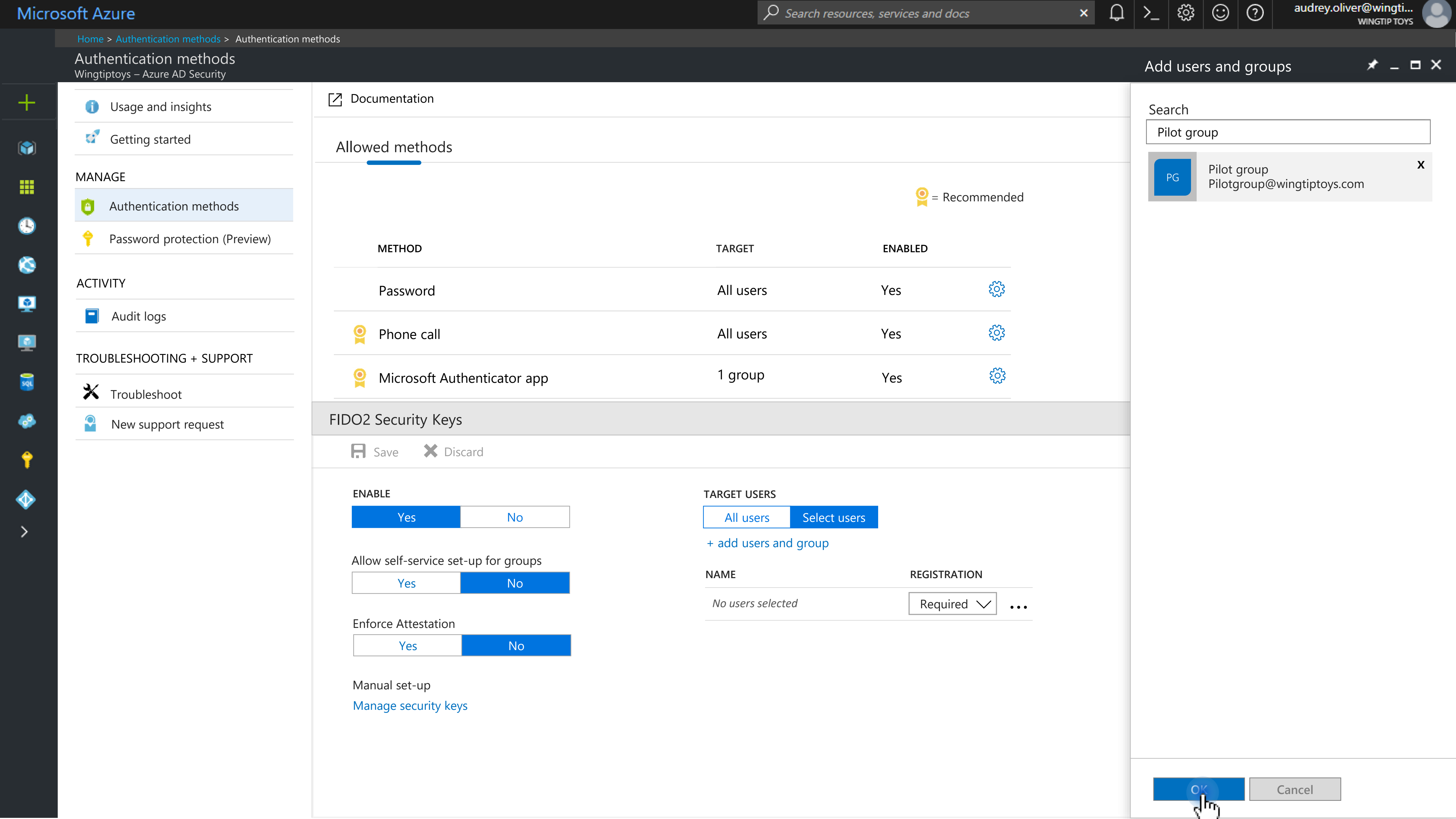
Add users and groups

Search

Pilot group

PG	Pilot group Pilotgroup@wingtiptoys.com
PG	Pilot gro[illegible]corp pilotgrpcorp@wingtiptoys.com
PG	Pilot group NYC pilotgrpmkt@wingtiptoys.com

OK   Cancel


Microsoft Azure
Search resources, services and docs
audrey.oliver@wingti...
WINGTIP TOYS
Home > Authentication methods > Authentication methods

Authentication methods
Wingtiptoys – Azure AD Security

Allowed methods

🎖 = Recommended

METHOD	TARGET	ENABLED
Password	All users	Yes
🎖 Phone call	All users	Yes
🎖 Microsoft Authenticator app	1 group	Yes

FIDO2 Security Keys

ENABLE
[✓ Yes] No

Allow self-service set-up for groups
Yes [✓ No]

Enforce Attestation
Yes [✓ No]

Manual set-up
Manage security keys

TARGET USERS
All users [✓ Select users]

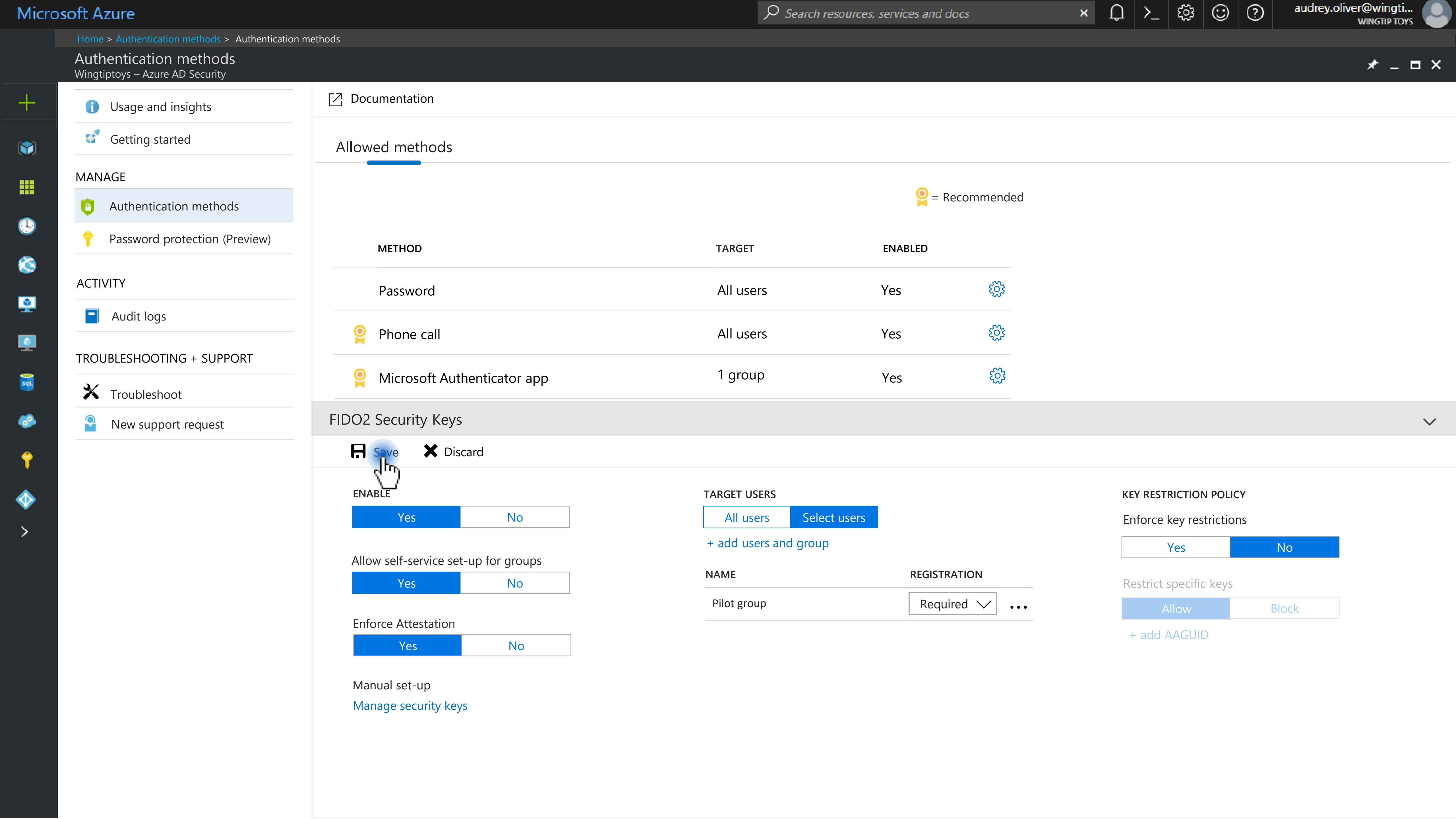
+ add users and group

NAME	REGISTRATION
No users selected	Required

Add users and groups

Search
Pilot group

PG Pilot group
Pilotgroup@wingtiptoys.com



Microsoft Azure

Search resources, services and docs

audrey.oliver@wingti...
WINGTIP TOYS

Home > Authentication methods > Authentication methods

Authentication methods
Wingtiptoys – Azure AD Security

Usage and insights

Getting started

MANAGE

Authentication methods

Password protection (Preview)

ACTIVITY

Audit logs

TROUBLESHOOTING + SUPPORT

Troubleshoot

New support request

Documentation

Allowed methods

= Recommended

METHOD	TARGET	ENABLED
Password	All users	Yes
Phone call	All users	Yes
Microsoft Authenticator app	1 group	Yes

FIDO2 Security Keys

Save Discard

ENABLE

[✓ Yes] No

Allow self-service set-up for groups

[✓ Yes] No

Enforce Attestation

[✓ Yes] No

Manual set-up

Manage security keys

TARGET USERS

All users [✓ Select users]

+ add users and group

NAME	REGISTRATION
Pilot group	Required

KEY RESTRICTION POLICY

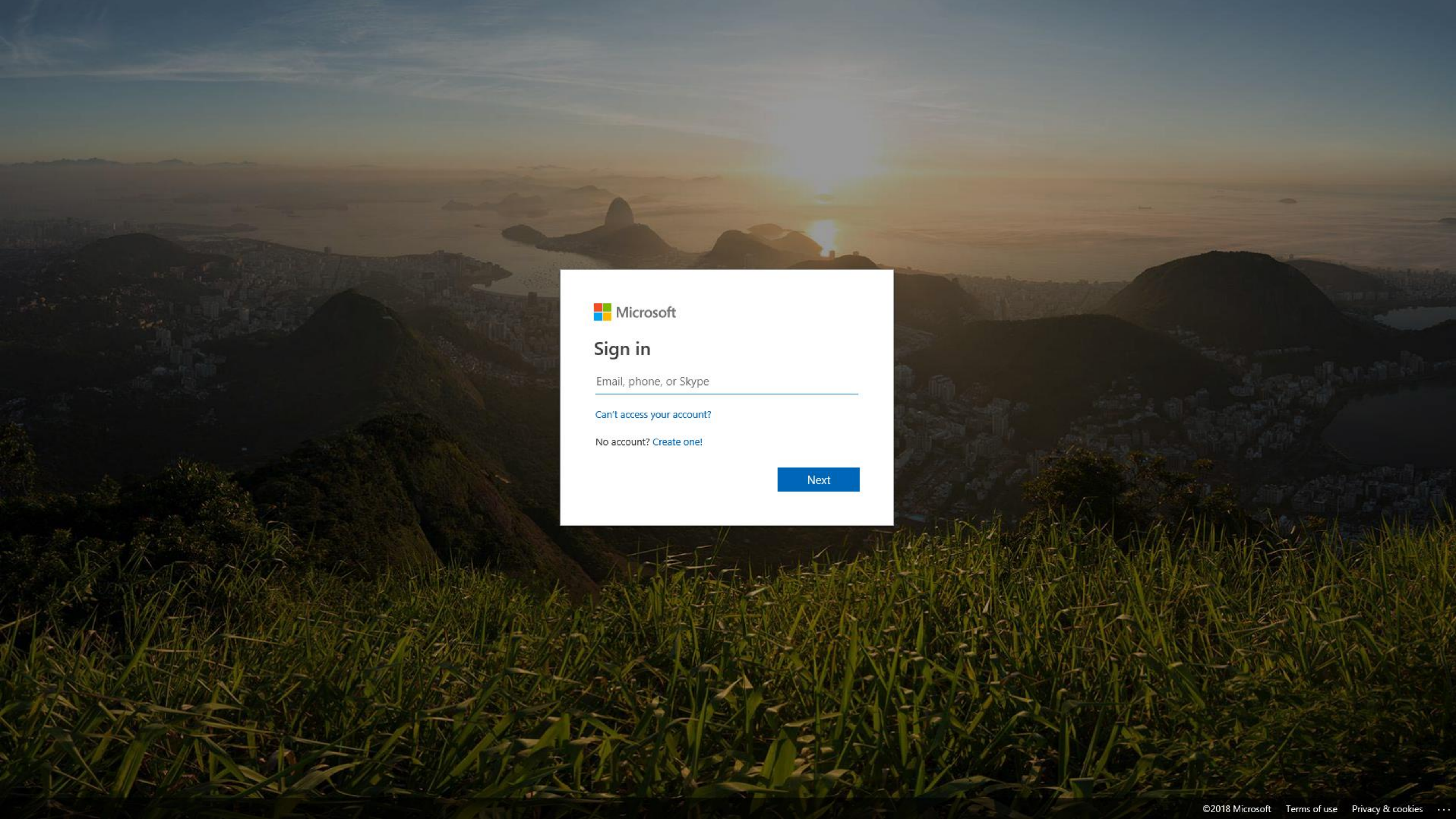
Enforce key restrictions

Yes [✓ No]

Restrict specific keys

[✓ Allow] Block

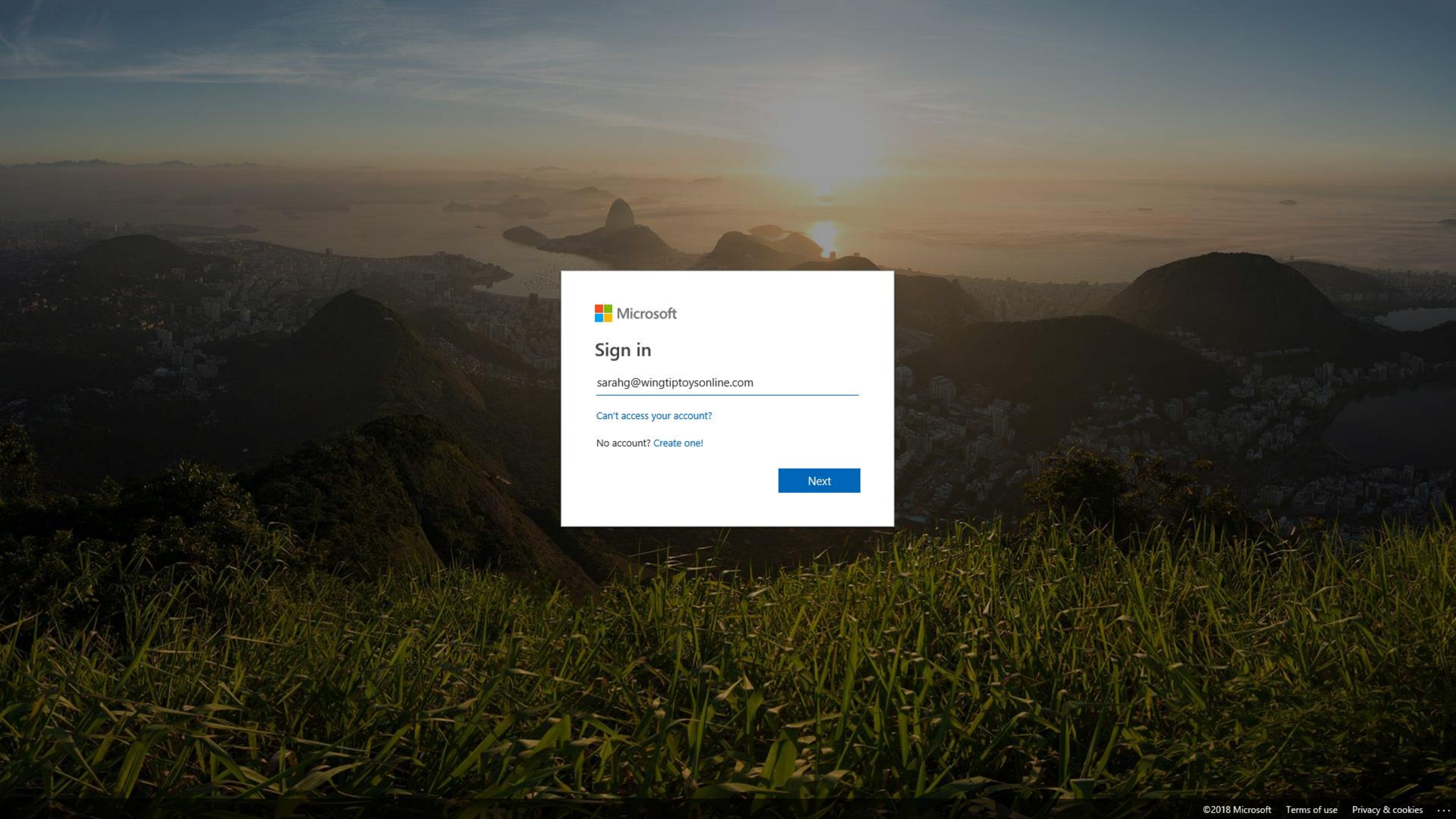
+ add AAGUID



Sign in

Can't access your account?

No account? Create one!

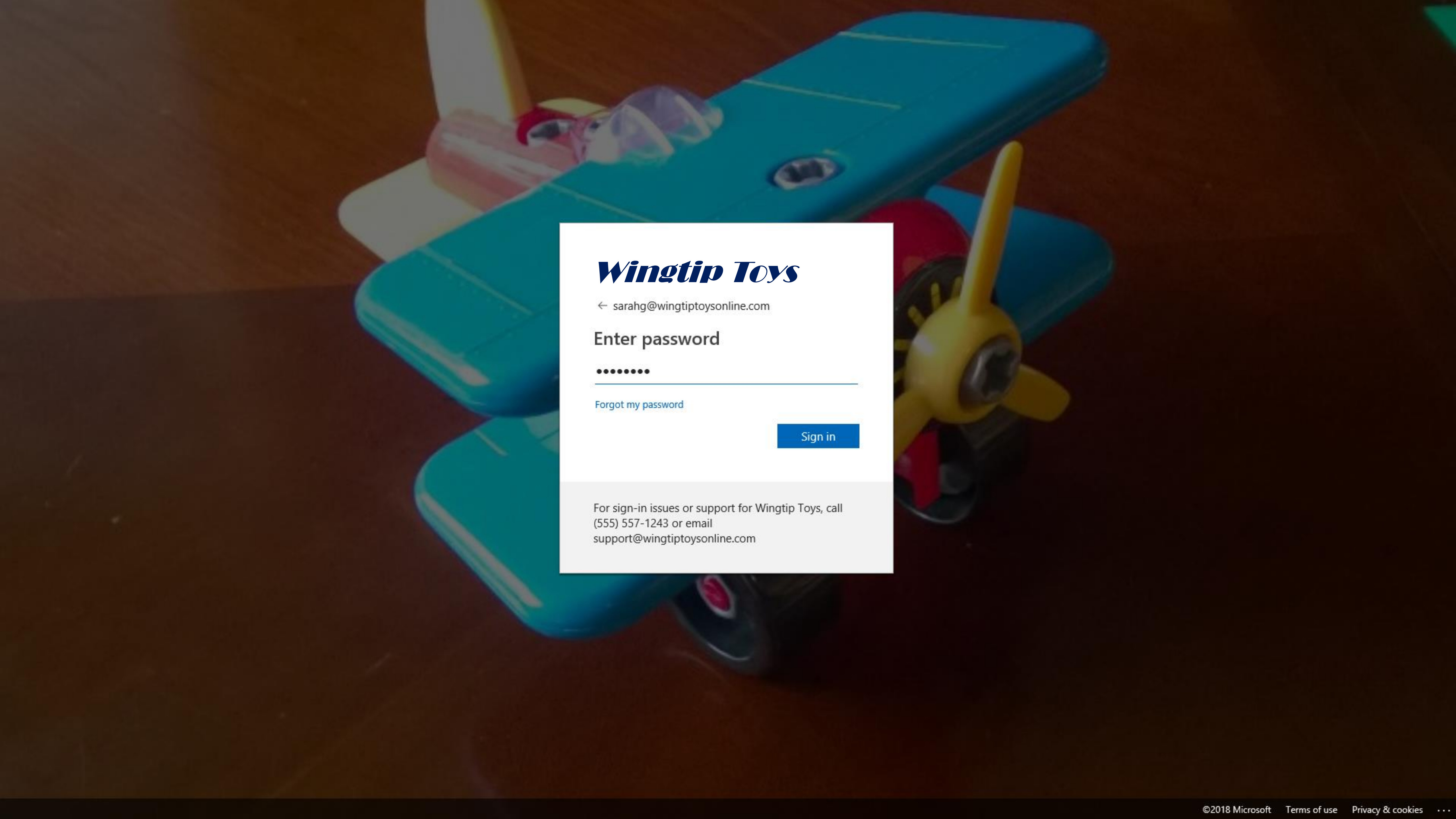


Sign in

sarahg@wingtiptoysonline.com

Can’t access your account?

No account? Create one!



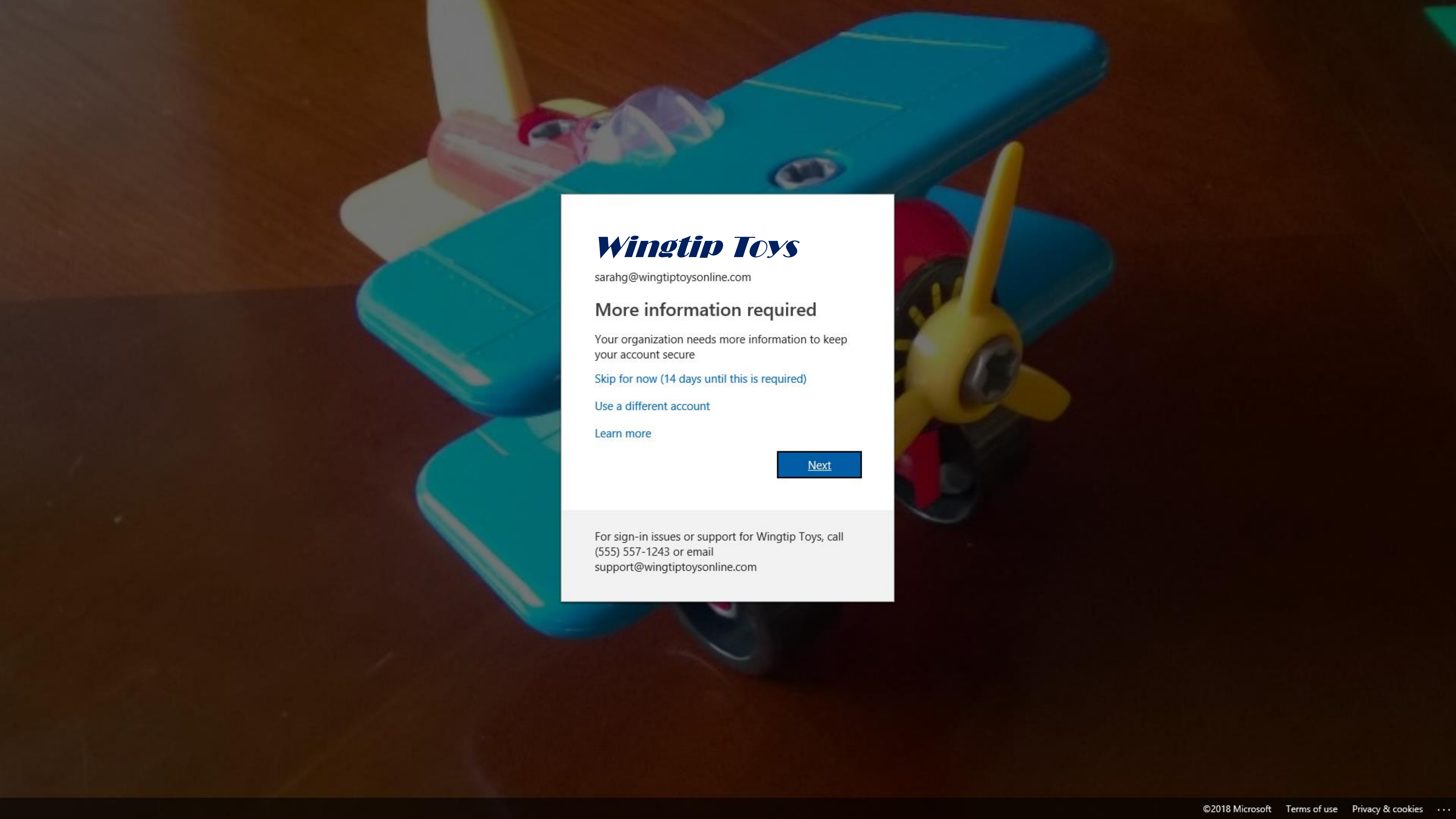
Wingtip Toys

← sarahg@wingtiptoysonline.com

Enter password

••••••••

For sign-in issues or support for Wingtip Toys, call (555) 557-1243 or email support@wingtiptoysonline.com



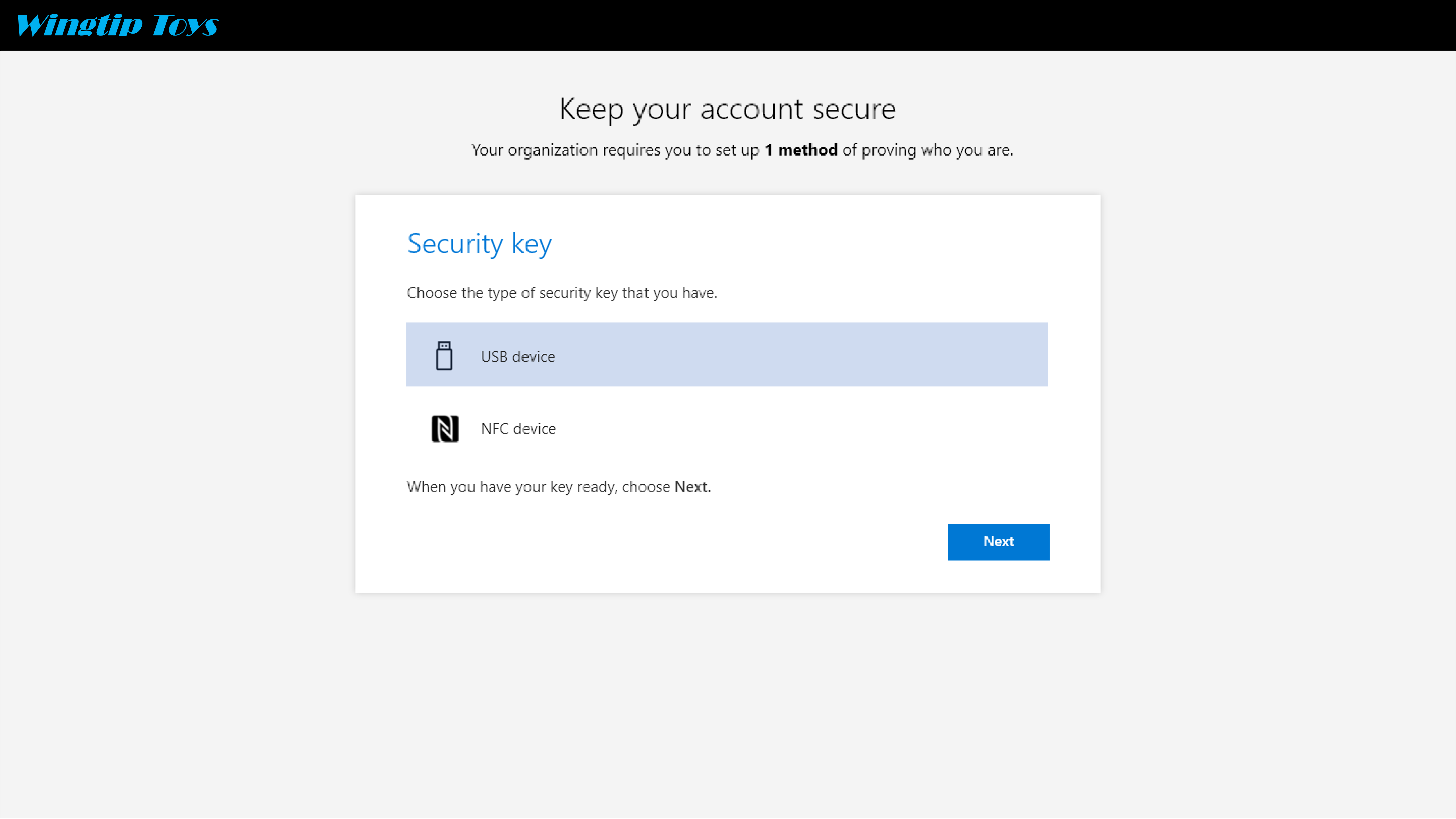
Wingtip Toys

sarahg@wingtiptoysonline.com

More information required

Your organization needs more information to keep your account secure

For sign-in issues or support for Wingtip Toys, call (555) 557-1243 or email support@wingtiptoysonline.com



Keep your account secure

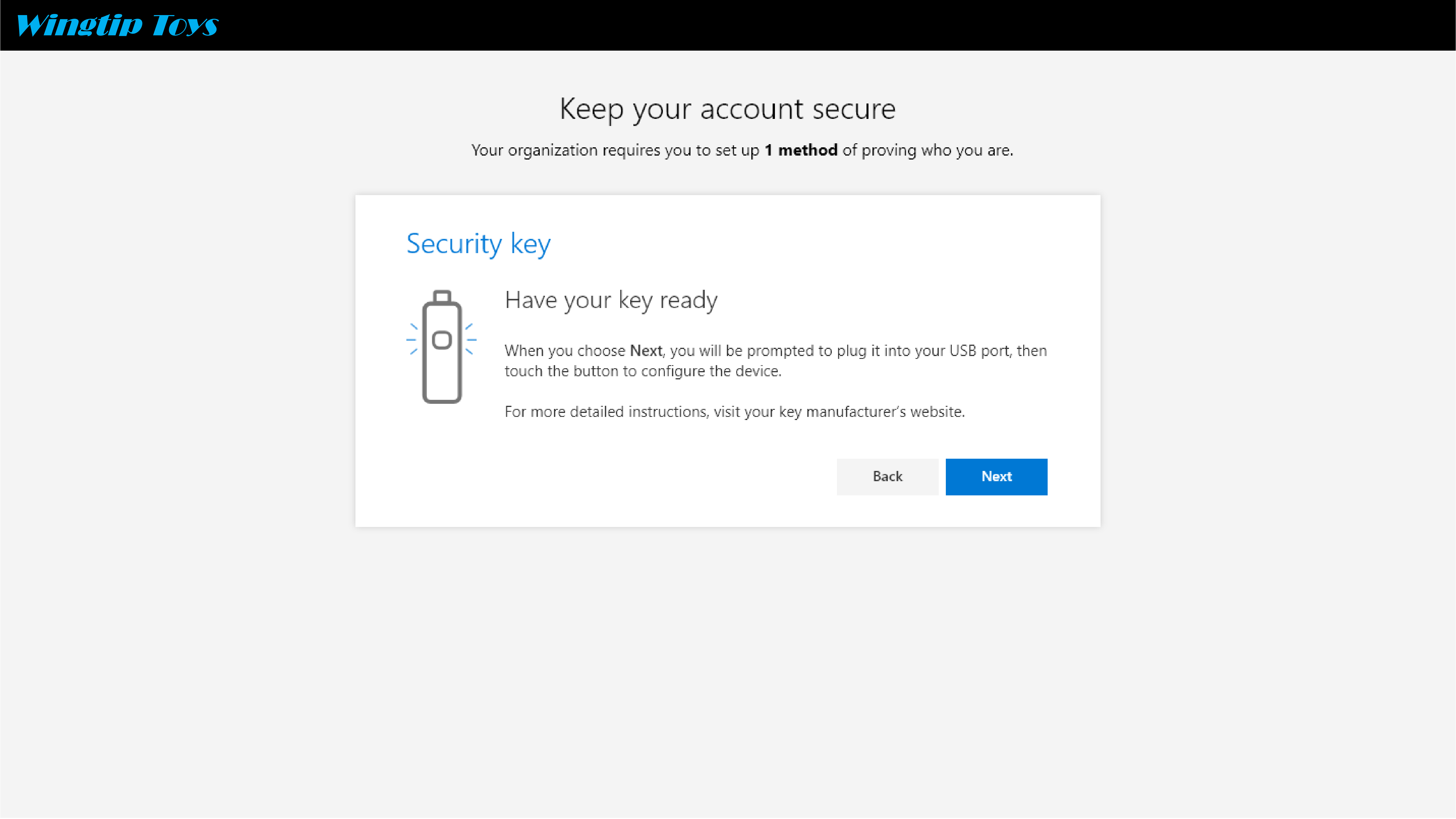
Your organization requires you to set up **1 method** of proving who you are.

Security key

Choose the type of security key that you have.

- USB device
- NFC device

When you have your key ready, choose **Next.**



Wingtip Toys

Keep your account secure

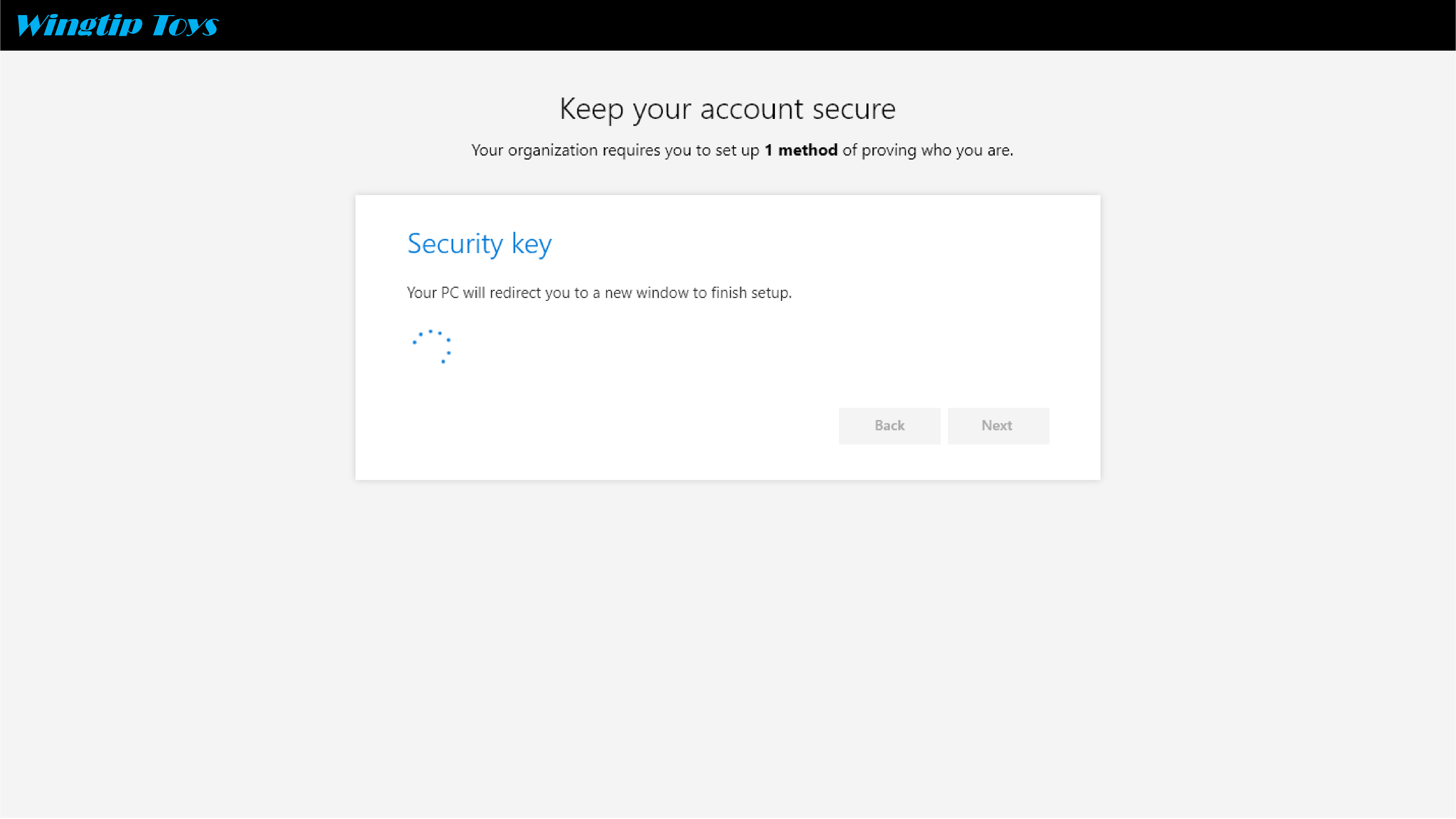
Your organization requires you to set up **1 method** of proving who you are.

Security key

Have your key ready

When you choose **Next**, you will be prompted to plug it into your USB port, then touch the button to configure the device.

For more detailed instructions, visit your key manufacturer's website.

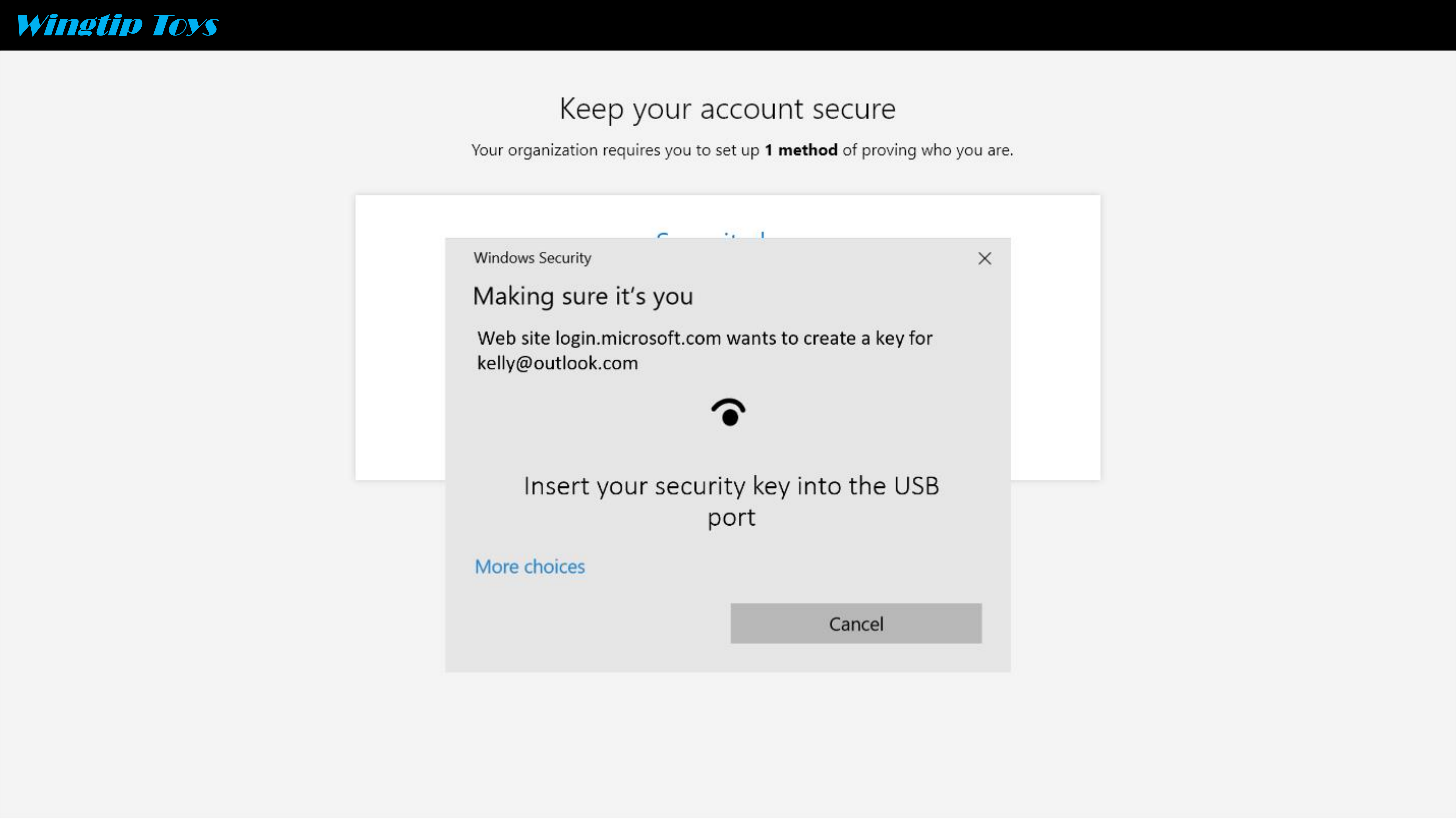


Keep your account secure

Your organization requires you to set up **1 method** of proving who you are.

Security key

Your PC will redirect you to a new window to finish setup.



Wingtip Toys

Keep your account secure

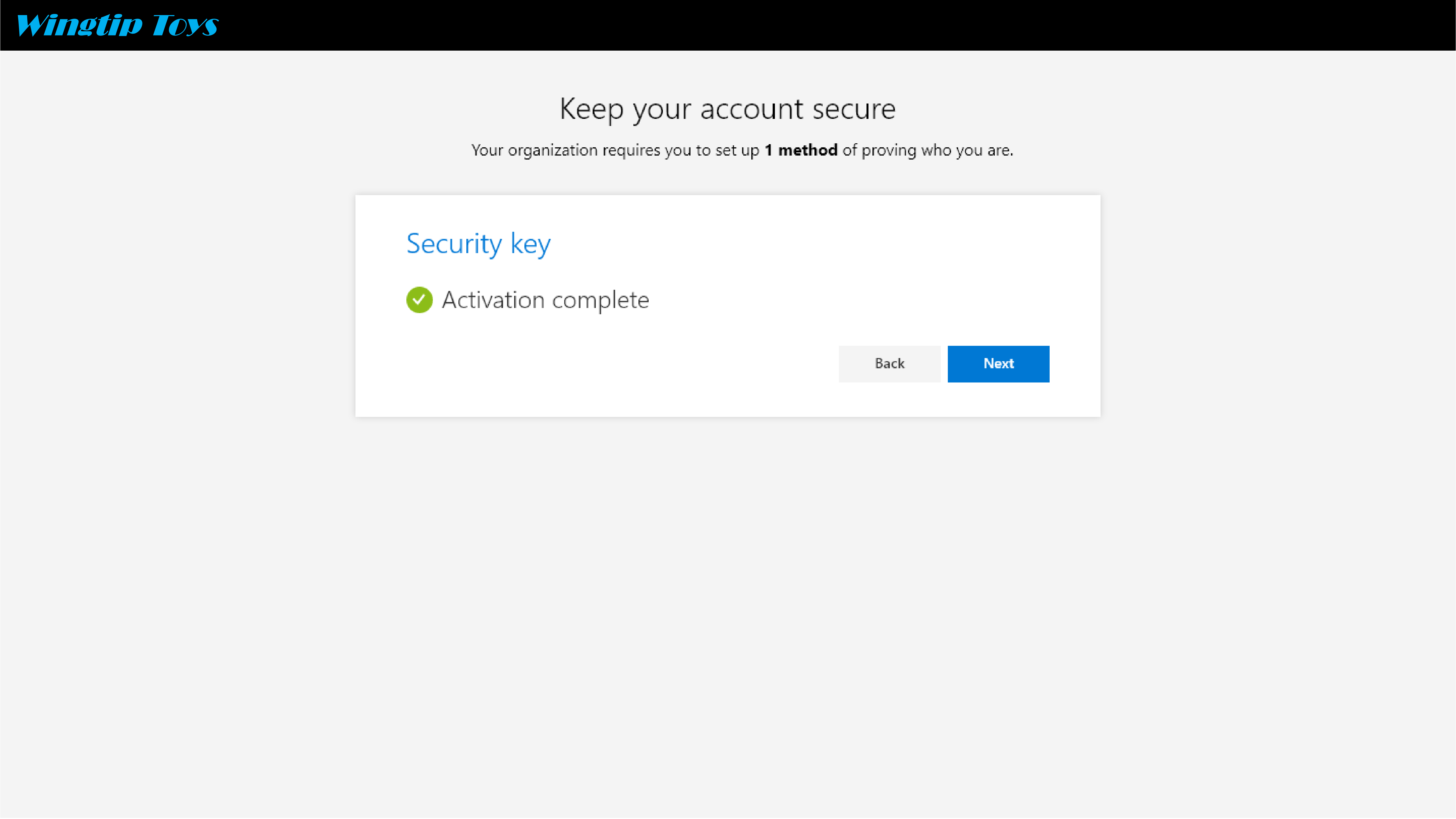
Your organization requires you to set up **1 method** of proving who you are.

Windows Security

Making sure it's you

Web site login.microsoft.com wants to create a key for kelly@outlook.com

Insert your security key into the USB port



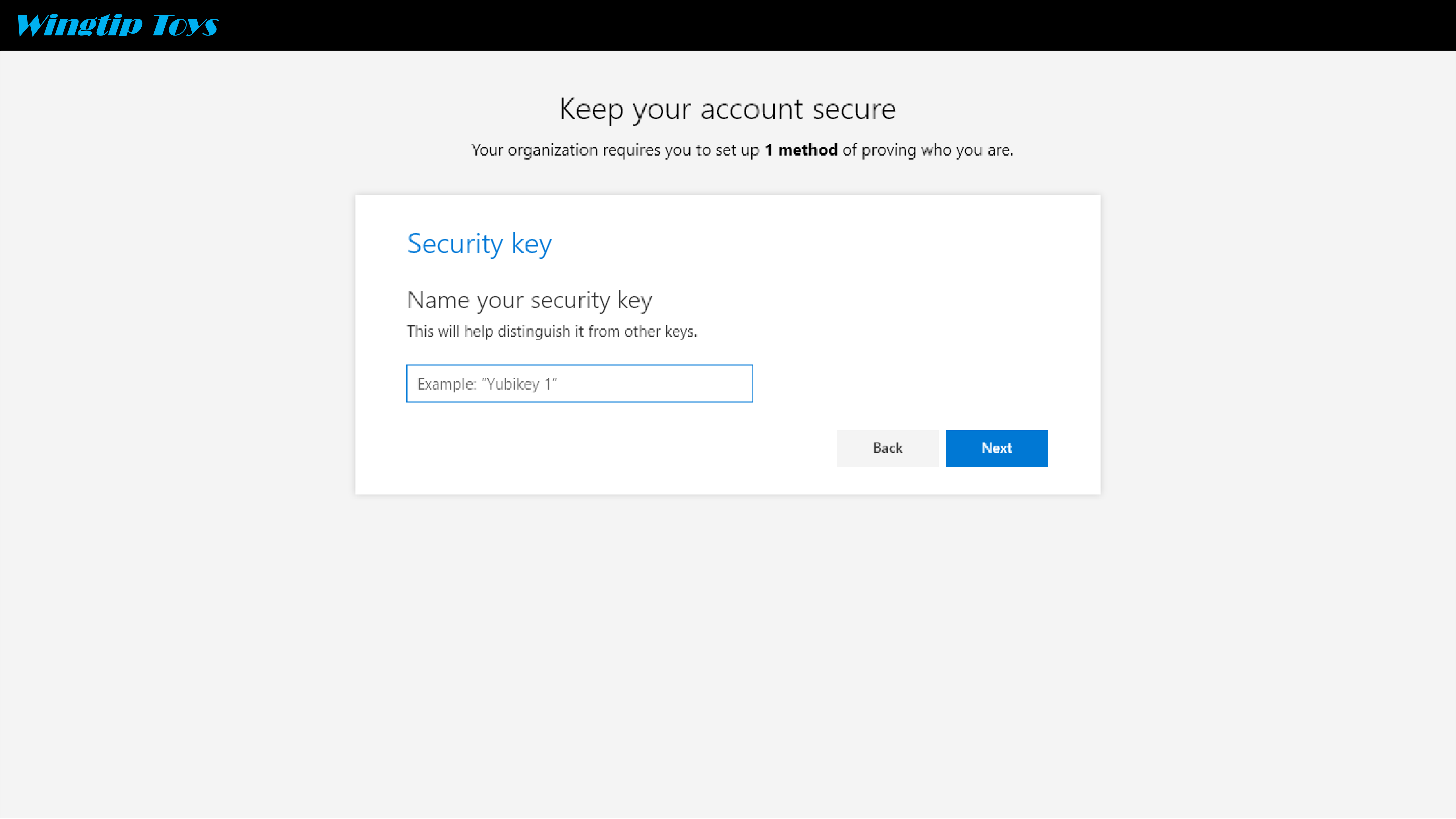
Wingtip Toys

Keep your account secure

Your organization requires you to set up **1 method** of proving who you are.

Security key

✓ Activation complete



Keep your account secure

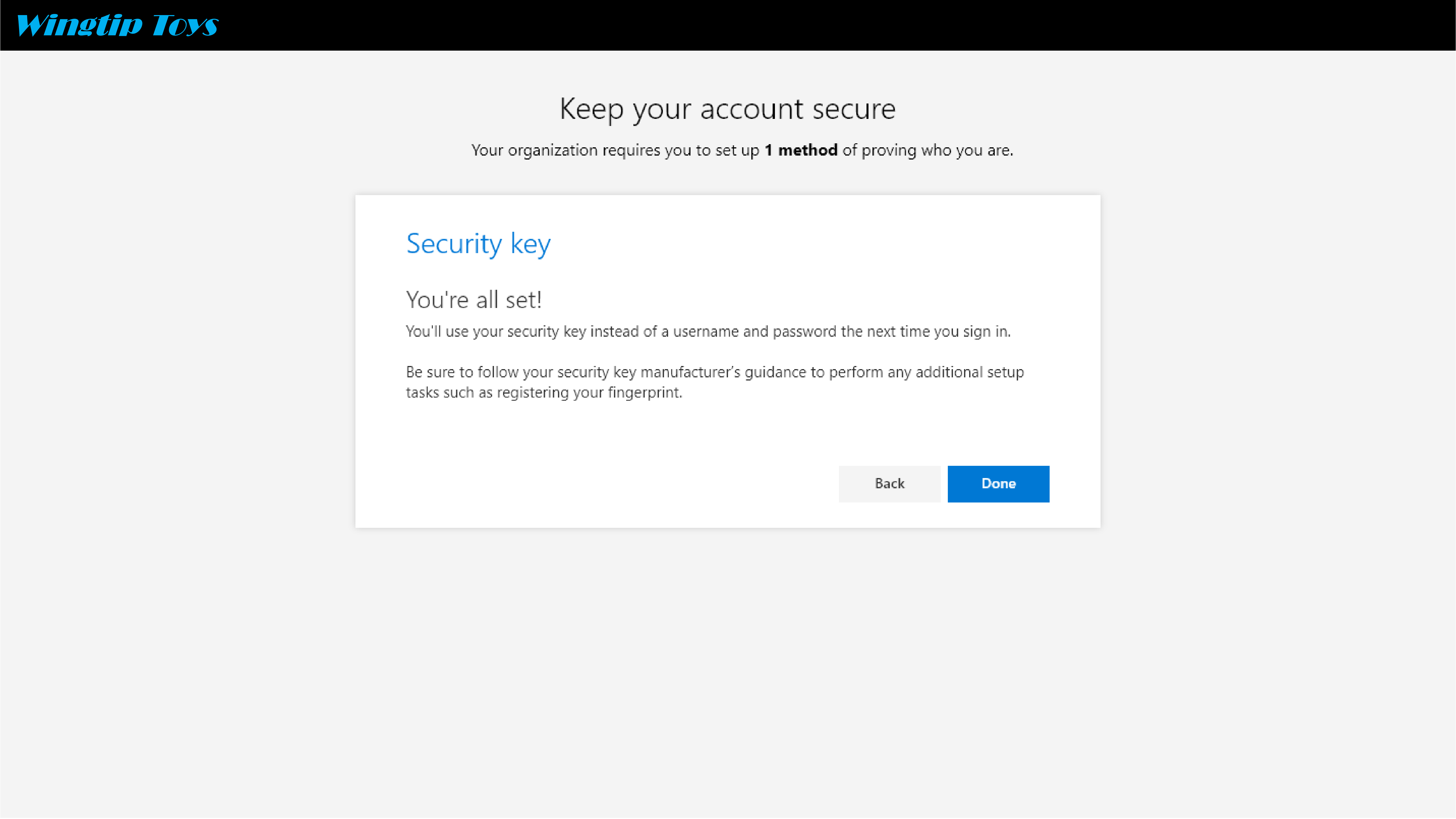
Your organization requires you to set up **1 method** of proving who you are.

Security key

Name your security key

This will help distinguish it from other keys.

Example: "Yubikey 1"



Wingtip Toys

Keep your account secure

Your organization requires you to set up **1 method** of proving who you are.

Security key

You're all set!

You'll use your security key instead of a username and password the next time you sign in.

Be sure to follow your security key manufacturer's guidance to perform any additional setup tasks such as registering your fingerprint.

FIDO2

Simple, common architecture for secure authentication flows

Secure Authentication Flow

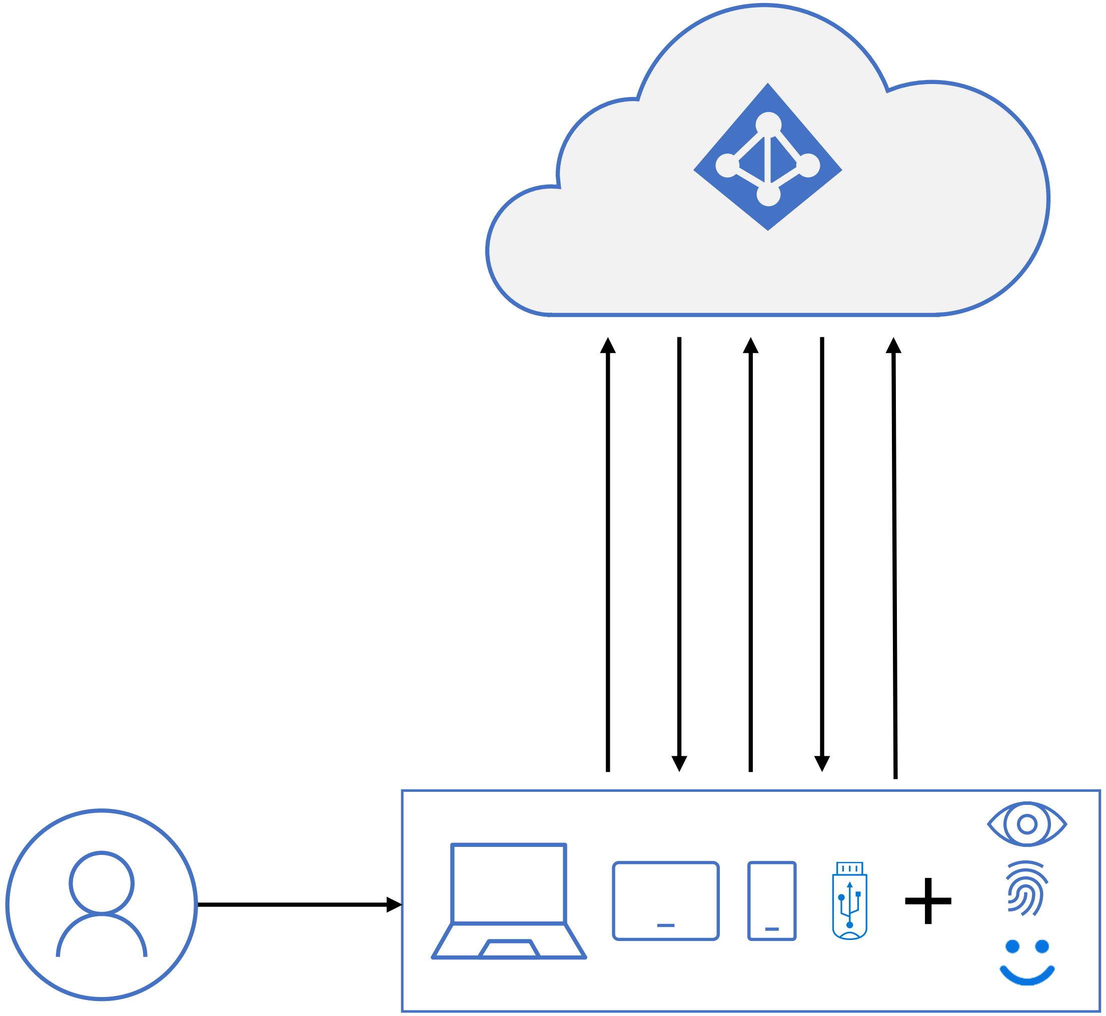
A simple, common architecture

Based on public-key technology

Private-keys are securely stored on the device

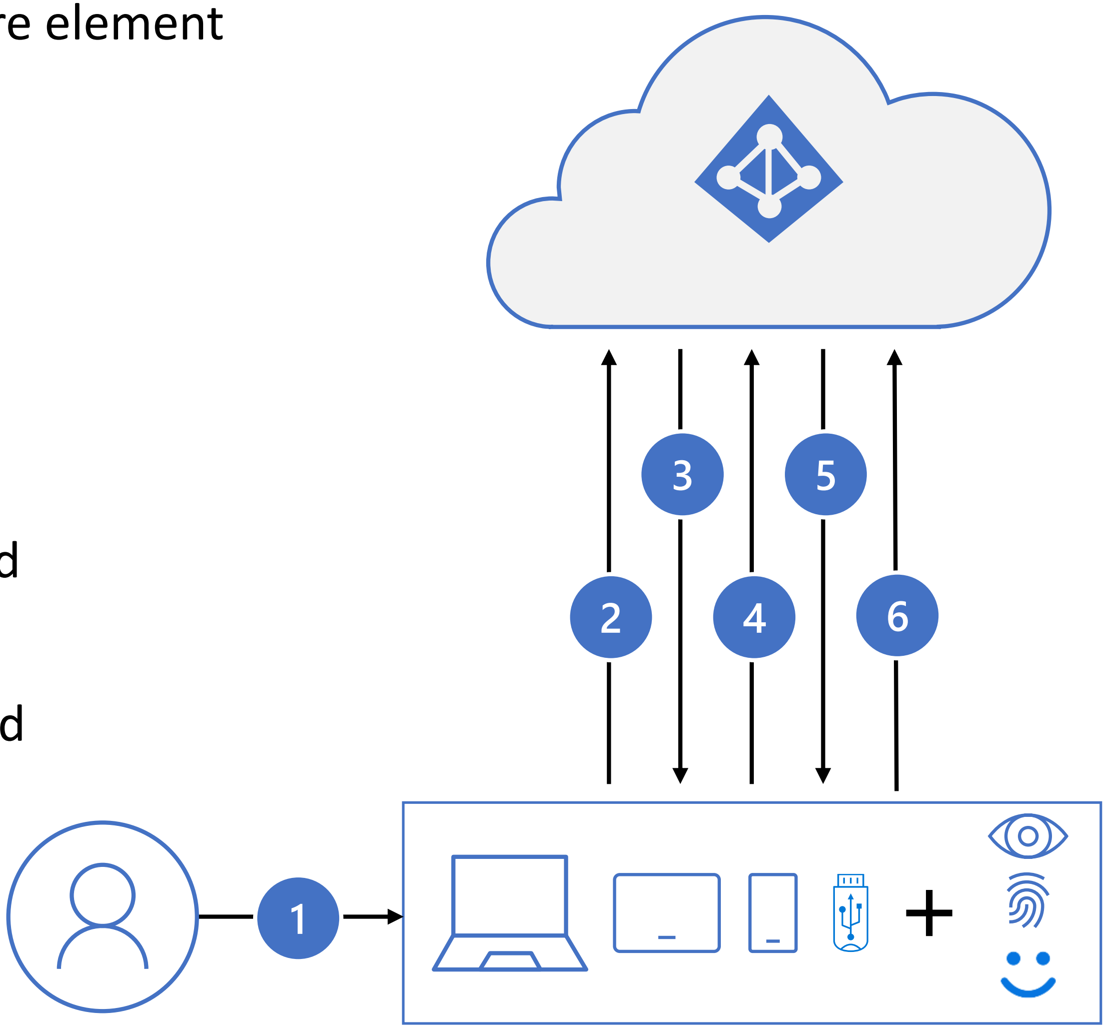
Requires a local gesture (e.g., biometric, PIN)

Private-keys are bound to a single device and never shared



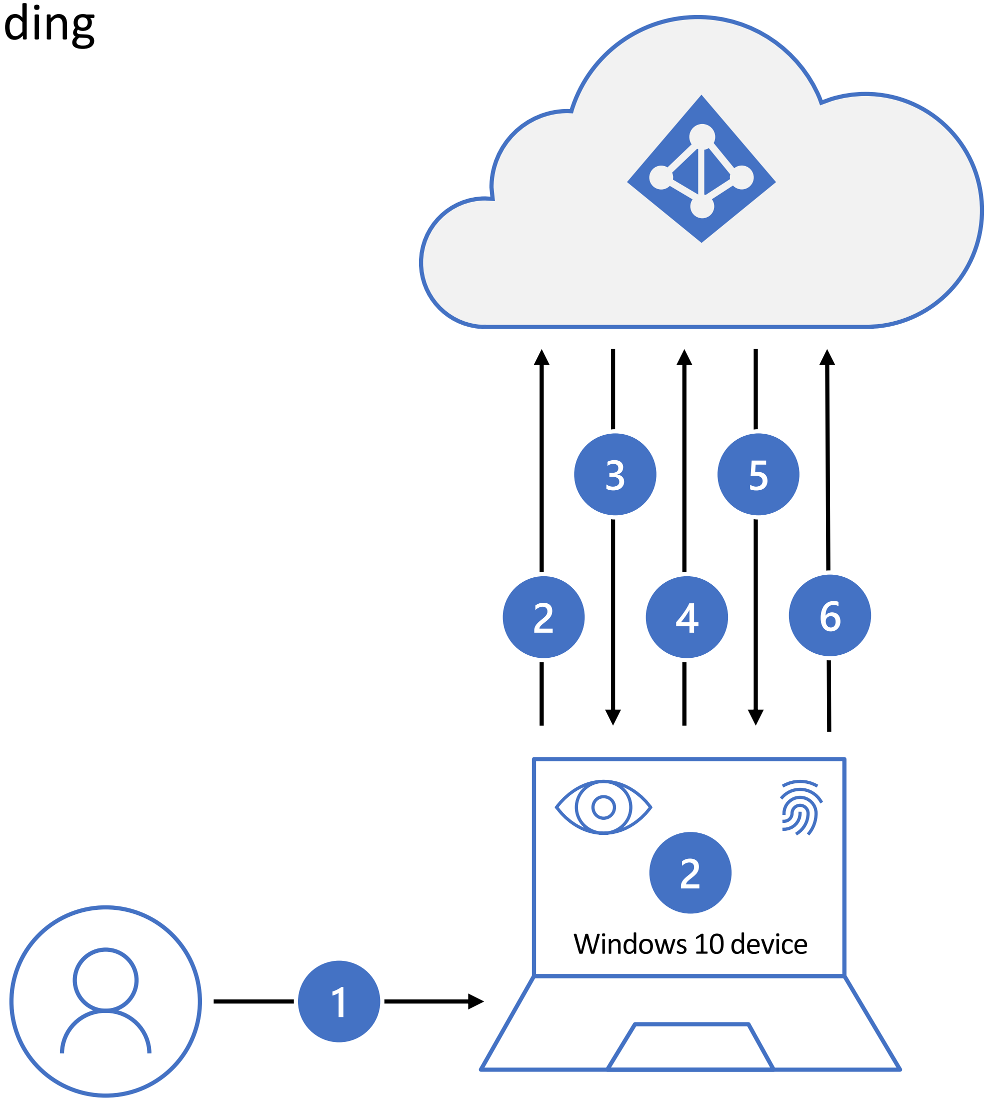
Secure Authentication Flow with Azure AD

1. User sign-in with bio-gesture unlocks secure element holding private key
2. Device sends authentication request
3. Azure AD sends back nonce
4. Device uses private key to sign nonce and returns to Azure AD with key ID
5. Azure AD returns refresh token + encrypted session key protected in secure element
6. Device returns the signed refresh token and derived session key to Azure AD to verify



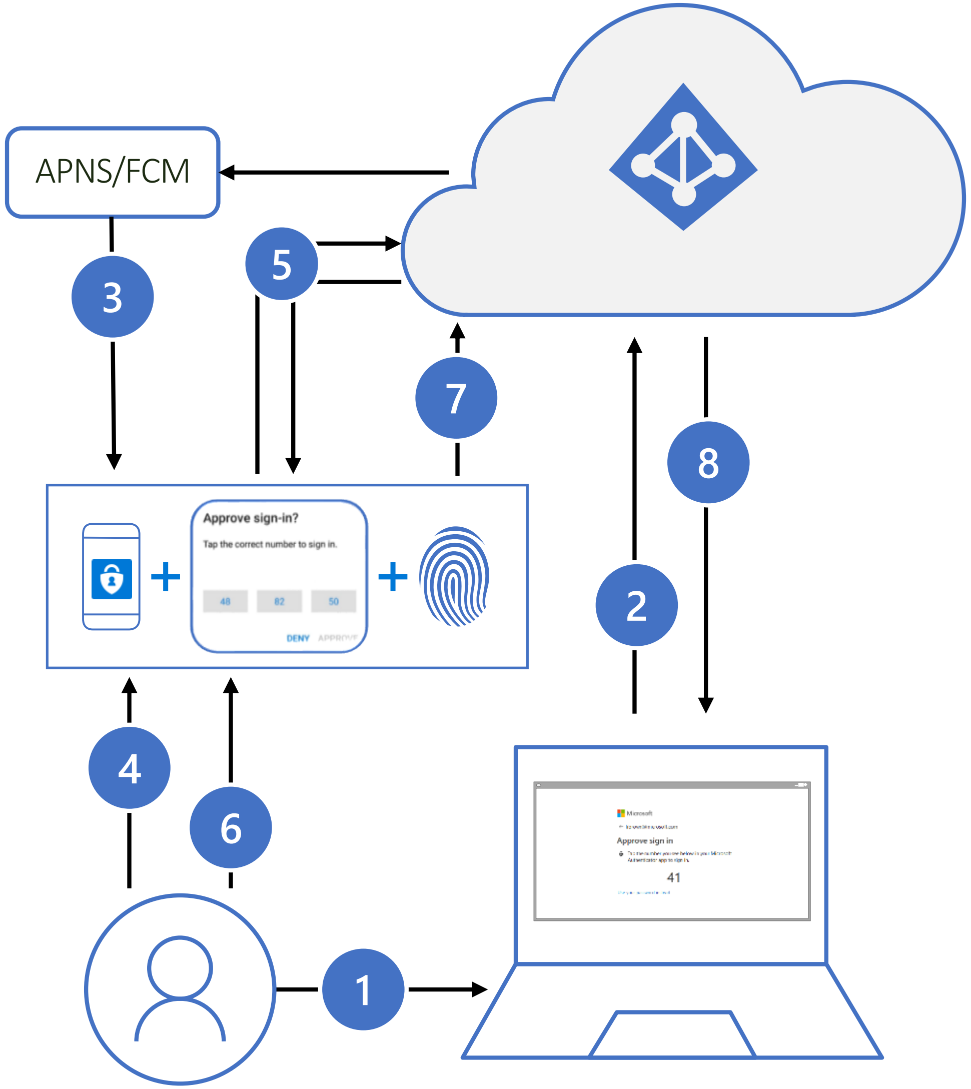
Windows 10 Hello for Business sign in

1. User sign-in with bio-gesture unlocks TPM holding private key
2. Windows sends “hello”
3. Azure AD sends back nonce
4. Windows uses private key to sign nonce and returns to Azure AD with key ID
5. Azure AD returns PRT + encrypted session key protected in TPM
6. Windows returns the signed PRT and derived session key to Azure AD to verify



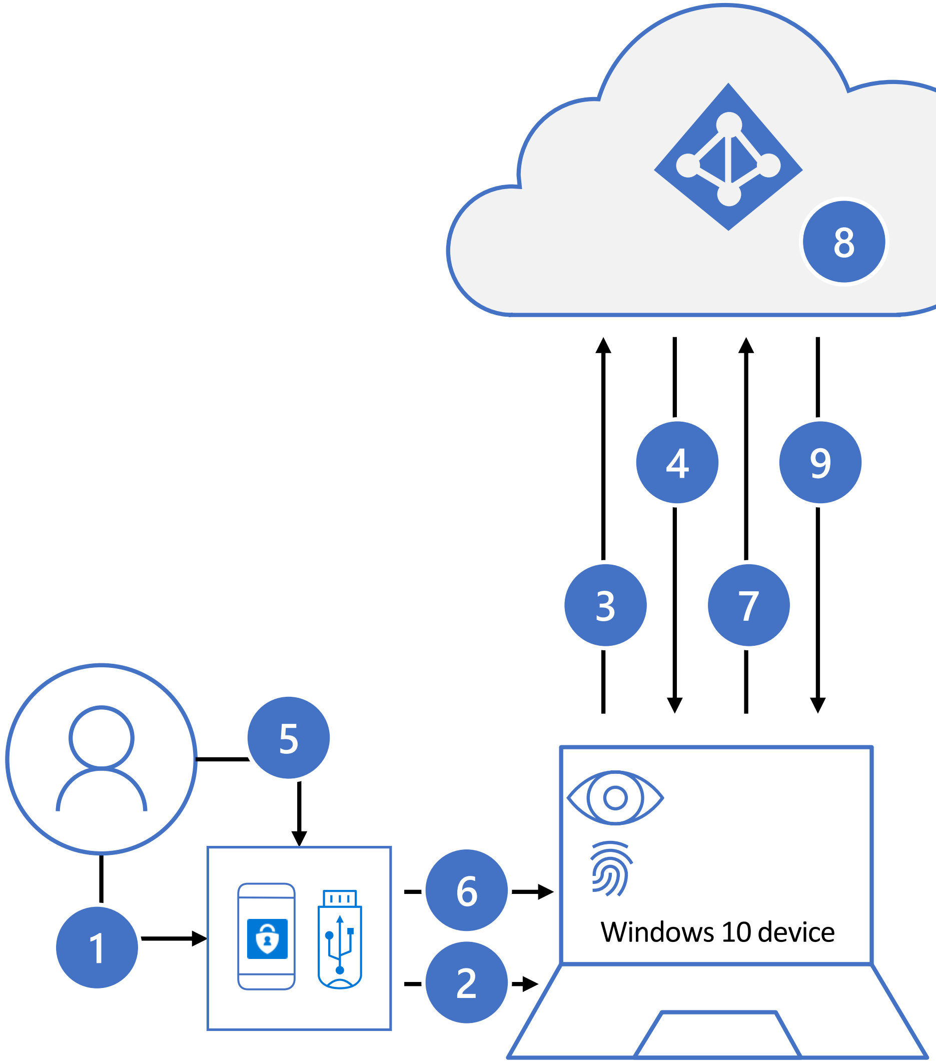
Microsoft Authenticator Password-less sign in (new)

1. User enters UPN
2. Azure AD detects user has strong credential, starts StrongCredential flow
3. Notification sent to app via APNS/FCM
4. User receives notification, opens app
5. App calls Azure AD, receives proof-of-presence challenge and nonce
6. User completes challenge, enters device biometric or PIN to unlock private key
7. Nonce is signed with private key and sent back to Azure AD
8. Azure AD performs public/private key validation and returns token


APNS/FCM
3
5
7
8
Approve sign-in?
Tap the correct number to sign in.
48
82
50
DENY
APPROVE
2
4
6
Microsoft
Approve sign in
Tap the number you see below in your Microsoft Authenticator app to sign in.
41
1

Strong Authentication with FIDO2 security key

1. User plugs FIDO2 security key into computer
2. Windows detects FIDO2 security key
3. Windows device sends auth request
4. Azure AD sends back nonce
5. User completes gesture to unlock private key stored in security key's secure enclave
6. FIDO2 security key signs nonce with private key
7. PRT token request with signed nonce is sent to Azure AD
8. Azure AD verifies FIDO key
9. Azure AD returns PRT and TGT to enable access to on-premises resources

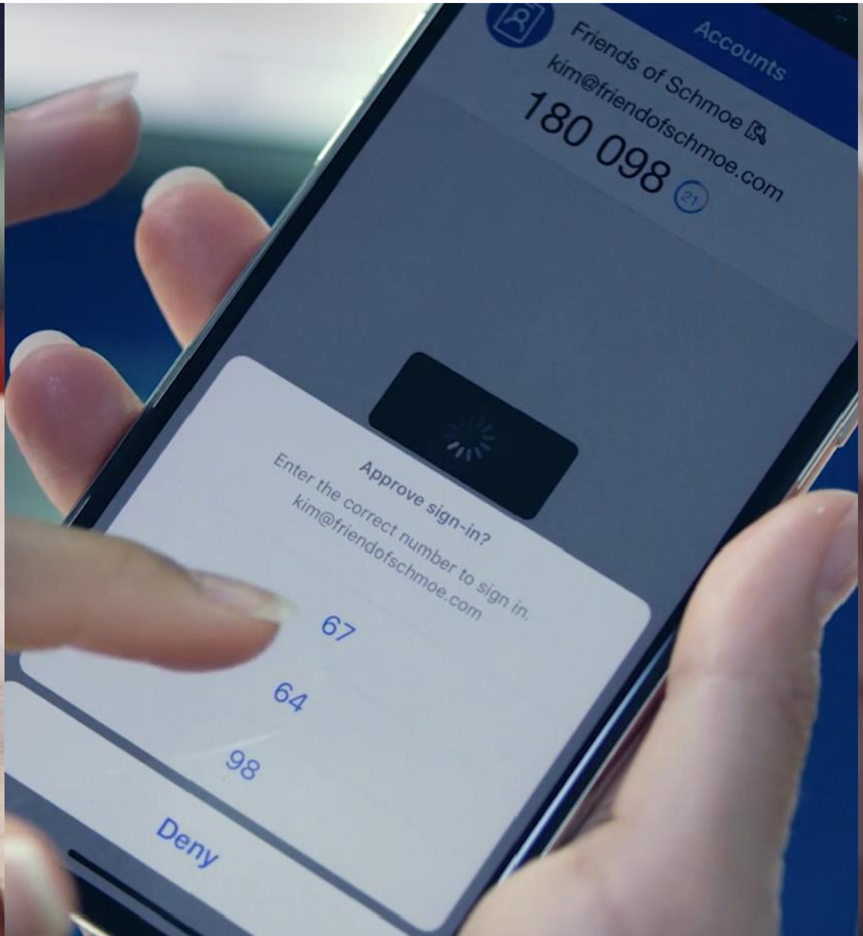


Three options for password-less authentication

All three use the same proven cryptographic authentication pattern

Windows Hello

Microsoft Authenticator



FIDO2 Security Keys

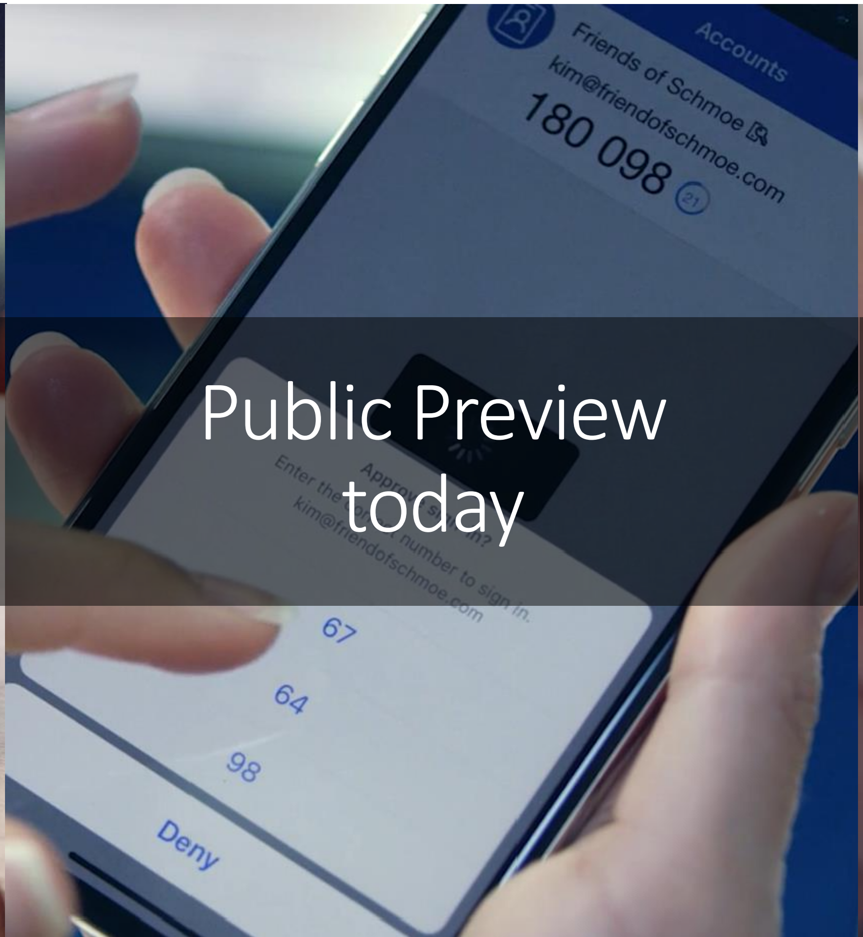
Getting to a world without passwords

High security, convenient methods of strong authentication

Windows Hello

Ready for production

Microsoft Authenticator



Public Preview today

FIDO2 Security Keys

Public Preview in 2019 Q1